ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система ідентифікації користувачів до ресурсів приватної організації»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олег Белан
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
БЕЛАН Олег
(прізвище, ім'я)

Керівник доктор філософії СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ВСТУП

Актуальність дослідження. В умовах стрімкого розвитку інформаційних технологій та цифрової трансформації бізнес-процесів, питання забезпечення надійного контролю доступу до корпоративних інформаційних ресурсів набуває критичного значення для приватних організацій. Протягом останнього десятиріччя кількість кіберінцидентів, пов'язаних з несанкціонованим доступом до корпоративних систем, зросла в декілька разів, що призводить до значних фінансових втрат, витоку конфіденційної інформації та репутаційних ризиків.

Системи ідентифікації та автентифікації користувачів є першою лінією оборони від несанкціонованого доступу до інформаційних ресурсів організації. Загрози, такі як атаки на паролі, соціальна інженерія, фішинг, викрадення облікових даних та використання скомпрометованих ідентифікаційних відомостей, вимагають впровадження багаторівневих та адаптивних систем ідентифікації. Приватні організації стикаються з особливими викликами при побудові систем ідентифікації користувачів: необхідністю балансування між безпекою та зручністю використання, інтеграцією з наявною IT-інфраструктурою, забезпеченням масштабованості рішень та оптимізацією витрат на впровадження та підтримку. Відсутність централізованого управління ідентифікаційними даними, неефективні процеси надання та відкликання доступу, а також недостатній моніторинг активності користувачів створюють додаткові ризики для інформаційної безпеки організації.

Актуальні рішення в сфері ідентифікації та автентифікації такі як багатофакторна автентифікація, біометричні методи ідентифікації, адаптивна автентифікація на основі аналізу ризиків, федеративне управління ідентифікаційними даним, відкривають нові можливості для підвищення рівня безпеки при збереженні зручності для кінцевих користувачів. Однак впровадження таких рішень потребує комплексного підходу, що враховує специфіку діяльності організації, її технічну готовність та фінансові можливості.

Об'єкт дослідження – процес управління ідентифікацією та автентифікацією

користувачів у приватній організації.

Предмет дослідження – методи та засоби побудови ефективної системи ідентифікації користувачів до ресурсів приватної організації, а також аналіз та оцінка їх ефективності в контексті забезпечення інформаційної безпеки.

Мета роботи – розробка рекомендацій щодо ефективної системи ідентифікації користувачів до ресурсів приватної організації з урахуванням сучасних вимог інформаційної безпеки.

Наукові завдання:

Дослідити теоретичні основи ідентифікації та автентифікації користувачів в інформаційних системах організацій.

Проаналізувати сучасні загрози та вразливості систем ідентифікації користувачів у приватних організаціях.

Дослідити та класифікувати існуючі методи та технології ідентифікації користувачів, оцінити їх переваги та недоліки..

Провести порівняльний аналіз сучасних програмних рішень та платформ для управління ідентифікаційними даними.

Розробити практичні рекомендації щодо впровадження та експлуатації системи ідентифікації користувачів з урахуванням специфіки приватних організацій.

Методи дослідження – аналіз літературних джерел та нормативних документів у сфері інформаційної безпеки, вивчення технічної документації сучасних систем управління ідентифікаційними даними, порівняльний аналіз існуючих рішень, моделювання архітектурних компонентів системи ідентифікації.

Практичне значення одержаних результатів: розроблено практичні рекомендації та архітектурні рішення для впровадження ефективної системи ідентифікації користувачів до ресурсів приватної організації, що дозволить підвищити рівень інформаційної безпеки при забезпеченні зручності використання для кінцевих користувачів та оптимізації витрат на впровадження та підтримку системи.

1 ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

1.1. Поняття ідентифікації та автентифікації користувачів

У наш час, коли цифрові технології швидко розвиваються та комп’ютерні системи стають невід’ємною частиною різних сфер життя, питання захисту інформації набуває особливої актуальності. Зростання кількості кіберзагроз, ускладнення методів несанкціонованого доступу до інформаційних ресурсів та збільшення обсягів конфіденційної інформації, що обробляється в цифровому форматі, зумовлюють необхідність розробки та впровадження ефективних механізмів контролю доступу до інформаційних систем.

Одним із елементів системи інформаційної безпеки є процеси ідентифікації та автентифікації користувачів, які становлять першу лінію оборони від несанкціонованого доступу до інформаційних ресурсів. Ці процеси є невід'ємною складовою комплексної системи управління доступом та відіграють ключову роль у забезпеченні конфіденційності, цілісності та доступності інформації. Теоретичне обґрунтування та практичне впровадження механізмів ідентифікації та автентифікації потребує глибокого розуміння їх сутності, взаємозв'язку та специфічних особливостей застосування в різноманітних інформаційних середовищах.

Ідентифікація користувачів у контексті інформаційної безпеки являє собою початковий етап процесу встановлення особистості суб'єкта, який намагається отримати доступ до інформаційної системи або її окремих компонентів. З теоретичної точки зору, ідентифікація представляє собою процес декларування користувачем своєї особистості шляхом надання певного ідентифікаційного атрибута або набору атрибутів, які мають унікально визначати його серед усіх інших користувачів системи.

Процес ідентифікації базується на принципі унікальності ідентифікаційних

даних, що означає неможливість існування двох різних користувачів з ідентичними ідентифікаторами в межах однієї інформаційної системи. Цей принцип є фундаментальним для забезпечення коректного функціонування всієї системи контролю доступу.

Цифрова ідентичність – це унікальне представлення суб'єкта, який бере участь в онлайн-транзакції. Цифрова ідентичність завжди унікальна в контексті цифрової послуги, але не обов'язково має бути пов'язана з конкретним реальним суб'єктом. Іншими словами, доступ до цифрової послуги може не означати, що реальне представлення суб'єкта є відомим. Перевірка ідентичності встановлює, що суб'єкт є тим, за кого він себе видає. Цифрова автентифікація – це процес визначення дійсності одного або кількох автентифікаторів, які використовуються для заявлення цифрової ідентичності. Автентифікація встановлює, що суб'єкт, який намагається отримати доступ до цифрової послуги, контролює технології, що використовуються для автентифікації. Для служб, у яких застосовуються повторні візити, успішна автентифікація забезпечує розумні гарантії на основі ризику, що суб'єкт, який отримує доступ до послуги сьогодні, є тим самим, хто отримував доступ до послуги раніше. Цифрова ідентичність створює технічну проблему, оскільки вона часто передбачає перевірку особи через відкриту мережу та завжди передбачає автентифікацію осіб через відкриту мережу. Це створює численні можливості для видавання себе за іншу особу та інших атак, які можуть призвести до шахрайських заяв про цифрову ідентичність суб'єкта. Постійна автентифікація абонентів є центральною в процесі пов'язування абонента з його онлайн-активністю. Автентифікація абонента виконується шляхом перевірки того, що заявник контролює один або кілька автентифікаторів, пов'язаних з певним абонентом. Успішна автентифікація призводить до надання покладаючій стороні ідентифікатора, псевдонімного або непсевдонімного та за бажанням, іншої ідентифікаційної інформації.

Надійність транзакції автентифікації характеризується показником, відомим як AAL. Надійніша автентифікація вимагає від зловмисників кращих можливостей та витрат більших ресурсів для успішного підриву процесу автентифікації.

Автентифікація з вищими AAL може ефективно знизити ризик атак. *AAL1* надає певну гарантію того, що заявник контролює автентифікатор, прив'язаний до облікового запису абонента. AAL1 вимагає однофакторної або багатофакторної автентифікації з використанням широкого спектру доступних технологій автентифікації. Для успішної автентифікації заявник повинен підтвердити володіння та контроль над автентифікатором за допомогою безпечного протоколу автентифікації.

Автентифікація AAL1 повинна відбуватися за допомогою будь-якого з наступних типів автентифікаторів:

- Запам'ятаний секрет
- Пошук секретного коду
- Позасмугові пристрої
- Пристрій однофакторного одноразового пароля
- Багатофакторний пристрій OTP
- Однофакторне криптографічне програмне забезпечення
- Однофакторний криптографічний пристрій
- Багатофакторне криптографічне програмне забезпечення
- Багатофакторний криптографічний пристрій

AAL2 забезпечує високу впевненість у тому, що заявник контролює автентифікатор(и), прив'язаний(і) до облікового запису абонента. Потрібне підтвердження володіння та контролю двох різних факторів автентифікації через протокол(и) безпечної автентифікації. На рівні AAL2 та вище потрібні затверджені криптографічні методи.

У AAL2 автентифікація має відбуватися за допомогою багатофакторного автентифікатора або комбінації двох однофакторних автентифікаторів. Багатофакторний автентифікатор потребує двох факторів для виконання однієї події автентифікації, наприклад, криптографічно захищеного пристрою з інтегрованим біометричним датчиком, який потрібен для активації пристрою.Коли використовується багатофакторний автентифікатор, МОЖЕ бути використаний будь-який з наступних варіантів:

- Багатофакторний пристрій OTP
- Багатофакторне криптографічне програмне забезпечення
- Багатофакторний криптографічний пристрій

Коли використовується комбінація двох однофакторних автентифікаторів, вона повинна включати автентифікатор Memorized Secret та один автентифікатор на основі володіння (тобто «щось, що у вас є») з наступного списку:

- Пошук секретного коду
- Позасмуговий пристрій
- Однофакторний пристрій OTP
- Однофакторне криптографічне програмне забезпечення
- Однофакторний криптографічний пристрій

Криптографічні автентифікатори, що використовуються в AAL2, ПОВИННІ використовувати затверджену криптографію. Аутентифікатори, придбані державними установами, повинні бути перевіреними на відповідність вимогам [5] . Програмні автентифікатори, що працюють в контексті операційної системи, можуть, де це можливо, намагатися виявити компрометацію платформи, на якій вони працюють (наприклад, шкідливим програмним забезпеченням), і не повинні завершувати операцію, коли така компрометація виявлена. Принаймні один автентифікатор, що використовується в AAL2, повинен бути стійким до повторного відтворення.

Процес автентифікації вважається стійким до атаки повторного відтворення (replay attack), якщо практично неможливо досягти успішної автентифікації шляхом запису та повторного відтворення попереднього автентифікаційного повідомлення. Стійкість до повторного відтворення є додатковим захистом до властивостей захищених автентифікованих каналів зв’язку, оскільки автентифікаційні дані можуть бути викрадені ще до надходження до захищеного каналу.Протоколи, що використовують одноразові значення (nonce) або виклики-підтвердження (challenge-response) для підтвердження "свіжості" транзакції, вважаються стійкими до атак повторного відтворення, оскільки перевіряючий легко виявить повторне використання старих повідомлень — вони не міститимуть

відповідних одноразових значень або актуальних даних про час.

