КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.853
УДК 004.056.5

Опірський Іван Романович
д.т.н., професор, завідувач кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Сікорський Роман Дмитрович
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0003-2964-6083
roman.sikorskyi.kb.2023@lpnu.ua

Мартинюк Дмитро Юрійович
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0004-8065-9274
dmytro.martyniuk.kb.2023@lpnu.ua

АНАЛІЗ ЕФЕКТИВНОСТІ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ЛЮДСЬКОГО ФАКТОРА У КІБЕРБЕЗПЕЦІ

Анотація. У цифровому середовищі, де інформація стала одним із найцінніших ресурсів, забезпечення її конфіденційності та цілісності є пріоритетом як для державних органів, так і для приватного сектору. З огляду на різноманітність кіберзагроз і стрімке зростання випадків несанкціонованого доступу до облікових записів, традиційна автентифікація за допомогою пароля вже не виконує захисної функції на належному рівні. Поширення методів соціальної інженерії, фішингових атак, використання шкідливого програмного забезпечення, а також технологій автоматизованого зламу паролів актуалізують потребу у використанні більш надійних способів автентифікації. Одним із таких засобів є двофакторна автентифікація, яка базується на комбінації щонайменше двох незалежних факторів перевірки особи. Попри її широку підтримку з боку провідних сервісів та платформ, ефективність 2FA на практиці значною мірою залежить не лише від технічної реалізації, а й від поведінки самого користувача. У цій роботі розглянуто комплексний підхід до аналізу стійкості систем двофакторної автентифікації, що включає як оцінку технічних рішень, так і вивчення людського фактора як потенційної вразливості. Проведено низку практичних досліджень з моделювання типових загроз: збою доставки кодів, втрати пристрою, маніпуляцій з часовими параметрами. У результаті виявлено, що несанкціонований доступ часто стає можливим унаслідок неправильного зберігання резервних кодів, недостатнього ознайомлення користувачів із принципами безпечної автентифікації та використання небезпечних методів передачі кодів, таких як SMS. Особливо підкреслено проблему відмови користувачів від налаштування додаткових засобів відновлення доступу, що може призводити до повної втрати облікового запису. Оцінено ефективність інструментів на зразок Google Authenticator, Authy, апаратних токенів та криптографічних стандартів FIDO2. Обґрунтовано необхідність інтеграції багаторівневих механізмів автентифікації з користувацькими інструкціями, перевіркою синхронізації часу та автоматизованим аналізом підозрілої активності. Встановлено, що оптимальне поєднання технологічної безпеки та цифрової грамотності користувача є основою для побудови ефективного механізму протидії сучасним загрозам у сфері кібербезпеки.

Ключові слова: двофакторна автентифікація; людський фактор; цифрова безпека; фішинг; соціальна інженерія; резервні коди.

ВСТУП

Кожного дня технології стають дедалі важливішими для нашого життя. Ми не можемо уявити собі наші будні без застосунків для доставки продуктів, перегляду фільмів, оренди авто або онлайн покупок. Отже, можна помітити, що утворилось нове, так зване цифрове суспільство. Кількість сервісів, які допомагають нам існувати, стала дедалі більшою, це спричинило розширення обсягів персональних та корпоративних даних, що потребують захисту. Через це, питання кібербезпеки набуло особливої актуальності, зокрема, в частині автентифікації користувачів при доступі до інформаційних систем.

Традиційні засоби для автентифікації, такі як от паролі, уже застарілі та втратили свою надійність. Використання слабких або повторюваних комбінацій, фішингові атаки, технічні вразливості, а також людська необачність, ось що стало причинами неефективності традиційних засобів. За висновками великої кількості дослідів встановлено, що більшість атак на інформаційні процеси було зроблено через компрометацію облікових записів. Саме тому міжнародні стандарти безпеки такі як ISO 27001 [1] та рекомендації NIST SP 800-63 [2], наголошують на важливості впровадження багатофакторної автентифікації (Multi-Factor Authentication, MFA), серед якої особливе місце займає двофакторна автентифікація (2FA).

Не дивлячись, на її технічну ефективність, це все може перекреслюватись чинниками людської поведінки. Необізнаність людей у темі цифрової грамотності, нехтування резервними методами відновлення доступу, невміння розпізнавати соціально-інженерні загрози, — усе це створює передумови для успішних кібератак навіть захищених систем.

Потреба у цьому дослідженні обумовлена зростаючим значенням двофакторної автентифікації як одного з базових інструментів захисту цифрової ідентичності в умовах постійного ускладнення кіберзагроз. Попри широке впровадження 2FA, значна кількість інцидентів несанкціонованого доступу все ще трапляється, що вказує на наявність не лише технічних, а й поведінкових чинників, які впливають на загальну ефективність цього методу.

Більшість наукових праць зосереджені переважно на технічних аспектах автентифікації — криптографічних алгоритмах, протоколах, рівнях захисту — при цьому людський фактор часто лишається поза увагою або розглядається поверхнево. Тим часом саме користувацька взаємодія з системами безпеки, нерозуміння принципів їхньої дії чи нехтування рекомендаціями часто стають вирішальними для успішної реалізації 2FA.

Тому актуальність цієї публікації полягає в комплексному підході до аналізу: поєднанні технічної оцінки інструментів двофакторної автентифікації з аналізом типових сценаріїв зловживань, обумовлених поведінкою користувачів. У фокусі дослідження — практичні аспекти впровадження 2FA, аналіз вразливостей, спричинених людськими помилками, та розробка рекомендацій, які можуть сприяти підвищенню загальної ефективності механізмів автентифікації в реальних умовах.

Актуальність дослідження проблеми 2FA. Інформаційна безпека є одним з пріоритетних напрямів державної та корпоративної політики у сфері цифрового розвитку. У зв’язку з активним впровадженням електронних сервісів, зростанням обсягів переданих і збережених даних, а також збільшенням частоти порушень цілісності та конфіденційності інформаційних систем, актуалізується необхідність підвищення рівня захисту механізмів автентифікації. Умови функціонування сучасного

кіберпростору висувають підвищені вимоги до ідентифікації користувачів, адже саме цей етап нерідко є початковою точкою компрометації.

Наявні підходи до автентифікації, зокрема застосування однофакторних засобів контролю доступу, демонструють обмежену ефективність у протидії технічно складним або цілеспрямованим атакам. У зв'язку з цим доцільним вбачається впровадження додаткових рівнів перевірки користувача, зокрема технологій, які передбачають багатофакторну автентифікацію. Однією з найбільш поширених і доступних у впровадженні форм багатофакторного захисту є двофакторна автентифікація, що вже набула широкого застосування в інфраструктурі критичних інформаційних систем, фінансових установах, освітньому секторі, державному управлінні, а також у середовищі пересічних користувачів.

Актуальність дослідження двофакторної автентифікації полягає у необхідності наукового осмислення принципів її функціонування, особливостей реалізації та обмежень, пов'язаних із практичним застосуванням у реальному середовищі. Незважаючи на поширеність даної технології, питання її ефективності, стійкості до різних класів загроз, зокрема в умовах впливу нештатних сценаріїв користування, потребує системного аналізу. З огляду на це, виникає потреба у ґрунтовному дослідженні сучасних механізмів 2FA, з метою оцінювання їх відповідності сучасним вимогам безпеки та формування рекомендацій щодо оптимізації практики автентифікації в різних секторах цифрового середовища.

Аналіз останніх досліджень і публікацій. Двофакторна автентифікація (2FA) — це один із найефективніших механізмів захисту облікових записів від несанкціонованого доступу. Численні наукові дослідження підтверджують її здатність значно знижувати ризики компрометації, особливо в контексті атак, заснованих на викрадених паролях. Водночас ефективність 2FA значною мірою визначається способом її впровадження та рівнем обізнаності користувачів щодо принципів її дії.

Bonneau et al. (2012) [3] у своєму метааналізі проаналізували 35 схем автентифікації, включно з традиційними паролями, біометричними методами, апаратними токенами та новітніми багатофакторними системами. Метою дослідження було створення уніфікованої системи оцінювання веб-схем автентифікації на основі трьох ключових критеріїв: зручність використання (usability), безпека (security) та простота розгортання (deployability).

