МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИКА РОЗРОБКИ І ВПРОВАДЖЕННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В СИСТЕМУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Кирило ЗАВЕДЕЯ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-41

Кирило ЗАВЕДЕЯ
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Заведеї Кирилу Андрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методика розробки і впровадження багатофакторної автентифікації в систему управління інформаційною безпекою організації”,
керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н., доцент
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.
3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи автентифікації, міжнародні стандарти, наукова та технічна література.*
4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати методи автентифікації та вимоги до багатофакторної автентифікації.
   4.2. Змоделювати методику розробки і впровадження багатофакторної автентифікації в систему управління інформаційною безпекою
   4.3. Впровадити багатофакторну автентифікацію в тестовому середовищі та оцінити ефективність впровадження.
   4.4. Надати рекомендації щодо подальшого вдосконалення системи MFA в організації.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Дослідження методів автентифікації та вимог до багатофакторної автентифікації.	15.04.2025	
4.	Моделювання методики розробки і впровадження багатофакторної автентифікації.	01.05.2025	
5.	Практична реалізація багатофакторної автентифікації в організації.	06.05.2025	
6.	Оцінка ефективності впровадження та рекомендації щодо практичного застосування.	09.05.2025	
7.	Формулювання висновків за результатами проведеного дослідження.	10.05.2025	
8.	Оформлення роботи.	10.05.2025	
9.	Оформлення презентації.	12.05.2025	
10.	Отримання рецензії на роботу.	__.06.2025	
11.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Кирило ЗАВЕДЕЯ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Заведея К.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методика розробки і впровадження багатофакторної автентифікації в систему управління інформаційною безпекою організації"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЗАВЕДЕЯ Кирило у кваліфікаційній роботі дослідив методи автентифікації та вимоги до багатофакторної автентифікації, розробив методику впровадження багатофакторної автентифікації, практично реалізував багатофакторну автентифікацію в організації, оцінив ефективність впровадження та розробив практичні рекомендації за темою дослідження.

ЗАВЕДЕЯ Кирило показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на одній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЗАВЕДЕЇ Кирила на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Заведея К.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ЗАВЕДЕЇ Кирила
на тему “Методика розробки і впровадження багатофакторної автентифікації в систему управління інформаційною безпекою організації”

Актуальність. У сучасних умовах стрімкої цифровізації бізнес-процесів та широкого впровадження віддаленого доступу до інформаційних ресурсів організацій зростає необхідність у забезпеченні надійного контролю доступу до критично-важливих інформаційних систем. Автентифікація користувачів залишається одним із найбільш уразливих елементів в системі інформаційної безпеки, що підтверджується щорічною статистикою кіберінцидентів, у яких компрометація облікових даних виступає первинним вектором атаки.

З огляду на зазначене дослідження розробки і впровадження багатофакторної автентифікації в систему управління інформаційною безпекою організації є актуальним науковим завданням.

Позитивні сторони.

1. У роботі всесторонньо досліджено методи автентифікації та вимоги до багатофакторної автентифікації, розроблена методика впровадження багатофакторної автентифікації дозволяє значно підвищити інформаційну безпеку організації.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу: більше 70 публікацій, в тому числі англомовних.

4. За результатами дослідження запропоновано рекомендації щодо впровадження розробленої методики в систему управління інформаційною безпекою організації.

Недоліки.

Доцільно було б приділити більше уваги класифікації програмних інструментів для оцінки ефективності засобів автентифікації.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач ЗАВЕДЕЯ Кирило заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Юрій ПЕПА
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методики розробки і впровадження багатофакторної автентифікації в СУІБ. Робота складається зі вступу, трьох розділів, що містять 16 рисунків, висновків і списку використаних джерел із 70 найменувань. Загальний обсяг роботи становить 91 аркуш, з яких 8 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка та обґрунтування методики впровадження багатофакторної автентифікації (MFA) в систему управління інформаційною безпекою організації для підвищення рівня захисту від несанкціонованого доступу та кіберзагроз.

Об'єктом дослідження є організаційно-технічне забезпечення системи управління інформаційною безпекою.

Предмет дослідження – методика розробки і впровадження багатофакторної автентифікації як складової системи організаційно-технічного забезпечення інформаційної безпеки організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, порівняння, класифікації, системного підходу до управління інформаційною безпекою.

Як результат у роботі досліджено методи автентифікації та вимоги до багатофакторної автентифікації, розроблено методику впровадження багатофакторної автентифікації, практично реалізовано та протестовано методику MFA в організації, оцінена ефективність впровадження та розроблено рекомендації щодо вдосконалення.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті автентифікації користувачів в СУІБ.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, АВТЕНТИФІКАЦІЯ, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ.

ABSTRACT

The qualification work is devoted to the study of the methodology for the development and implementation of multifactor authentication in ISMS. The work consists of an introduction, three chapters containing 16 figures, conclusions and the list of references containing 70 items. The total volume of the work is 91 pages, of which 8 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop and substantiate a methodology for implementing multi-factor authentication (MFA) in an organization's information security management system to increase the level of protection against unauthorized access and cyber threats.

The object of the study is the organizational and technical support of the information security management system..

The subjects of the study is the methodology for developing and implementing multi-factor authentication as a component of the organizational and technical support system for information security of the organization..

Research methods. To solve the above scientific task, the methods of analysis, comparison, classification and a systematic approach to information security management were used in the work.

As a result, the work investigates authentication methods and requirements for multifactor authentication, develops a methodology for implementing multifactor authentication, implements and tests MFA in an organization, evaluates the effectiveness of implementation, and develops recommendations for improvement.