AAL3 забезпечує дуже високий рівень впевненості в тому, що заявник контролює автентифікатор, прив'язаний до облікового запису абонента. Автентифікація в AAL3 базується на доказі володіння ключем за допомогою криптографічного протоколу. Автентифікація AAL3 повинна використовувати апаратний автентифікатор та автентифікатор, який забезпечує стійкість до іменування себе за верифікатора — один і той самий пристрій може відповідати обом цим вимогам. Для автентифікації в AAL3 заявники повинні довести володіння та контроль над двома різними факторами автентифікації за допомогою безпечного протоколу автентифікації.

Автентифікація AAL3 повинна відбуватися за допомогою однієї з комбінацій автентифікаторів.

Можливі комбінації:

- Багатофакторний криптографічний пристрій
- Однофакторний криптографічний пристрій , що використовується разом із запам'ятовуваним секретом
- Багатофакторний пристрій OTP (програмний або апаратний) , що використовується разом з однофакторним криптографічним пристроєм
- Багатофакторний пристрій OTP (лише апаратний), що використовується разом з однофакторним криптографічним програмним забезпеченням
- Однофакторний пристрій OTP (лише апаратний), що використовується разом із багатофакторним криптографічним програмним автентифікатором
- Однофакторний пристрій OTP (лише апаратний), що використовується разом з однофакторним криптографічним програмним автентифікаторомта запам'ятовуваним секретним ключем

Повторна автентифікація Періодична повторна автентифікація сеансів абонентів повинна виконуватися. На AAL3 автентифікація абонента повинна повторюватися принаймні один раз на 12 годин протягом тривалого сеансу використання, незалежно від активності користувача. Повторна автентифікація

абонента повинна повторюватися після будь-якого періоду бездіяльності тривалістю 15 хвилин або довше. Повторна автентифікація повинна використовувати обидва фактори автентифікації. Сеанс повинен бути завершений після досягнення будь-якого з цих часових обмежень. Верифікатор може запропонувати користувачеві виконати активність безпосередньо перед тайм-аутом бездіяльності.

Таблиця 1.1.

Зведені вимоги AAL

Вимога	ALL1	ALL2	ALL3
Дозволені типи автентифікаторів	Запам’ятований секрет; Out-of-Band; SF OTP Device; MF OTP Device	MF OTP Device; MF Crypto Software; MF Crypto Device; або Memorized Secret разом з : • OTP Device • Crypto Software	SF OTP Device разом з MF Crypto Device або Software; SF OTP Device разом з SF Crypto Software разом з секретом.
Повторна автентифікація	30 днів	12 годин або 30 хвилин бездіяльності	12 годин або 15 хвилин бездіяльності
Контроль безпеки	Низький рівень	Помірний рівень	Високий рівень
Стійкість до компрометації верифікатором	Не обов’язково	Не обов’язково	Обов’язково
Опір повторному відтворенню	Не обов'язково	Обов'язково	Обов'язково
Політика зберігання записів	Обов'язково	Обов'язково	Обов'язково
Контроль конфіденційності	Обов'язково	Обов'язково	Обов'язково

1.2. Класифікація ідентифікаційних атрибутів

Ідентифікаційні атрибути, що використовуються в процесі ідентифікації користувачів, можна класифікувати за різними критеріями. За природою походження розрізняють:

Статичні атрибути - характеризуються незмінністю або мінімальною варіативністю протягом тривалого періоду часу. До цієї категорії належать біометричні характеристики, такі як відбитки пальців, геометрія долонь, структура райдужної оболонки ока, особливості сітківки ока та генетичні маркери. Ці атрибути забезпечують високий рівень унікальності ідентифікації, проте їх незмінність може становити ризик у випадку компрометації, оскільки неможливо "змінити" біометричну характеристику подібно до паролю.

Динамічні атрибути - підлягають регулярним змінам та можуть модифікуватися користувачем або системою. Найпоширенішими представниками цієї категорії є паролі, PIN-коди, секретні фрази та відповіді на контрольні питання. Головною перевагою динамічних атрибутів є можливість їх регулярного оновлення для підтримання належного рівня безпеки. Водночас вони потребують активного управління з боку користувачів та адміністраторів системи

Поведінкові атрибути - характеристики базуються на унікальних паттернах дій та звичок користувача. До них належать особливості клавіатурного почерку (ритм та швидкість набору тексту), манера роботи з мишею, навігаційні шаблони при використанні додатків, голосові характеристики та особливості підпису. Ці атрибути мають перевагу в тому, що їх складно підробити, проте вони можуть змінюватися під впливом зовнішніх факторів, таких як стрес, втома або фізичний стан користувача.

За рівнем конфіденційності поділяються на:

Публічні атрибути - не вимагають конфіденційного зберігання та можуть бути відомі широкому колу осіб. Типовими прикладами є ім'я користувача, електронна адреса, номер телефону або ідентифікаційні номери в публічних реєстрах. Хоча ці атрибути самостійно не забезпечують достатнього рівня безпеки для автентифікації, вони відіграють важливу роль у процесах ідентифікації та можуть використовуватися як частина багатофакторних схем.

Конфіденційні атрибути - вони потребують захищеного зберігання та обмеженого доступу. До цієї категорії належать паролі, криптографічні ключі, біометричні шаблони та особиста інформація, яка може використовуватися для

автентифікації. Компрометація таких атрибутів може призвести до серйозних порушень безпеки, тому вони потребують застосування спеціальних методів захисту, включаючи шифрування, хешування та контроль доступу.

Критичні атрибути - Критичні ідентифікаційні атрибути характеризуються найвищим рівнем чутливості та потребують максимального захисту. Зазвичай це стосується головних криптографічних ключів, основних адміністративних паролів та біометричних еталонів для систем високого рівня безпеки. Втрата або компрометація критичних атрибутів може призвести до катастрофічних наслідків для безпеки всієї системи.

Ефективна організація процесу ідентифікації повинна базуватися на дотриманні низки фундаментальних принципів:

Принцип унікальності передбачає, що кожен ідентифікатор може бути асоційований лише з одним користувачем у межах конкретної інформаційної системи. Порушення цього принципу призводить до неможливості точного визначення особистості користувача та створює передумови для виникнення конфліктів доступу.

Принцип постійності вимагає збереження ідентифікаційних даних користувача протягом усього періоду його роботи з системою. Зміна ідентифікатора може призвести до втрати зв'язку з історією дій користувача та ускладнити процеси аудиту.

Принцип простоти використання орієнтований на забезпечення зручності для кінцевого користувача та мінімізацію ймовірності помилок під час введення ідентифі

Автентифікація користувачів являє собою критично важливий процес верифікації заявленої під час ідентифікації особистості користувача. На відміну від ідентифікації, яка є простим декларуванням особистості, автентифікація передбачає активне підтвердження достовірності цієї заяви шляхом перевірки спеціальних автентифікаційних факторів. Теоретичною основою процесу автентифікації є концепція доведення особистості, яка базується на принципі, що законний користувач повинен володіти певною інформацією, предметами або

характеристиками, недоступними для сторонніх осіб. Цей принцип знаходить своє втілення в різноманітних методах автентифікації, кожен з яких має свої переваги та обмеження.

1.3Стандарти та нормативні вимоги до ідентифікації користувачів

ISO/IEC 27001 та ISO/IEC 27002

Стандарт ISO/IEC 27001 "Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційною безпекою - Вимоги" встановлює основні принципи управління доступом користувачів до інформаційних ресурсів організації.

Ключові вимоги стандарту щодо ідентифікації користувачів:

- Обов'язкова ідентифікація всіх користувачів перед наданням доступу до системи
- Використання унікальних ідентифікаторів для кожного користувача
- Регулярний перегляд та оновлення прав доступу
- Забезпечення конфіденційності автентифікаційної інформації

ISO/IEC 27002 надає детальні рекомендації щодо реалізації контролів безпеки, включаючи управління доступом користувачів. Стандарт визначає необхідність формальної процедури реєстрації та скасування реєстрації користувачів, а також встановлення чітких ролей та обов'язків.

NIST SP 800-63 Digital Identity Guidelines

Національний інститут стандартів і технологій США (NIST) розробив комплексні рекомендації щодо цифрової ідентичності в документі SP 800-63, який складається з чотирьох частин:

NIST SP 800-63A (Enrollment and Identity Proofing) визначає процеси реєстрації користувачів та підтвердження їх ідентичності. Стандарт встановлює три рівні забезпечення ідентичності (IAL1, IAL2, IAL3) залежно від ризиків та вимог системи.

NIST SP 800-63B (Authentication and Lifecycle Management) описує вимоги

до автентифікаторів та їх управління протягом життєвого циклу. Визначає три рівня забезпечення автентифікації (AAL1, AAL2, AAL3).

NIST SP 800-63C (Federation and Assertions) регулює федеративну ідентифікацію та використання затверджень ідентичності між різними системами.

IEEE 802.1X

Стандарт IEEE 802.1X забезпечує механізм контролю доступу до мережі на основі портів. Він використовує протокол EAP (Extensible Authentication Protocol) для автентифікації користувачів перед наданням доступу до мережевих ресурсів.

Основні компоненти архітектури 802.1X:

- Supplicant (клієнт) - пристрій, що запитує доступ
- Authenticator (автентифікатор) - пристрій, що контролює доступ
- Authentication Server (сервер автентифікації) - зазвичай RADIUS сервер

Закон України "Про захист персональних даних"

Закон України "Про захист персональних даних" від 1 червня 2010 року № 2297-VI [8]є основним нормативно-правовим актом, що регулює відносини у сфері захисту персональних даних в Україні та визначає правові засади збирання, обробки, зберігання та використання відомостей про фізичних осіб. У 2010 році парламент України ратифікував Конвенцію 108, і з метою імплементації її і Директив ЄС ухвалив Закон "Про захист персональних даних" який набрав чинності 1 січня 2011 року та неодноразово зазнавав змін та доповнень протягом свого існування.

Метою закону є захист основних прав і свобод людини і громадянина при обробці персональних даних, зокрема права на недоторканність приватного життя, особисту та сімейну таємницю. Закон поширюється на відносини, що виникають при обробці персональних даних, яка здійснюється повністю або частково з використанням засобів автоматизації, а також при обробці персональних даних, що містяться у базі персональних даних або призначені для внесення до неї, якщо така обробка здійснюється без використання засобів автоматизації.