Результати дослідження показали, що більшість схем, заснованих лише на паролях, мають низькі показники безпеки, навіть попри відносну зручність для користувачів. Натомість методи, які передбачають багатофакторну автентифікацію, демонструють значно вищий рівень захисту, хоча можуть поступатися в зручності або вимагати складнішої інфраструктури. До прикладу, автори підкреслили, що поєднання кількох незалежних факторів автентифікації (наприклад, знання + володіння) суттєво підвищує стійкість до атак, зокрема фішингу, атаки методом перебору та викрадення паролів.

Для кращого розуміння порівняльної ефективності різних методів автентифікації, нижче подано узагальнене візуальне представлення класифікації Bonneau et al (див. рис. 1).

Рис.1. Система порівняння схем веб-автентифікації

На відміну від перших авторів, Brostoff і Sasse (2013) [7] у польових дослідженнях показали, що зручність і простота інтерфейсу 2FA-систем прямо впливають на готовність користувачів впроваджувати ці механізми. Понад 40% опитаних респондентів у їх дослідженні відмовлялися від додаткових факторів автентифікації через незручність або відсутність розуміння їх необхідності, а саме (див. табл. 1 та рис. 2)

Таблиця 1

Причини відмови від 2FA

Причина	Частка серед відмовників (%)
Надто складно для використання	45%
Не довіряють технології	30%
Не бачать необхідності	25%

Рис. 2. Причини відмови від 2FA

ISSN 2663 - 4023

Також, автори дослідили фактори, які впливають на протилежну реакцію користувачів(див. рис. 3):

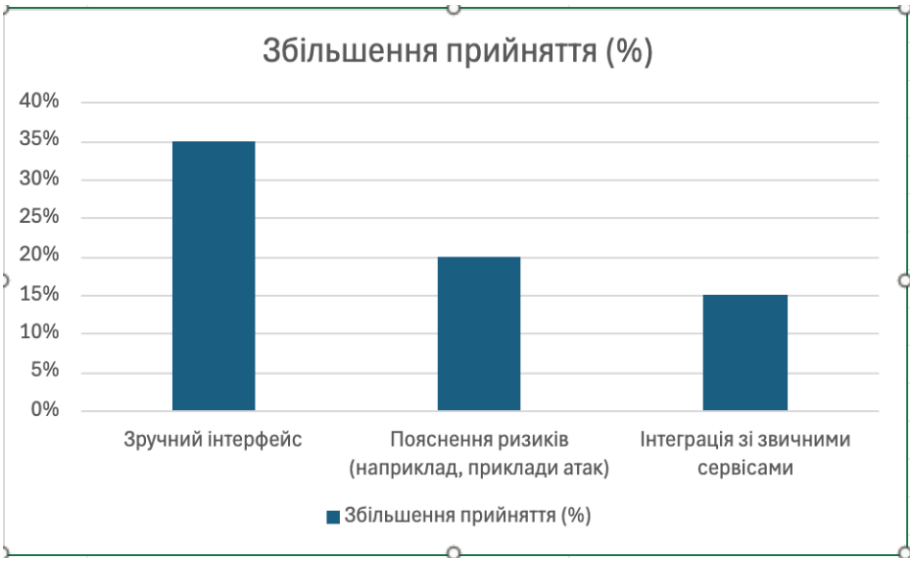

Рис. 3. Фактори, що підвищують прийняття 2FA

Звичайно ж, без уваги не залишились і статистичні дані, що напряму залежать від демографічних чинників (див. рис. 4):

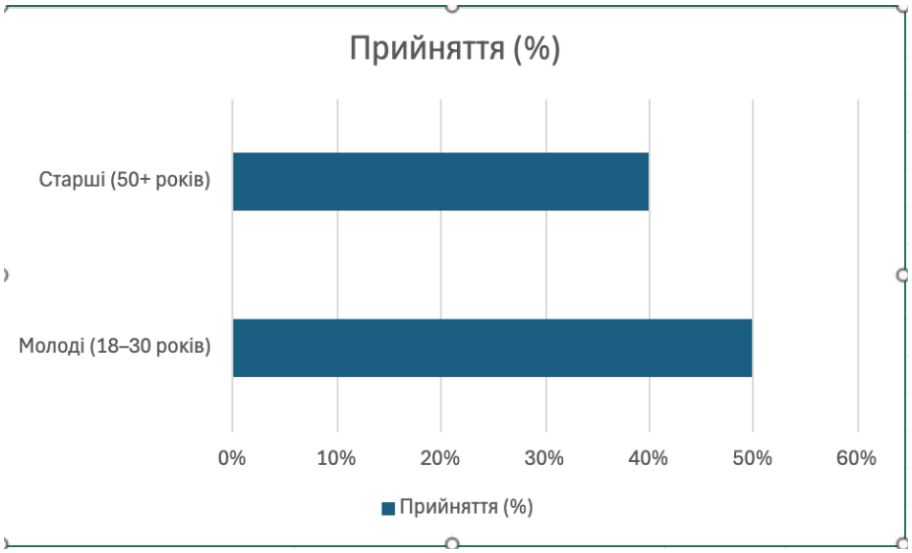

Рис. 4. Прийняття 2FA за віком

Отже, на підставі проведеного аналізу можна виокремити такі ключові положення:

1. **Зручність~Безпека:** Якщо 2FA-система не оптимізована для користувача, навіть найбезпечніший метод не буде використовуватися.
2. **Ключове значення UX:** Простота інтерфейсу та пояснення необхідності 2FA зменшують відмову на 40–50%.
3. **Персоналізація:** Різні групи користувачів потребують різних підходів (наприклад, SMS-коди для старших, push-сповіщення для молоді).

Kim, Sukh і Kwon (2022) [6] акцентували увагу на зростаючій кількості атак типу SIM-swapping(див. рис. 5), зокрема на території США, де кількість зареєстрованих інцидентів зросла з 1,300 у 2018 році до понад 3,800 у 2021 році. Це підтверджує вразливість SMS як методу доставки одноразових кодів.[6]

Рис. 5. Принцип роботи SIM-swapping методу

FIDO Alliance (2021) [5], у свою чергу, аргументує переваги апаратних токенів та протоколів FIDO2/WebAuth як захисту, стійкого до фішингу, завдяки криптографічному підтвердженню особи без передачі секретної інформації. FIDO2 дозволяє користувачам використовувати звичайні пристрої для легкої автентифікації в онлайн-сервісах як у мобільному, так і в робочому середовищі. Специфікації FIDO2 є специфікацією веб-автентифікації (WebAuth) Всесвітнього веб-консорціуму (W3C) і відповідним протоколом клієнт-автентифікатор (CTAP) FIDO Alliance.

Згідно з рекомендаціями NIST SP 800-63B (2020) [2], організаціям слід уникати використання слабких факторів автентифікації, таких як SMS або голосові дзвінки, натомість переходити до криптографічних токенів (hardware-bound), які не можна скопіювати або перехопити.

Отже, наукові праці однозначно свідчать про ефективність 2FA в запобіганні компрометації даних, особливо при використанні сучасних методів автентифікації, таких як апаратні токени чи біометрія. Проте, якщо користувачі не розуміють принципів дії або надають перевагу зручності над безпекою, навіть найкращі технічні рішення можуть бути обійдені.

