Міністерство освіти і науки України
Харківського національного університету імені В.Н. Каразіна
Навчально-наукового інституту комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Безпека інформаційних і комунікаційних систем»

В.о. зав. кафедрою КІСМТ
Марина ЄСІНА
"Допущено до захисту"

" " _____2024р.

**Пояснювальна записка**

до кваліфікаційної роботи магістра

на тему: "Засоби багатофакторної аутентифікації"

оцінка "_____"

Голова ЕК
Лемешко О.В.

Керівник: к.т.н., доцент
Мелкозьорова О.М.

Рецензент: д.т.н., с.н.с., професор
Толстолузька О.Г.

Виконавець: студент групи КБ-61
Павленко Е.О.

Харків 2024

# РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 4 рисунки та 3 таблиці. Список використаних джерел містить 16 найменувань і займає 2 сторінки. Загальний обсяг роботи 64 сторінки.

Метою роботи є оцінка ефективності використання різних методів аутентифікації, аналіз можливих кіберзагроз та дослідження інструментів захисту від кібератак на облікові записи або на ресурс в цілому.

У дослідженні використовувалися методи теоретичного аналізу існуючих підходів до багатофакторної аутентифікації та захисту інформаційних систем, включаючи біометрію, криптографію, WAF, IDS/IPS та шифрування даних.

В результаті роботи було виявлено, що багатофакторна автентифікація є ефективним методом захисту від атак, таких як фішинг та компрометація даних. Сучасні інструменти, зокрема біометрія та адаптивні механізми, значно знижують ризик несанкціонованого доступу та порушенню достуності.

Рекомендується застосовувати багатофакторну аутентифікацію та інші інструменти захисту у корпоративних мережах, фінансовому секторі та хмарних платформах. Також важливо впроваджувати системи моніторингу загроз та навчання персоналу для мінімізації ризиків.

Робота має наукову та практичну значущість. Вона сприяє розвитку теоретичних основ безпеки та може бути інтегрована у реальні інформаційні системи для підвищення їх надійності.

Подальші дослідження мають бути спрямовані на удосконалення адаптивних моделей аутентифікації та інтеграцію з технологіями штучного інтелекту для виявлення загроз у реальному часі. Також варто продовжити роботу над захистом аутентифікаційних протоколів та даних у хмарних сервісах.

Ключові слова: БАГАТОФАКТОРНА АУТЕНТИФІКАЦІЯ, МЕТОДИ АУТЕНТИФІКАЦІЇ, СТАНДАРТИ АУТЕНТИФІКАЦІЇ, КІБЕРЗАГРОЗИ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ІНСТРУМЕНТИ ЗАХИСТУ.

# ABSTRACT

This diploma thesis consists of an introduction, three chapters, general conclusions, a list of references, include 4 figures and 3 tables. The list of references contains 16 entries and takes up 2 pages. The total volume of the work is 64 pages.

The goal of this work is to evaluate the effectiveness of various authentication methods, analyze potential cyber threats, and explore tools for protecting accounts or the entire resource from cyberattacks.

The research used methods of theoretical analysis of existing approaches to multi-factor authentication and information system protection, including biometrics, cryptography, WAF, IDS/IPS, and data encryption.

As a result of the study, it was found that multi-factor authentication is an effective method of protection against attacks such as phishing and data compromise. Modern tools, including biometrics and adaptive mechanisms, significantly reduce the risk of unauthorized access and disruption of availability.

It is recommended to use multi-factor authentication and other security tools in corporate networks, the financial sector, and cloud platforms. It is also important to implement threat monitoring systems and employee training to minimize risks.

The work has scientific and practical significance. It contributes to the development of the theoretical foundations of security and can be integrated into real information systems to increase their reliability.

Further research should be focused on improving adaptive authentication models and integrating them with artificial intelligence technologies to detect threats in real time. It is also worth continuing work on protecting authentication protocols and data in cloud services.

Keywords: MULTI-FACTOR AUTHENTICATION, AUTHENTICATION METHODS, AUTHENTICATION STANDARDS, CYBER THREATS, UNAUTHORIZED ACCESS, SECURITY TOOLS.

ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

МФА — багатофакторна аутентифікація

2FA — двофакторна аутентифікація

CAC — Common Access Card

CDN — Content Delivery Network

CCM — Cloud Control Matrix

CSA — Cloud Security Alliance

DoS — відмова в обслуговувані

EAP — Extensible Authentication Protocol

FIDO — Fast Identity Online

FIDO U2F — Universal 2nd Factor

HMAC — Hash-based Message Authentication Code

HOTP — HMAC-Based One-Time Password

IDS — Intrusion Detection System

IPS — Intrusion Prevention System

NFC — Near Field Communication

OIDC — OpenID Connect

PCI DSS — Payment Card Industry Data Security Standard

PIV — Personal Identity Verification

RADIUS — Remote Authentication Dial-In User Service

SAML — Security Assertion Markup Language

SSL — Secure Sockets Layer

TLS — Transport Layer Security

TOTP — Time-Based One-Time Password

USB — Universal Serial Bus

VPN — Virtual Privat Network

WAF — Web Application Firewall

# ВСТУП

У сучасних інформаційних системах питання безпеки даних є одним із найбільш пріоритетних, оскільки кіберзагрози стають дедалі складнішими. Широке впровадження інформаційних технологій у приватному й корпоративному секторах підвищило кількість конфіденційних даних, доступ до яких має бути надійно захищений. Однак традиційні засоби захисту, зокрема, однофакторна аутентифікація за допомогою пароля, стають недостатньо ефективними у боротьбі з сучасними кіберзлочинами, такими як фішинг, атаки методом грубої сили та викрадення облікових даних.

Багатофакторна аутентифікація (МФА) дозволяє підвищити рівень безпеки шляхом поєднання декількох незалежних факторів перевірки, що значно ускладнює несанкціонований доступ до інформаційних ресурсів. МФА використовує комбінацію методів аутентифікації, таких як знання (пароль), володіння (мобільний пристрій або апаратний токен), та унікальні фізичні ознаки користувача (біометричні дані).

Дослідження актуальності та переваг МФА в контексті інформаційних систем набуває особливого значення, оскільки правильний вибір методів і їх поєднання дозволяє не лише посилити захист, але й забезпечити зручність користувачів. Таким чином, аналіз різних підходів до аутентифікації та рекомендації щодо їх застосування є важливими для ефективного управління кібербезпекою як у приватному, так і в корпоративному секторах.

Метою роботи є оцінка ефективності використання різних методів аутентифікації, аналіз можливих кіберзагроз та дослідження інструментів захисту від кібератак на облікові записи або в ціому на ресурс.

Об'єктом дослідження є процес ауентифікації та впровадження декількох факторів аутентифікації.

Предметом дослідження є методи аутентифікації, що використовуться для підтвердження особистості та можуть поєднуватись між собою

# 1. ОГЛЯД НАЯВНОЇ ЛІТЕРАТУРИ З БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

Багатофакторна аутентифікація вже давно стала важливою та обговорюваною темою. Використання лише одного пароля для захисту облікового засобу або важливих(секретних) даних стало ризикованим та неефективним. Розвиток технологій дає можливість як і покращити захист, так і більше можливостей його зламати, саме тому, для зменшення подібних ризиків, варто ретельніше обирати шляхи захисту, їх вид та кількість.

В науковій літературі вже більше десяти років йдеться обговорення про альтернативні методи аутентифікації та їх посилення. Розробляється безліч механізмів, які тестуються у різних ситуаціях зламу, з метою зробити рівень безпека максимальним.

Сьогодні, із швидким розвитком інформаційного суспільства та все більш складним середовищем комп'ютерних мереж, багатофакторна аутентифікація як одна з технологій захисту безпеки відіграє важливу роль як в IT-науці, так і в бізнесі. Як безпечно ввести багатофакторну аутентифікацію без впливу на користувальницький досвід, привернуло широку увагу дослідників у галузі захисту бізнес-безпеки та мережевої безпеки.

Метою роботи «A Security Protection Technology Based on Multi-factor Authentication»[1] є застосування технології багатофакторної аутентифікації до систем захисту корпоративної безпеки, розробка та проектування технології захисту безпеки на основі динамічної авторизації з використанням багатофакторної аутентифікації, а також надання підприємствам єдиних методів управління ідентифікацією та правами доступу. Це є фундаментом довіри та безпеки для забезпечення безперебійної та стабільної роботи користувачів. Оригінальний головний ключ k піддається вторинній багатофакторній обробці, що підвищує здатність користувача до аутентифікації та ефективно усуває ризик легкого викрадення пароля та приховування особистості. Для задоволення заданих вимог безпеки VoIP пропонується протокол багатофакторної аутентифікації SIP для VoIP-середовища з використанням технології багатофакторної аутентифікації для

вирішення проблеми безпеки. Результати тестування продуктивності показують, що через вплив шифрування та дешифрування даних час відгуку зашифрованої бази даних на 100 секунд більший, ніж незашифрованої, але темп зростання на 10% менший, ніж у незашифрованої. Тому продуктивність цієї схеми є кращою, коли обсяг даних більший.

Стаття «Multi-Factor Authentication for e-Government Services using a Smartphone Application and Biometric Identity Verification»[2] присвячена вирішенню проблем безпеки в електронних урядових сервісах через використання багатофакторної аутентифікації (MFA). Автори, Mohammad AlRousan та Benedetto Intrigila, пропонують інноваційну модель, що комбінує одноразові паролі (OTP), біометричну ідентифікацію (розпізнавання обличчя чи відбитків пальців) та мобільний додаток для створення безпечної платформи доступу.

Основна увага приділяється усуненню недоліків традиційних методів аутентифікації, таких як паролі, які легко піддаються атакам через слабкі мережі. У моделі передбачено автоматизовану перевірку ідентичності через спеціалізовані кіоски, де користувачі можуть зареєструватися, надати свої біометричні дані, встановити додаток та підтвердити безпеку.

Ця модель виділяється завдяки її простоті для користувачів, оскільки вона мінімізує взаємодію після початкового налаштування, а також завдяки зосередженню на безпеці через контрольовані урядові мережі. Автори підкреслюють важливість використання новітніх функцій смартфонів, таких як біометрія, для підвищення захисту. У статті наголошується, що впровадження моделі може значно знизити ризики кібератак та забезпечити надійний захист даних громадян, водночас спрощуючи їх доступ до урядових сервісів.

Незважаючи на перспективність, модель потребує подальших досліджень та тестування в реальних умовах. Авторами передбачено створення прототипу, який дозволить оцінити її ефективність і вдосконалити реалізацію.

Стаття «An Extensive Formal Analysis of Multi-factor Authentication Protocols»[3] є глибоким аналізом протоколів багатофакторної аутентифікації (MFA), таких як Google 2-step та FIDO U2F. Автори Чарлі Жаком і Стів Креймер

дослідили їх ефективність у контексті сучасних загроз, включаючи фішинг, компрометацію пристроїв, атак на TLS-канали та людські помилки.

Для аналізу використано інструмент Proverif та понад 6 000 сценаріїв загроз. Автори визначили ключові ризики, наприклад, слабкість SMS-кодів у Google 2-step та компрометацію пристроїв користувачів. Водночас протокол FIDO U2F виявився більш стійким завдяки криптографічному підпису, що забезпечує контекстну аутентифікацію.

У статті було розроблено нову, детальну модель загроз для протоколів багатофакторної аутентифікації, яка враховує кілька важливих аспектів безпеки. Модель орієнтована на реальні сценарії атак, де атакуючий може мати частковий або повний контроль над мережею або пристроєм користувача. Крім того, вона охоплює можливість зараження пристроїв шкідливим ПЗ, що дає зловмисникам змогу перехоплювати введені дані або маніпулювати ними. Враховано також людські помилки, як от недбалість у перевірці безпеки або сприйняття фішингових атак, що знижує загальну ефективність протоколів безпеки. Ця модель є основою для аналізу вразливостей та надає можливість перевірки різних сценаріїв атак на протоколи.

Протокол Google 2-step виявився вразливим до атак, що використовують перехоплення SMS, зокрема під час передачі кодів для підтвердження аутентифікації. Також були виявлені проблеми безпеки у випадках використання довірених пристроїв, де користувач може бути підданий атакам, які маніпулюють умовами аутентифікації. Для зменшення цих ризиків було запропоновано додати додаткову інформацію, таку як контекстні дані про дії користувача. Це дозволило б виявити підозрілі дії та покращити загальний рівень безпеки протоколу.

Протокол FIDO U2F забезпечує високий рівень безпеки завдяки використанню апаратного токена, який генерує та зберігає криптографічні ключі, що ускладнює атакування. Однак він все ще має вразливості, якщо пристрій користувача, наприклад, комп'ютер, повністю скомпрометовано. У такому випадку атакуючий може отримати доступ до критичних даних, навіть зберігаючи надійність самого токена. Ця уразливість підкреслює важливість захисту пристроїв на всіх етапах їх використання для збереження надійності MFA.

У методології автори використовували автоматизацію для систематичної перевірки всіх можливих комбінацій загроз, що дозволило здійснити глибокий аналіз безпеки кожного протоколу. Завдяки цьому вдалося виявити конкретні слабкі місця кожного з них. У результатах аналізу чітко визначено, які загрози усуваються кожним протоколом, а які залишаються невирішеними. Такий підхід дозволяє отримати точне уявлення про безпеку кожного протоколу у різних умовах загроз.

Стаття завершується рекомендаціями щодо покращення протоколів, включаючи можливість розширення Google 2-step за допомогою елементів FIDO U2F. Робота є цінним внеском у сферу розробки безпечних аутентифікаційних систем, пропонуючи перевірені рішення для покращення безпеки в умовах сучасних загроз.

Стаття «Designing of User Authentication Based on Multi-factor Authentication on Wireless Networks»[4] детально описує процес створення багатофакторної аутентифікації (MFA) для безпечного доступу до бездротових мереж. Автори розглядають концепцію MFA, яка об'єднує три ключові фактори аутентифікації: знання користувача (паролі), володіння (одноразові паролі через SMS або email) та біометричні дані (фото обличчя).

Запропонований метод передбачає багатоступеневу процедуру: реєстрацію, верифікацію та OTP-аутентифікацію. Унікальна особливість системи полягає в необхідності підтвердження мобільного номера та email, що мінімізує ризики шахрайства.

Дослідження підтверджує, що така аутентифікація є як безпечною, так і зручною, забезпечуючи користувачам простий, але надійний спосіб захисту доступу до мереж. Водночас модель має потенціал для вдосконалення у практичному застосуванні.

Стаття «On Secret Sharing with Newton's Polynomial for Multi-Factor Authentication»[5] досліджує застосування інтерполяційного методу Ньютона для покращення схем розподілу секретів у багатофакторній аутентифікації (MFA). Автори пропонують застосовувати поліном Ньютона в схемах розподілу секретів завдяки його здатності значно спрощувати процес розширення системи

аутентифікації. У традиційній схемі Шаміра, побудованій на поліномі Лагранжа, додавання нового фактора вимагає повного перерахунку коефіцієнтів для всіх існуючих точок. Поліном Ньютона, навпаки, дозволяє додати нову точку, обчисливши лише додатковий коефіцієнт, зберігаючи попередні без змін. Це робить систему більш адаптивною до змін, знижує обчислювальну складність і підвищує ефективність обробки даних.