Основні поняття, визначені законом, включають персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або

може бути конкретно ідентифікована а також володільця персональних даних - фізичну особу, якої стосуються персональні дані, розпорядника персональних даних - орган державної влади, орган місцевого самоврядування, юридичну або фізичну особу, які визначають мету обробки персональних даних, склад персональних даних, що підлягають обробці, та процедури їх обробки. Третя особа – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій володільцем чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону ЗАКОН УКРАЇНИ №2297–VI — Офіційне інтернет-представництво Президента України .

Об'єктами захисту є персональні дані, які можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Закон встановлює принципи обробки персональних даних, серед яких: законність та справедливість обробки, обробка персональних даних лише для конкретних і заздалегідь визначених цілей, відповідність і необмежність обробки персональних даних цілям їх збирання, точність і у разі необхідності оновлення персональних даних, зберігання персональних даних у формі, що дозволяє визначити суб'єкта персональних даних, не довше ніж цього вимагають цілі, для яких вони збираються та обробляються.

Особливо важливим принципом є згода на обробку, оскільки не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Згода на обробку персональних даних має бути усвідомленою, конкретною та добровільною вказівкою бажання суб'єкта персональних даних у вигляді письмової заяви або іншої дії, що однозначно засвідчує надання суб'єктом персональних даних дозволу на обробку його персональних даних відповідно до сформульованої мети їх обробки.

. Суб'єкт також має право отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким

передаються його персональні дані, отримувати на його вимогу безоплатно інформацію про обробку його персональних даних та вимагати її виправлення або знищення у володільця та розпорядника персональних даних або подавати заяву про це до уповноваженого державного органу з питань захисту персональних даних.

Закон встановлює особливий порядок обробки чутливих персональних даних, до яких належать дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство у політичних партіях та професійних спілках, засудження до кримінального покарання, а також дані, що стосуються здоров'я, статевого життя, біометричні або генетичні дані. Обробка таких даних забороняється, за винятком випадків, коли суб'єкт персональних даних дав однозначну згоду на обробку таких даних, або обробка необхідна для захисту життєво важливих інтересів суб'єкта персональних даних чи іншої особи, якщо суб'єкт персональних даних фізично або юридично нездатний дати згоду.

2 ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

2.1 Порівняльний аналіз методів ідентифікації

Ідентифікація користувачів є фундаментальним процесом встановлення особи користувача перед наданням доступу до інформаційних ресурсів системи. Цей процес базується на використанні різноманітних автентифікаторів – об'єктів або даних, які дозволяють системі підтвердити заявлену ідентичність користувача.

Сучасні методи ідентифікації класифікуються за типом факторів автентифікації, які використовуються в процесі верифікації:

Фактор знання (що знає користувач) – включає секретну інформацію, відому лише користувачу, таку як паролі, PIN-коди, відповіді на секретні питання.

Фактор володіння (що має користувач) – охоплює фізичні або цифрові об'єкти, які знаходяться в розпорядженні користувача, наприклад смарт-карти, апаратні токени, мобільні пристрої.

Фактор властивості (ким є користувач) – базується на унікальних біометричних характеристиках людини, включаючи відбитки пальців, геометрію обличчя, райдужну оболонку ока.

Контекстні фактори (де перебуває/коли використовує) – враховують обставини доступу, такі як геолокація, часові параметри, IP-адреса, характеристики пристрою.

Запам’ятовані секрети - Паролі та PIN-коди залишаються найбільш поширеним методом ідентифікації завдяки простоті впровадження та низькій вартості реалізації. Основною перевагою є відсутність потреби в додатковому обладнанні та універсальність застосування. Однак цей метод демонструє значні недоліки у сфері безпеки: високу вразливість до атак підбору, словникових атак, фішингу та соціальної інженерії. Додатковою проблемою є схильність користувачів до створення слабких паролів та їх повторного використання в різних системах.

Look-up секрети представляють собою попередньо створені таблиці з одноразовими кодами доступу. Цей метод забезпечує вищий рівень безпеки порівняно зі статичними паролями, оскільки кожен код може використовуватися лише один раз. Проте існують обмеження у кількості доступних кодів та необхідність фізичного зберігання таблиці, що створює ризики втрати або компрометації.

Одноразові паролі - технологія одноразових паролів генерує унікальні коди доступу з обмеженим терміном дії, що значно підвищує рівень безпеки системи. Паролі можуть генеруватися на основі часу або лічильника . Основними перевагами є захист від атак повторного відтворення та високий рівень стійкості до перехвату. Недоліками є необхідність синхронізації між сервером та клієнтським пристроєм, а також залежність від додаткового обладнання або програмного забезпечення.

Позасмугова автентифікація - метод Out-of-Band автентифікації передбачає верифікацію через незалежний комунікаційний канал, найчастіше через SMS-повідомлення або мобільні додатки. Це забезпечує додатковий рівень захисту, оскільки зловмиснику необхідно одночасно скомпрометувати два різні канали зв'язку. Однак існує залежність від якості мобільного зв'язку та потенційні вразливості каналу передачі даних.

Апаратні токени, смарт карти - фізичні пристрої безпеки забезпечують високий рівень захисту завдяки зберіганню криптографічних ключів у захищеному апаратному середовищі. Смарт-карти та USB-токени характеризуються стійкістю до програмних атак та складністю підробки. Основними недоліками є необхідність спеціального обладнання для зчитування, відносно висока вартість впровадження та ризик втрати або пошкодження пристрою.

Біометричні технології використовують унікальні фізіологічні або поведінкові характеристики людини для ідентифікації. До найпоширеніших методів належать:

- **Дактилоскопічна ідентифікація** – використання відбитків пальців, що характеризується високою точністю та швидкістю обробки

- **Розпізнавання обличчя** – аналіз геометричних характеристик обличчя за допомогою комп'ютерного зору
- **Сканування райдужної оболонки** – найточніший біометричний метод з найнижчим рівнем помилкових спрацювань
- **Аналіз голосу** – розпізнавання унікальних характеристик голосу користувача

Перевагами біометричних методів є зручність використання, неможливість втрати або передачі іншій особі, а також висока точність ідентифікації. Недоліками є потенційні помилки розпізнавання через зовнішні фактори, етичні питання конфіденційності біометричних даних та неможливість зміни біометричних характеристик у разі їх компрометації.

Багатофакторна автентифікація (MFA) являє собою метод захисту, який вимагає від користувача надання двох або більше незалежних доказів автентичності для підтвердження своєї ідентичності. Цей підхід ґрунтується на принципі комбінування різних категорій факторів автентифікації, що значно ускладнює можливість несанкціонованого доступу до системи навіть у випадку компрометації одного з факторів.

Найпоширенішою реалізацією є двофакторна автентифікація, яка зазвичай поєднує фактор знання (пароль) з фактором володіння (мобільний телефон для отримання SMS-коду або спеціальний додаток для генерації одноразових паролів). Трифакторна автентифікація додає третій компонент, часто у вигляді біометричної характеристики або контекстного фактора.

Ключові переваги багатофакторної автентифікації включають експоненційне підвищення рівня безпеки, ефективний захист від атак на основі викрадених паролів, можливість гнучкого налаштування комбінацій факторів відповідно до рівня ризику та специфіки застосування. Водночас впровадження MFA супроводжується певними викликами, зокрема підвищенням складності процесу входу для користувачів, необхідністю додаткової технічної інфраструктури та потенційними проблемами доступності при відмові одного з компонентів системи.

Адаптивна автентифікація

Адаптивна або ризик-орієнтована автентифікація представляє собою інтелектуальний підхід до верифікації користувачів, який динамічно коригує вимоги до процесу автентифікації на основі комплексного аналізу ризиків поточної спроби доступу. Система здійснює оцінку множини параметрів, включаючи поведінкові паттерни користувача, контекстні дані сесії та характеристики середовища доступу, формуючи індивідуальний профіль ризику для кожного запиту.

Технологія адаптивної автентифікації базується на аналізі таких ключових компонентів як історичні дані активності користувача (звичні години роботи, географічні локації, типи пристроїв), контекстна інформація про поточну сесію (IP-адреса, характеристики мережі, параметри браузера), поведінкова біометрія (швидкість набору тексту, особливості роботи з мишею, навігаційні паттерни) та алгоритми машинного навчання для виявлення аномалій у поведінці.

За результатами аналізу система може застосовувати різні стратегії реагування: від спрощеного процесу входу для довірених сценаріїв до посилених вимог автентифікації при виявленні підозрілої активності. Це дозволяє оптимізувати баланс між безпекою та зручністю використання, мінімізуючи навантаження на користувачів у звичайних умовах та підвищуючи рівень захисту при потенційних загрозах.

Федеративне управління ідентичністю

Федеративне управління ідентичністю (FIM) є архітектурним підходом, який дозволяє організаціям спільно використовувати ідентифікаційну інформацію та надавати доступ до ресурсів на основі довірчих відносин між різними доменами безпеки. Цей механізм особливо актуальний для великих корпоративних структур з множинними підрозділами, хмарних середовищ та міжорганізаційної співпраці.

Основними компонентами федеративної системи є постачальник ідентичності (Identity Provider, IdP), який виконує автентифікацію користувачів та надає інформацію про їх ідентичність, та постачальник сервісів (Service Provider, SP), який надає доступ до ресурсів на основі отриманих ідентифікаційних даних.

Взаємодія між цими компонентами здійснюється через стандартизовані протоколи, такі як SAML, OAuth або OpenID Connect.

Федеративний підхід забезпечує значні переваги для організацій, включаючи централізоване управління користувачами, спрощення процесів надання та відкликання доступу, зменшення адміністративного навантаження та підвищення безпеки через уніфіковані політики автентифікації. Користувачі отримують можливість єдиного входу до множини систем без необхідності запам'ятовувати різні набори облікових даних.

Single Sign-On (SSO) є технологією, яка дозволяє користувачам отримувати доступ до множини додатків та сервісів після однократної автентифікації. Цей підхід значно спрощує користувацький досвід, зменшує кількість паролів, які необхідно запам'ятовувати, та знижує ризики безпеки, пов'язані з використанням слабких або повторюваних паролів. Сучасні реалізації SSO можуть базуватися на різних технологічних підходах, включаючи веб-базовані рішення з використанням cookies та токенів сесії, корпоративні системи на основі Active Directory та Kerberos, хмарні платформи з підтримкою федеративних протоколів. Кожен з цих підходів має свої особливості впровадження та сфери оптимального застосування.