Статистичні дані про успішні атаки на системи з 2FA

Незважаючи на загальновизнану ефективність двофакторної автентифікації (2FA) у підвищенні безпеки облікових записів, останні дослідження демонструють, що цей захист не є абсолютним. Актуальні звіти вказують на існування численних векторів атак, які дозволяють зловмисникам обходити 2FA за допомогою соціальної інженерії, атак на

канали передачі кодів (зокрема, SMS та push-сповіщення), а також через використання шкідливого програмного забезпечення.[16]

Згідно з дослідженням компанії Google, навіть серед користувачів, які застосовують двофакторну автентифікацію (2FA), приблизно 15% стали жертвами фішингових атак, що дозволили зловмисникам перехопити тимчасові коди доступу[4]. Такі атаки часто здійснюються через підроблені вебсайти, які імітують інтерфейси справжніх сервісів, а також за допомогою MITM-проксі, що передають трафік у реальному часі між користувачем і цільовим сайтом.[17]

У загальному контексті, за даними IBM X-Force Threat Intelligence Index 2022, фішинг залишився найпоширенішим методом атак: 41% усіх зареєстрованих інцидентів починалися саме з фішингових повідомлень [8]. Зі статистики Anti-Phishing Working Group (APWG), лише у четвертому кварталі 2021 року було зареєстровано понад 1,025,968 фішингових атак (див. рис. 6) — це найвищий рівень, зафіксований за всю історію спостережень [9].

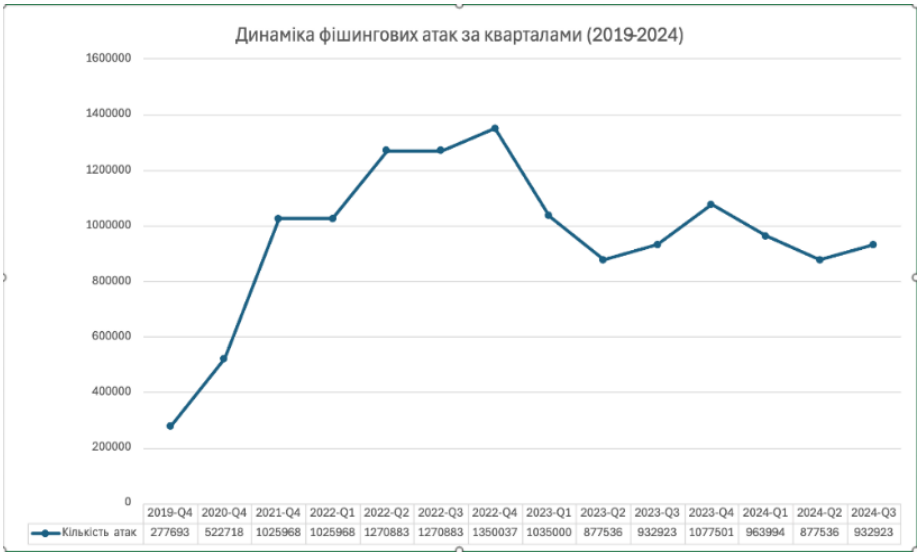

Рис. 6. Динаміка кількості фішинг атак за останніх 5 років

Основні сценарії обходу 2FA (див. рис. 7)**:**

1. *Фішингові проксі-сервіси.* Зловмисники застосовують інструменти на кшталт *EvilProxy* або *Modlishka*, які здатні перехопити як облікові дані, так і коди двофакторної автентифікації (2FA) в реальному часі [10], [15], [20].
2. *MFA Fatigue* (виснаження від багаторазових запитів автентифікації)**.** За даними звіту Microsoft, атаки групи *Nobelium* у 2022 році часто реалізовувалися шляхом надсилання великої кількості push-запитів, що виснажувало жертв і змушувало їх випадково підтвердити вхід [11].
3. *Зловживання SMS-каналом.* За статистикою Федеральної комісії зі зв'язку США (FCC), відбувається стрімке зростання атак типу *SIM-swapping*, які дозволяють отримати контроль над мобільним номером жертви і, відповідно, над 2FA-кодами [12].
4. *Шкідливе програмне забезпечення.* Мобільні трояни такі як, до прикладу, Cerberus або BRATA, здатні перехоплювати одноразові коди з Google Authenticator або читати push-сповіщення, не привертаючи увагу користувача [13].

ISSN 2663 - 4023

Додаткові статистичні дані:

1. За даними звіту Proofpoint (2023), 83% компаній у світі повідомляли про спроби фішингу, які були спрямовані саме на обхід систем 2FA [14].
2. Дослідження IBM X-Force (2022) показало, що у 36% успішних атак на облікові записи з 2FA було використано соціальну інженерію [8].
3. Згідно з звітом FIDO Alliance, традиційна SMS-аутентифікація вважається вразливою і не рекомендована для використання в середовищах з високим рівнем ризику [5].

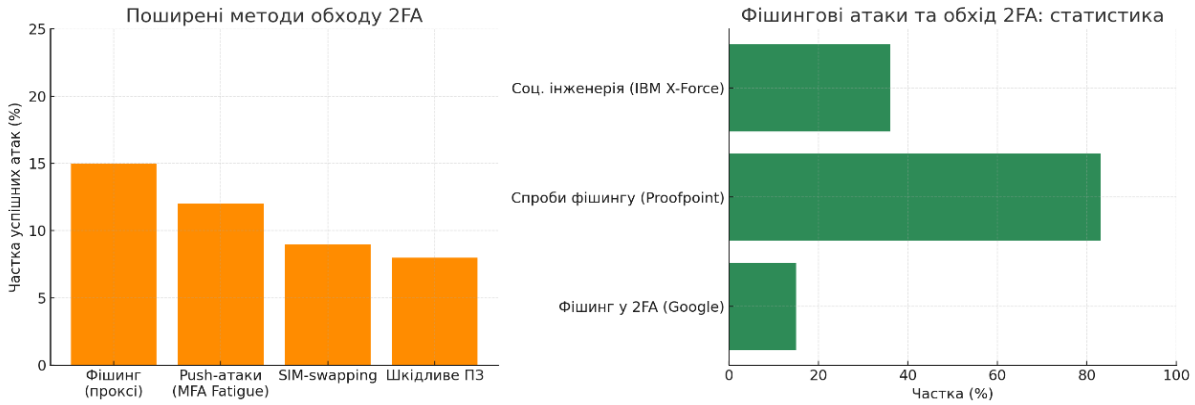

Рис. 7. Розподіл використання методів обходу 2FA

Дослідження впливу людського фактора на безпеку автентифікації

Одним із головних викликів у забезпеченні ефективності 2FA досі вважається людський фактор. Дослідження, проведені компанією Google показали, що понад 30% користувачів, навіть маючи можливість активувати 2FA, не роблять цього оскільки виникають складності з налаштуванням або просто не хочуть витрачати свій час [4].

Значна частина користувачів застосовує ненадійні методи резервного копіювання доступу, наприклад, зберігає резервні коди у незахищених текстових файлах або пересилає їх через електронну пошту. Це збільшує ризики компрометації навіть за наявності 2FA [2], [18]

В свою чергу, дослідження корпорації IBM доводять, що рівень обізнаності про технологію 2FA впливає на її ефективність. Результати експериментів показали, що після проходження тренінгів із цифрової безпеки ймовірність успішного фішингового нападу на користувача знижується в середньому на цілих 65% [8].

Провівши аналіз досліджень Brostoff et al. [3] та протоколу ISO 27001:2022 [1], зроблено висновки про ефективність 2FA, яка є високою у запобіганні несанкціонованому доступу, але її дієвість суттєво залежить від рівня усвідомлення користувачами загроз. Незважаючи на технологічні переваги, найслабшим елементом системи автентифікації досі залишається людський фактор, що вимагає комплексного підходу до навчання користувачів та вибору найбільш захищених методів автентифікації.

Принципи роботи багатофакторної автентифікації

Багатофакторна автентифікація (MFA, Multi-Factor Authentication) є одним із ключових механізмів забезпечення безпеки цифрових облікових записів [19]. З назви зрозуміло, що при такому виді автентифікації передбачено використання двох або більше незалежних факторів для верифікації особи.(див. рис. 8) Це значно знижує ризик несанкціонованого доступу, навіть якщо один із факторів зловмисник вдасться обійти (NIST 800-63B, 2020) [2].

Рис. 8. Принцип роботи MFA

Основні фактори автентифікації

Система MFA використовує три основні категорії факторів (ISO/IEC 27001:2022) [1]:

1. Знання (Something you know) — паролі, PIN-коди, відповіді на секретні питання.
2. Володіння (Something you have) — мобільний телефон, апаратний токен, смарт-карта.
3. Біометрія (Something you are) — відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока.