У традиційній схемі Шаміра розподіл секрету здійснюється через побудову полінома, де кожна частина секрету відповідає певній точці на поліномі. Поліном Лагранжа, використовуваний у цьому процесі, забезпечує точну інтерполяцію для відновлення секрету, але має суттєве обмеження: додавання нової точки вимагає перерахунку всіх базисних поліномів і коефіцієнтів. Це обумовлено тим, що кожна точка впливає на структуру полінома.

Натомість у методі Ньютона використовується інакший підхід до побудови полінома: кожен коефіцієнт обчислюється незалежно, використовуючи розділені різниці. Це означає, що додавання нової точки впливає лише на кінцевий член полінома. Наприклад, при розширенні полінома Ньютона для нової точки додається лише один додатковий коефіцієнт і новий базисний множник, тоді як всі попередні обчислення залишаються незмінними.

Така модульність дозволяє не лише швидше адаптувати систему до змін, а й значно знижує обчислювальну складність, особливо для систем, де фактори аутентифікації часто оновлюються або додаються. Це робить метод Ньютона більш ефективним і масштабованим у контексті багатофакторної аутентифікації, яка потребує гнучкості та динамічності в умовах сучасних систем безпеки.

У статті детально розглянуто використання полінома Ньютона для багатофакторної аутентифікації (MFA) у системах, які комбінують біометричні фактори (наприклад, відбитки пальців чи розпізнавання обличчя), паролі або фізичні ключі. У запропонованій моделі кожен фактор представляється точкою на поліномі, який визначає доступ до системи. Наприклад, у системі, що вже має два біометричних фактори (відбиток пальця і розпізнавання обличчя), ці точки є основою для створення полінома, а додавання нових факторів (наприклад, пароля

або ще одного біометричного сенсора) потребує лише обчислення додаткового коефіцієнта.

Автори наводять приклади, де цей підхід демонструє суттєві переваги. Уявімо, що в MFA-системі, яка використовується у каршерінгу, початково є лише два біометричних фактори, але згодом потрібно інтегрувати третій (наприклад, новий тип сенсора). Використовуючи поліном Лагранжа, це вимагало б повного перерахунку всіх компонентів полінома. Проте метод Ньютона дозволяє додати новий фактор шляхом обчислення лише одного нового множника, зберігаючи всі попередні обчислення.

Ця властивість полінома Ньютона має критичне значення для адаптивних систем, які повинні швидко реагувати на зміни. Наприклад, у системах, де наявні компоненти можуть виходити з ладу або вимоги до безпеки можуть змінюватися (як-от у банківських чи транспортних системах), можливість додавати нові фактори без необхідності повного оновлення структури значно спрощує обслуговування і знижує обчислювальні витрати.

Загалом, цей підхід демонструє перевагу у швидкості обробки, масштабованості системи та її здатності до динамічних змін. Це робить поліном Ньютона ідеальним інструментом для багатофакторної аутентифікації в сучасних інтерактивних системах.

У висновках статті підкреслюється значущість застосування полінома Ньютона в системах багатофакторної аутентифікації (MFA), особливо в контексті динамічних систем, які вимагають частого додавання або модифікації факторів. Автори наголошують, що використання цього методу значно спрощує адаптацію MFA-систем до змін, оскільки додавання нового фактора не потребує повного перерахунку попередніх коефіцієнтів, як у методі Лагранжа.

Цей підхід робить системи більш гнучкими, масштабованими та ефективними, знижуючи обчислювальну складність і час обробки. Висновки демонструють, що поліном Ньютона ідеально підходить для сучасних додатків MFA, таких як фінансові платформи, системи доступу до фізичних об’єктів і транспортні сервіси.

Автори рекомендують використовувати цей метод у сценаріях, де важливими є адаптивність, мінімізація обчислювальних витрат і можливість швидкого розширення.

Стаття «One Time Password Generation for Multifactor Authentication using Graphical Password»[6] досліджує недоліки традиційних методів аутентифікації, таких як текстові паролі, і пропонує нову двофакторну систему для підвищення безпеки доступу до критичних ресурсів. Вона поєднує графічний пароль і динамічний одноразовий пароль (OTP), що створюється через криптографічну функцію. Користувач обирає серію зображень під час реєстрації, що стає основою для генерації пароля. Для підвищення безпеки в систему інтегруються випадкові числа (seed-фактори), що додаються до пароля.

Ця система забезпечує надійний захист від атак, таких як перехоплення даних, атаки типу грубої сили або повторні атаки. Користувачам потрібно вибрати зображення, які вони вибрали під час реєстрації, і система генерує динамічний OTP на основі обраних зображень і додаткових факторів. Генерація пароля залежить від унікальних факторів, що надають захист від традиційних атак, включаючи перехоплення чи підбори паролів.

Графічні паролі забезпечують кращий захист від традиційних методів злому, таких як атаки «dictionary» або «brute-force», через їх складність і відсутність звичних текстових шаблонів. Оскільки користувач вибирає зображення з великої кількості варіантів, ці паролі значно важче підібрати автоматизованими методами. Система також використовує криптографічні методи для захисту перед криптоаналізом, забезпечуючи більшу гнучкість у створенні паролів, що дозволяє користувачам формувати надійні паролі без необхідності запам'ятовувати складні комбінації символів. Це робить її ідеальним рішенням для захисту онлайн-сервісів, таких як банківські платформи.

Автори акцентують, що запропонована схема забезпечує надійний захист і дозволяє зменшити ймовірність успішних атак, зокрема атак типу «man-in-the-middle», що є важливим для критичних онлайн-сервісів, де безпека доступу є пріоритетною.

Стаття «A Review of Two-Factor Authentication Security Challenges in the Cyberspace»[7] аналізує сучасні виклики у сфері двофакторної аутентифікації (2FA). Автори досліджують недоліки однофакторної аутентифікації, такі як вразливість до кейлогерів, перехоплення паролів і слабкість текстових паролів. Водночас 2FA, хоч і підвищує рівень безпеки, має свої обмеження, включаючи затримки в отриманні SMS, високу вартість апаратних токенів і труднощі використання.

У статті детально описуються три основні категорії факторів аутентифікації. Перший, фактор знання, включає паролі, PIN-коди чи секретні слова. Хоча ці методи прості, вони є вразливими до атак, таких як кейлогери чи «dictionary attack». Другий, фактор володіння, охоплює апаратні токени, смарт-карти чи мобільні пристрої. Вони забезпечують додатковий рівень захисту, але створюють адміністративні труднощі, такі як їхня заміна чи обслуговування. Третій, фактор біометрії, використовує фізичні чи поведінкові характеристики (відбитки пальців, сканування обличчя), які є унікальними, але вимагають дорогого обладнання та можуть викликати помилкові спрацювання.

У статті зазначено, що хоча впровадження 2FA значно підвищує безпеку, наприклад, у банківських системах чи урядових установах, воно не є ідеальним. Проблеми, пов’язані з його впровадженням, включають затримки в передачі SMS для OTP, високу вартість виготовлення та підтримки апаратних токенів і незручності для користувачів, яким доводиться постійно мати при собі кілька аутентифікаторів. Автори рекомендують пошук альтернативних рішень, які поєднують простоту використання з високим рівнем безпеки, для усунення недоліків традиційної 2FA.

Стаття «Biometric Authentication as a Service on Cloud: Novel Solution»[8] аналізує впровадження біометричної аутентифікації як хмарного сервісу. Автори статті наголошують, що біометрична аутентифікація має значні переваги над традиційними методами, такими як паролі чи токени. Фізіологічні характеристики (відбитки пальців, сканування райдужки, обличчя) є унікальними для кожної людини, що ускладнює їх підробку чи викрадення. Поведінкові параметри, як-от голос чи ритм набору тексту, також відрізняються індивідуальністю, додаючи

рівень складності для зловмисників. На відміну від паролів, які можуть бути вкрадені або вгадані, біометричні дані забезпечують вищий рівень безпеки завдяки своїй незмінності та індивідуальності.

У статті детально розглядається використання концепції «Single Sign-On» (SSO) для спрощення процесу аутентифікації. За цією моделлю користувач проходить аутентифікацію один раз, отримуючи доступ до всіх пов'язаних систем і сервісів, що забезпечує зручність і підвищує ефективність роботи. Для забезпечення безпеки дані користувача, включаючи біометричну інформацію, зберігаються у зашифрованому вигляді, що знижує ризик компрометації.

Запропонований підхід базується на поєднанні кількох біометричних методів, наприклад, голосу та відбитків пальців. Це дозволяє підвищити точність аутентифікації, оскільки різні методи доповнюють один одного, зменшуючи ймовірність помилкових спрацювань або компрометації. Наприклад, якщо один з факторів буде вразливим до атаки, інші залишаються надійними. Завдяки цьому модель відповідає сучасним вимогам до захисту даних і є особливо корисною в умовах хмарних обчислень, де безпека та простота доступу є ключовими вимогами.

Цей підхід дозволяє використовувати SSO для автоматизованого управління доступом до різних ресурсів, що значно скорочує необхідність багаторазового введення даних і підвищує продуктивність користувачів.

Система «Single Sign-On» (SSO), описана в статті, значно спрощує процес аутентифікації. Один раз увійшовши до системи, користувач отримує доступ до всіх пов'язаних ресурсів, усуваючи потребу повторного введення облікових даних. Усі біометричні дані, такі як відбитки пальців і голос, зберігаються у зашифрованому вигляді для захисту від компрометації.

Гібридний підхід, що об'єднує кілька біометричних методів, забезпечує вищу точність аутентифікації. Якщо один фактор вразливий, інші залишаються надійними, що мінімізує ризики та підвищує надійність доступу. Це робить модель ефективною для застосування в хмарних сервісах, де важливі як безпека, так і зручність для користувачів.

У статті акцентується увага на недоліках біометричних технологій, які, попри високу точність, мають свої обмеження. Наприклад, голос можна фальсифікувати

за допомогою спеціальних програм або записів, а сканери райдужки часто вимагають дорогого обладнання, яке не завжди є доступним. Також існують фактори зовнішнього середовища, як-от недостатнє освітлення або шум, які можуть впливати на ефективність цих методів.

Автори рекомендують гібридний підхід, що поєднує кілька біометричних факторів, таких як голос і відбитки пальців. Це дозволяє компенсувати недоліки одного методу завдяки перевагам іншого. Наприклад, якщо сканування райдужки недоступне через технічні проблеми, система все ще може ідентифікувати користувача за голосом або відбитком пальця.

Такий підхід особливо актуальний для хмарних обчислень, де ключовими вимогами є захист даних і зручний доступ. Використання багатофакторної біометрії у хмарних сервісах забезпечує баланс між безпекою і зручністю, дозволяючи системам залишатися ефективними навіть за умов змінного середовища чи обмежень обладнання.

Стаття «Multi-Factor Authentication for Secured Financial Transactions in Cloud Environment»[9] детально розглядає модель багатофакторної аутентифікації (MFA) для захисту фінансових транзакцій у хмарних середовищах. Автори запропонували нову модель аутентифікації, що поєднує низькоентропійні паролі, голосову ідентифікацію та криптографію на еліптичних кривих для забезпечення високої безпеки. Голосова ідентифікація базується на методі Mel Frequency Cepstral Coefficients (MFCC), який аналізує унікальні акустичні особливості голосу користувача. Цей підхід підвищує захист від атак, зокрема фальсифікацій, оскільки голосові відбитки є складними для відтворення. Крім того, голосові дані використовуються разом із іншими аутентифікаційними факторами, що забезпечує багаторівневу перевірку і знижує ризики зловживань.

Модель аутентифікації базується на складній архітектурі, яка використовує декілька серверів для генерації сесійного ключа і забезпечення надійного зв’язку. Унікальність системи полягає в інтеграції голосових відбитків користувача, отриманих через алгоритм MFCC, з хешуванням IMSI-коду SIM-картки, що додає кожному користувачеві індивідуальність. Хешування IMSI забезпечує додатковий рівень безпеки, захищаючи передані дані від компрометації.

Система реалізує симетричне шифрування AES, яке кодує всі повідомлення, зокрема запити на аутентифікацію та передачу сесійних ключів. Цей підхід захищає дані навіть у випадку атаки типу «man-in-the-middle».

Алгоритми оптимізовані для мінімізації затримок, завдяки чому система здатна обробляти до тисячі запитів одночасно з середнім часом відповіді близько 12 секунд. Це робить модель ефективною для реальних умов, таких як онлайн-банкінг, забезпечуючи надійність та продуктивність навіть при значному навантаженні.

Загалом, багаторівневий підхід, заснований на інтеграції біометричних, криптографічних і сим-кодових даних, гарантує високий рівень безпеки для сучасних фінансових транзакцій.

Система демонструє високу стійкість до різноманітних атак завдяки багатофакторному підходу. У випадку викрадення SIM-картки, навіть із доступом до IMSI-коду, атакуючий не зможе отримати сесійний ключ, оскільки для його створення потрібні унікальні голосові та хешовані дані, які зберігаються захищено. Стійкість до атак «man-in-the-middle» забезпечується симетричним шифруванням AES та використанням унікальних ключів для кожної сесії.

Захист серверів аутентифікації реалізовано через багаторівневу перевірку, яка вимагає поєднання низькоентропійного пароля, біометричних даних і зашифрованих сесійних ключів. Це унеможливлює несанкціонований доступ навіть у разі часткового компрометування системи. Завдяки цим особливостям модель є практичною для застосування у фінансових та хмарних сервісах, де безпека даних є критичною.

# 2. СУТНІСТЬ БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

## 2.1 Основи багатофакторної аутентифікації та її переваги

Сьогодні кібербезпека стала значною проблемою в багатьох галузях діяльності. Приватні та державні компанії встановлюють політику безпеки та приймають закони, щоб забезпечити відповідність компаній та державних установ цим політикам або стикнутися з наслідками. Існує кілька проблем управління безпекою щодо кібербезпеки, причому однією з загальних слабких ланок є пароль. Двофакторна аутентифікація (2FA) є двостороннім процесом перевірки, який спрямований на вирішення існуючої проблеми однофакторної аутентифікації. Двофакторна аутентифікація поділяється на три фактори аутентифікації:

- Фактор знання — це те, що знає користувач, наприклад, використання пароля, PIN-коду або секретного слова.
- Фактор володіння — це те, що має користувач. Це може варіюватися від посвідчення особи до токена безпеки або смартфона.
- Фактор властивості — це те, що ти є, наприклад, використання біометричних факторів, таких як відбиток пальця, розпізнавання обличчя та сканування райдужної оболонки ока.

Ступінь посилення шляху аутентифікації зображений на рисунку 2.1.


Рисунок 2.1 — Фактори аутентифікації

Двофакторна аутентифікація зміцнює протокол безпеки, використовуючи два методи для перевірки особи користувача. Цей додатковий рівень безпеки

ускладнює для кіберзлочинців доступ до пристроїв користувачів або клієнтських облікових записів. Хоча 2FA є кращою за однофакторну аутентифікацію, вона все ще не є на 100% стійкою. Використання 2FA може забезпечити кращий захист, але ускладнює процес входу. Також варто враховувати, що 2FA включає набори факторів авторизації. Якщо один фактор або пристрій втрачено, це може викликати проблеми, особливо якщо цей фактор містить доступ до банківського рахунку або інших цінних даних.