Ефективне впровадження SSO вимагає ретельного планування архітектури системи, врахування вимог інтеграції з наявними додатками, забезпечення належного рівня безпеки сесій та розробки процедур управління життєвим циклом доступу користувачів. Особливу увагу необхідно приділяти питанням відкликання доступу та управління сесіями при звільненні співробітників або зміні їх ролей в організації.

Для проведення об'єктивного порівняльного аналізу методів ідентифікації користувачів було визначено систему критеріїв оцінки, що охоплює ключові аспекти функціонування систем автентифікації. Кожен критерій оцінюється за п'ятибальною шкалою, де 1 бал відповідає найнижчому рівню, а 5 балів – найвищому.

Критерії оцінки:

Рівень безпеки – стійкість методу до різних типів атак, включаючи брутфорс, фішинг, перехоплення даних та соціальну інженерію.

Зручність використання – простота процедури автентифікації для кінцевого користувача, швидкість проходження ідентифікації.

Надійність – стабільність роботи системи, частота помилкових відмов та помилкових допусків.

Масштабованість – можливість ефективного функціонування при збільшенні кількості користувачів.

Вартість впровадження – загальні витрати на реалізацію, включаючи апаратне забезпечення, програмне забезпечення та навчання персоналу.

Вартість обслуговування – поточні експлуатаційні витрати, включаючи технічну підтримку та оновлення.

Швидкість автентифікації – час, необхідний для завершення процесу ідентифікації.

Стійкість до атак – специфічна оцінка захищеності від поширених типів кібератак.

Паролі та PIN-коди

Рівень безпеки: 2/5 Паролі демонструють низький рівень безпеки через схильність користувачів до створення простих комбінацій. Статистика показує, що понад 80% користувачів використовують паролі довжиною менше 8 символів, а 23% користувачів використовують один із 10 найпоширеніших паролів. Уразливості включають атаки підбору, словникові атаки, фішинг та витоки з баз даних.

Зручність використання: 5/5 Максимальна оцінка через простоту використання – користувач просто вводить знайому комбінацію символів. Не потребує додаткового обладнання або навчання.

Надійність: 3/5 Середня надійність через можливість забування паролів користувачами. Приблизно 78% користувачів забувають пароль щонайменше раз на місяць.

Масштабованість: 5/5 Відмінна масштабованість – система може обслуговувати мільйони користувачів без значного збільшення навантаження на інфраструктуру.

Вартість впровадження: 5/5 Мінімальні витрати на впровадження – потребує лише програмної реалізації логіки автентифікації.

Вартість обслуговування: 4/5 Низькі поточні витрати, основні витрати пов'язані з технічною підтримкою користувачів при відновленні паролів.

Швидкість автентифікації: 4/5 Висока швидкість – середній час введення пароля становить 3-5 секунд.

Стійкість до атак: 1/5 Найнижча оцінка через вразливість до широкого спектру атак: брутфорс, словникові атаки, фішинг, кейлогери, атаки на бази даних.

Біометрична ідентифікація (відбитки пальців)

Рівень безпеки: 4/5 Високий рівень безпеки завдяки унікальності біометричних характеристик. Ймовірність співпадіння відбитків пальців у двох людей становить приблизно 1 до 64 мільярдів.

Зручність використання: 5/5 Максимальна зручність – користувач просто торкається сенсора. Процес займає 1-2 секунди.

Надійність: 3/5 Середня надійність через можливі помилки розпізнавання при пошкодженнях шкіри, забрудненні сенсора або сухості пальців. FAR (False Accept Rate) становить 0.001-0.01%, FRR (False Reject Rate) – 1-3%.

Масштабованість: 4/5 Добра масштабованість, хоча потребує спеціалізованого обладнання для кожного робочого місця.

Вартість впровадження: 3/5 Середні витрати через необхідність закупівлі біометричних сенсорів (50-200$ за пристрій).

Вартість обслуговування: 3/5 Середні витрати на калібрування та очищення сенсорів, заміну пошкоджених пристроїв.

Швидкість автентифікації: 5/5 Дуже висока швидкість – процес займає 0.5-2 секунди.

Стійкість до атак: 3/5 Середня стійкість. Захищений від традиційних атак на паролі, але вразливий до атак з використанням підроблених відбитків та replay-атак.

Розпізнавання обличчя

Рівень безпеки: 3/5 Середній рівень безпеки. Сучасні системи 3D-розпізнавання (як Face ID) мають високу точність, але 2D-системи можуть бути обмануті фотографіями.

Зручність використання: 5/5 Максимальна зручність – безконтактний метод, користувач просто дивиться на камеру.

Надійність: 3/5 Середня надійність через залежність від освітлення, кута зйомки, змін зовнішності. Точність варіює від 95% до 99.9% залежно від технології.

Масштабованість: 4/5 Добра масштабованість, особливо при використанні існуючих камер безпеки.

Вартість впровадження: 3/5 Середні витрати – від 100$ за просту камеру до 1000$ за спеціалізовані 3D-сенсори.

Вартість обслуговування: 3/5 Середні витрати на оновлення алгоритмів та калібрування камер.

Швидкість автентифікації: 5/5 Дуже висока швидкість – процес займає 1-3 секунди.

Стійкість до атак: 2/5 Низька стійкість до атак з використанням фотографій, відео або масок (для простих систем).

Одноразові паролі (OTP)

Рівень безпеки: 4/5 Високий рівень безпеки завдяки обмеженому терміну дії кодів (зазвичай 30-60 секунд).

Зручність використання: 4/5 Висока зручність при використанні мобільних додатків, дещо менша при SMS-доставці через можливі затримки.

Надійність: 4/5 Висока надійність, основні проблеми пов'язані з синхронізацією часу між сервером та клієнтом.

Масштабованість: 5/5 Відмінна масштабованість – система може обслуговувати мільйони користувачів.

Вартість впровадження: 4/5 Низькі витрати при використанні програмних рішень, вищі при використанні апаратних токенів.

Вартість обслуговування: 4/5 Низькі поточні витрати, основні витрати пов'язані з SMS-доставкою (0.01-0.05$ за повідомлення).

Швидкість автентифікації: 3/5 Середня швидкість – користувач повинен отримати код та ввести його (15-30 секунд).

Стійкість до атак: 4/5 Висока стійкість до більшості атак, але вразливий до SIM-swapping та перехоплення SMS.

Апаратні токени

Рівень безпеки: 5/5 Найвищий рівень безпеки завдяки апаратному зберіганню криптографічних ключів та стійкості до програмних атак.

Зручність використання: 3/5 Середня зручність – користувач повинен мати токен при собі та вставити його в пристрій або торкнутися NFC-сенсора.

Надійність: 5/5 Дуже висока надійність – апаратні токени рідко виходять з ладу та мають тривалий термін служби (5-10 років).

Масштабованість: 3/5 Середня масштабованість через необхідність фізичного розповсюдження токенів серед користувачів.

Вартість впровадження: 2/5 Високі витрати – вартість якісних токенів становить 25-50$ за пристрій.

Вартість обслуговування: 4/5 Низькі поточні витрати після початкового впровадження.

Швидкість автентифікації: 4/5 Висока швидкість – процес займає 2-5 секунд.

Стійкість до атак: 5/5 Найвища стійкість до всіх типів віддалених атак, включаючи фішинг та man-in-the-middle.

Смарт-карти

Рівень безпеки: 4/5 Високий рівень безпеки завдяки апаратному зберіганню ключів та можливості комбінування з PIN-кодом.

Зручність використання: 2/5 Низька зручність через необхідність носити карту та використовувати зчитувач.

Надійність: 4/5 Висока надійність, але карти можуть пошкоджуватися при неакуратному поводженні.

Масштабованість: 3/5 Середня масштабованість через необхідність виготовлення та розповсюдження карт.

Вартість впровадження: 2/5 Високі витрати на карти (5-15$ за карту) та зчитувачі (50-200$ за пристрій).

Вартість обслуговування: 3/5 Середні витрати на заміну пошкоджених карт та обслуговування зчитувачів.

Швидкість автентифікації: 3/5 Середня швидкість – процес займає 5-10 секунд включно з введенням PIN-коду.

Стійкість до атак: 4/5 Висока стійкість до віддалених атак, але вразливі до фізичного доступу та side-channel атак.

Багатофакторна автентифікація

Рівень безпеки: 5/5 Найвищий рівень безпеки завдяки комбінуванню різних факторів автентифікації.

Зручність використання: 2/5 Найнижча зручність через необхідність проходження кількох етапів автентифікації.

Надійність: 4/5 Висока надійність, хоча залежить від надійності окремих компонентів.

Масштабованість: 3/5 Середня масштабованість через складність управління кількома факторами.

Вартість впровадження: 2/5 Високі витрати через необхідність впровадження кількох технологій одночасно.

Вартість обслуговування: 2/5 Високі поточні витрати на підтримку кількох систем автентифікації.

Швидкість автентифікації: 2/5 Найповільніша автентифікація через необхідність проходження кількох етапів.

Стійкість до атак: 5/5 Найвища стійкість до всіх типів атак завдяки багатошаровому захисту.

Загальний бал

Паролі/PIN – 29/40Відбитки пальців – 30/40

Розпізнавання обличчя – 28/40

Одноразові паролі – 32/40

Апаратні токени – 31/40

Смарт-карти – 25/40

MFA – 25/40

2.2. Аналіз результатів за сферами застосування

Після вивчення всіх методів автентифікації було визначено, які з них найкраще підходять для різних сфер. Кожна галузь має свої особливості - комусь важливіша безпека, комусь зручність, а комусь ціна. Далі показано, що рекомендується використовувати в кожній сфері.

- **Корпоративне середовище**

Рекомендовані методи:

1. Одноразові паролі (32/40) – оптимальний баланс безпеки та зручності
2. Апаратні токени (31/40) – для високочутливих систем
3. Відбитки пальців (30/40) – для фізичного доступу до приміщень

Обґрунтування: Корпоративне середовище вимагає високого рівня безпеки при збереженні продуктивності співробітників. Одноразові паролі забезпечують оптимальне співвідношення цих факторів.