Кожен із цих факторів має свої переваги та недоліки. Наприклад, паролі можуть бути зламані або перехоплені через фішингові атаки, а біометричні дані — викрадені та підроблені (Bonneau et al., 2012) [3].

Типові види реалізації двофакторної автентифікації (2FA)

Двофакторна автентифікація (2FA) найбільш поширена форма MFA, що застосовується як в організаціях, так і в особистих акаунтах.

Найчастіші сценарії впровадження:

1. Одноразові паролі (OTP, One-Time Passwords) — генеруються мобільними додатками або надсилаються через SMS або електронну пошту.
2. Апаратні токени — фізичні пристрої (наприклад, YubiKey), які генерують або передають OTP.
3. Push-сповіщення — запити на підтвердження входу, що надсилаються в мобільний застосунок.
4. Біометрична автентифікація — використання розпізнавання обличчя чи відбитків пальців у поєднанні з паролем.

ISSN 2663 - 4023

Популярні інструменти для MFA

Зараз компанії пропонують багато різних рішень для багатофакторної автентифікації, що впроваджуються в корпоративні та персональні акаунти. Нижче наведено порівняння найпоширеніших серед них (див. табл. 2):

Таблиця 2

Порівняння найпоширеніших інструментів для MFA

Інструмент	Тип автентифікації	Платформи	Підтримка резерву	Захищеність (оцінка)
Google Authenticator	TOTP	Android, iOS	Немає	Середня
Microsoft Authenticator	TOTP, push	Android, iOS	Так	Висока
Authy	TOTP + cloud backup	Android, iOS, PC	Так	Висока
YubiKey (FIDO2)	Апаратний токен	Кросплатформен ий	Не потрібна	Дуже висока
SMS-коди	OTP через SMS	Усі	Частково	Низька

За даними Microsoft Digital Defense Report 2022, використання FIDO2-токенів або мобільних автентифікаторів значно знижує ризик успішних атак у порівнянні з SMS-кодами [5]. Google Security Blog (2021) також вказує, що більшість атак на 2FA стосуються методів, які залежать від мережевих каналів зв'язку (наприклад, SMS або електронна пошта) [4].

Отже, багатофакторна автентифікація є надзвичайно важливим інструментом захисту, який поєднує різні категорії факторів автентифікації. Вибір оптимального механізму залежить здебільшого від двох факторів, від рівня безпеки, який потрібно забезпечити, а також важливим фактором є зручність для користувачів.

Постановка проблеми. Попри високу ефективність 2FA, користувачі часто нехтують її використанням через незручність, а також можуть ставати жертвами соціальної інженерії. Зловмисники знаходять нові способи обходу 2FA, такі як перехоплення SMS-кодів, атаки на голосову пошту та використання фішингових сторінок. Тому важливо не лише впроваджувати 2FA, але й підвищувати рівень обізнаності користувачів щодо безпечного використання цієї технології.

Мета статті підвищення ефективності захисту даних користувачів шляхом комплексного аналізу надійності двофакторної автентифікації з урахуванням людського фактора, ідентифікації ключових вразливостей у поведінці користувачів та розробки практичних рекомендацій для мінімізації пов'язаних ризиків у сфері інформаційної безпеки.

ПРАКТИЧНЕ ТЕСТУВАННЯ ВРАЗЛИВОСТЕЙ 2FA

Проведемо кілька практичних досліджень для виявлення потенційних вразливостей у системах двофакторної автентифікації (2FA), які можуть виникати як внаслідок технічних збоїв, так і під впливом людського фактора. Метою цих дослідів є моделювання типових ситуацій, у яких 2FA може бути скомпрометована або неефективною, а також аналіз поведінки користувачів у таких умовах.

Досліди поділено за типами загроз:

1. Симуляція збою доставки кодів через блокування мережі: проаналізуємо, як система реагує на відсутність каналу зв'язку для доставки коду, і чи є альтернативні шляхи автентифікації.
2. Втрата доступу до пристрою з 2FA: моделюємо ситуацію, коли користувач втрачає смартфон або інший пристрій, який генерує або отримує код підтвердження. Перевіряємо, чи можна безпечно відновити доступ до облікового запису.
3. Маніпуляція часовими налаштуваннями для обходу 2FA: досліджуємо можливість обману TOTP-системи (типово використовується в Google Authenticator та інших додатках) шляхом зміни часу на пристрої.

Ці симуляції дозволяють оцінити не лише надійність самої технології, а й вразливість користувача до соціальної інженерії та впливу стресових ситуацій. В результаті ми зможемо сформулювати конкретні рекомендації для підвищення безпеки 2FA-систем з урахуванням реальних ризиків.

Симуляція збою доставки кодів через блокування мережі

Перевіримо поведінку системи автентифікації у випадку збою надсилання 2FA-коду через електронну пошту (SMTP). Дослідимо реакцію системи та доступні альтернативи для завершення входу.

Сконструюємо алгоритм дослідження (див. рис. 9):

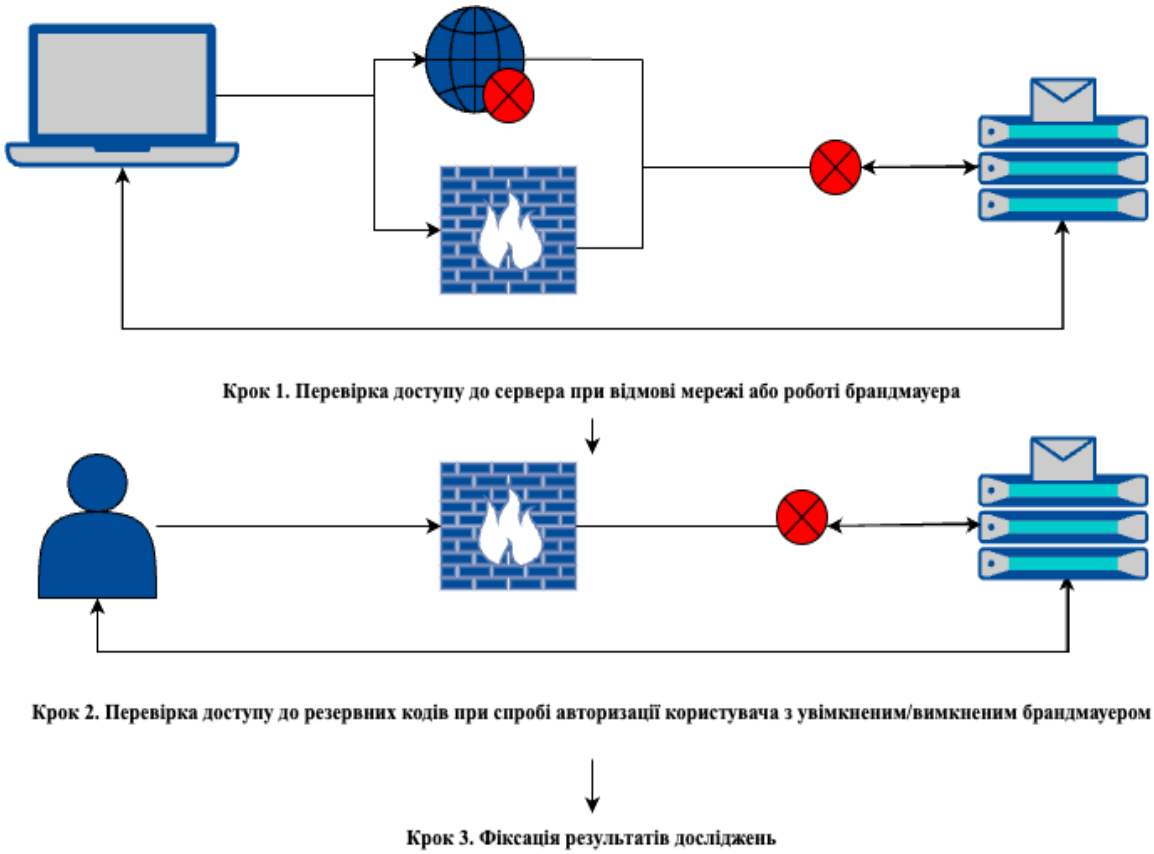

Рис. 9. Алгоритм симуляції збою доставки резервних кодів

ISSN 2663 - 4023

Використаємо тестову платформу Mailtrap для створення імітованого SMTP-сервера. Створимо тестовий Inbox та відправимо тестовий SMTP-пакет через GUI пристрою (див. рис. 10):

```
node sendMail.js
Лист відправлено: 250 2.0.0 Ok: queued
```