Незважаючи на посилення безпеки, пов'язане з двофакторною аутентифікацією, вона страждає від історичних перешкод, починаючи від того, що користувачам доводиться постійно носити апаратні токени безпеки, мати доступ до обладнання для використання багатофакторної аутентифікації, нести додаткові витрати на вхідні SMS, затримку у отриманні кодів і закінчення терміну дії токенів аутентифікації до використання. Ці перешкоди призвели до збільшення кількості носіїв токенів безпеки серед різних користувачів. Однак більшість з них змушені використовувати їх, через необхідність використання на роботі, при цьому постійне утримання токена та слідкування за його збереженням є незручним та заважає багатьом користувачам.

Тим не менш варто пам'ятати, що багатофакторна аутентифікація є вкрай важливою для збереження цілісності та захищеності даних. Однофакторний метод зазвичай передбачає використання паролю. Паролі використовуються як доказ особистості. В ідеалі вони повинні бути легкими для запам'ятовування і важкими для здогадки. Користувачі не завжди дотримуються цих двох факторів, оскільки вони обирають легкі для здогадки та запам'ятовування паролі, що робить їх вразливими для кіберзлочинців. Паролі за своєю суттю слабкі: користувачі мають звичку вибирати прості або короткі паролі для запам'ятовування або використовувати один і той же пароль для кількох облікових записів. З технологічними досягненнями хакерам стало простіше підбирати, вгадувати паролі або збирати їх за допомогою таких технологій, як кейлогери.

Однофакторна аутентифікація передбачає прямий доступ до облікового запису лише використанням одного фактору (Рисунок 2.2), у той момент як

багатофакторна аутентифікація додає іншу гілку на шляху аутентифікації додаючи ще, як мінімум, один фактор (Рисунок 2.3).


Рисунок 2.2 — Вхід із використанням одного фактору

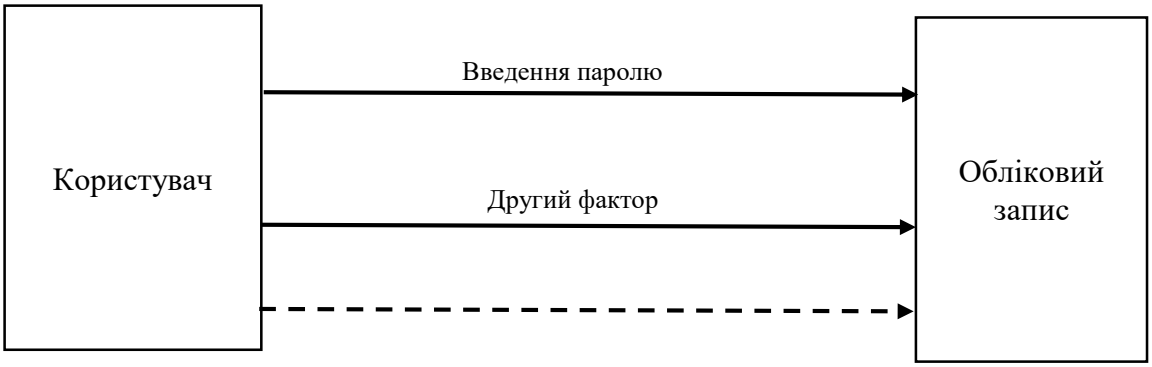


Рисунок 2.3 — Багатофакторна аутентифікація

Двофакторна аутентифікація є унікальним двоступеневим процесом перевірки, який вирішує існуючу проблему однофакторної аутентифікації: простий пароль і ім’я користувача. Вона набула популярності по всьому світу, забезпечуючи безпеку мільйонам користувачів і організаціям на тлі кібератак.

Біометрична технологія є просунутою формою ідентифікації. Біометрична аутентифікація використовує такі характеристики користувача, як відбитки пальців, розпізнавання обличчя, геометрію руки та сітчатку ока, і зберігає ці дані. Користувачі потім використовують ці характеристики для аутентифікації себе, порівнюючи їх із збереженими даними та надаючи доступ, коли досягається відповідність. Розвиток цієї технології має свої недоліки, від імітації голосу в біометрії голосу та збору відбитків пальців за допомогою невеликої стрічки до

додаткових апаратних пристроїв, необхідних для виявлення сітківки ока та відбитків пальців.

## 2.2 Класифікація засобів багатофакторної аутентифікації

Засоби багатофакторної аутентифікації базову класифікацію за такими ознаками: знання, володіння, властивість. Знання це те що є відомим, тобто пароль або пін-код, який користувач запам’ятовує та може використовувати для аутентифікації. Володіння охоплює використання сторонніх предметів-аутентифікаторів, таких як смарт-картки, фізичні токени або мобільні телефони, вони ускладнюють отримання несанкціонованого доступу тим, що для входу потрібно мати конкретний фізичний об’єкт. Властивість це безпосередньо те, що належить користувачу, доступ надається завдяки перевірці біометричних даних (відбитки пальців, сканування райдужної оболонки ока, тощо)[10].

За одним з видів класифікації аутентифікатори можуть відноситись до апаратних засобів, програмних засобів або хмарних рішень. Апаратні засоби це фізичні носії, що використовуються шляхом підключення до USB-порту або за допомогою NFC технології. Програмні засоби це комп’ютерні або мобільні додатки, що встановлюються на пристрій, з якого буде відбуватись аутентифікація. А також хмарні рішення це сервіси, що використовуються для управління МФА без додаткових пристроїв або програм[11].

Програмні засоби багатофакторної аутентифікації забезпечують функціональність для багаторівневого підтвердження особи користувачів, інтегруючи різні фактори перевірки шляхом використання додаткового програмного забезпечення, щоб ускладнити несанкціонований доступ. Основні можливості таких засобів включають генерацію одноразових паролів (OTP), інтеграцію біометричних методів (відбитки пальців, розпізнавання обличчя), підтримку фізичних токенів та можливість використання мобільних додатків для аутентифікації.

Апаратні засоби багатофакторної аутентифікації забезпечують високий рівень безпеки, поєднуючи фізичні пристрої з іншими факторами аутентифікації. До таких засобів належать токени (наприклад RSA SecurID), смарт-карти, USB-ключі (YubiKey) або ж пристрої з біометричними сканерами.

Апаратні засоби здатні генерувати унікальні коди або використовувати криптографічні ключі для підтвердження особи користувача. Наприклад, USB-ключі YubiKey працюють із криптографією відкритого ключа, забезпечуючи надійний доступ до онлайн-сервісів. Смарт-карти часто використовуються в корпоративному середовищі, взаємодіючи з інфраструктурою PKI.

Ключовою перевагою апаратних засобів є їхня стійкість до атак на мережі, оскільки зловмисники не можуть перехопити або дублювати фізичний пристрій. Однак їх використання пов'язане з ризиками, такими як втрата чи фізичне пошкодження пристрою. Апаратні засоби МФА часто застосовуються у фінансовій сфері, урядових організаціях, тощо.

Хмарні засоби багатофакторної аутентифікації — це рішення, які дозволяють забезпечити безпечний доступ до ресурсів через хмарні сервіси. Вони інтегрують декілька рівнів перевірки, таких як одноразові паролі (OTP), біометрія або апаратні токени, й забезпечують доступ до додатків через інтернет.

Основна перевага хмарних MFA — це централізоване керування доступом до різних платформ. Наприклад, такі сервіси як Microsoft Azure AD чи Google Workspace забезпечують можливість масштабованого керування ідентифікацією для великих організацій. Такі системи адаптуються до можливих ризиків. При вході з незвичних пристроїв чи локацій вони підвищують рівень перевірки, забезпечуючи гнучкість та безпеку.

Спосіб реалізації аутентифікації це один з головних важелів при виборі способу аутентифікації. Кожен користувач спирається на свої можливості та/або бажання: використовувати програми чи брати з собою фізичний носій. Методи аутентифікації, між іншим, мають різні напрямки класифікації, що представлені на Рисунку 2.4. Даний рисунок в більш повній мірі розкриває шляхи аутентифікації, відносно вже розглянутого.

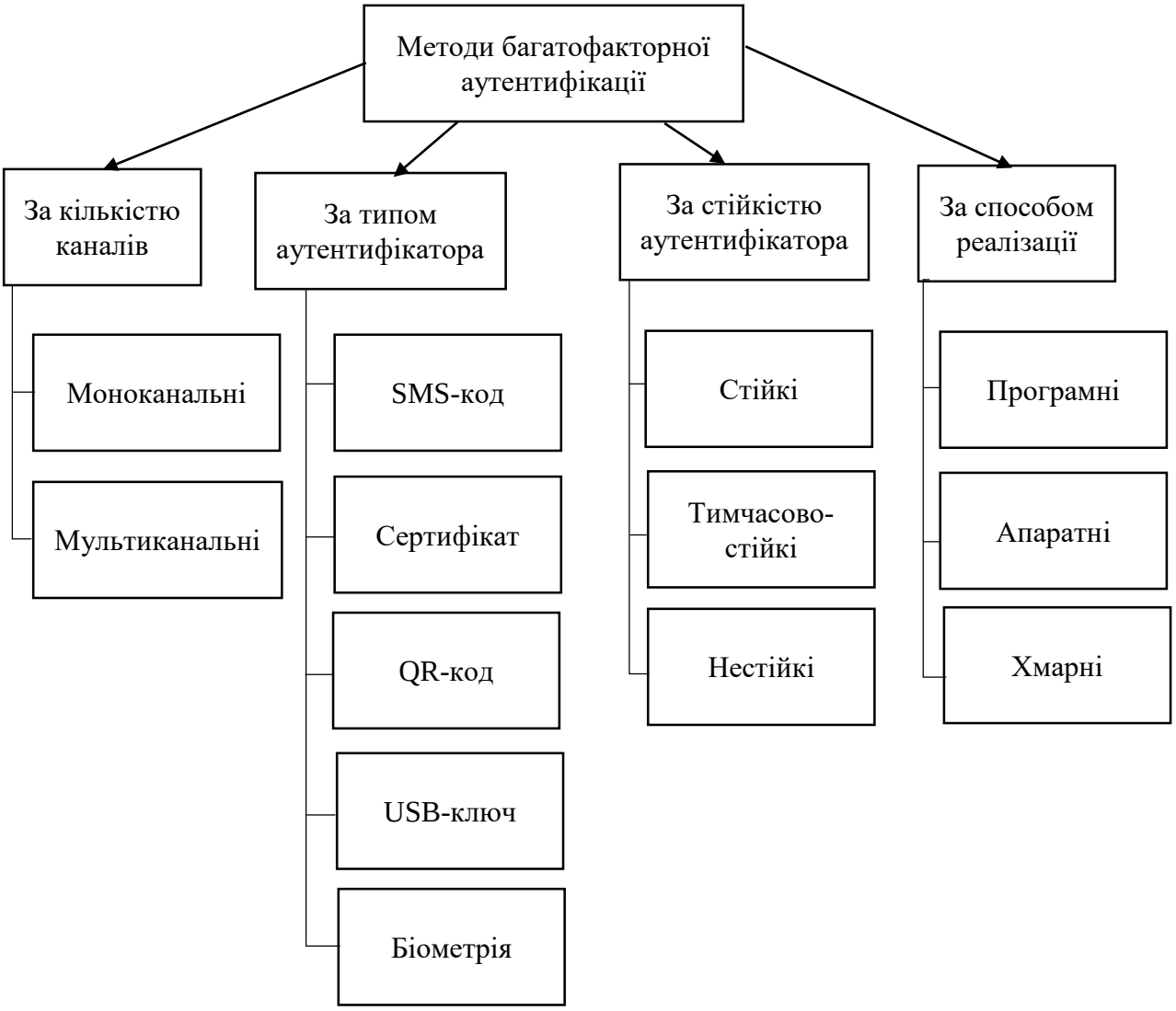


Рисунок 2.4 — Класифікації методів аутентифікації

## 2.3 Стандарти та протоколи аутентифікації

Під час багатофакторної аутентифікації моожуть використовуватись різні стандарти та протоколи. Вони можуть мати як загальне значення, так і використовуватись в конкретних випадках.

Протоколи TOTP (Time-Based One-Time Password) та HOTP (HMAC-Based One-Time Password) використовуються при аутентифікації за допомогою другого фактору — генерації одноразових кодів (OTP). Це єфективний спосіб підвищення рівня захисту, який додає необхідність використовувати додаткове програмне забезпечення чи фізичний носій.

TOTP заснований на алгоритмі HMAC (Hash-based Message Authentication Code), але використовує час як додатковий фактор для зміни пароля. Принцип роботи полягає у використанні секретного ключа, який знаходиться на сервері та у додатку користувача. За допомогою цього ключа та поточного часу генерується новий пароль, який діє зазвичай 30 секунд. Короткочасність життя кожного такого паролю надає змогу мінімізувати ризик несанкціонованого доступу до облікового запису. Цей протокол зручний у реалізації та не потребує значного розуміння.

HOTP працює за схожим принципом але з однією відмінністю: протокол використовує лічильник для генерації нових паролів. З генерацією кожного нового паролю на сервері збільшується лічильник, важливо щоб він збільшувався паралельно із користувацьким лічильником входів до системи.

В цілому обидва протоколи мають схожий порядок дій з точки зору користувача, хоча і мають деякі відмінності зазначені у таблиці 2.1.

Таблиця 2.1 — протоколи аутентифікації TOTP та HOTP

| Характеристика | TOTP | HOTP |
|---|---|---|
| Тип | Часовий | Лічильниковий |
| Генерація пароля | На основі поточного часу | На основі збільшуваного лічильника |
| Часова залежність | Так, пароль змінюється через час | Немає, пароль змінюється при кожному запиті |
| Синхронізація | Потрібна точна синхронізація часу | Потрібна синхронізація лічильника |
| Застосування | Підходить для частої аутентифікації | Підходить для систем, де необхідно обмежити кількість запитів |

OAuth 2.0 та OpenID Connect — це два протоколи авторизації та аутентифікації, які широко використовуються в сучасних веб-додатках і мобільних

застосунках для забезпечення безпечного доступу до ресурсів без необхідності безпосередньо зберігати паролі користувачів.

OAuth 2.0 — це протокол авторизації, який дозволяє стороннім додаткам отримувати обмежений доступ до ресурсів на сервері, не вимагаючи від користувачів надавати свої облікові дані безпосередньо. Це досягається через використання «токенів доступу» (access tokens), які надаються після того, як користувач авторизується у провайдера і надасть дозвіл на доступ до своїх даних. Важливою перевагою OAuth 2.0 є те, що цей протокол дозволяє розділяти авторизацію (права доступу) і аутентифікацію (перевірку особи), що знижує ризики безпеки, пов'язані з обробкою паролів.

OAuth 2.0 підтримує кілька варіантів отримання токенів доступу в залежності від типу взаємодії між клієнтом, сервером та користувачем. Зокрема, розрізняють кодову авторизацію, аутентифікацію через користувацький агент (наприклад, браузер), а також інтеграцію з сервером пристрою (для мобільних додатків).

OpenID Connect (OIDC) є розширенням OAuth 2.0 і додає функціональність аутентифікації. Якщо OAuth 2.0 відповідає за авторизацію (контроль доступу), то OpenID Connect — за аутентифікацію (підтвердження особи). OpenID Connect використовує ті самі механізми, що і OAuth 2.0, але додає новий тип токена — ID-токен (ID token), який містить інформацію про користувача, наприклад, його ім’я, електронну пошту та інші дані. Це дозволяє клієнтським додаткам не лише отримати доступ до ресурсів, але й підтвердити, що користувач є тим, за кого себе видає.