- **Мобільні додатки**

Рекомендовані методи:

1. Відбитки пальців (30/40) – найкраща зручність для мобільних пристроїв
2. Розпізнавання обличчя (28/40) – для пристроїв з якісними камерами
3. Паролі/PIN (29/40) – як резервний метод

Обґрунтування: Мобільні користувачі пріоритизують зручність та швидкість, тому біометричні методи є оптимальними.

- **Банківські системи**

Рекомендовані методи:

1. MFA (25/40) – незважаючи на низьку зручність, забезпечує найвищу безпеку
2. Апаратні токени (31/40) – для VIP-клієнтів
3. Одноразові паролі (32/40) – для масових користувачів

Обґрунтування: Фінансові установи повинні пріоритизувати безпеку над зручністю через високі ризики фінансових втрат.

- **Державні служби**

Рекомендовані методи:

1. Апаратні токени (31/40) – для службовців з доступом до секретної інформації
2. MFA (25/40) – для критично важливих систем
3. Смарт-карти (25/40) – для масового використання громадянами

Обґрунтування: Державні системи потребують найвищого рівня безпеки та можуть інвестувати в дорогі рішення заради національної безпеки.

- **Інтернет-сервіси**

Рекомендовані методи**:**

1. Одноразові паролі (32/40) – як додатковий фактор безпеки
2. Паролі/PIN (29/40) – як основний метод
3. Відбитки пальців (30/40) – для мобільних додатків

Обґрунтування: Інтернет-сервіси повинні балансувати безпеку з масовою доступністю та простотою використання.

Проведений порівняльний аналіз методів ідентифікації та автентифікації демонструє складну картину сучасного стану інформаційної безпеки, де кожен підхід має свої унікальні переваги та обмеження, що вимагає ретельного підходу до вибору оптимального рішення для конкретних організаційних потреб. Одноразові паролі виявилися найбільш збалансованим рішенням, отримавши найвищу загальну оцінку в 32 бали з 40 можливих, що пояснюється їх здатністю забезпечувати високий рівень безпеки при відносно низьких витратах на

впровадження та підтримку, водночас зберігаючи прийнятний рівень зручності для кінцевих користувачів та демонструючи відмінну масштабованість навіть у великих корпоративних середовищах. Апаратні токени, незважаючи на свою репутацію найбезпечнішого методу автентифікації, показали обмежену практичність через високі витрати на закупівлю, розгортання та управління, особливо в організаціях з великою кількістю співробітників, а також через складності з логістикою розподілу та заміни пристроїв, що робить їх ідеальними переважно для критично важливих систем з обмеженою кількістю користувачів. Біометричні методи ідентифікації продемонстрували революційний потенціал у сфері користувацького досвіду, забезпечуючи майже миттєву автентифікацію без необхідності запам'ятовування паролів чи носіння додаткових пристроїв, однак їх впровадження стикається з серйозними викликами, включаючи проблеми надійності розпізнавання в різних умовах освітлення, вологості або при фізичних змінах користувача, а також з етичними та правовими питаннями збереження та обробки біометричних даних, які в багатьох юрисдикціях вважаються особливо чутливою інформацією. Багатофакторна автентифікація представляє собою найкомплексніший підхід до забезпечення безпеки, комбінуючи декілька незалежних факторів перевірки особи, що теоретично забезпечує найвищий рівень захисту, проте практичне впровадження таких систем часто стикається з опором користувачів через збільшення часу та складності процесу входу, що може негативно впливати на продуктивність роботи та загальне сприйняття системи. Традиційні текстові паролі, незважаючи на всі їх відомі недоліки та вразливості, залишаються фундаментальним елементом більшості систем безпеки, головним чином через їх простоту впровадження, відсутність додаткових апаратних вимог та універсальну сумісність з практично всіма існуючими системами, однак їх ефективність критично залежить від дотримання користувачами правил створення складних унікальних паролів та регулярної їх зміни, що в реальних умовах часто не виконується. Аналіз показує, що найперспективнішим напрямком розвитку є створення адаптивних систем автентифікації, які використовують штучний інтелект та машинне навчання для динамічної оцінки ризиків кожної конкретної

спроби доступу, враховуючи такі фактори як час та місце входу, використовуваний пристрій, поведінкові патерни користувача та поточний рівень загроз, щоб автоматично визначати необхідний рівень автентифікації - від простого введення пароля для рутинних операцій до багатофакторної перевірки для критичних дій. Економічні аспекти впровадження різних методів автентифікації також відіграють вирішальну роль у прийнятті рішень, оскільки організації повинні збалансувати витрати на безпеку з реальними ризиками та потенційними збитками від порушень, при цьому важливо враховувати не лише прямі витрати на технології, але й непрямі витрати на навчання персоналу, технічну підтримку, можливі простої системи та вплив на продуктивність співробітників. Технологічні тренди свідчать про поступовий перехід до безпарольних методів автентифікації, таких як WebAuthn, FIDO2 та інші стандарти, які обіцяють поєднати високий рівень безпеки з покращеним користувацьким досвідом, однак їх масове впровадження все ще стримується проблемами сумісності з застарілими системами та необхідністю значних інвестицій в оновлення інфраструктури. Регуляторні вимоги в різних індустріях також суттєво впливають на вибір методів автентифікації, особливо в фінансовому секторі, охороні здоров'я та державних установах, де існують жорсткі стандарти та вимоги до підтвердження особи, що часто вимагає впровадження специфічних технологій або їх комбінацій незалежно від їх зручності чи вартості. Психологічні аспекти сприйняття безпеки користувачами також відіграють важливу роль, оскільки навіть найдосконаліші системи можуть виявитися неефективними, якщо користувачі знаходять способи їх обходу або відмовляються їх використовувати через складність або незрозумілість, що підкреслює важливість врахування людського фактора на всіх етапах планування та впровадження систем автентифікації..

3 АНАЛІЗ ЕФЕКТИВНОСТІ ПРАКТИЧНИХ СИСТЕМИ ТА ЇХ ПОРІВНЯННЯ

3.1 Характеристика Google Authenticator

Google Authenticator є однією з найпоширеніших мобільних програм для генерації одноразових паролів , що використовується як другий фактор автентифікації в системах багатофакторної ідентифікації користувачів. Додаток був розроблений компанією Google у 2010 році і став стандартом де-факто для реалізації двофакторної автентифікації в корпоративному середовищі та для індивідуальних користувачів.

Основне призначення Google Authenticator полягає у створенні додаткового рівня безпеки для процесу автентифікації користувачів. Якщо традиційна автентифікація базується на принципі "щось, що ви знаєте" (пароль), то Google Authenticator реалізує принцип "щось, що ви маєте" (мобільний пристрій з генератором кодів). Це значно підвищує загальний рівень безпеки системи, оскільки потенційний зловмисник повинен отримати доступ не лише до пароля користувача, але й до його мобільного пристрою. Google Authenticator базується на стандарті RFC 6238, який описує алгоритм TOTP (Time-based One-Time Password). Цей алгоритм є розширенням більш раннього стандарту HOTP (HMAC-based One-Time Password, RFC 4226) і використовує поточний час як рухомий фактор для генерації одноразових паролів.

Процес початкового налаштування Google Authenticator включає генерацію та обмін секретним ключем між сервером автентифікації та мобільним додатком. Цей процес зазвичай відбувається через QR-код, який містить закодовану інформацію у форматі URI:

otpauth://totp/Example:alice@google.com?secret=JBSWY3DPEHPK3PXP&issuer=Example

Рис. 3.1 Приклад QR-коду

Структура URI включає:

- Тип OTP
- Мітку облікового запису
- Секретний ключ в Base32 кодуванні
- Ім'я емітента для ідентифікації сервісу

Безпека Google Authenticator базується на кількох криптографічних принципах:

Секретний ключ: Зазвичай має довжину 80 біт (16 символів в Base32) або 160 біт (32 символи), що забезпечує достатній рівень ентропії для протидії атакам методом повного перебору. Ключ генерується за допомогою криптографічно стійкого генератора псевдовипадкових чисел.

Хеш-функція HMAC-SHA1: Використовується для перетворення секретного ключа та часової мітки в одноразовий пароль. HMAC забезпечує як цілісність, так і автентичність генерованого коду, а SHA-1, незважаючи на теоретичні вразливості, залишається достатньо безпечним для цього конкретного застосування завдяки обмеженому часу життя кодів.

Часова синхронізація: Критично важливим аспектом є точна синхронізація часу між клієнтом та сервером. Допустиме відхилення зазвичай складає ±1-2 часових вікна (30-60 секунд), що забезпечує баланс між безпекою та зручністю використання.

Переваги використання в корпоративному середовищі

Впровадження Google Authenticator значно підвищує загальний рівень безпеки корпоративної системи автентифікації. Статистичні дані показують, що двофакторна автентифікація з використанням TOTP може заблокувати до 99.9% автоматизованих атак на облікові записи користувачів. Це особливо актуально в контексті зростаючої кількості фішингових атак та компрометації паролів.

Багатофакторна автентифікація з Google Authenticator захищає від найпоширеніших типів атак:

- Атаки методом повного перебору паролів
- Фішингові атаки (частково, оскільки код діє обмежений час)
- Використання скомпрометованих паролів з витоків даних
- Атаки типу "людина посередині" (при правильній реалізації)

Google Authenticator відрізняється відносною простотою впровадження в існуючу IT-інфраструктуру організації. Більшість сучасних систем управління ідентичністю та доступом (IAM) мають вбудовану підтримку TOTP або можуть бути легко інтегровані з відповідними бібліотеками.Для кінцевих користувачів процес налаштування також є інтуїтивно зрозумілим: сканування QR-коду та введення згенерованого 6-значного коду. Це мінімізує потребу в технічній підтримці та навчанні персоналу. Використання Google Authenticator не вимагає додаткових витрат на апаратне забезпечення, на відміну від фізичних токенів або смарт-карт. Єдині витрати пов'язані з розробкою або налаштуванням серверної частини та можливим навчанням користувачів.

Недоліки та обмеження

Основним недоліком Google Authenticator є повна залежність від мобільного пристрою користувача. Втрата, пошкодження або розрядка телефону може призвести до блокування доступу користувача до корпоративних систем. Це створює додаткові вимоги до планування аварійного відновлення доступу. Google Authenticator традиційно не підтримував синхронізацію ключів між пристроями, що створювало проблеми при заміні телефону або його втраті. Хоча останні версії додатка частково вирішили цю проблему через Google-аккаунт, багато організацій все ще стикаються з необхідністю ручного відновлення доступу. Незважаючи на підвищену безпеку, TOTP коди все ще можуть бути скомпрометовані через атаки фішингу в реальному часі, коли зловмисник миттєво використовує отриманий від жертви код для автентифікації в справжній системі. Неточний час на мобільному пристрої може призвести до генерації неправильних кодів. Хоча більшість сучасних смартфонів автоматично синхронізують час, проблеми все ще можуть виникати в середовищах з обмеженим доступом до Інтернету або при використанні старих пристроїв.