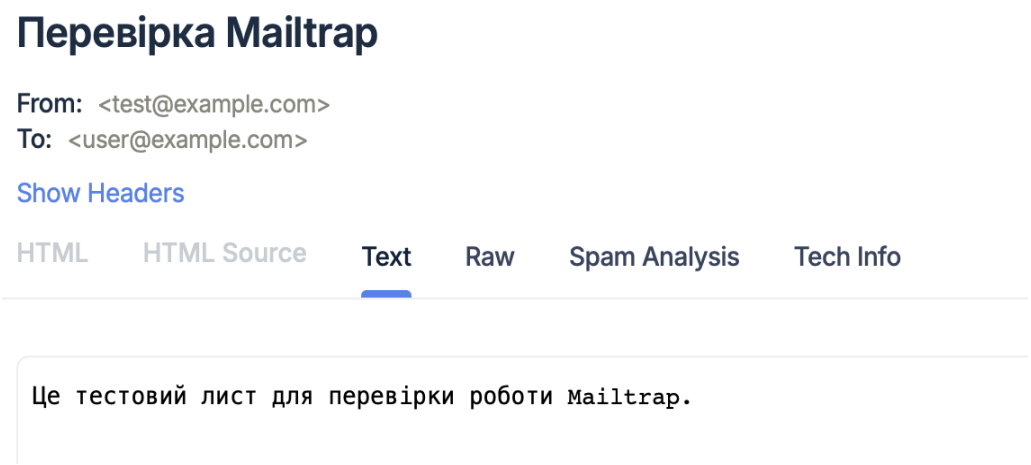

Рис. 10. Перевірка роботи Mailtrap тестовим пакетом

Тепер відключимо WI-FI з'єднання та спробуємо надіслати пакет ще раз (отримаємо негативний результат):

```
[romansikorskiy@MacBook-Air-Roman ~ % node sendMail.js
Помилка: Error: getaddrinfo ENOTFOUND smtp.mailtrap.io
    at GetAddrInfoReqWrap.onlookupall [as oncomplete] (node:dns:122:26)
    {
        errno: -3008,
        code: 'EDNS',
        syscall: 'getaddrinfo',
        hostname: 'smtp.mailtrap.io',
        command:'CONN'
    }
```

Також перевіримо чи буде проходити SMTP трафік, якщо налаштувати брандмауер (у нашому випадку Lulu), очевидно, що брандмауер буде повідомляти про спроби пакетів пройти, на що ми даємо негативну відповідь та отримуємо ось такий результат:

```
[romansikorskiy@MacBook-Air-Roman ~ % node sendMail.js
Помилка: Error: getaddrinfo ENCONNREFUSED 127.0.0.1:2525 smtp.mailtrap.io
    at TCPConnectWrap.afterConnect [as oncomplete] (node:net:1636:16)
    {
        errno: -61,
        code: 'ESOCKET',
        syscall: 'connect',
        hostname: '127.0.0.1',
        port: 2525,
        command:'CONN'
    }
```

ISSN 2663 - 4023

Перейдемо ближче до суті, спробуємо авторизувати користувача за допомогою двофакторної перевірки. Зробимо дві спроби:

– перша з увімкненим брандмауером, що унеможливить трафік SMTP-пакета до нашої скрині;

```
node login2fa.js
Email: user@example.com
Пароль:
 Помилка надсилання коду: connect ECONNREFUSED 127.0.0.1:2525
[Введіть резервний код:
Вхід за резервним кодом.
```

- друга - без нього ,що дасть нам можливість отримати наш код підтвердження на скриньку.

```
node login2fa.js
[Email: user@example.com
[Пароль:
 Код надіслано на email. Перевірте пошту Mailtrap.
[Введіть код з email:
 Успішний вхід.
```

У висновку бачимо, що технічна частина 2FA працює як очікується: система реагує на збій, не блокує вхід, а переходить до запасного методу. Проте з боку користувача важливо заздалегідь зберегти резервні коди.

Отже, система реагує безперебійно лише за умови наявності альтернативних методів входу (наприклад, резервні коди). У разі відсутності таких – користувач блокується. Це доводить, що технічна вразливість у парі з впливом людського фактору (втрата резервних кодів) утворюють потенційну загрозу безпеці середовища.

Втрата доступу до пристрою з 2FA

Проведемо другий дослід, що полягає у втраті доступу до пристрою з 2FA. Для виконання доступу використано додаток Google Authenticator, а також створено тестовий аккаунт на GitHub. Нижче наведено послідовність дій у даному дослідженні(див. рис. 11):

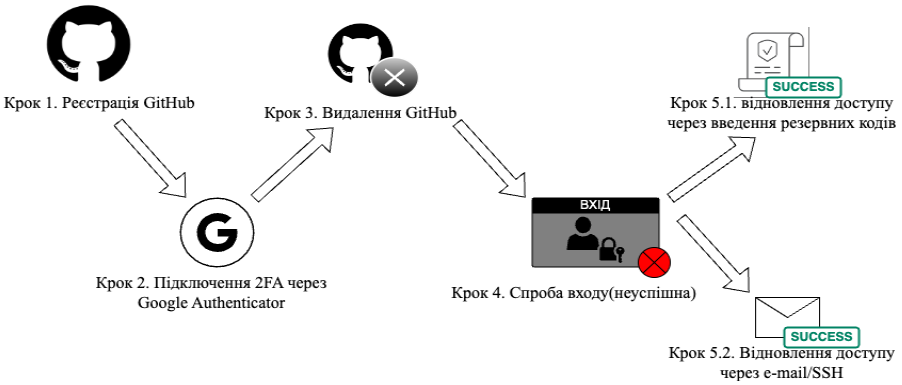

Рис. 11. Алгоритм симуляції збою доставки резервних кодів

Після створення акаунту, увімкнемо 2FA, через обраний додаток, для цього в Google Authenticator відскануємо QR-код на GitHub, за результатами виконаних дій отримаємо факт того, що тепер крім паролю та логіну, користувачу потрібно вводити код з додатка, який з часом змінюється. До речі, після підключення 2FA згенеровано 16 резервних кодів, тобто, якщо буде якийсь збій у додатку, список з ними треба буде обов'язково завантажити на ПК, без цієї дії 2FA не виконати.

ISSN 2663 - 4023

Для експерименту змодельована ситуація, де ми у ролі недосвідченого користувача, що деінсталював програму для автентифікації(при спробі увійти нам всерівно потрібно ввести додатковий код) (див. рис. 12).

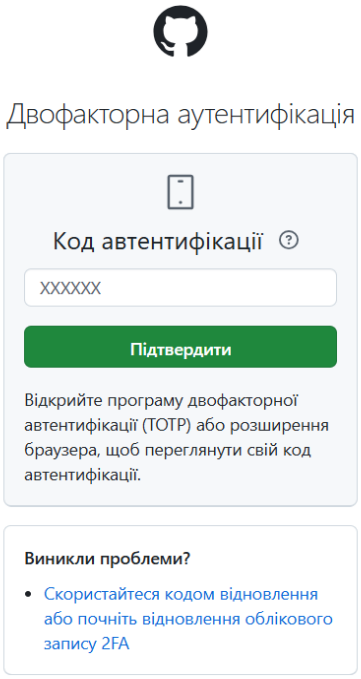

Рис. 12. Вікно вводу коду автентифікації GitHub

Для вирішення даної проблеми маємо опцію: Скористайтеся кодом відновлення або почніть відновлення облікового запису 2FA, саме для цього і потрібні резервні коди, які завантажено з GitHub, при вводі будь-якого з них отримано доступ до аккаунту.