Ключовою особливістю OpenID Connect є спрощення процесу реєстрації та входу у додатки, оскільки користувачі можуть використовувати свої облікові записи в таких сервісах, як Google чи Facebook, для доступу до сторонніх додатків без необхідності створювати нові паролі. Тому цей протокол особливо популярний для реалізації функцій «єдиного входу» (Single Sign-On, SSO).

В сукупності OAuth 2.0 та OpenID Connect утворюють потужну платформу для авторизації та аутентифікації, що дозволяє користувачам безпечно входити в додатки без передачі своїх паролів стороннім сервісам, а розробникам —

зменшувати ризики безпеки, пов’язані з обробкою конфіденційних даних. У таблиці 2.2 наведено порівняльну характеристику даних протоколів.

Таблиця 2.2 — Порівняння OAuth 2.0 та OpenID Connect

| Характеристика | OAuth 2.0 | OpenID Connect |
|---|---|---|
| Основна мета | Авторизація (доступ до ресурсів) | Аутентифікація (підтвердження особи) |
| Тип токена | Токен доступу | ID-токен + токен доступу |
| Додаткові дані | Дані про доступ до ресурсів | Інформація про користувача |
| Складність | Простий у реалізації | Більш складний через додаткові функції |
| Приклад використання | API для доступу до даних (GitHub, Spotify) | Вхід через Google, Facebook («Sign in with...») |

SAML (Security Assertion Markup Language) — це відкритий стандарт для обміну даними про аутентифікацію та авторизацію між різними доменами. Його основне призначення — забезпечити безпечну передачу даних про користувача між постачальниками ідентичності (IdP) та постачальниками сервісів (SP). SAML реалізує механізм єдиного входу (SSO), що дозволяє користувачам входити в різні веб-додатки за допомогою одного набору облікових даних, спрощуючи авторизацію і підвищуючи зручність.

SAML працює через передачу «асерцій» — структурованих повідомлень про користувача, які включають інформацію про його аутентифікацію та права доступу. Ці асерції передаються у форматі XML, що робить SAML гнучким для інтеграції між системами.

Процес авторизації включає кілька етапів: користувач намагається отримати доступ до сервісу, і якщо він не аутентифікований, його перенаправляють до IdP

для введення облікових даних. Після перевірки IdP генерує SAML-асерцію, яка передається в SP для надання доступу.

SAML підтримує взаємодію між різними доменами, дозволяючи інтегрувати внутрішні системи з зовнішніми постачальниками послуг без дублювання аутентифікації. Цей стандарт часто використовують у корпоративних середовищах для централізованого управління доступом. Однак через складність налаштування і формат XML, SAML може бути важчим у використанні порівняно з іншими протоколами, такими як OAuth 2.0 або OpenID Connect..

FIDO (Fast Identity Online) — це набір відкритих стандартів, розроблених для забезпечення безпечної і зручної аутентифікації користувачів в Інтернеті. Головною метою FIDO є заміна паролів на більш надійні методи, такі як біометрія, апаратні ключі або інші форми двофакторної аутентифікації, що не тільки підвищують рівень безпеки, але й зменшують кількість проблем, пов'язаних із забутими паролями або їхнім використанням на слабких платформах.

FIDO спрямований на вирішення проблеми вразливостей, пов'язаних із паролями, які часто стають мішенню для хакерських атак, таких як фішинг, перебір паролів і крадіжка даних. Протокол FIDO дозволяє створювати більш безпечні методи входу в систему, не вимагаючи від користувачів зберігати складні паролі, які можуть бути вкрадені або зламані.

Однією з основних концепцій FIDO є використання криптографічних ключів для аутентифікації. При реєстрації у сервісі створюється пара криптографічних ключів — один приватний, який зберігається тільки на пристрої користувача, і один публічний, який зберігається на сервері. Під час спроби входу в систему сервіс надсилає запит на аутентифікацію, і користувач повинен підтвердити свою особу за допомогою одного з методів, таких як відбитки пальців, розпізнавання обличчя, або введення PIN-коду на спеціальному апаратному ключі, наприклад, на USB-накопичувачі (як YubiKey).

Завдяки такому підходу, навіть якщо публічний ключ потрапить у руки зловмисника, приватний ключ залишатиметься захищеним на пристрої користувача. Це забезпечує набагато більш високий рівень безпеки, оскільки всі

операції виконуються локально, і немає необхідності передавати або зберігати паролі в Інтернеті.

FIDO складається з двох основних стандартів: FIDO U2F (Universal 2nd Factor) і FIDO2. FIDO U2F — це протокол для двофакторної аутентифікації, який використовує фізичні пристрої, такі як USB-токени або Bluetooth-ключі. FIDO2, з іншого боку, поєднує два компоненти: WebAuthn (API для взаємодії з веб-сайтами) і CTAP (Client to Authenticator Protocol), який визначає, як пристрій-аутентифікатор взаємодіє з комп'ютером або мобільним пристроєм.

Однією з основних переваг FIDO є те, що він знижує ризики фішингових атак, оскільки під час аутентифікації за допомогою FIDO користувачі не передають паролі або особисті дані через Інтернет. Також FIDO дозволяє працювати з різними платформами і пристроями, забезпечуючи універсальність і зручність використання. Більше того, оскільки стандарт є відкритим і підтримується великою кількістю компаній та організацій, він стає все більш популярним і широко використовується для підвищення рівня безпеки в різних веб-додатках, мобільних сервісах і навіть в корпоративних системах.

Kerberos — це протокол аутентифікації, який забезпечує перевірку ідентичності користувачів і ресурсів у мережі, гарантуючи доступ лише авторизованим особам. Розроблений в MIT у 1980-х роках, він став основою для систем безпеки, таких як Microsoft Active Directory. Kerberos працює за моделлю клієнт-сервер, використовуючи криптографію для забезпечення конфіденційності та цілісності даних.

Протокол базується на використанні «білетів» (tickets) — зашифрованих об'єктів, що підтверджують ідентичність користувача і дають доступ до ресурсів. Це дозволяє уникнути передачі паролів у мережі, роблячи систему стійкою до атак типу «перехоплення». Процес аутентифікації включає два основні етапи: отримання «Ticket Granting Ticket» (TGT) від центру аутентифікації (AS) і подальше звернення до сервісу надання білетів (TGS) для отримання білета доступу до конкретного ресурсу.

Kerberos гарантує захист від підроблених облікових даних і забезпечує цілісність даних, але вимагає синхронізації годин між пристроями та залежить від

працездатності серверів аутентифікації. Незважаючи на ці обмеження, Kerberos залишається популярним у корпоративних мережах завдяки високій безпеці та масштабованості, підтримуючи тисячі користувачів і ресурсів в організаціях.

X.509 — це стандарт для структури сертифікатів електронної ідентифікації, який визначає, як повинні виглядати цифрові сертифікати, що використовуються для аутентифікації та шифрування в мережах. Основною метою X.509 є забезпечення довіри між учасниками електронних комунікацій через використання криптографічних ключів та сертифікатів, що підтверджують ідентичність користувачів, серверів та іншої техніки.

X.509 був розроблений Міжнародним електротехнічним комітетом (IEC) в рамках серії стандартів для телекомунікацій, і з того часу став основою для багатьох протоколів безпеки, зокрема для таких, як TLS/SSL, що використовуються для захисту інтернет-з'єднань. Стандарт описує формат сертифікатів, які містять публічний ключ, інформацію про власника сертифіката та дані, які підтверджують автентичність цього сертифіката.

Сертифікат X.509 містить кілька ключових компонентів. Одним з них є публічний ключ, який використовують для шифрування або перевірки підписів, що належать конкретному власнику сертифіката. Це дозволяє зберігати конфіденційність комунікацій або перевіряти цілісність і авторство переданих даних. Окрім публічного ключа, сертифікат також містить інформацію про власника — це може бути ім’я організації, адреса електронної пошти, а також серійний номер сертифіката та термін його дії.

Один з найбільш важливих аспектів сертифіката X.509 — це цифровий підпис, який підтверджує, що сертифікат був виданий авторитетним центром сертифікації (CA). Цей підпис дозволяє перевірити, що сертифікат не було підроблено і що він насправді належить тій особі або організації, яка зазначена в сертифікаті. Сертифікат X.509 може бути використаний для різних цілей: для забезпечення безпечного доступу до веб-сайтів (через протокол HTTPS), для підпису електронних документів, для захисту електронної пошти або для аутентифікації користувачів у корпоративних мережах.

Стандарт X.509 передбачає також використання ієрархії довіри, в якій кожен сертифікат, виданий центром сертифікації, може бути підтверджений лише за умови, що користувач довіряє цьому центру сертифікації. Ієрархія може включати кореневий центр сертифікації, підкорінні центри та кінцеві сертифікати, що дозволяє побудувати складну систему довіри, де кожен учасник може перевірити достовірність сертифіката за допомогою ланцюга сертифікацій.

X.509 є основою для багатьох сучасних технологій безпеки, таких як використання цифрових підписів для підтвердження цілісності даних, шифрування даних за допомогою публічних і приватних ключів, а також для аутентифікації користувачів і серверів у глобальних мережах, включаючи Інтернет. Сертифікати X.509 є важливими для створення надійної інфраструктури відкритих ключів (PKI), яка забезпечує безпеку в численних онлайн-додатках, від банківських транзакцій до електронної комерції.

RADIUS (Remote Authentication Dial-In User Service) — це протокол для аутентифікації, авторизації та обліку доступу в мережах. Спочатку розроблений для віддаленого доступу через телефонні лінії, сьогодні він використовується для управління доступом до мережевих ресурсів, таких як VPN і бездротові мережі. Протокол працює за принципом клієнт-сервер, де сервер RADIUS перевіряє ідентичність користувача, а клієнтом є пристрій, що забезпечує доступ, наприклад, точка доступу або VPN-сервер.

Процес аутентифікації починається, коли клієнт передає запит із обліковими даними користувача на сервер RADIUS. Сервер перевіряє ці дані, звертаючись до бази даних або системи аутентифікації (LDAP, Active Directory), і надає дозвіл або відмову в доступі. Крім аутентифікації, RADIUS також виконує авторизацію, визначаючи доступні ресурси, та облік, реєструючи запити для моніторингу і виставлення рахунків.

RADIUS використовує криптографічні методи для безпеки, але передача паролів у незашифрованому вигляді в деяких випадках є його вразливістю. Для підвищення безпеки застосовуються додаткові методи шифрування, як IPsec або TLS. Цей протокол є важливим для централізованого управління доступом у великих корпоративних мережах, університетах та у провайдерів інтернету.

Біометричні стандарти, зокрема ISO/IEC 19794, є набором керівних принципів і специфікацій, які забезпечують узгоджене та надійне збирання, зберігання і обмін біометричними даними між різними системами та платформами. Серія стандартів ISO/IEC 19794, розроблена Міжнародною організацією стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), визначає формати і протоколи для різних видів біометричної інформації, таких як відбитки пальців, розпізнавання обличчя, райдужна оболонка ока, голосове розпізнавання та інші.

Основна мета цих стандартів — забезпечити сумісність і взаємодію біометричних систем, що використовуються для ідентифікації та аутентифікації. Дотримуючись стандартів ISO/IEC 19794, біометричні дані, зібрані однією системою, можуть бути використані і зрозумілі іншою системою, незалежно від виробника чи технології. Це надзвичайно важливо для таких застосувань, як контроль на кордонах, доступ до приміщень, правоохоронні органи та охорона здоров'я, де різні установи або організації можуть потребувати обміну або порівняння біометричних даних.

Серія стандартів ISO/IEC 19794 поділяється на кілька частин, кожна з яких охоплює певний тип біометричної модальності або аспект обміну біометричними даними. Наприклад, ISO/IEC 19794-2 фокусується на форматі даних для зображень відбитків пальців, а ISO/IEC 19794-5 визначає дані для зображень обличчя. Інші частини стандарту визначають формати для райдужних оболонок ока, голосових записів та навіть підписів. Ці специфікації надають детальні вказівки щодо того, як біометричні дані мають бути зібрані, збережені та передані в стандартизованому, безпечному та конфіденційному вигляді.

Одним з ключових аспектів серії ISO/IEC 19794 є акцент на якість і послідовність даних. Біометричні системи залежать від точних, високоякісних даних для надійної ідентифікації або аутентифікації. Наприклад, зображення відбитка пальця має бути достатньо високої роздільної здатності та чіткості, щоб система могла точно зіставити його з наявними шаблонами. Стандарти допомагають забезпечити правильне збирання та обробку цих даних, мінімізуючи помилки та випадки хибнопозитивних або хибнонегативних результатів.

Крім того, ISO/IEC 19794 надає рекомендації щодо забезпечення конфіденційності та безпеки біометричних даних. Оскільки біометрична інформація є дуже чутливою, унікальною для кожної особи та не може бути легко змінена або замінена, надзвичайно важливо захистити ці дані від несанкціонованого доступу та зловживань. Стандарт включає рекомендації щодо шифрування, безпечного зберігання та передачі біометричних даних, щоб забезпечити їх захист від перехоплення чи зміни під час використання.

Стандарти ISO/IEC 19794 є необхідними для впровадження біометричних технологій. Вони дозволяють створити стандартизований підхід до біометричних даних, які можуть бути однаково зрозумілі та надійні, що сприяє розвитку біометричних систем у різних сферах. Створення загальної основи дозволяє організаціям уникати обмежень, пов'язаних з використанням власницьких технологій, і забезпечує можливість еволюції та інтеграції біометричних систем у майбутньому.

Cloud Control Matrix (CCM) — це набір стандартів і керівних принципів, розроблений Cloud Security Alliance (CSA), який допомагає організаціям оцінювати та забезпечувати безпеку хмарних середовищ. CCM визначає набір контрольних заходів, що охоплюють всі аспекти безпеки у хмарних технологіях, включаючи конфіденційність, цілісність, доступність та відповідність вимогам законодавства.

Основна мета CCM полягає в тому, щоб допомогти користувачам і постачальникам хмарних послуг зрозуміти, як найкраще управляти ризиками, що виникають при використанні хмарних технологій, і встановити стандарти для належної організації безпеки. Матриця дозволяє організаціям формулювати політики та стратегії безпеки, враховуючи специфічні потреби та виклики, що виникають при переході до хмарної інфраструктури.

CCM містить велику кількість контрольних заходів, розбитих на різні домени, кожен з яких стосується конкретної області безпеки. Наприклад, у ньому є контроль за доступом, управлінням даними, захистом конфіденційності, аудитом, моніторингом, інцидентами безпеки, а також контроль за фізичною безпекою дата-центрів, де розташовані хмарні сервери. Це дає можливість організаціям

комплексно оцінювати свої хмарні середовища, забезпечуючи належний рівень безпеки.

Один із важливих аспектів CCM полягає в тому, що він пропонує інструменти для оцінки безпеки та відповідності вимогам на різних етапах використання хмарних послуг. Він допомагає організаціям, які використовують хмари для зберігання даних або розгортання додатків, розуміти, які конкретні заходи з безпеки вони повинні впровадити, а також допомагає їм визначити, де може бути потрібна допомога з боку постачальника хмарних послуг для досягнення необхідного рівня безпеки.