3.2 Характеристика YubiKey

YubiKey представляє собою лінійку апаратних токенів безпеки, розроблених шведською компанією Yubico, що заснована у 2007 році. Ці пристрої є фізичними ключами автентифікації, які забезпечують найвищий рівень захисту для систем ідентифікації користувачів у корпоративному середовищі. На відміну від програмних рішень, YubiKey реалізує апаратний рівень безпеки, що робить його практично неможливим для копіювання або емуляції зловмисниками. Основна філософія YubiKey полягає у створенні "щось, що ви маєте" - фізичного фактора автентифікації, який не залежить від програмного забезпечення на пристрої користувача. Це усуває цілий клас вразливостей, пов'язаних із шкідливим програмним забезпеченням, фішинговими атаками та компрометацією мобільних пристроїв. YubiKey підтримує множину протоколів автентифікації, включаючи

FIDO U2F, FIDO2/WebAuthn, OTP, PIV, OpenPGP та інші, що робить його універсальним рішенням для різноманітних корпоративних потреб.

Компанія Yubico позиціонує свої продукти як рішення для організацій, що потребують найвищого рівня безпеки, включаючи урядові установи, фінансові інституції, технологічні компанії та інші підприємства з критично важливими даними. Статистика показує, що використання YubiKey може знизити ризик успішних фішингових атак на 99%, що робить його одним з найефективніших засобів захисту облікових записів користувачів.

Рис.3.2 – YubiKey фізичний токен

YubiKey побудований на основі спеціалізованого мікроконтролера з вбудованими криптографічними модулями. Основні апаратні компоненти включають:

- Безпечний елемент (Secure Element): Спеціалізований чіп, призначений для безпечного зберігання криптографічних ключів та виконання криптографічних операцій. Цей компонент сертифікований відповідно до стандартів Common Criteria та FIPS 140-2, що забезпечує високий рівень захисту від фізичних атак та зворотного інжинірингу.
- Криптографічний процесор: Виконує всі криптографічні операції, включаючи генерацію ключів, цифрові підписи, хешування та шифрування.

Підтримує сучасні алгоритми, такі як RSA-2048/4096, ECDSA P-256/P-384, Ed25519 та інші.

- Інтерфейс підключення: В залежності від моделі, YubiKey може мати USB-A, USB-C, Lightning або NFC інтерфейси для підключення до різних типів пристроїв. Деякі моделі поєднують кілька інтерфейсів в одному пристрої.
- Сенсорна кнопка: Фізична кнопка, яка слугує як додатковий фактор підтвердження намірів користувача. Натискання кнопки необхідне для активації більшості криптографічних операцій, що запобігає несанкціонованому використанню токена.

Технологічна перевага YubiKey полягає в підтримці широкого спектру стандартів автентифікації та криптографічних протоколів, що забезпечує універсальність та сумісність з різноманітними системами.

FIDO U2F (Universal 2nd Factor) представляє собою відкритий стандарт для двофакторної автентифікації, розроблений альянсом FIDO. Цей протокол використовує криптографію на основі еліптичних кривих для створення унікальних ключових пар для кожного окремого сервісу. Процес автентифікації включає криптографічний механізм челлендж-респонс, що робить абсолютно неможливими фішингові атаки, оскільки кожна відповідь є унікальною та прив'язаною до конкретного домену.

FIDO2/WebAuthn являє собою найновіший стандарт для безпарольної автентифікації, що дозволяє користувачам повністю відмовитися від традиційних паролів при автентифікації в веб-сервісах. WebAuthn використовує асиметричну криптографію, де приватний ключ ніколи не покидає межі YubiKey, а відповідний публічний ключ реєструється на сервері сервісу. Цей підхід забезпечує найвищий рівень безпеки та зручності використання.

Yubico OTP є власним протоколом компанії Yubico, що генерує 44-символьні одноразові паролі з високим рівнем криптографічного захисту. Кожен згенерований OTP містить унікальний ідентифікатор токена, лічильник використання, мітку часу для попередження атак повтору та код автентифікації повідомлення (MAC) для забезпечення цілісності даних.

Підтримка стандартних алгоритмів OATH-HOTP та OATH-TOTP забезпечує сумісність з популярними додатками, такими як Google Authenticator та іншими генераторами одноразових паролів. Це дозволяє використовувати YubiKey як апаратну заміну програмних генераторів кодів, забезпечуючи значно вищий рівень безпеки.

PIV (Personal Identity Verification) є стандартом, розробленим Національним інститутом стандартів і технологій США (NIST) для урядових і корпоративних систем ідентифікації. PIV дозволяє зберігати на YubiKey цифрові сертифікати X.509 для автентифікації, цифрового підпису та шифрування документів і комунікацій.

Підтримка стандарту OpenPGP надає можливість зберігання PGP ключів та виконання операцій шифрування, розшифрування та цифрового підпису електронної пошти та файлів безпосередньо на апаратному рівні.

Переваги використання

Максимальний рівень безпеки YubiKey досягається завдяки апаратній природі пристрою, що робить його практично неуразливим для більшості сучасних атак. Імунітет до фішингу забезпечується протокольною прив'язкою до конкретних доменів, захист від шкідливого програмного забезпечення досягається виконанням всіх операцій всередині токена, а стійкість до атак SIM-swapping обумовлена незалежністю від телефонних мереж.

Простота використання поєднується з високою безпекою: більшість операційних систем та браузерів підтримують YubiKey без встановлення додаткового програмного забезпечення, один токен може використовуватися для автентифікації в десятках сервісів, а швидкість автентифікації часто перевищує традиційні методи.Економічна ефективність для організацій проявляється через зниження витрат на технічну підтримку, зменшення ризиків витоків даних, підвищення продуктивності співробітників та тривалий термін служби пристроїв.

Недоліки та обмеження

Серед обмежень слід відзначити вартість впровадження, особливо для великих організацій, необхідність забезпечення резервних токенів та можливі

витрати на модернізацію інфраструктури. Ризики фізичної втрати або пошкодження потребують розробки процедур відновлення доступу, а технічні обмеження включають питання сумісності з деякими системами та складність корпоративного управління.

3.3 Характеристика SMS-кодів автентифікації

SMS-коди автентифікації представляють собою метод двофакторної автентифікації, який використовує короткі текстові повідомлення з одноразовими паролями (OTP), що надсилаються на мобільний телефон користувача. Цей підхід був впроваджений як простий та доступний спосіб підвищення безпеки облікових записів користувачів у порівнянні з традиційною автентифікацією лише за паролем. SMS-автентифікація базується на принципі "щось, що ви знаєте" (пароль) та "щось, що ви маєте" (мобільний телефон), створюючи додатковий рівень захисту від несанкціонованого доступу.

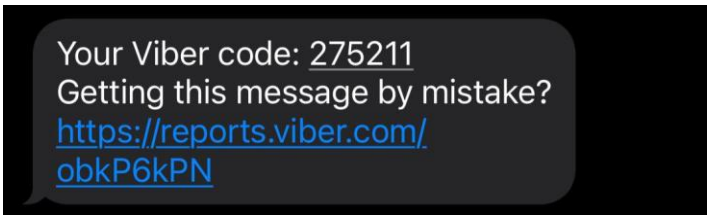

Рис. 3.3 Приклад SMS-коду

Основна філософія SMS-автентифікації полягає у використанні широко розповсюдженої мобільної інфраструктури для доставки тимчасових кодів безпеки. На відміну від спеціалізованих апаратних рішень, SMS-коди не потребують додаткових пристроїв або програмного забезпечення, оскільки практично всі мобільні телефони підтримують прийом текстових повідомлень. SMS одноразові паролі є найпоширенішим методом багатофакторної автентифікації, який використовують 86% компаній, що свідчить про його широке впровадження у корпоративному середовищі.

Статистичні дані показують, що SMS OTP досі залишається найширше використовуваним методом двофакторної автентифікації, яким користується приблизно одна третина мобільних користувачів. Проте, незважаючи на популярність, експерти з кібербезпеки все частіше піддають сумніву надійність цього методу через численні вразливості та успішні атаки.

Технічна реалізація SMS-автентифікації

MS-автентифікація базується на інфраструктурі стільникових мереж та протоколах передачі коротких повідомлень. Основні технічні компоненти включають:

- Система генерації OTP: Серверна частина, що відповідає за створення унікальних одноразових паролів. Зазвичай використовуються алгоритми HOTP (HMAC-based One-Time Password) або TOTP (Time-based One-Time Password), які генерують числові коди довжиною 4-8 цифр з обмеженим терміном дії (зазвичай 5-10 хвилин).
- SMS-шлюз: Інтерфейс між серверами автентифікації та мобільними операторами, який забезпечує доставку повідомлень через мережі стільникового зв'язку. Шлюз може бути власним або наданим третьою стороною, що впливає на швидкість доставки та надійність сервісу.
- Мобільна мережева інфраструктура: Включає базові станції, центри комутації повідомлень (SMSC) та протоколи сигналізації SS7 (Signaling System 7), які забезпечують маршрутизацію та доставку SMS-повідомлень до кінцевого пристрою користувача.
- Клієнтський пристрій: Мобільний телефон або смартфон користувача, який отримує SMS-повідомлення та відображає код автентифікації. Не потребує спеціального програмного забезпечення, оскільки використовує стандартний функціонал обробки текстових повідомлень.

Процес автентифікації включає наступні етапи: генерацію унікального коду на сервері, відправлення коду через SMS-шлюз, доставку через мобільну мережу, отримання користувачем та введення коду в систему для підтвердження автентифікації.

SMS-автентифікація використовує декілька стандартизованих алгоритмів для генерації одноразових паролів:

HOTP (HMAC-based One-Time Password) визначений у RFC 4226 та базується на лічильнику використання. Кожен новий код генерується на основі секретного ключа та інкрементального лічильника, що забезпечує унікальність кожного пароля.

TOTP (Time-based One-Time Password) описаний у RFC 6238 та використовує поточний час як основу для генерації коду. Цей підхід забезпечує автоматичне оновлення паролів через певні інтервали часу без необхідності синхронізації лічильників.