Проте, бувають ситуації, коли документ з резервними кодами було видалено, наприклад, після планової чистки ПК. У такому випадку отримаємо подальші інструкції (див. рис. 13):

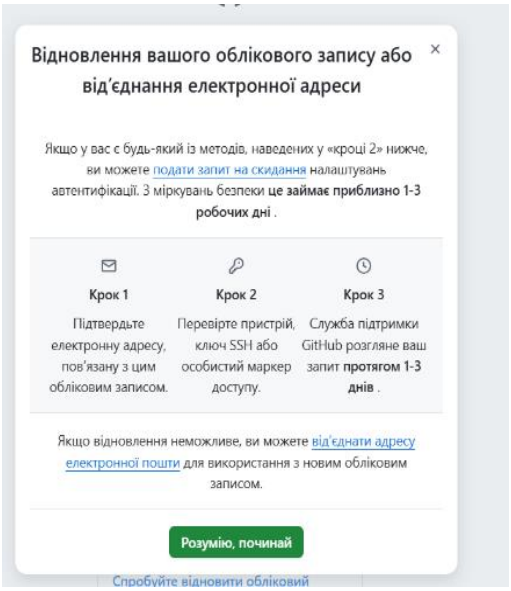

Рис. 13. Інструкція відновлення облікового запису

Тобто тут надано інструкцію(див. рис. 14), щодо повернення акаунта у 3 кроки, спершу етап підтвердження електронної адреси, після етап перевірки пристрою, ключ SSH або особистий маркер доступу, який можна встановити при налаштуванні автентифікації і тільки після цього передати запит в службу підтримки, що оброблятиметься протягом 1–3 днів, тому так просто зайти зловмиснику не вийде, тобто якщо розглядати цей момент зі сторони соціальної інженерії, то є проблеми, а саме — налаштування для другого кроку є необов'язковими, тому якщо людина їх не встановила аккаунт не можливо відновити. У такому випадку GitHub пропонує нам від'єднати адресу і використовувати вже новий обліковий запис, тобто доступ до старого буде втрачено.

Отже, у висновку, система 2FA працює безперебійно і є досить надійною, можна зробити багато налаштувань для відновлення аккаунту, що може вирішити проблеми втрати доступу до облікового запису через людський фактор, проте ці заходи протидії помилкам не є обов'язковими, тому це може привести до втрати доступу. Окрема увага факту того, що встановити 2FA не можливо без завантаження кодів відновлення, що однозначно дуже добре, бо це значно скорочує шанс помилки.

Маніпуляція часовими налаштуваннями для обходу 2FA

У третьому досліді перевіримо, чи можна обійти двофакторну автентифікацію (2FA), засновану на алгоритмі TOTP, за допомогою маніпуляції локальним часом на пристрої, який генерує одноразові коди. Дослід базується на використанні сервісу GitHub, генератора TOTP-кодів Raivo OTP (на іншому пристрої), та ручної зміни системного часу. Нижче наведено покрокову інструкцію(див. рис. 14):

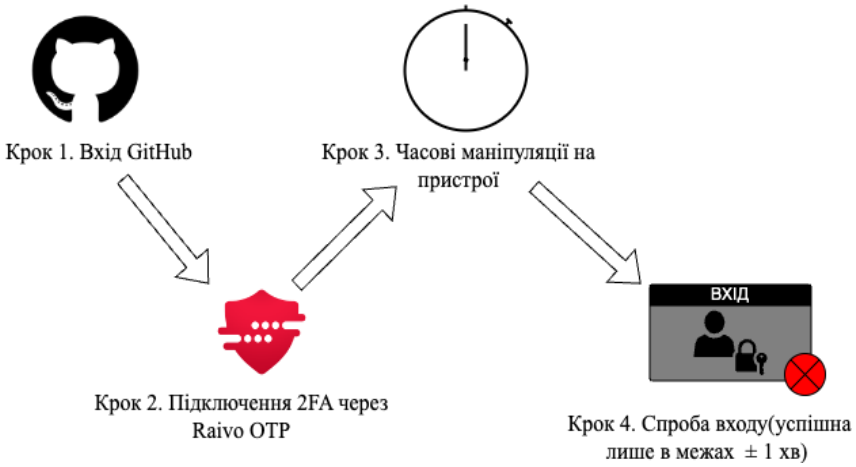

Рис.14. Алгоритм маніпуляції часовими налаштуваннями для обходу 2FA

У даному дослідженні створено тестовий Github — акаунт, на якому налаштована двофакторна автентифікація (2FA) за допомогою коду отриманого з утиліти Raivo, що генерує їх на іншому пристрої. Поки доступ до акаунта можливий. Далі змінено налаштування системного часу: спочатку на -30 секунд, після на +30 секунд та -1 хвилину, у всіх випадках доступ досі можливий.

Після цього змінено налаштування на +2, -3,+5 хвилин та у всіх випадках отримаємо помилку доступу (коди не є дійсними) (див. рис. 15).

ISSN 2663 - 4023

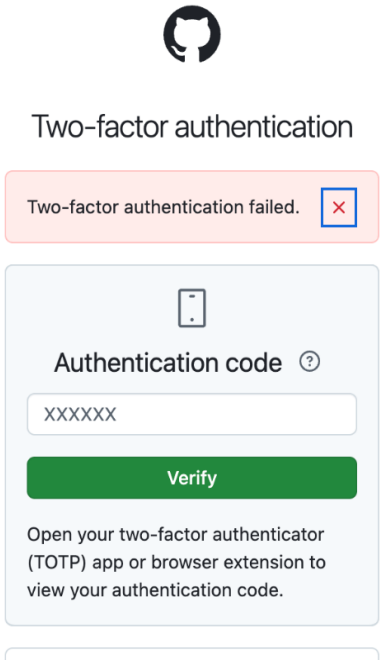

Рис. 15. Демонстрація помилки доступу

Отже, висновки, щодо експерименту:

1. маніпуляція локальним часом не дозволяє обійти TOTP-2FA, якщо сервер суворо дотримується часових вікон (як от GitHub);
2. найбільший шанс «вгадати» дійсний код — при спробах в межах ±1 хвилини, далі — без шансів;
3. спроби «брутфорсити»(brute force) зсув часу швидко блокуються або лімітуються кількістю спроб на сервері;
4. Raivo поводиться очікувано — генерує коди відповідно до встановленого часу, не повідомляючи про розсинхронізацію.

Отже, TOTP є надійною формою 2FA, і проста маніпуляція часом не дозволяє обійти захист, якщо сервер налаштований правильно (як у випадку з GitHub). Проте витік секретного ключа TOTP або соціальна інженерія — реальні загрози, проти яких TOTP сам по собі безсилий.

Отож, усі три практичні досліди показали, що навіть найпоширеніші сценарії використання 2FA містять потенційні вразливості. Очевидно, що основною передумовою для цього дослідження була необхідність перевірити, наскільки 2FA є стійкою до цілком можливих загроз — технічних збоїв, втрати доступу до пристроїв, спроб обійти рівні безпеки і недбалості користувачів.

Щодо причин виникнення проблем можна виразити ось ці 4 основні чинники:

1. Недостатня інформованість користувачів щодо важливості збереження резервних кодів та налаштувань для відновлення доступу.
2. Орієнтація деяких сервісів на зручність, а не на безпеку, що призводить до спрощеної логіки відновлення акаунтів.
3. Використання застарілих або нестійких каналів передачі кодів, таких як SMS або незахищені поштові сервіси.

4. Технічні обмеження TOTP, пов'язані з часовими вікнами, які легко порушуються при маніпуляції системним часом або внаслідок розсинхронізації пристроїв.