CCM відрізняється тим, що він також є частиною більш широкої ініціативи CSA з розвитку найкращих практик безпеки для хмарних обчислень, включаючи інші інструменти і стандарти, що доповнюють CCM, наприклад, Security, Trust & Assurance Registry (STAR), який дозволяє перевірити відповідність постачальників хмарних послуг вимогам безпеки.

Управління ризиками в хмарних середовищах за допомогою CCM є важливим інструментом для тих організацій, які бажають переконатися, що вони дотримуються необхідних стандартів безпеки та ефективно захищають свої дані в умовах постійно змінюваних технологічних ландшафтів. Він дозволяє забезпечити високий рівень безпеки, допомагаючи організаціям мінімізувати ризики, що виникають через вразливості у хмарних системах, і дає можливість провести глибшу оцінку та аудит існуючих хмарних рішень.

IEEE 802.1X — це стандарт, що описує протокол аутентифікації в мережах для забезпечення безпеки доступу до комп’ютерних мереж. Він був розроблений для використання в локальних мережах Ethernet, зокрема для бездротових мереж Wi-Fi, щоб забезпечити захист від несанкціонованого доступу. Протокол 802.1X працює на рівні каналу передачі даних (Layer 2) моделі OSI і є важливою частиною інфраструктури безпеки в мережах, що використовують методи аутентифікації та шифрування.

Суть роботи IEEE 802.1X полягає в тому, що він здійснює контроль за доступом до мережі, перевіряючи автентичність користувача або пристрою перед тим, як дозволити доступ до мережевих ресурсів. Він використовує архітектуру

клієнт-сервер, де три основні компоненти: supplicant (клієнт), authenticator (аутентифікатор) і authentication server (сервер аутентифікації). Клієнт — це пристрій, який намагається підключитися до мережі (наприклад, ноутбук або смартфон), аутентифікатор — це пристрій або точка доступу, який контролює доступ і взаємодіє з сервером аутентифікації, а сервер аутентифікації (зазвичай це RADIUS-сервер) відповідає за перевірку облікових даних користувача.

Процес аутентифікації в рамках IEEE 802.1X включає кілька етапів. Спочатку пристрій клієнта (supplicant) відправляє запит на доступ до мережі через аутентифікатор (наприклад, точку доступу). Аутентифікатор блокує доступ до мережі до тих пір, поки користувач не пройде перевірку через сервер аутентифікації. Потім аутентифікатор пересилає запит до сервера аутентифікації, який перевіряє облікові дані користувача або пристрою (зазвичай це логін і пароль або інші методи аутентифікації, такі як сертифікати чи токени). Якщо сервер аутентифікації підтверджує правильність даних, аутентифікатор дозволяє клієнту підключитися до мережі, і доступ надається.

Однією з ключових переваг IEEE 802.1X є його здатність забезпечити централізоване управління доступом. Використання серверів аутентифікації, таких як RADIUS, дозволяє організаціям легко управляти доступом користувачів до мережі та контролювати, хто має право підключатися. Це важливо як для великих підприємств, так і для малих організацій, оскільки дозволяє запровадити єдину політику безпеки для всієї мережі. 802.1X забезпечує високий рівень захисту, оскільки доступ надається лише тим користувачам або пристроям, які успішно пройшли аутентифікацію.

Протокол IEEE 802.1X часто застосовується в поєднанні з іншими методами безпеки, такими як шифрування, для забезпечення безпеки в бездротових мережах Wi-Fi, де атаки на доступ можуть бути особливо небезпечними. Крім того, 802.1X може бути використаний не тільки в бездротових мережах, але й в проводових мережах Ethernet, що дозволяє організаціям контролювати доступ до своїх локальних мереж.

Важливою характеристикою IEEE 802.1X є його гнучкість, оскільки він підтримує різні методи аутентифікації, які можуть бути налаштовані відповідно до

потреб користувачів або організацій. Це може бути традиційна аутентифікація за допомогою паролів, використання сертифікатів або більш сучасні методи.

2.4 Огляд методів аутентифікації

SMS та електронна пошта є найпопулярнішими типами багатофакторної аутентифікації, оскільки вони, як відомо, прості та економічно ефективні. В обох варіантах надсилається обмежений за часом одноразовий код на пристрій користувача електронною поштою чи SMS-повідомленням. Потім користувач повинен отримати доступ до коду у своїх текстових повідомленнях або електронних листах і ввести його протягом зазначеного часу, щоб отримати доступ до свого облікового запису. Зловмиснику потрібно буде ввести пароль і код доступу через SMS/електронну пошту, щоб подолати цей додатковий захід безпеки, через що зламати обліковий запис буде складніше.

Такий метод може використовувати будь-хто, однак захищеність даного методу є не достатньо високою. Такі коди можуть бути перехоплені зловмисним програмним забезпеченням або, якщо зловмисник отримає доступ до поштової скриньки або телефону користувача. Окрім цього даний метод має залежність від мобільного або інтернет зв’язку, при відсутності доступу до яких неможливо буде отримати доступ.

TOTP (Time-Based One-Time Password) — це метод аутентифікації, який генерує одноразові паролі, що діють лише протягом обмеженого проміжку часу. Ці паролі створюються на основі поточного часу та секретного ключа, який відомий лише користувачу та системі, що його використовує. TOTP є частиною стандарту RFC 6238. TOTP-генератор зазвичай представлений у вигляді мобільного додатку. На відміну від попереднього методу тут використовується обмеження у часі, здебільшого 30 секунд. Перевагою цього методу є використання секретного ключа, без якого, навіть зі знанням паролю, буде важко отримати доступ. А також TOTP не потребує підключення до мобільної мережі, оскільки працює локально на пристрої користувача. Для цього методу є важливою синхронізація часу: якщо годинник на пристрої користувача не синхронізований із сервером, це може призвести до неправильних кодів.

Подібним до попереднього є метод аутентифікації HOTP (HMAC-Based One-Time Password), який заснований на криптографічному алгоритмі HMAC і лічильнику. HOTP-генератор комбінує секретний ключ з лічильником, який збільшується з кожним новим запитом на генерацію пароля. Криптографічна функція HMAC обробляє цю інформацію, створюючи одноразовий код. Коли користувач намагається увійти до облікового запису, він вводить код, отриманий з генератора. HOTP не залежить від часу, тому коди залишаться дійсними, поки не буде згенеровано новий. Це зменшує ризик повторного використання коду зловмисниками. Лічильник одночасно є перевагою і недоліком. Кожен раз, коли код генерується, лічильник повинен бути синхронізований між сервером і клієнтом. Якщо вони не збігаються, можуть виникнути проблеми з верифікацією. Така ситуація можлива у випадку, коли користувач згенерував код, але не використав його.

Апаратні токени це фізичні пристрої, що використовуються для генерації одноразових паролів або для підтвердження особи користувача шляхом його підключення до пристрою за допомогою USB або NFC. Зазвичай такі пристрої доволі компактні та використовують більшість протоколів аутентифікації. Окрім локальної генерації кодів, рівень безпеки підтримується необхідністю мати при собі конкретний фізичний токен. Для окремих користувачів такий варіант є доволі ефективним, але для великих організацій може бути фінансово складним.

Біометрія є одним із найбільш надійних методів аутентифікації, оскільки для отримання несанкціонованого доступу потрібно буде підробити унікальні людські властивості. Більш поширеним є використання відбитків пальців, така технологія є на більшості сучасних телефонах, а також може бути використовуватись разом з іншими пристроями за допомогою додаткового невеликого гаджету. Це дуже зручний та швидкий метод, який не потребує наявності інших сторонніх об’єктів. Сканери обличчя та райдужки ока також є простими та ефективними, однак потребують більшого та складнішого устаткування.

І останній метод FIDO2 — це відкритий стандарт для безпарольної аутентифікації, який розроблений Фондом відкритої аутентифікації (FIDO Alliance)[12]. FIDO2 складається з двох основних компонентів: WebAuthn (Web

Authentication) і CTAP (Client To Authenticator Protocol). Цей стандарт забезпечує більш безпечний та зручний спосіб аутентифікації користувачів, уникаючи традиційних паролів. Коли користувач реєструється в сервісі, його пристрій (наприклад, смартфон або апаратний токен) генерує пару ключів: публічний та приватний. Публічний ключ передається на сервер, а приватний ключ зберігається на пристрої. При вході в обліковий запис сервер надсилає запит на аутентифікацію. Користувач використовує свій пристрій для підписання цього запиту, використовуючи приватний ключ. Сервер перевіряє підпис за допомогою збереженого публічного ключа. Завдяки використанню ключів, користувач може входити в систему без введення пароля, що суттєво знижує ризик фішингу та атак на паролі.

## 2.5 Комбінування методів аутентифікації

Використання лише одного методу аутентифікації вже давно не є ефективним для забезпечення високого рівня безпеки, тому актуальним є впровадження багатофакторної аутентифікації (МФА) з використанням як мінімум двох методів. Такий підхід дозволяє суттєво підвищити надійність системи захисту, адже зловмиснику необхідно обійти кілька рівнів безпеки одночасно, що ускладнює несанкціонований доступ.

Комбінація методу аутентифікації за допомогою знання (пароль) та володіння (SMS-код або апаратний токен) є однією з найпоширеніших форм багатофакторної аутентифікації. Цей підхід став популярним через свою простоту та доступність для користувачів.

У цьому випадку, коли користувач намагається увійти в систему, він спочатку вводить свій пароль, який є відомим лише йому. Цей пароль може бути як простим, так і складним, залежно від політики безпеки конкретного сервісу. Після успішного введення пароля система надсилає одноразовий код, який користувач отримує через SMS на зареєстрований номер телефону або електронну пошту. Цей код діє обмежений час і, як правило, використовується для підтвердження особи. Отримавши код, користувач вводить його в спеціальне поле для підтвердження доступу.

Зручність цього методу полягає в тому, що він дозволяє швидко й легко отримати доступ до системи без потреби в додаткових пристроях, окрім мобільного телефону. Багато користувачів вже мають смартфони, що робить цей варіант дуже доступним. Проте, SMS-коди можуть бути перехоплені зловмисниками, які використовують шкідливе програмне забезпечення або техніки соціальної інженерії. Також варто враховувати, що у разі втрати доступу до мобільного телефону користувач може зіткнутися з труднощами при спробі відновити доступ до свого облікового запису.

Комбінація знання та властивості є одним із найсучасніших підходів до аутентифікації, що передбачає використання пароля разом із біометричними даними, такими як відбиток пальця або розпізнавання обличчя. Цей метод не тільки підвищує зручність для користувачів, але й істотно підвищує рівень безпеки облікових записів.

Перш ніж користувач отримує доступ до системи, він вводить свій пароль, який служить першим рівнем захисту. Навіть якщо цей пароль виявиться скомпрометованим, зловмисник не зможе пройти аутентифікацію без фізичного доступу до біометричних даних. Це робить систему значно стійкішою до атак, оскільки біометричні дані є унікальними для кожної особи і не можуть бути легко скопійовані або підроблені.

Біометричні методи підтвердження особи забезпечують швидку та зручну верифікацію. Користувачі можуть пройти аутентифікацію всього за кілька секунд, не витрачаючи часу на введення складних паролів. Крім того, біометричні технології активно розвиваються, що дозволяє зменшити ризики, пов'язані з помилками розпізнавання або неякісними сканерами.

Комбінація володіння та властивості являє собою потужний метод аутентифікації, який поєднує фізичний токен, такий як смартфон або апаратний ключ, із біометричною аутентифікацією. Цей підхід суттєво підвищує рівень захисту, оскільки він виключає необхідність запам'ятовування паролів, які часто стають слабким місцем в системах безпеки. Замість того щоб покладатися лише на щось, що користувач знає, цей метод вимагає від нього фізичної присутності токена, що робить доступ до системи набагато безпечнішим.

Коли користувач намагається увійти до свого облікового запису, він повинен одночасно застосувати фізичний токен і пройти біометричну перевірку, наприклад, сканування відбитка пальця чи обличчя. Це значно ускладнює життя потенційним зловмисникам, оскільки їм потрібно не лише отримати доступ до фізичного пристрою, але й мати можливість успішно пройти біометричну верифікацію. Такі захисні механізми значно знижують ризики фішингових атак, які часто намагаються обманом отримати паролі, а також атаки методом підбору паролів, оскільки в разі використання цього методу немає потреби у введенні паролів.

Цей безпарольний доступ не лише покращує безпеку, але й підвищує зручність для користувачів. Адже багато людей мають проблеми з управлінням великою кількістю паролів, і часто використовують однакові паролі для кількох облікових записів, що може призводити до серйозних наслідків. Завдяки використанню фізичних токенів і біометрії, користувачі можуть уникнути цих проблем і мати більш зручний і безпечний досвід.

Проте, незважаючи на численні переваги, впровадження такого методу аутентифікації може потребувати значних витрат. Це пов'язано з необхідністю придбання спеціального обладнання для біометричної верифікації та відповідних фізичних токенів. Для великих організацій чи підприємств такі витрати можуть бути обґрунтованими в контексті захисту критично важливих даних, проте для малих бізнесів це може стати серйозним фінансовим навантаженням.

## 2.6 Слабкі сторони МФА

Багатофакторна аутентифікація вважається одним із найбільш ефективних методів захисту даних та облікових записів, значно підвищуючи рівень безпеки в цифровому середовищі порівняно з використанням лише одного паролю, що робить дані менш вразливими до хакерських атак. Однак, як і будь-яка інша технологія, багатофакторна аутентифікація має свої недоліки та слабкі сторони, які можуть вплинути на її ефективність та зручність використання.

Одним із головних недоліків Багатофакторної аутентифікації є те, що вона ускладнює процес входу для користувачів. Більшість методів МФА вимагають додаткових дій, таких як введення одноразового коду з SMS або мобільного додатка, сканування відбитку пальця або використання апаратного токена. Це може

бути незручно для користувачів, особливо якщо вони часто здійснюють вхід на різні пристрої або мають обмежений доступ до додаткових факторів.

Окрім збільшення часу на вхід, складність такої авторизації включає й саме використання додаткових факторів. Частина користувачів не зможе легко освоїти такий метод аутентифікації. Що може призвести до помилок в процесі авторизації, неправильного введення даних, тощо. В такому випадку дехто може взагалі відмовитись від використання засобів МФА.

Ще однією перешкодою впровадження багатофакторної аутентифікації є її вартість, особливо для великих організацій, які мають забезпечити такою системою численні облікові записи та комп'ютери. При розрахунках вартості впровадження МФА береться до уваги розробка та інтеграція самої системи МФА, закупівля апаратних токенів або інших пристроїв для аутентифікації. А також необхідно організувати підтримку користувачів, які можуть стикатись з проблемами під час використання МФА (втрата факторів, складності з входом). Окрім цього потрібно провести навчання персоналу та за необхідності оновити політики безпеки, що також несе додаткові витрати.

При реалізації багатофакторної аутентифікації немалу роль грає сумісність програм та сервісів із додатковими факторами аутентифікації. Не кожна система може легко адаптуватись до роботи з МФА. Старі інформаційні системи або програмне забезпечення можуть не підтримувати сучасні методи багатофакторної аутентифікації, що ускладнює, або робить неможливим, їх інтеграцію. У таких випадках організації повинні або модернізувати свої системи, або залишати їх вразливими для кібератак.