SMS-протокол доставки базується на стандартах GSM та включає протоколи MAP (Mobile Application Part) для маршрутизації повідомлень та SS7 для сигналізації між елементами мережі.

Переваги використання

Простота впровадження є основною перевагою SMS-автентифікації: більшість користувачів вже мають мобільні телефони, не потребується встановлення додаткових додатків або апаратного забезпечення, інтеграція з існуючими системами відносно проста та не вимагає значних технічних змін.Широка сумісність забезпечується підтримкою всіма типами мобільних пристроїв, від базових телефонів до смартфонів, незалежністю від операційної системи та доступністю практично у всіх географічних регіонах з мобільним покриттям.Економічна ефективність проявляється через низьку вартість впровадження для організацій, відсутність необхідності у спеціалізованому обладнанні, мінімальні витрати на технічну підтримку та швидкий процес розгортання в корпоративному середовищі.

Недоліки та вразливості

- SMS MFA вважається небезпечним через вразливості, такі як SIM-свопінг, експлойти SS7 та фішингові атаки, які можуть перехопити коди підтвердження. Основні ризики безпеки включають:

- **SIM-свопінг атаки**: Зловмисники можуть переконати мобільного оператора перенести номер телефону жертви на SIM-карту, яка знаходиться під їх контролем, що дозволяє перехоплювати всі SMS-повідомлення.
- **Вразливості протоколу SS7**: Потенційні ризики та вразливості в SMS-безпеці включають перехоплення SMS під час передачі, SIM-свопінг, смішинг, автоматизоване SMS-шахрайство, соціальну інженерію, спуфінг ID відправника, розповсюдження шкідливого ПЗ, відсутність шифрування та вразливості операторів.
- **Фішинг та соціальна інженерія**: Серйозною слабкістю SMS OTP є його сприйнятливість до фішингових атак та тактик соціальної інженерії, що дозволяє зловмисникам обманом змусити користувачів надати свої коди автентифікації.
- **Відсутність шифрування**: SMS-повідомлення не зашифровані за замовчуванням, що робить їх сприйнятливими до перехоплення хакерами через експлуатацію вразливостей у мобільних мережах або використання складних техніک зламу.
- **Залежність від мобільної мережі**: Затримки у доставці повідомлень, відсутність мобільного покриття та технічні збої операторів можуть унеможливити доступ користувачів до своїх облікових записів.

Технічні обмеження включають обмежену довжину SMS-повідомлень, можливі затримки у доставці, залежність від якості мобільного зв'язку та складності забезпечення надійної доставки в роумінгу.

Використання SMS-автентифікації більше не є достатнім для захисту від спроб захоплення облікових записів. У зв'язку з цим організації все частіше переходять на більш безпечні альтернативи, такі як апаратні токени безпеки, біометричну автентифікацію та безпарольні рішення. Незважаючи на визнані вразливості, SMS-коди залишаються важливим перехідним рішенням для організацій, які поступово модернізують свою інфраструктуру безпеки, особливо в регіонах з обмеженим доступом до передових технологій автентифікації.

3.4 Характеристика адаптивної автентифікації

Адаптивна автентифікація представляє собою інтелектуальну систему управління доступом, яка динамічно адаптує процес автентифікації на основі аналізу ризиків та контекстуальної інформації про спробу входу користувача. Розроблена для корпоративного середовища, ця технологія базується на принципах штучного інтелекту та машинного навчання для забезпечення оптимального балансу між безпекою та зручністю користування. На відміну від традиційних статичних методів автентифікації, адаптивна система постійно аналізує множину факторів ризику та приймає рішення про необхідність додаткових кроків перевірки в режимі реального часу.Основна філософія адаптивної автентифікації полягає у створенні "розумної" системи безпеки, яка інтелектуально ідентифікує шкідливі спроби на основі визначених факторів ризику та пропонує користувачам завершити додатковий крок для підтвердження своєї особи. Система будує профіль кожного користувача, який містить інформацію про зареєстровані пристрої, ролі користувачів, географічне розташування та інші характеристики поведінки. Коли користувачі намагаються увійти в систему, їм присвоюється оцінка ризику.

Ринок адаптивної автентифікації демонструє значне зростання: прогнозується оцінка ринку в $2,98 мільярда до 2030 року, зростання з CAGR 15,52% з 2025 по 2030 рік. Це свідчить про зростаючий попит на інтелектуальні рішення безпеки в корпоративному секторі та визнання адаптивної автентифікації як ключової технології майбутнього.

- Адаптивна автентифікація базується на складній технічній архітектурі, що поєднує декілька ключових компонентів:

- Система збору контекстуальних даних: Модуль, який відповідає за збирання та аналіз різноманітної інформації про спробу автентифікації. Включає геолокацію користувача, характеристики пристрою (IP-адреса, тип браузера, операційна система, відбиток пристрою), часові патерни доступу, мережеві параметри та поведінкові метрики користувача.

- Двигун аналізу ризиків (Risk Engine): Оцінює різні фактори ризику, пов'язані зі спробою входу користувача, щоб визначити рівень автентифікації, який потрібен. Ці фактори можуть включати інформацію про пристрій, місцезнаходження, патерни поведінки тощо. Двигун використовує алгоритми машинного навчання для створення динамічних моделей ризику та присвоєння числових оцінок кожній спробі автентифікації.
- Модуль машинного навчання та ШІ: Адаптивна MFA, що працює на ШІ, використовує контекстуальні дані для обчислення ризику, пов'язаного зі спробою входу користувача, дозволяючи системі динамічно обирати найбільш відповідний метод автентифікації. Система постійно навчається на історичних даних та адаптується до нових загроз і патернів поведінки користувачів.
- Політики безпеки та правила: Рішення адаптивної автентифікації присвоюють оцінку ризику на основі поведінки та контексту, і вони реагують на сприйнятий ризик на основі правил, встановлених IT-відділом. Ці правила можуть відрізнятися за оцінкою ризику, роллю користувача, місцезнаходженням, пристроєм тощо.
- Інтерфейс управління та моніторингу: Централізована консоль для налаштування політик безпеки, моніторингу автентифікаційних подій, аналізу звітів про безпеку та управління користувачами. Забезпечує реальний час відстеження спроб автентифікації та аномальної активності.

Адаптивна автентифікація покладається на оцінку ризику в системі та застосування критеріїв до цього ризику для визначення результатів автентифікації. У надзвичайно спрощених схемах автентифікації система може призначати різним запитам доступу профілі високого, середнього або низького ризику.

- Низький ризик: Автентифікація з використанням стандартних облікових даних (логін/пароль). Застосовується для знайомих пристроїв, звичних місць доступу та нормальних патернів поведінки користувача.
- Середній ризик: Додаткова перевірка через SMS, електронну пошту або push-сповіщення. Активується при незначних відхиленнях від нормальної поведінки або доступі з нових пристроїв.

- Високий ризик: Багатофакторна автентифікація з використанням біометричних даних, апаратних токенів або додаткових кроків верифікації. Застосовується при виявленні підозрілої активності, доступі з невідомих локацій або аномальних патернах поведінки.
- Критичний ризик: Блокування доступу та ескалація до служби безпеки. Відбувається при виявленні явних ознак зловмисної активності або спроб компрометації акаунта.

Переваги використання в корпоративному середовищі

Балансування безпеки та зручності є ключовою перевагою адаптивної автентифікації: Бізнеси використовують адаптивну автентифікацію для балансування вимог безпеки з користувацьким досвідом. Система автоматично підлаштовується під контекст користування, мінімізуючи кількість додаткових кроків для довірених користувачів та посилюючи захист при підозрілій активності.Проактивний захист забезпечується через постійний моніторинг та аналіз загроз у реальному часі, автоматичне виявлення аномалій до їх ескалації, адаптацію до нових типів атак через машинне навчання та зменшення кількості успішних атак через інтелектуальне блокування підозрілих спроб.Операційна ефективність проявляється через зменшення навантаження на службу технічної підтримки завдяки автоматизації процесів автентифікації, покращення продуктивності користувачів через зменшення перешкод для легітимного доступу, централізоване управління політиками безпеки та детальну звітність для аудиту та комплаєнсу.Масштабованість та гнучкість забезпечується через підтримку великих корпоративних середовищ з тисячами користувачів, інтеграцію з існуючими системами ідентифікації (Active Directory, LDAP, SAML), настроювані політики для різних ролей та підрозділів організації.

Недоліки впровадження

Складність конфігурації та управління є основним викликом для організацій: налаштування ефективних політик ризику потребує глибокого розуміння бізнес-процесів та загроз безпеки, необхідність постійного моніторингу та коригування алгоритмів машинного навчання, потреба в кваліфікованих фахівцях з

кібербезпеки для управління системою.Технічні обмеження включають залежність від якості та повноти даних для навчання алгоритмів, можливі помилкові спрацьювання (false positives), що можуть заблокувати легітимних користувачів, затримки в прийнятті рішень при складних обчисленнях ризику та необхідність інтеграції з різноманітними корпоративними системами.Фінансові витрати охоплюють високу початкову вартість впровадження та ліцензування рішень enterprise-класу, необхідність в додатковій апаратній інфраструктурі для обробки великих обсягів даних, витрати на навчання персоналу та постійну технічну підтримку, а також потенційні втрати продуктивності під час періоду адаптації співробітників.

Адаптивної автентифікація побудована для майбутнього та дозволяє новим та захоплюючим факторам, таким як IoT, стати частиною будь-якої валідації транзакцій. Розвиток включає інтеграцію з технологіями Інтернету речей, покращення алгоритмів штучного інтелекту для більш точного виявлення загроз, розширення біометричних методів автентифікації та адаптацію до нових типів кіберзагроз.Тенденції розвитку також включають більшу автоматизацію процесів управління ризиками, покращення інтеграції з хмарними платформами, розвиток стандартів взаємодії між різними системами безпеки та зростаючу увагу до збереження приватності користувачів при аналізі поведінкових даних.

3.5. Розробка рекомендацій щодо застосування-системи ідентифікації користувачів до ресурсів приватної організації

При виборі оптимального рішення для захисту корпоративних систем необхідно враховувати специфіку організації, рівень критичності даних та технічні можливості впровадження. Кожен метод автентифікації має свої переваги та обмеження, тому важливо знайти баланс між безпекою, зручністю користування та економічною доцільністю. Статистика показує, що багатофакторна автентифікація здатна заблокувати понад 99% автоматизованих атак на користувацькі акаунти, що робить її необхідною складовою корпоративної безпеки.