Врахувавши усі нюанси та провівши практичні досліди, можна виокремити рекомендації для розробників та користувачів:

1. Для забезпечення надійного захисту акаунтів необхідно впроваджувати багаторівневі механізми відновлення доступу, що передбачають обов'язкове налаштування резервних кодів — це заздалегідь згенеровані одноразові ключі, які користувач повинен зберігати в безпечному місці, наприклад, у фізичному вигляді або в захищеному менеджері паролів. Додатковий або другий пристрій, наприклад, інший смартфон чи планшет, забезпечує альтернативний канал доступу до 2FA-кодів у разі втрати основного засобу автентифікації. Усі запити на відновлення повинні проходити перевірку — надсилання сповіщень на всі пов'язані канали, затримку виконання (наприклад, 24 години) та верифікацію через додаткову інформацію. Такий підхід мінімізує ризики компрометації навіть у складних ситуаціях.

2. Щоб підвищити ефективність систем багатофакторної автентифікації, важливо не лише впроваджувати технічні засоби захисту, а й забезпечити користувачів чіткими, зрозумілими інструкціями щодо їх використання. Зокрема, слід надати докладні рекомендації щодо створення, збереження та використання резервних кодів. Користувач повинен розуміти, що ці коди є критично важливими для відновлення доступу в разі втрати основного засобу автентифікації, тому їх слід зберігати у захищеному місці — наприклад, у шифрованому менеджері паролів або в фізичному форматі (роздрукованими й схованими у надійному місці). Також необхідно акцентувати увагу на потенційних ризиках у разі нехтування безпековими налаштуваннями. Це може включати конкретні приклади: наприклад, втрату доступу до облікового запису без можливості його відновлення, або ризик компрометації акаунту, якщо резервні коди зберігаються у відкритому вигляді (наприклад, у блокноті на робочому столі чи у вхідній поштовій скриньці). Корисно також впроваджувати інструкції у вигляді покрокових гідів або інтерактивних підказок під час налаштування 2FA, щоб підвищити ймовірність правильного виконання користувачем усіх дій. Це створює більшу усвідомленість і відповідальність користувача, що є ключовим у боротьбі з соціальними інженерними атаками.

3. Не покладатися лише на SMS чи поштові коди**,** адже SMS та e-mail залишаються вразливими до атак, таких як SIM-swapping, перехоплення повідомлень, або компрометації поштової скриньки. Тому варто переходити до більш захищених методів автентифікації. Серед них — апаратні токени (наприклад, YubiKey, SoloKey) та мобільні додатки з криптографічним захистом, як-от Google Authenticator, Raivo OTP, Authy. Ці засоби працюють з протоколами TOTP або FIDO2/WebAuth[5] і не передають дані по незахищених каналах.

4. Перевіряти синхронізацію часу**,** оскільки алгоритм TOTP базується на поточному часі, навіть невелика розбіжність між часом на пристрої користувача та сервером може призвести до помилки автентифікації. Рекомендовано впровадити механізм автоматичної перевірки синхронізації часу під час логіну та сповіщення користувача у разі виявлення розбіжностей. Це підвищить надійність системи і полегшить діагностику у випадках відмови в доступі.

5. Для запобігання брутфорс-атакам необхідно:

- Обмежити кількість спроб введення коду (наприклад, 5 за сесію);
- Запровадити затримки у часі між спробами (наприклад, зростаюча затримка);

– Використовувати CAPTCHA після кількох невдалих спроб;
– У разі підозрілої активності — тимчасово блокувати акаунт або вимагати додаткову верифікацію.

6. Ще одним важливим аспектом захисту механізмів TOTP є використання шифрування секретного ключа на рівні додатку з динамічним розшифруванням лише в момент потреби (наприклад, при автентифікації користувача). Це мінімізує час, протягом якого ключ доступний у відкритому вигляді в оперативній пам'яті. Також рекомендується використовувати сучасні алгоритми шифрування (наприклад, AES-256) у поєднанні з унікальними ключами шифрування для кожного користувача або пристрою. В середовищах, де можлива інтеграція, доцільно застосовувати зовнішні сервіси керування ключами (наприклад, AWS KMS, Azure Key Vault, HashiCorp Vault), які централізовано зберігають, шифрують і контролюють доступ до ключів. Такі сервіси часто мають вбудовану підтримку журналювання, автоматичної ротації ключів та політик доступу, що значно підвищує рівень безпеки усього процесу автентифікації.

Усі виявлені вразливості та проблемні аспекти засвідчують, що ефективність систем двофакторної автентифікації значною мірою залежить як від технічної реалізації, так і від поведінки користувача. З урахуванням результатів проведених експериментів та аналізу реакції систем на нестандартні ситуації, можна сформулювати наступні висновки.

ВИСНОВКИ

У результаті дослідження ефективності двофакторної автентифікації (2FA), що базувалося на практичному моделюванні типових загроз, було підтверджено важливість як технічної реалізації системи автентифікації, так і впливу людського фактору. Аналіз охопив три основні сценарії загроз: збій доставки кодів, втрату доступу на пристрої з 2FA, а також маніпуляції з часовими налаштуваннями і ось до яких висновків він привів:

1. Симуляція збою доставки кодів через блокування мережі (SMTP) свідчить, що 2FA через e-mail є найменш захищеним методом автентифікації. У разі втрати мережевого покриття або роботи брандмауера користувач втрачає можливості отримати код підтвердження. Надійність такого методу залежить лише від наявності попередньо налаштованих резервних способів входу. Отже, найменш захищеним за критерієм стійкості до технічних збоїв є 2FA через e-mail/SMS.

2. У випадку втрати пристрою з активованим 2FA (Google Authenticator) доведено, що система загалом здатна надати необхідний рівень безпеки, але лише за умови, що користувач зберіг резервні коди або активував додаткові канали відновлення (наприклад, SSH-ключ або маркер доступу). Якщо ж цього зроблено не було, доступ до облікового запису фактично втрачається. Таким чином, критичним фактором у безпеці 2FA виступає саме людський фактор, і захищеність системи напряму залежить від цифрової грамотності користувача.

3. Моделювання маніпуляції часовими налаштуваннями (TOTP, Raivo OTP) показало, що система надійно блокує спроби автентифікації поза допустимим часовим вікном (±2 хвилини). Що доводить те, що TOTP підтвердив свою ефективність як захищений протокол, за умови коректної реалізації серверної логіки. Проте навіть він не може протидіяти витоку секретного ключа чи соціальній інженерії — отже, потребує поєднання з іншими методами захисту.

4. Найбільш захищеними за критерієм технічної надійності та водночас найзручнішими і універсальними є апаратні токени (наприклад, YubiKey, FIDO2) та

програмні TOTP-додатки (Raivo OTP, Google Authenticator), які працюють незалежно від інших додатків, мережевого з'єднання або мобільного зв'язку, і не піддаються впливу мережевих атак. Усі протестовані методи підтвердили свою стійкість до типових технічних вразливостей, за винятком SMS- та e-mail-ідентифікації, які залишаються вразливими до перехоплення, затримок доставки, або повного блокування.