В той же час МФА залежить від доступу до технологій, таких як мобільні мережі або інтернет, для отримання кодів або доступу до аутентифікаторів. В умовах відсутності інтернету або мобільного сигналу користувач може не мати змоги пройти аутентифікацію. Якщо користувач втратить доступ до одного з факторів аутентифікації, виникне багато складнощів із відновленням доступу, в гіршому випадку доступ до облікового запису або даних буде втрачено назавжди.

Втрата фактору аутентифікації може виникнути також при несправності аутентифікатора. Якщо апаратний токен вийде з ладу, знадобиться багато часу на

його заміну або відновлення. При цьому, у випадку заміни токена, доведеться також підключати його як новий фактор аутентифікації й можливі складнощі при відключенні від облікового запису старого токена.

Незважаючи на те, що багатофакторна аутентифікація значно ускладнює життя хакерам, вона не є панацеєю. Зловмисники постійно шукають нові способи обійти захист. Один із таких способів – соціальна інженерія. Соціальна інженерія — це вид атак, який використовує знання про людську психологію та поведінку, щоб отримати доступ до конфіденційної інформації або ресурсів. Зловмисники проводять дослідження жертви, щоб знайти слабкі місця в системі безпеки та зібрати інформацію, яка допоможе їм отримати доступ.

Між іншим отримати доступ також можливо при перехопленні деяких факторів аутентифікації. SMS-коди та електронні листи можуть бути перехоплені через мережеві властивості, або через сторонній доступ до телефону або поштової скриньки. Біометричні дані також можуть бути отримані в результаті витоку даних, або підроблені зловмисниками.

І нарешті, не можна виключити ризик помилкового блокування. Система може помилково визначити ваші дії як підозрілі і заблокувати доступ до облікового запису. З огляду на можливі недоліки, організації та фізичні особи мають ретельно оцінювати ефективність того чи іншого методу багатофакторної аутентифікації та обирати той спосіб, який буде найбільш ефективним та зручним для конкретних цілей та враховувати можливі складнощі.

# 3. АНАЛІЗ ІНСТРУМЕНТІВ ЗАХИСТУ ПРОТИ МОЖЛИВИХ КІБЕРАТАК

## 3.1 Класифікація загроз

Безпека інформаційних систем є однією з найважливіших складових у сучасному світі цифрових технологій, де зростає значення захисту конфіденційних даних і запобігання несанкціонованому доступу. Постійне удосконалення методів аутентифікації і захисту від загроз сприяє підвищенню надійності сучасних систем, проте одночасно виникають нові виклики. У цьому контексті загрози для систем безпеки можна класифікувати за різними ознаками: джерелами загроз, цілями атак, а також методами, які використовуються для їх реалізації. Залежно від характеру і складності атак, системи безпеки можуть бути піддані як зовнішнім, так і внутрішнім загрозам, які впливають на їх цілісність, доступність і конфіденційність.

Актуальність дослідження цих загроз зумовлена постійною еволюцією методів зловмисників, а також новими вразливостями, що з'являються в результаті розвитку технологій. Сучасні методи аутентифікації, такі як багатофакторна аутентифікація, значно зменшують ризики несанкціонованого доступу, проте не виключають можливості для успішних атак.

У таблиці 3.1 розглянуто найімовірніші типи загроз для системи аутентифікації.

Таблиця 3.1 — Класифікація загроз

| **Тип загрози** | **Користувач** | **Пристрій** | **Мережа** | **Сервер** |
|---|---|---|---|---|
| Пасивний | Перехоплення паролів | Аналіз трафіку | Прослуховування | — |
| Активний | Соціальна інженерія | Введення вірусів | DDoS-атаки | Експлуатація вразливостей |

Внутрішні загрози в інформаційних системах – це потенційні ризики, які походять від авторизованих користувачів, таких як співробітники, підрядники або партнери організації. На перший погляд, ці люди можуть здаватися надійними, адже вони мають легальний доступ до ресурсів компанії. Проте саме цей доступ робить їх дії, навмисні чи випадкові, одними з найнебезпечніших.

Одним із поширених джерел внутрішніх загроз є людські помилки. Співробітники можуть ненавмисно видалити важливі файли, некоректно налаштувати системи або випадково розкрити конфіденційну інформацію, наприклад, відповівши на шахрайський лист. Такі помилки найчастіше трапляються через брак знань або неуважність, але наслідки можуть бути катастрофічними.

Інша категорія – зловмисні дії. Іноді мотивовані особистими образами, фінансовими труднощами або тиском конкурентів, співробітники можуть умисно завдавати шкоди. Це може бути крадіжка корпоративної інформації, розголошення комерційної таємниці або саботаж внутрішніх процесів.

Соціальна інженерія є ще одним прикладом. Навіть досвідчені працівники можуть піддатися маніпуляціям зловмисників, які через обман, довіру або психологічний тиск здатні отримати доступ до даних або ресурсів організації.

Таким чином, внутрішні загрози часто є недооціненими, адже вони ховаються «всередині» компанії. Ефективне управління такими ризиками потребує не лише технічних заходів захисту, а й розвитку культури кібербезпеки серед персоналу, постійного навчання і чітких процедур безпеки.

Зовнішні загрози в інформаційних системах – це ризики, які походять від осіб або організацій, що не мають авторизованого доступу до ресурсів компанії. Їх основна мета – порушити роботу систем, викрасти дані чи нанести шкоду репутації. Такі загрози постійно еволюціонують, використовуючи нові вразливості та технології.

Одним із найпоширеніших методів зовнішніх атак є кібератаки. Зловмисники можуть шукати слабкі місця в програмному забезпеченні або мережевій інфраструктурі, щоб проникнути в систему. Вони застосовують складні техніки,

такі як експлойти, шкідливе програмне забезпечення чи атаки типу відмова в обслуговуванні (DDoS), які перевантажують сервери й виводять їх з ладу.

Фішинг – ще одна серйозна загроза. Зловмисники створюють підроблені сайти або розсилають шахрайські електронні листи, які виглядають як повідомлення від довірених джерел. Мета – змусити жертву надати конфіденційну інформацію, наприклад, логіни, паролі або дані банківських карток. Такі атаки є особливо небезпечними через їхню масовість і психологічний вплив на користувачів.

Ще однією технікою є атаки грубою силою, коли зловмисники автоматично підбирають паролі, використовуючи потужні обчислювальні системи. Цей метод хоч і потребує часу, але може бути ефективним, якщо користувачі застосовують слабкі або повторювані паролі.

Зовнішні загрози є постійною загрозою для організацій, оскільки вони часто невидимі до моменту атаки. Захист від них потребує комплексного підходу: постійного оновлення систем, впровадження багатофакторної аутентифікації, моніторингу трафіку та навчання користувачів, аби ті розпізнавали ознаки шахрайства.

Загрози інформаційним системам класифікують не лише за джерелом, але й за цілями, яких прагнуть досягти зловмисники. Таке групування дозволяє краще розуміти потенційні ризики й ефективніше захищати ресурси організації. Основними цілями є отримання несанкціонованого доступу, порушення цілісності даних та порушення доступності системи.

Отримання несанкціонованого доступу — це одна з найпоширеніших цілей зловмисників, які прагнуть проникнути в інформаційну систему або базу даних без відповідного дозволу. Така загроза є особливо небезпечною, адже надає атакуючим можливість викрасти, змінити чи знищити конфіденційну інформацію, що може призвести до значних фінансових або репутаційних втрат для організації.

Зловмисники використовують різноманітні техніки для досягнення своєї мети. Одним із найпростіших, але водночас ефективних методів є підбір паролів. Якщо користувачі застосовують слабкі або поширені паролі, наприклад, «123456»

чи «password», це значно полегшує злам. Автоматизовані системи можуть у короткі строки перевіряти тисячі можливих комбінацій, доки не знайдуть правильну.

Інший підхід базується на використанні вразливостей у програмному забезпеченні. Наприклад, недоліки в коді вебдодатків чи недостатній захист мережевих протоколів можуть дати зловмисникам можливість проникнути до системи, обходячи звичайні механізми захисту. Такі вразливості часто виявляються через неправильну конфігурацію систем або несвоєчасне оновлення програм.

Окрему небезпеку становлять спроби обходу двофакторної аутентифікації. Хоч цей метод значно підвищує рівень безпеки, зловмисники можуть застосовувати техніки перехоплення одноразових кодів або створення фішингових сторінок, щоб отримати інформацію про облікові дані користувачів.

Мета цих дій отримання контролю над системою чи інформаційними ресурсами, використовуючи їх для викрадення даних, фінансового шахрайства або подальших атак.

Порушення цілісності даних це одна з ключових загроз для інформаційних систем, яка полягає у спотворенні, зміні або знищенні даних. Цілісність даних є критично важливою, особливо для організацій, які працюють з фінансовою, медичною чи юридичною інформацією. Порушення цього принципу може спричинити серйозні наслідки, такі як помилки у розрахунках, неправильні бізнес-рішення або навіть загроза життю у випадку медичних записів.

Зловмисники, які порушують цілісність даних, можуть переслідувати різні цілі: дискредитацію організації, саботаж, шахрайство або створення умов для подальших атак. Боротися з такими загрозами можна за допомогою багаторівневого захисту: обмеження доступу до даних, впровадження систем виявлення змін, регулярне резервне копіювання та аудит інформаційних систем. Важливо також навчати персонал, щоб зменшити ризик людських помилок, які можуть сприяти таким інцидентам.

Порушення доступності системи є серйозною загрозою для інформаційних систем, яка спрямована на те, щоб зробити ресурси або сервіси недоступними для їхніх легітимних користувачів. Така загроза може мати катастрофічні наслідки, особливо для організацій, чия робота залежить від постійного функціонування

інформаційних технологій, наприклад, банків, медичних установ чи онлайн-сервісів.

Одним із найпоширеніших методів порушення доступності є DDoS-атаки (розподілені атаки типу відмова в обслуговуванні). Під час таких атак зловмисники одночасно надсилають величезну кількість запитів до сервера, що призводить до перевантаження системи. Внаслідок цього сервер не може обробляти запити від реальних користувачів і стає недоступним. Для проведення DDoS-атак часто використовуються бот-мережі, які складаються з тисяч або навіть мільйонів заражених пристроїв.

Загрози для інформаційних систем класифікуються не лише за методами, які використовуються для реалізації атак. Сучасні зловмисники мають у своєму розпорядженні широкий спектр технік, які дозволяють порушувати безпеку систем, використовуючи слабкі місця в технологіях, поведінці користувачів або фізичних пристроях.

Соціальна інженерія, як вже згадувалось, є однією з найбільш небезпечних загроз у сфері інформаційної безпеки, адже вона базується не на технічних вразливостях систем, а на людському факторі. Зловмисники використовують психологічні маніпуляції, щоб отримати доступ до конфіденційної інформації, зламати системи чи завдати іншої шкоди.

Одним із найпоширеніших проявів соціальної інженерії є фішинг. У цьому випадку зловмисники створюють електронні листи або вебсайти, які виглядають як офіційні ресурси, наприклад, банку чи популярної онлайн-платформи. Користувача просять ввести свої облікові дані, мотивуючи це необхідністю підтвердити акаунт, змінити пароль або вирішити іншу «проблему». Отримані таким чином дані одразу потрапляють до рук атакуючих і це стає вже наполовину отриманим доступом до облікового запису.

Ще один метод це виманювання інформації через безпосередню комунікацію. Наприклад, зловмисник може телефонувати жертві, представляючись співробітником технічної підтримки, і переконувати надати пароль, код підтвердження або інші критично важливі дані.

Особливість соціальної інженерії в тому, що вона не потребує складних технічних знань. Її ефективність залежить від майстерності маніпуляцій і недостатньої підготовки жертв до подібних атак.

Атаки на паролі є одним із найпоширеніших методів зламу інформаційних систем, адже паролі залишаються основним засобом аутентифікації для більшості користувачів. Зловмисники використовують різноманітні техніки, щоб отримати доступ до облікових записів, обходячи захисні механізми або експлуатуючи слабкі місця у створенні та зберіганні паролів.

Одним із найпростіших і водночас найефективніших методів є атак и грубою силою. Вони передбачають систематичний перебір усіх можливих комбінацій символів, доки не буде знайдено правильний пароль. Хоча цей процес може зайняти багато часу, сучасні комп’ютери здатні виконувати мільйони перевірок щосекунди, що робить слабкі паролі особливо вразливими.

Ще одним поширеним методом є словникові атаки, які працюють за принципом використання списків поширених або передбачуваних паролів. Такі списки можуть включати популярні комбінації на кшталт «123456», «password» чи «qwerty», які користувачі часто обирають через зручність запам’ятовування. Словникові атаки значно прискорюють процес зламу, якщо користувачі не дотримуються рекомендацій щодо створення складних паролів.

Більш технологічно складним є використання так званої райдужної таблиці, тобто попередньо створених хеш-таблиць. У цих таблицях містяться хеші паролів і відповідні їм комбінації символів. Зловмисники можуть швидко знайти відповідність між хешем, збереженим у базі даних, і фактичним паролем, що дозволяє обійти систему аутентифікації без прямого доступу до паролів.

Атаки на паролі можуть включати й інші методи, такі як перехоплення паролів у незашифрованому трафіку або використання зламаних баз даних із попередніх витоків. Часто зловмисники використовують паролі, які були вкрадені з інших систем, оскільки багато користувачів схильні повторно використовувати ті самі комбінації.

Атаки на біометричні дані стають все більш актуальними з розвитком технологій, що використовують біометричні методи аутентифікації. Біометрія, така

як розпізнавання обличчя, відбитків пальців чи райдужної оболонки ока, забезпечує зручний і надійний спосіб підтвердження особи, оскільки ці дані є унікальними для кожної людини. Однак, як і будь-яка технологія, біометричні системи мають свої вразливості, які можуть бути використані зловмисниками.

Один із найпоширеніших методів атак на біометричні дані — це підробка відбитків пальців. Зловмисники можуть створювати копії відбитків, використовуючи різні матеріали, наприклад, силікон або гель, щоб імітувати реальний відбиток. Ці копії можуть бути виготовлені на основі фотографій, отриманих через неякісне сканування чи за допомогою спеціальних пристроїв для зняття відбитків. Технології сканування відбитків пальців, які використовуються в багатьох смартфонах і платіжних системах, можуть бути вразливими до таких атак, якщо не використовуються додаткові заходи перевірки, наприклад, аналіз пульсу або теплоємності.

Розпізнавання інших біометричних характеристик, таких як райдужна оболонка ока або голос, також має свої вразливості. Наприклад, голосові біометричні системи можуть бути зламані за допомогою запису голосу людини або використання технологій синтезу мови. Сканери райдужної оболонки можуть бути обмануті за допомогою високоякісних зображень або 3D-моделей ока, що робить їх схожими на оригінальні.

Атаки на апаратні ключі стали популярним методом зламу систем, що використовують багатофакторну аутентифікацію для підвищення рівня безпеки. Апаратні ключі, такі як USB-токени або смарт-карти, призначені для захисту облікових записів та систем, додаючи додатковий рівень захисту після введення пароля або пін-коду. Однак, незважаючи на високий рівень безпеки, апаратні ключі не є неприступними і можуть стати ціллю для зловмисників, особливо коли йдеться про фізичний доступ до пристрою.

Одним з основних методів атаки є клонування апаратних ключів. Це можливо, якщо зловмисник здобуде фізичний доступ до пристрою, на якому зберігається секретна інформація або ключ. Клонування може бути здійснено за допомогою спеціальних пристроїв, які копіюють інформацію з апаратного ключа, створюючи його точну копію.