Малі та середні підприємства

Для компаній з обмеженим бюджетом та невеликою кількістю співробітників найбільш прийнятним варіантом буде поступове впровадження багатофакторної автентифікації, починаючи з найкритичніших систем.

Google Authenticator стане оптимальним стартовим рішенням завдяки своїй простоті впровадження та відсутності додаткових витрат на обладнання. Процес налаштування інтуїтивно зрозумілий навіть для користувачів без глибоких технічних знань - достатньо відсканувати QR-код та ввести згенерований код. Це мінімізує потребу в технічній підтримці та навчанні персоналу. Однак варто врахувати ризики, пов'язані з втратою мобільних пристроїв співробітників. Необхідно розробити процедури відновлення доступу та регулярно створювати резервні копії налаштувань автентифікації. Керівництву слід також забезпечити навчання співробітників основам кібербезпеки для запобігання фішинговим атакам.

Фінансові установи та критично важливі об'єкти

Організації, які працюють з конфіденційною фінансовою інформацією або критично важливими даними, потребують найвищого рівня захисту. Для таких установ рекомендується впровадження YubiKey як основного засобу автентифікації.

Апаратні токени забезпечують практично абсолютний захист від фішингових атак завдяки криптографічній прив'язці до конкретних доменів. Підтримка сучасних стандартів FIDO2/WebAuthn дозволяє повністю відмовитися від паролів для більшості корпоративних сервісів, що суттєво підвищує загальний рівень безпеки.Впровадження потребує ретельного планування, включаючи забезпечення резервних токенів для кожного співробітника та розробку процедур управління життєвим циклом пристроїв. Варто також врахувати витрати на навчання персоналу та можливу необхідність модернізації деяких корпоративних систем для повної сумісності.

Великі корпорації з розгалуженою структурою

Підприємства з тисячами співробітників та складною організаційною структурою отримають найбільшу користь від адаптивної автентифікації. Ця технологія дозволяє створити гнучку систему безпеки, яка автоматично адаптується до потреб різних категорій користувачів.Система аналізує множину факторів ризику - від геолокації та характеристик пристрою до патернів поведінки користувача - і динамічно визначає необхідний рівень автентифікації. Це означає, що співробітники, які працюють з офісу на корпоративних пристроях, можуть проходити спрощену автентифікацію, тоді як віддалені працівники або ті, хто намагається отримати доступ з незвичних локацій, стикатимуться з додатковими перевірками.

Впровадження адаптивної автентифікації потребує значних інвестицій та кваліфікованого персоналу для налаштування та підтримки системи. Однак довгострокові переваги включають суттєве покращення користувацького досвіду, зменшення навантаження на службу технічної підтримки та проактивний захист від нових типів загроз.

Категоричні застереження щодо SMS-автентифікації

Попри широке розповсюдження SMS-кодів як методу двофакторної автентифікації, їхнє використання в корпоративному середовищі стає все більш ризикованим. Сучасні зловмисники активно експлуатують вразливості мобільних мереж та використовують техніки SIM-свопінгу для перехоплення кодів підтвердження. Особливо небезпечними є атаки через вразливості протоколу SS7, які дозволяють перехоплювати SMS-повідомлення на рівні телекомунікаційної інфраструктури. Відсутність шифрування в SMS-протоколі робить цей метод автентифікації неприйнятним для організацій з високими вимогами до безпеки.

Якщо організація все ще використовує SMS-автентифікацію, її слід розглядати виключно як тимчасове рішення з чітким планом переходу на більш безпечні альтернативи. Для критично важливих систем SMS-коди мають бути заборонені на рівні корпоративної політики безпеки.

Успішне впровадження багатофакторної автентифікації потребує системного підходу та поетапної реалізації. Починати варто з аудиту існуючих систем та класифікації даних за рівнем критичності.

На першому етапі рекомендується впровадити багатофакторну автентифікацію для найбільш критичних систем - фінансових додатків, систем управління персоналом та баз даних з конфіденційною інформацією. Це дозволить отримати досвід роботи з новими технологіями та виявити потенційні проблеми на обмеженій кількості систем.

Другий етап включає розширення багатофакторної автентифікації на всі корпоративні додатки та сервіси. Важливо враховувати специфіку різних підрозділів та забезпечити гнучкість політик безпеки для різних категорій користувачів.

Заключний етап передбачає впровадження єдиної системи управління ідентичністю (Single Sign-On) з інтегрованою багатофакторною автентифікацією. Це дозволить забезпечити централізоване управління доступом та покращити користувацький досвід.

Вибір оптимального методу багатофакторної автентифікації залежить від специфічних потреб організації, але загальні принципи залишаються незмінними. Безпека повинна бути багатошаровою, а рішення - масштабованими та адаптованими до майбутніх викликів.Для більшості організацій рекомендується гібридний підхід, який поєднує різні методи автентифікації залежно від контексту та рівня ризику. Це може включати використання програмних генераторів кодів для повсякденних операцій, апаратних токенів для критично важливих систем та адаптивних алгоритмів для автоматичного управління рівнем безпеки. Ключовим фактором успіху є не лише технічна реалізація, але й організаційна підтримка ініціатив з кібербезпеки. Без належного навчання персоналу, адекватного фінансування та підтримки керівництва навіть найдосконаліші технічні рішення не зможуть забезпечити належний рівень захисту корпоративних активів. Вибір оптимального методу багатофакторної автентифікації залежить від специфічних потреб організації, але загальні принципи залишаються незмінними. Безпека

повинна бути багатошаровою, а рішення - масштабованими та адаптованими до майбутніх викликів. Для більшості організацій рекомендується гібридний підхід, який поєднує різні методи автентифікації залежно від контексту та рівня ризику. Це може включати використання програмних генераторів кодів для повсякденних операцій, апаратних токенів для критично важливих систем та адаптивних алгоритмів для автоматичного управління рівнем безпеки.

ВИСНОВКИ

У роботі проведено комплексне дослідження систем ідентифікації користувачів, визначено їх теоретичні основи та практичне застосування. Сьогодні питання безпечної ідентифікації та автентифікації користувачів набуває критичного значення в умовах зростаючих кіберзагроз та необхідності захисту конфіденційної інформації.

Проведено аналіз теоретичних основ систем ідентифікації користувачів. Визначено ключові поняття ідентифікації та автентифікації, класифіковано типи ідентифікаційних систем за різними критеріями. Встановлено, що сучасні стандарти та нормативні вимоги до ідентифікації користувачів постійно еволюціонують відповідно до нових викликів інформаційної безпеки.Здійснено дослідження та класифікацію існуючих методів ідентифікації користувачів. Проведено порівняльний аналіз методів ідентифікації за критеріями надійності, зручності використання та економічної ефективності. Аналіз результатів за сферами застосування показав, що вибір конкретного методу ідентифікації залежить від специфіки організації та рівня необхідної безпеки.

Виконано детальний аналіз ефективності практичних систем ідентифікації та їх порівняння. Досліджено характеристики провідних систем: Google Authenticator як представника багатофакторної автентифікації, YubiKey як апаратного токена безпеки, SMS-кодів як методу автентифікації та адаптивної автентифікації як інноваційного підходу. Кожна з цих систем має свої переваги та обмеження, що необхідно враховувати при виборі оптимального рішення.

Результати дослідження показали, що Google Authenticator забезпечує високий рівень безпеки завдяки генерації одноразових кодів, YubiKey відзначається максимальною стійкістю до фішингових атак, SMS-коди залишаються найбільш доступним методом, а адаптивна автентифікація пропонує оптимальний баланс між безпекою та зручністю використання.

Досліджено розробку рекомендацій для різних типів організацій - від малих

підприємств до великих корпорацій з розгалуженою структурою. Розроблено диференційовані рекомендації, що враховують специфічні потреби фінансових установ, критично важливих об'єктів та організацій з різним рівнем IT-зрілості. Створено комплексну поетапну стратегію впровадження багатофакторної автентифікації, яка включає початковий аудит систем, класифікацію даних за критичністю, поступове розширення захисту та інтеграцію з існуючою IT-інфраструктурою.

Таким чином, правильна реалізація систем ідентифікації користувачів є критично важливою для забезпечення комплексної безпеки інформаційних систем організації та захисту від сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Haber M. Why Identity Security Should Be the Basis of Modern Cybersecurity. URL: https://www.tandfonline.com/doi/full/10.1080/00332828.2023.2270510#d1e113 (дата звернення: 11.03.2025)

2. Sule M.-J. Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. URL:https://www.sciencedirect.com/science/article/abs/pii/S0160791X21002098 (дата звернення: 11.03.2025).

3. NIST Special Publication 800-63B URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата звернення: 12.04.2025).

4. Стандарт NIST SP 800-63-3 URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf (дата звернення: 12.03.2025).

5. FIPS 140-2 Federal Information Processing Standard Publication 140-2, Security Requirements for Cryptographic Modules, May 25, 2001 (with Change Notices through December 3, 2002) URL: https://doi.org/10.6028/NIST.FIPS.140-2 (дата звернення: 12.03.2025).

6. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.», URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (дата звернення 14.03.2025.)

7. SMS Authentication Security Considerations - NIST Special Publication 800-63B Digital Identity Guidelines. 2017. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf (дата звернення: 14.03.2025)

8. ЗАКОН УКРАЇНИ №2297–VI Про захист персональних даних. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 13.03.2025).

9. ISO/IEC 15408-1:2019 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO, 2019.

10. WebAuthn Specification - W3C Web Authentication: An API for accessing Public Key Credentials Level 2. W3C Recommendation, 2021. URL: https://www.w3.org/TR/webauthn-2/ (дата звернення: 17.03.2025).

11.Google Authenticator Політика конфіденційності - https://www.gstatic.com/policies/privacy/pdf/20240916/pe84lsmf/google_privacy_policy_ru.pdf (дата звернення: 17.03.2025).

12. Google Authenticator. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=ru (дата звернення: 13.04.2025).

13. YubiKey Technical Data Sheet https://docs.yubico.com/hardware/yubikey/datasheet/_static/YubiKey_technical_data_sheet.pdf (дата звернення: 16.04.2025)

14. YubiKey Technical Manual https://docs.yubico.com/hardware/yubikey/yk-tech-manual/webdocs.pdf (дата звернення 16.04.2025)

15. Yubico Best Practices https://docs.yubico.com/hardware/yubikey-guidance/best-practices/webdocs.pdf (дата звернення: 16.04.2025)