Таким чином, загальна ефективність 2FA напряму залежить від обраного методу автентифікації та рівня підготовленості користувача. Успішна реалізація захисту вимагає поєднання надійної технології з продуманою взаємодією між системою і користувачем, включно з обов'язковим інформуванням про ризики, необхідністю зберігання резервних кодів і налаштуванням альтернативних каналів відновлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization (ISO/IEC 27001:2022). (2022).
2. National Institute of Standards and Technology (NIST). Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. Gaithersburg, MD: NIST (2020). https://pages.nist.gov/800-63-3/sp800-63b.html
3. Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. *IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44
4. *Google Security Blog. How Google Accounts are attacked: Insights from millions of users.* (2021). https://security.googleblog.com/2021/
5. *FIDO Alliance. FIDO2: Moving the World Beyond Passwords.* (2021). https://fidoalliance.org/fido2/'
6. Kim, M., Sukh, J., & Kwon, H. (2022). A study of the emerging trends in SIM swapping crime and effective countermeasures. *Proceedings of the 7th IEEE/ACIS International Conference on Big Data, Cloud Computing, and Data Science (BCD 2022)*, 240–245. https://doi.org/10.1109/BCD54882.2022.9900510
7. Brostoff, S., Sasse, M. A. (2013). Are Passfaces more usable than passwords? A field trial investigation. *Proceedings of the Sixth International Conference on Information Security*, 161–174. https://doi.org/10.1007/978-1-4471-0515-2_27
8. IBM Security. (2022). *X-Force Threat Intelligence Index 2022*. International Business Machines Corporation. https://www.ibm.com/reports/threat-intelligence
9. Anti-Phishing Working Group. (2022). *Phishing activity trends report: 4th quarter 2021*. APWG. https://apwg.org/trendsreports/
10. Zscaler. (2022). *EvilProxy phishing-as-a-service platform targets MFA-protected accounts.* Zscaler. https://www.zscaler.com/blogs/security-research/evilproxy-phishing-service
11. Microsoft. (2022). *Defending Ukraine: Early lessons from the cyber war*. Microsoft Security Blog. https://www.microsoft.com/enus/security/blog/2022/04/27/defending-ukraine-early-lessons-from-the-cyber-war/
12. Federal Communications Commission. (2021). *FCC acts to protect consumers from SIM swapping scams.* https://www.fcc.gov/document/fcc-acts-protect-consumers-sim-swapping-scams
13. ThreatFabric. (2022). *Mobile malware BRATA evolves with new features*. https://www.threatfabric.com/blogs/brata-targeting-latam.html
14. Proofpoint. (2023). *2023 State of the Phish Report: Threat Actors Double Down on Emerging and Tried-and-Tested Tactics to Outwit Employees.* https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2023-state-phish-report-threat-actors-double-down-emerging-and-0
15. ENISA. Threat Landscape 2022: Cybersecurity threats facing Europe. European Union Agency for Cybersecurity. (2022). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
16. *2023 Data Breach Investigations Report.* (2023). Verizon. https://www.verizon.com/business/resources/reports/dbir/
17. *Understanding phishing attacks and how to prevent them. Cloudflare Learning Center.* (2022). Cloudflare. https://www.cloudflare.com/learning/security/threats/phishing-attacks/

18. *Global Cybersecurity Outlook 2023. WEF*. (2023). World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2023
19. *CIS Controls v8. CIS*. (2021). CIS (Center for Internet Security). https://www.cisecurity.org/controls/cis-controls/
20. *Cybersecurity and Infrastructure Security Agency (CISA). Protecting Against Phishing.* (2022). CISA. https://www.cisa.gov/protecting-against-phishing

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Ivan Opirskyy
Doctor of Technical Sciences, Professor, Head of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Roman Sikorskyi
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0003-2964-6083
roman.sikorskyi.kb.2023@lpnu.ua

Dmytro Martyniuk
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0004-8065-9274
dmytro.martyniuk.kb.2023@lpnu.ua

ANALYSIS OF THE EFFECTIVENESS OF TWO-FACTOR AUTHENTICATION AND THE HUMAN FACTOR IN CYBERSECURITY

Abstract. In the digital environment, where information has become one of the most valuable resources, ensuring its confidentiality and integrity is a top priority for both government institutions and the private sector. Given the growing diversity of cyber threats and the rapid increase in incidents of unauthorized access to user accounts, traditional password-based authentication methods are no longer sufficient to provide an adequate level of protection. The widespread use of social engineering techniques, phishing attacks, malicious software, and automated password-cracking technologies has emphasized the urgent need for more secure and resilient authentication mechanisms. One such method is two-factor authentication (2FA), which relies on the combination of at least two independent factors for identity verification. Although 2FA is supported by most modern digital services and platforms, its effectiveness in practice is determined not only by its technical implementation but also by the behavior of the end user. This paper presents a comprehensive approach to analyzing the resilience of two-factor authentication systems, addressing both technological solutions and the human factor as a potential vulnerability. A series of practical experiments were conducted to simulate typical threat scenarios, including code delivery failures, device loss, and manipulation of time parameters. The results reveal that unauthorized access often becomes possible due to poor storage of backup codes, users' limited awareness of authentication principles, and the use of insecure delivery channels such as SMS. Particular attention is drawn to the issue of users refusing to configure additional recovery mechanisms, which may lead to permanent account loss. The study evaluates the effectiveness of tools such as Google Authenticator, Authy, hardware tokens, and cryptographic protocols like FIDO2. The findings justify the need to integrate multi-level authentication systems with clear user guidance, time synchronization checks, and automated suspicious activity monitoring. It is concluded that an optimal combination of technical safeguards and user digital literacy forms the foundation for building robust authentication mechanisms capable of countering contemporary cybersecurity threats.

Keywords: two-factor authentication; human factor; digital security; phishing; social engineering; backup codes.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization (ISO/IEC 27001:2022). (2022).
2. National Institute of Standards and Technology (NIST). Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. Gaithersburg, MD: NIST (2020). https://pages.nist.gov/800-63-3/sp800-63b.html

3. Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. *IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44
4. *Google Security Blog. How Google Accounts are attacked: Insights from millions of users.* (2021). https://security.googleblog.com/2021/
5. *FIDO Alliance. FIDO2: Moving the World Beyond Passwords.* (2021). https://fidoalliance.org/fido2/'
6. Kim, M., Sukh, J., & Kwon, H. (2022). A study of the emerging trends in SIM swapping crime and effective countermeasures. *Proceedings of the 7th IEEE/ACIS International Conference on Big Data, Cloud Computing, and Data Science (BCD 2022)*, 240–245. https://doi.org/10.1109/BCD54882.2022.9900510
7. Brostoff, S., Sasse, M. A. (2013). Are Passfaces more usable than passwords? A field trial investigation. *Proceedings of the Sixth International Conference on Information Security*, 161–174. https://doi.org/10.1007/978-1-4471-0515-2_27
8. IBM Security. (2022). *X-Force Threat Intelligence Index 2022*. International Business Machines Corporation. https://www.ibm.com/reports/threat-intelligence
9. Anti-Phishing Working Group. (2022). *Phishing activity trends report: 4th quarter 2021*. APWG. https://apwg.org/trendsreports/
10. Zscaler. (2022). *EvilProxy phishing-as-a-service platform targets MFA-protected accounts.* Zscaler. https://www.zscaler.com/blogs/security-research/evilproxy-phishing-service
11. Microsoft. (2022). *Defending Ukraine: Early lessons from the cyber war*. Microsoft Security Blog. https://www.microsoft.com/enus/security/blog/2022/04/27/defending-ukraine-early-lessons-from-the-cyber-war/
12. Federal Communications Commission. (2021). *FCC acts to protect consumers from SIM swapping scams.* https://www.fcc.gov/document/fcc-acts-protect-consumers-sim-swapping-scams
13. ThreatFabric. (2022). *Mobile malware BRATA evolves with new features*. https://www.threatfabric.com/blogs/brata-targeting-latam.html
14. Proofpoint. (2023). *2023 State of the Phish Report: Threat Actors Double Down on Emerging and Tried-and-Tested Tactics to Outwit Employees.* https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2023-state-phish-report-threat-actors-double-down-emerging-and-0
15. ENISA. Threat Landscape 2022: Cybersecurity threats facing Europe. European Union Agency for Cybersecurity. (2022). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
16. *2023 Data Breach Investigations Report.* (2023). Verizon. https://www.verizon.com/business/resources/reports/dbir/
17. *Understanding phishing attacks and how to prevent them. Cloudflare Learning Center.* (2022). Cloudflare. https://www.cloudflare.com/learning/security/threats/phishing-attacks/
18. *Global Cybersecurity Outlook 2023. WEF.* (2023). World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2023
19. *CIS Controls v8. CIS.* (2021). CIS (Center for Internet Security). https://www.cisecurity.org/controls/cis-controls/
20. *Cybersecurity and Infrastructure Security Agency (CISA). Protecting Against Phishing.* (2022). CISA. https://www.cisa.gov/protecting-against-phishing