Іншим методом атаки є здійснення фізичного доступу до пристроїв, які використовуються для захисту ключів. Зловмисник може фізично зламати або модифікувати пристрій, щоб витягти з нього секретні дані або зламати механізм захисту. Це особливо актуально для смарт-карт або USB-ключів, що мають обмежену кількість захисних механізмів від стороннього втручання. У разі доступу до таких пристроїв зловмисник може спробувати обійти вбудовані алгоритми шифрування або інші механізми захисту.

Атаки на протоколи аутентифікації спрямовані на компрометацію самого процесу підтвердження особи, що дозволяє зловмисникам обійти захист систем і отримати доступ до конфіденційної інформації. Протоколи аутентифікації є основним елементом безпеки, тому атаки на них є одними з найнебезпечніших для інформаційних систем. Однією з найбільш розповсюджених атак є атаки типу «людина посередині», під час яких зловмисник перехоплює комунікацію між двома сторонами, наприклад, між користувачем і сервером. Під час такої атаки зловмисник може змінювати, читати або перенаправляти повідомлення, що дозволяє йому отримати доступ до чутливих даних, таких як паролі, токени або інші облікові дані.

Інша поширена атака на протоколи аутентифікації — це replay-атака. Вона полягає в тому, що зловмисник перехоплює аутентифікаційний запит або відповідь, наприклад, під час введення пароля або отримання одноразового коду, і відправляє його повторно. Оскільки в такому випадку аутентифікація проводиться за допомогою збереженого запиту, система не розпізнає, що доступ був отриманий несанкціоновано. Цей тип атак може бути ефективним, якщо протокол аутентифікації не має механізмів захисту від повторного використання повідомлень, таких як одноразові паролі або таймстампи.

Важливим аспектом є те, що багато сучасних систем використовують комбінацію паролів і додаткових методів аутентифікації, таких як смарт-карти, апаратні ключі чи біометрія, однак зловмисники продовжують використовувати різноманітні методи для компрометації цих протоколів.

У сфері багатофакторної аутентифікації (БФА) відомо чимало випадків успішних атак, де зловмисники змогли обійти систему аутентифікації, незважаючи на використання додаткових методів захисту.

Атака на систему Google через SIM-заміну у 2017 році. В тій ситуації злочинці скористалися методом заміни SIM-карти (SIM swapping), щоб обійти захист, використовуючи двофакторну аутентифікацію (2FA) через SMS. Вони отримали контроль над телефонним номером користувача і, таким чином, змогли отримати доступ до його акаунтів, навіть незважаючи на те, що активована двофакторна аутентифікація. Ця атака стала однією з найбільш резонансних, оскільки постраждав один із топ-менеджерів Google, а виявлена вразливість демонструє, наскільки важливою є безпека телефонних номерів у контексті 2FA.

Атака на криптовалютні біржі (2019-2020): Кілька криптовалютних бірж, таких як Binance, зазнали успішних атак через компрометацію методів двофакторної аутентифікації. У деяких випадках зловмисники використовували фішинг для отримання облікових даних користувачів і доступу до акаунтів, які мали активовану 2FA через апаратні ключі чи SMS-коди. В результаті хакери змогли зняти великі суми криптовалют з акаунтів постраждалих користувачів.

Атака на Twitter (2020): Під час цієї атаки група молодих зловмисників отримала доступ до акаунтів відомих публічних осіб і політиків за допомогою внутрішнього доступу до інтерфейсу адміністратора в системі. Зловмисники, використовуючи SIM-swapping, отримували доступ до акаунтів співробітників служби підтримки Twitter, що дозволяло їм скидати паролі та публікувати фейкові повідомлення.

Причини успіху атак на системи багатофакторної аутентифікації різняться в залежності від конкретного випадку, але все ще можна виділити кілька загальних факторів, які притаманні більшості атак.

Перш за все це вразливості в каналах зв'язку. У випадках, де використовуються SMS або голосові дзвінки для 2FA, вразливості у мобільних мережах або технології заміни SIM-карт можуть стати серйозним джерелом проблем. Атаки на систему «SIM swapping», коли зловмисники отримують доступ до SIM-карти жертви, дозволяють їм обійти 2FA, що значно послаблює захист.

Використання дюдського фактору і соціальної інженерії насправді мають неабияку ефективність. У багатьох випадках успіх атак можна пояснити використанням соціальної інженерії, коли зловмисники обманом отримують облікові дані або фактичний доступ до користувацьких акаунтів. Це можуть бути фішингові атаки або маніпуляції з персоналом компанії.

Деякі методи аутентифікації, зокрема апаратні ключі або біометрія, не завжди забезпечують стійкий захист. З розвитком інформаційних технологій та зростанням загроз зловмисники все частіше адаптують свої методи атак до нових методів аутентифікації.

Використання біометричних даних, таких як відбитки пальців або розпізнавання обличчя, стає все більш популярним, проте це створює нові вразливості. Зловмисники вивчають способи підробки цих даних (наприклад, створення фальшивих відбитків пальців або використання фото для фальсифікації систем розпізнавання обличчя). Технології виявлення підробок поки не настільки ефективні, щоб запобігти таким атакам.

Протоколи аутентифікації, які базуються на SMS або електронній пошті, стають все менш надійними, оскільки зловмисники можуть використовувати атаки на ці канали. Тому все більше організацій переходять на більш безпечніші протоколи, такі як додатки для генерації кодів або апаратні токени, що знижують ризики.

Незважаючи на те, що банаьофакторна аутентифікація суттєво підвищує рівень безпеки, зловмисники вивчають способи обходу таких систем. Наприклад, нові атаки на апаратні токени або використання шкідливого програмного забезпечення для перехоплення одноразових паролів (OTP).

Атаки на системи багатофакторної аутентифікації демонструють, що навіть найсучасніші технології не є повністю захищеними від зловмисників. Тому важливо постійно оновлювати системи безпеки, підвищувати обізнаність користувачів та використовувати кілька рівнів захисту для забезпечення максимальної безпеки. Враховуючи зростання складності атак і нові загрози, необхідно орієнтуватися на комплексний підхід, який поєднує як технічні рішення, так і заходи з навчання персоналу.

## 3.2 Інструменти та шляхи захисту від кібератак

Fail2ban — це інструмент для захисту серверів від атак брутфорсу, який автоматично блокує підозрілі IP-адреси після кількох невдалих спроб аутентифікації. Він аналізує логи сервісів (SSH, Apache, Nginx, FTP) і визначає підозрілу активність. Якщо з певної IP-адреси спостерігається багато невдалих спроб входу, Fail2ban блокує її через фаєрвол, зменшуючи ймовірність успішної атаки.

Fail2ban підтримує налаштування фільтрів для різних сервісів, має можливість автоматично відправляти сповіщення та запускати додаткові скрипти. Інструмент гнучкий, дозволяє налаштовувати параметри блокування і інтегруватися з іншими системами безпеки.

Конфігурація Fail2ban здійснюється через кілька основних файлів, що дозволяють налаштувати різні аспекти роботи цього інструмента.

/etc/fail2ban/jail.conf — це основний конфігураційний файл, який визначає, які сервіси потрібно моніторити, а також містить правила для блокування підозрілих IP-адрес.

/etc/fail2ban/filter.d/ — в цій директорії знаходяться фільтри для різних сервісів. Фільтри визначають, які шаблони для логів використовувати для виявлення підозрілих дій.

/etc/fail2ban/action.d/ — тут зберігаються сценарії дій, що виконуються після спрацювання фільтру. Це можуть бути різні методи блокування, наприклад, через фаєрвол, що перешкоджає подальшим спробам підключення з підозрілих IP-адрес.

Щоб налаштувати Fail2ban для захисту SSH, необхідно відредагувати конфігураційний файл jail.local або, якщо цей файл не існує, редагувати jail.conf. У цьому файлі можна вказати параметри для моніторингу підключень через SSH і блокування підозрілих IP-адрес.

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
```

maxretry = 3

bantime = 600

findtime = 600

Параметр enabled вмикає Fail2ban для моніторингу підключень через SSH. Якщо значення enabled = true, то Fail2ban почне перевірку підключень за заданим фільтром. Далі port вказує порт, на якому працює SSH, зазвичай це порт 22. Команда filter визначає фільтр, який використовуватиметься для пошуку неуспішних спроб входу через SSH. Для SSH існує стандартний фільтр sshd, який шукає відповідні записи в логах про неуспішні спроби авторизації. Шлях до лог-файлу вказується у рядку logpath, де Fail2ban буде шукати записи про невдалі спроби входу. Для SSH це зазвичай файл /var/log/auth.log.

Після невдалих спроб входу вказаних у рядку maxretry Fail2ban заблокує IP-адресу. В даному прикладі, після 3-х невдалих спроб доступу, IP-адреса буде заблокована на час вказаний у bantime в секундах, тобто на 10 хвилин. У рядку findtime вказується період часу в секундах, протягом якого Fail2ban відслідковує невдалі спроби входу. Якщо за 600 секунд (10 хвилин) кількість невдалих спроб входу перевищує значення maxretry, то IP-адреса буде заблокована.

Fail2ban використовує фільтри для пошуку конкретних патернів у логах, що дозволяє виявляти підозрілі або несанкціоновані дії. Фільтр для SSH зберігається в файлі sshd.conf

[Definition]

failregex = ^%(__prefix_line)sFailed password for .* from <HOST> port \d+ ssh2$

ignoreregex =

Регулярний вираз failregex шукає рядки в логах, що вказують на невдалу спробу входу через SSH. Шаблон <HOST> замінюється на IP-адресу, яка намагається підключитися. Це дозволяє Fail2ban виявляти конкретні спроби доступу з несанкціонованих IP-адрес.

Вираз ignoreregex дозволяє визначити шаблони, які будуть ігноруватися. Якщо у логах є рядки, що відповідають цьому виразу, Fail2ban не буде на них реагувати. Наприклад, можна ігнорувати певні типи спроб, які не є підозрілими.

WAF (Web Application Firewall) — це інструмент безпеки, який захищає веб-додатки від різноманітних атак, зокрема SQL-ін'єкцій, міжсайтних скриптів (XSS), атак типу «відмова в обслуговуванні» (DoS) та інших уразливостей на рівні додатків. WAF працює як проміжний шар між користувачем і веб-додатком, аналізуючи HTTP/HTTPS трафік, фільтруючи шкідливі запити та дозволяючи лише легітимний доступ.

WAF може бути розміщений як на мережевому рівні (апаратний або хмарний WAF), так і на рівні додатка (програмний WAF). Він використовує різні методи захисту, включаючи підписки для виявлення атак, аналіз поведінки, правила на основі контексту і політики доступу. Основною перевагою WAF є те, що він забезпечує додатковий рівень захисту для веб-додатків, навіть якщо інші механізми безпеки не виявили уразливості.

ModSecurity — це відкритий веб-захисний модуль для веб-серверів Apache, Nginx, та IIS, який працює як веб-застосунковий фаєрвол (WAF). Він дозволяє захищати веб-додатки від атак, таких як SQL-ін'єкції, міжсайтні скрипти (XSS), атаки типу DoS та інші уразливості на рівні додатків.

```
SecRule ARGS|ARGS_NAMES|REQUEST_HEADERS|XML:/* "(union.*select.*\()" \
    "id:1000001,phase:2,deny,status:403,msg:'SQL Injection Attempt'"
```

Команда ARGS перевіряє всі параметри запитів, що передаються через URL або форму. Це дозволяє виявляти SQL-ін'єкції, які можуть бути вставлені в ці параметри. REQUEST_HEADERS перевіряє заголовки запитів. Атаки можуть також приховуватися в заголовках HTTP-запитів, тому це важливий компонент для виявлення небезпечних запитів. XML:/ в свою чергу перевіряє XML-параметри в запитах. Якщо веб-сайт приймає запити в форматі XML, то це правило дозволяє також аналізувати їх на наявність небезпечних шаблонів.

Міжсайтні скрипти (XSS) можуть використовуватися для виконання шкідливого JavaScript-коду на веб-сторінках.

```
SecRule ARGS|ARGS_NAMES|REQUEST_HEADERS|XML:/* "<script.*?>" \
    "id:1000002,phase:2,deny,status:403,msg:'XSS Attack Attempt'"
```

Правило шукає тег <script> або інші патерни, пов'язані з XSS-атаками, у запитах. Правило phase:2 застосовується після аналізу заголовків запиту, але до передачі запиту в веб-додаток. Якщо знайдено співпадіння з патерном deny блокує запит та status:403 відповідає помилкою 403 (заборонено).

Щоб захистити ваш сервер від DoS або атак Грубою силою, можна створити правило для обмеження кількості запитів з одного IP за певний період часу:

```
SecRule IP:REQ_COUNT "@ge 100" \
    "id:1000005,phase:1,deny,status:429,msg:'Too Many Requests from IP'"
```

В наведеному прикладі IP:REQ_COUNT це лічильник запитів з певної IP-адреси. Параметр @ge 100 вказує на те, що правило спрацьовує, коли IP-адреса зробила 100 або більше запитів. Це правило блокує запити і відповідає помилкою 429 (занадто багато запитів).

Одним з неменш важливих елементів при аутентифікації є захищеність паролю від зламу. Існують різні способи його захисту і ModSecurity пропонує ще один спосіб за допомогою обмеження довжини параметрів:

```
SecRule REQUEST_ARGS:"^password$" "@gt 32"\
 "id:3,phase:2,t:none,msg:'Password too long',deny,log,auditlog"
```

У наведеному правилі SecRule REQUEST_ARGS:"^password$" вказує, що правило буде застосовуватися до параметра з ім'ям «password», який передається в запиті. Частина "@gt 32" означає, що значення параметра «password» повинно бути порівняне за довжиною. Оператор "@gt" означає «більше ніж». Тобто, якщо значення параметра більше 32 символів, правило спрацює.

"id:3,phase:2,t:none,msg:'Password too long',deny,log,auditlog" містить декілька параметрів правила. id:3 це унікальний ідентифікатор правила для подальшої ідентифікації та налаштування. phase:2 це фаза виконання правила. t:none це тип перевірки, який в даному випадку не використовує додаткову перевірку.

msg:'Password too long': Повідомлення, яке буде записано в лог, якщо правило спрацює.Якщо правило спрацювало, параметр deny відхилить запит. А log,auditlog запише інформацію про подію в лог-файли.

Cloudflare — це сервіс для захисту та оптимізації веб-сайтів. Він працює як Content Delivery Network (CDN), кешуючи контент на серверах по всьому світу, що

прискорює завантаження сайтів і знижує навантаження на сервери. Основна функція Cloudflare — це захист від атак, таких як DDoS, SQL-ін'єкції, XSS та інших загроз, через фільтрацію трафіку перед тим, як він досягне сайту.

```
config.rate_limiting = {
  mode: "standard",
  interval: "1s",
  threshold: 5,
};
```

Параметр mode встановлює тип обмеження. Interval визначає інтервал часу для обмеження. В даному випадку 1s означає, що обмеження застосовуються до кожної секунди. Параметр threshold вказує максимальну кількість запитів, які можуть бути зроблені з однієї IP-адреси за визначений інтервал часу. У даному прикладі значення 5 означає, що дозволено не більше 5 запитів за секунду.

Це правило обмежує кількість запитів, які може здійснити одна IP-адреса за короткий проміжок часу. Це дозволяє ефективно запобігти атакам типу DDoS (де зловмисники намагаються перевантажити сервер численними запитами) і брутфорс-атакам (коли спроби підбору паролів виконуються за допомогою великої кількості запитів).

Для захисту від CSRF-атак використовується правило:

```
config.waf = {
  mode: "on",
  custom_rules: [
    {
      mode: "block",
      match: "csrf",
      condition: "http.request.header.origin != 'https://yourdomain.com'",
    },
  ],
};
```

Це правило блокує запити, які надходять з інших доменів, якщо сервер не очікує таких запитів.

Для захисту від DoS/DDoS можна використовувати Fail2ban разом з iptables для блокування зловмисних IP-адрес, які генерують високий рівень трафіку. Fail2Ban і iptables — це потужне поєднання для захисту серверів від зловмисників, зокрема від атак грубою силою, зловмисних сканувань і інших загроз, які спричиняють надмірне навантаження на сервер, або спробу зламати паролі облікових записів. Fail2Ban — це інструмент для моніторингу лог-файлів і автоматичного блокування IP-адрес, які здійснюють підозрілі або шкідливі дії. Iptables — це інструмент для налаштування брандмауера в Linux, що дозволяє управляти доступом до серверів на рівні мережі.

Fail2Ban сканує логи сервера на наявність підозрілих або небажаних дій (наприклад, багато невдалих спроб входу через SSH або HTTP). Коли Fail2Ban виявляє таку активність, він автоматично додає відповідні iptables правила для блокування IP-адреси, з якої надходять шкідливі запити.

IDS (Intrusion Detection System) і IPS (Intrusion Prevention System) — це системи для захисту комп'ютерних мереж і серверів від зловмисних атак.

IDS виявляє шкідливу активність, аналізуючи мережевий або системний трафік, але не блокує її. Система лише генерує сповіщення про підозрілі події, щоб адміністратор міг реагувати. Наприклад, Snort і Suricata — популярні інструменти IDS, які аналізують пакети і виявляють підозрілі активності, такі як атака грубою силою або сканування портів.

IPS працює подібно до IDS, але додає ще одну функцію — активне блокування загроз. Якщо IPS виявить шкідливий трафік, він може заблокувати зловмисні пакети або навіть відключити з'єднання. Це дозволяє системам оперативно реагувати на атаки, наприклад, Suricata може працювати як IPS і блокувати атаки в реальному часі.

Базовий конфігураційний файл Snort має такий вигляд:

```
config version=3.0
# Загальні налаштування
output tcp_last_resort 127.0.0.1
input eth0
# Завантаження сигнатур
```

```
var RULE_PATH /etc/snort/rules
include $RULE_PATH/local.rules
include $RULE_PATH/snort.conf
```

Цей конфігураційний файл вказує, що Snort буде слухати інтерфейс eth0 і записувати результати в лог-файл. Також задається шлях до каталогу з правилами.

Правило alert tcp any any -> any 21-25,80,443 (msg:"TCP Port Scan"; sid:10000; rev:1;) спрацьовує, коли виявлено спробу підключення до портів 21, 22, 80 або 443 з будь-якого IP-адреси.

Базовий конфігураційний файл Suricata має наступний вигляд:

```
version: "4.0"
interface: eth0
af-packet: 0
http: enabled
```

Цей конфігураційний файл вказує, що Suricata буде слухати інтерфейс eth0 і аналізувати HTTP-трафік. Для виявлення спроби надіслати шкідливий вміст буде використовуватись наступне правило:

```
- rule:
    id: 10002
    rev: 1
    msg: "Exploit attempt"
    detection:
      flow: to_server
      http:
        request:
          method: POST
          uri: "/admin/login.php"
          body:
            content: "evil_payload"
```

Воно спрацьовує, коли виявлено POST-запит до URL "/admin/login.php" з шкідливим вмістом.

Для Snort та Suricata також доступні додаткові можливості. Вони дозволяють аналізувати різні протоколи (HTTP, FTP, SMTP тощо) та виявляти атаки, специфічні для цих протоколів. Системи об'єднують дані з різних джерел для виявлення складних атак. А також використовують машинне навчання для виявлення нових типів атак.

Rate limiting (обмеження швидкості) — це механізм, який обмежує кількість запитів, які клієнт може зробити до сервера за певний проміжок часу, наприклад, намагаючись увійти в обліковий запис. Обмеження швидкості може допомогти зупинити певні види зловмисної діяльності ботів. Цей механізм використовується для захисту серверів від перевантаження, а також для запобігання зловмисним атакам, таким як DDoS. І так само даний механізм допомагає зупинити спроби зламу паролів атаками грубої сили та словником. Він також може зменшити навантаження на веб-сервери.

За допомогою Python та бібліотеки Redis можна реалізувати механізм Rate Limiting, який обмежує кількість запитів до системи:

```
from flask import Flask, request
import redis

app = Flask(__name__)
redis_client = redis.Redis(host='localhost', port=6379, db=0)

def get_client_ip():
    return request.remote_addr

def limit_reached(ip):
    # Налаштування ліміту
    limit = 100  # 100 запитів за хвилину
    period = 60  # 1 хвилина

    key = f"rate_limit:{ip}"
    current_count = int(redis_client.get(key) or 0)
```

```
    redis_client.incr(key)
    redis_client.expire(key, period)

    return current_count >= limit

@app.route('/protected_resource')
def protected_resource():
    ip = get_client_ip()
    if limit_reached(ip):
        return "Rate limit exceeded", 429
    # Обробка запиту
    return "Resource accessed"
```

Даний код для кожного клієнта (ідентифікуємого за IP-адресою) в Redis зберігає лічильник, який показує кількість запитів за певний період. Функція limit_reached перевіряє, чи не перевищив клієнт встановлений ліміт запитів.

Змінні limit і period визначають максимальну кількість дозволених запитів та період, за який цей ліміт діє. Ці значення можна налаштовувати залежно від потреб.

Функція redis_client.incr(key) збільшує лічильник на одиницю для кожного нового запиту. Функція redis_client.expire(key, period) встановлює час життя ключа в Redis, після закінчення якого лічильник скидається.

Якщо клієнт перевищив ліміт, функція повертає відповідь 429 Too Many Requests, що сигналізує про перевищення ліміту. Якщо ліміт не перевищено, виконується обробка запиту.

VeraCrypt — це потужне, безкоштовне та відкрите програмне забезпечення, призначене для надійного шифрування даних. Воно дозволяє створювати зашифровані томи, які можна використовувати як звичайні диски, після введення пароля чи використання ключового файлу. Програма являє собою своєріний сейф для інформації, який захищає її від несанкціонованого доступу.

Принцип роботи VeraCrypt полягає в шифруванні даних «на льоту». Це означає, що дані автоматично шифруються під час запису на диск і дешифруються при зчитуванні, без помітного впливу на продуктивність. Програма підтримує різні

алгоритми шифрування, такі як AES, Serpent, Twofish, а також їх комбінації для підвищення надійності. Користувачі можуть створювати:

1) Зашифровані контейнери — файли, які діють як віртуальні зашифровані диски.

2) Повне шифрування дисків — захист для всього розділу або фізичного диска.

3) Системне шифрування — повний захист операційної системи.

VeraCrypt також підтримує приховані томи, які дозволяють створити «прихований» шар у зашифрованому контейнері. Це забезпечує додаткову конфіденційність, оскільки навіть під тиском користувач може розкрити пароль від зовнішнього тому, не викриваючи прихованого. Програма є кросплатформенною та доступна для Windows, macOS та Linux.

OpenVPN — це програмне рішення з відкритим кодом для створення захищених віртуальних приватних мереж (VPN). Воно використовується для шифрування інтернет-з’єднань, забезпечення конфіденційності даних та анонімності користувачів.

OpenVPN створює захищений тунель між клієнтом і сервером, шифруючи весь переданий трафік. Це дозволяє захищати дані під час їх передачі через публічні мережі, наприклад Wi-Fi, приховувати реальну IP-адресу користувача, забезпечуючи анонімність та отримувати доступ до географічно обмеженого контенту, підключаючись до серверів у потрібній країні.

OpenVPN використовує надійні криптографічні протоколи, такі як TLS/SSL, а також підтримує різні алгоритми шифрування, наприклад AES-256, що забезпечує високий рівень безпеки.

# ВИСНОВКИ

Дослідження багатофакторної аутентифікації підтвердило її ефективність у забезпеченні високого рівня безпеки інформаційних систем. Аналіз сучасних методів показав, що комбінація кількох факторів аутентифікації, таких як паролі, біометричні дані та одноразові токени, значно ускладнює реалізацію атак на облікові записи користувачів. Особливо перспективними є адаптивні підходи, які враховують контекст доступу, наприклад, місцезнаходження або поведінкові шаблони. Світові тенденції свідчать про активне впровадження криптографічних рішень у багатофакторну аутентифікацію.

Отримані результати мають широкі перспективи застосування. Зокрема, вони можуть бути використані у корпоративних системах для захисту внутрішніх ресурсів, у державних електронних сервісах для захисту персональних даних громадян, у фінансових платформах для забезпечення безпеки онлайн-транзакцій, а також у хмарних сервісах, де адаптивна багатофакторна аутентифікація здатна знизити ризики несанкціонованого доступу. Впровадження біометричних даних як додаткового рівня захисту поступово стає стандартом для багатьох галузей.

З наукової точки зору було зроблено значний внесок у вдосконаленні теоретичних основ багатофакторної аутентифікації та вивченні сучасних загроз. Практична значущість роботи полягає в можливості інтеграції запропонованих підходів у програмні та апаратні рішення для підвищення рівня безпеки.

Для подальшого розвитку багатофакторної аутентифікації доцільно зосередитися на дослідженні адаптивних моделей, які враховують динамічні ризики під час доступу до систем. Інтеграція цих методів із сучасними системами штучного інтелекту дозволить створювати більш ефективні механізми кіберзахисту. Результати дослідження можуть бути впроваджені у системах фінансових, державних та хмарних організацій, що дозволить забезпечити ще вищий рівень безпеки та зручності для користувачів.

У проведеному дослідженні були систематизовані основні загрози для інформаційних систем, а також проаналізовані сучасні інструменти захисту, такі як

Fail2Ban, WAF, IDS/IPS і шифрування даних. Отримані результати підтверджують, що використання цих технологій значно знижує ризики компрометації конфіденційності, цілісності та доступності інформації. Особлива увага приділена загрозам, спрямованим на протоколи аутентифікації, методам соціальної інженерії та можливостям багатофакторної аутентифікації, що відповідає світовим тенденціям у сфері кіберзахисту.

Результати дослідження мають практичну цінність у різних сферах, які потребують високого рівня інформаційної безпеки. Зокрема, запропоновані підходи можуть бути використані для захисту державних установ від несанкціонованого доступу та кібершпіонажу, у фінансовому секторі для безпеки транзакцій та збереження клієнтських даних, у критично важливих інфраструктурах, таких як енергетика та телекомунікації, а також у хмарних сервісах для підвищення стійкості до атак.

Узагальнення класифікації загроз і аналіз методів захисту сприяють подальшому розвитку теорії кібербезпеки. Практичні рішення, описані в роботі, можуть бути інтегровані у сучасні системи захисту, підвищуючи їхню ефективність.

Для подальшого розвитку у цій сфері доцільно вдосконалювати алгоритми виявлення загроз, зокрема таких, що базуються на соціальній інженерії та спрямовані на аутентифікаційні протоколи. Важливо інтегрувати сучасні інструменти, такі як WAF і IDS/IPS, із системами штучного інтелекту для підвищення швидкості й ефективності реагування на загрози.

Результати цього дослідження закладають основу для впровадження комплексного підходу до захисту інформаційних систем, що дозволить суттєво підвищити їхню безпеку у сучасному цифровому середовищі.

# ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гуо Ю. та ін. Технологія захисту інформації на основі багатофакторної аутентифікації // 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC) : матеріали конф. – Tumkur, Karnataka, India, 2022. – С. 1-5.

2. Альрусан М., Інтригіла Б. Мультифакторна автентифікація для електронних урядових послуг з використанням смартфонних додатків та біометричної ідентифікації // Journal of Computer Science. – 2020. – Т. 16, № 2. – С. 217-224.

3. Жакомм С., Кремер С. Розширений формальний аналіз протоколів багатофакторної аутентифікації // ACM Transactions on Privacy and Security. – 2021. – Т. 24, № 2. – С. 1-34.

4. Русдан М., Манурунг Д. Проектування аутентифікації користувачів на основі багатофакторної аутентифікації в бездротових мережах // Journal of Advanced Research in Dynamical and Control Systems. – 2020. – Т. 12, № 1. – С. 201-209.

5. Беззатєєв С., Давидов В., Ометов А. Про розподіл секрету з використанням полінома Ньютона для багатофакторної аутентифікації // Cryptography. – 2020. – Т. 4, № 34. – С. 1-11.

6. Ханкарі Н. Б., Кале Г. В. Генерація одноразового пароля для багатофакторної аутентифікації з використанням графічного пароля // International Journal Of Engineering Research and General Science. – 2020. – Т. 3, № 5. – С. 489-494.

7. Камау Дж., Мвуря М. Огляд проблем безпеки двофакторної аутентифікації в кіберпросторі // International Journal of Advanced Computer Technology. – 2022. – Т. 11, № 5. – С. 1-6.

8. Валлабху Х., Сатьянараяна Р. В. Біометрична аутентифікація як хмарна послуга: Нове рішення // International Journal of Soft Computing and Engineering (USCE). – 2012. – Т. 2, № 4. – С. 163-165. – ISSN 2231–2307.

9. Прабакаран Д., Рамачандран С. Багатофакторна аутентифікація для захищених фінансових транзакцій у хмарному середовищі // Computers Materials & Continua. – 2022. – Т. 70, № 1. – С. 1781-1798.

10. Микконен Т., Кучерявый Ю. Многофакторная аутентификация: обзор // Cryptography. – 2018. – Т. 2, № 1. – С. 1.

11. Панда С., Гупта М., Хота Ч. Систематичний огляд багатофакторної аутентифікації для облачної інфраструктури // Future Internet. – 2023. – Т. 15, № 4. – С. 146.

12. Smith, J. (2023). FIDO2: The Future of Secure Authentication [Електронний ресурс] // TechBullion. – 2023. – Режим доступу: https://techbullion.com/fido2-the-future-of-secure-authentication/

13. Дудикевич, В. та ін. До питання безпечної багатофакторної аутентифікації у веб-застосунках // Український журнал досліджень з інформаційної безпеки. – Київ, 2025. – Т. 25, № 2. – С. 76-82.

14. Сінгх С., Сінгх Т. Д. Системний огляд різних схем багатофакторної аутентифікації // INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING. – 2019. – Т. 7, № 2. – С. 503-510.

15. Чжао Г., Лі Й., Ду Л., Чжао С. Асинхронне рішення аутентифікації з викликом-відповіддю на основі смарт-карти в хмарному середовищі // 2015 2nd International Conference on Information Science and Control Engineering : матеріали конф. – Шанхай, Китай, 2015. – С. 156-159.

16. Стасєв, Ю. В., Гончаренко, К. Г., Мороз, В. І. Аналіз методу багатофакторної аутентифікації користувачів інформаційних систем на основі райдужної оболонки ока // Системи обробки інформації. – Київ, 2023. – Т. 3 (174). – С. 63-69.