Scope of application. The developed approaches can be used in the planning and implementation of the enterprise information security management system in the context of user authentication to the organization's system.

Keywords: ENTERPRISE INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT SYSTEM, AUTHENTICATION, MULTI-FACTOR AUTHENTICATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AAL	Authenticator Assurance Level
API	Application Programming Interface
CDE	Cardholder Data Environment
FIDO2	Fast Identity Online 2
HMAC	Hash-Based Message Authentication Code
HOTP	HMAC-Based One-Time Password
HTTPS	HyperText Transfer Protocol Secure
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
MITM	Man-In-The-Middle
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OAuth	Open Authorization
OTP	One-Time Password
PCI DSS	Payment Card Industry Data Security Standard
SAML	Security Assertion Markup Language
SFA	Single-Factor Authentication
SMS	Short Message Service
TOTP	Time-Based One-Time Password
TLS	Transport Layer Security
U2F	Universal 2nd Factor
URL	Uniform Resource Locator
2FA	Two-Factor Authentication

ВСТУП

Актуальність теми. У сучасних умовах стрімкої цифровізації бізнес-процесів та широкого впровадження віддаленого доступу до інформаційних ресурсів організацій зростає необхідність у забезпеченні надійного контролю доступу до критично-важливих інформаційних систем. Автентифікація користувачів залишається одним із найбільш уразливих елементів в системі інформаційної безпеки, що підтверджується щорічною статистикою кіберінцидентів, у яких компрометація облікових даних виступає первинним вектором атаки.

З огляду на зазначене дослідження методики розробки і впровадження багатофакторної автентифікації в систему управління інформаційною безпекою організації є актуальним науковим завданням.

Мета роботи полягає у розробці та обґрунтуванні методики впровадження MFA в систему управління інформаційною безпекою організації для підвищення рівня захисту від несанкціонованого доступу.

Об'єкт дослідження **–** організаційно-технічне забезпечення системи управління інформаційною безпекою.

Предмет дослідження – методика розробки і впровадження багатофакторної автентифікації як складової системи організаційно-технічного забезпечення інформаційної безпеки організації.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати методи автентифікації та вимоги до багатофакторної автентифікації.

2. Розробити методику впровадження багатофакторної автентифікації в систему управління інформаційною безпекою

3. Впровадити багатофакторну автентифікацію в тестовому середовищі та оцінити ефективність впровадження.

4. Надати рекомендації щодо подальшого вдосконалення системи MFA в організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Практичне значення одержаних результатів. Отримані результати дослідження підтвердили ефективність впровадження MFA-рішення з урахуванням особливостей бізнес-процесів та ресурсів. Запропонований підхід сприяє зміцненню інформаційної безпеки, зниженню ризику несанкціонованого доступу та може бути інтегрований у систему управління інформаційною безпекою.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» 27 лютого 2025 року.

Розділ 1 МЕТОДИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЇ

1.1 Основні загрози та ризики автентифікації користувачів в інформаційних системах

Інформаційні системи стали критично важливими елементами сучасного цифрового середовища, охоплюючи всі аспекти діяльності. Вони забезпечують обробку, зберігання й передавання великого обсягу даних, які нерідко мають конфіденційний, стратегічний або персональний характер. У зв’язку з цим питання захисту інформації в таких системах набуває особливої актуальності.

Розвиток кіберзлочинності, зростання кількості складних атак, а також широке використання мережевих і хмарних технологій вимагають впровадження ефективних механізмів захисту.

Автентифікація користувачів є фундаментальним процесом у сфері онлайн-безпеки. Він передбачає перевірку особи користувача, який запитує доступ до певних ресурсів, таких як системи, додатки або цифрові платформи [1].

Через недостатнє розуміння заходів безпеки організації, що використовують технології Інтернету речей, автентифікація користувачів стає вразливою до різноманітних кібератак. Кібератаки легше і дешевше організувати, ніж фізичні атаки, вони можуть здійснюватися віддалено і тому часто залишаються непоміченими, доки дані не будуть втрачені, знищені, заперечені, порушені, викривлені або підроблені чи піддані маніпуляціям [2].

Коли користувачі реєструють обліковий запис на сайті або в додатку, який використовує парольний вхід, їм пропонується створити ім'я користувача та пароль. Однак, якщо пароль є передбачуваним, це може призвести до вразливостей у процесі автентифікації. Передбачувані імена користувачів можуть полегшити зловмисникам пошук конкретних користувачів. Замість того, щоб використовувати повний перебір, зловмисники шукатимуть акаунти з

легкими для вгадування паролями, які використовуються занадто часто. Вони спробують використати поширені облікові дані, такі як «admin», «admin1» і «password1». За відсутності обмежень на слабкі паролі, навіть сайти, захищені від атак грубого перебору, можуть виявитися скомпрометованими [3].

Атаки грубого перебору та атаки за словниками були розроблені протягом останнього десятиліття як прості методи зламу паролів шляхом перебору всіх можливих комбінацій до тих пір, поки доступ не буде надано і автентифікація не буде успішною. В міру того, як концепції, що лежать в основі цих атак, ставали все більш відомими і зрозумілими для спільнот, що займаються питаннями безпеки, змінювався і підхід зловмисників до використання бот-мереж для злому паролів з переважним застосуванням сили проти простих систем [2].

Атака «Людина посередині» (Man-In-The-Middle, MITM). Ця атака зазвичай організовується зловмисником віддалено, щоб перехопити лінію зв'язку між користувачами або системами. Сценарій MITM-атаки класифікується як атака високої складності, оскільки зловмисник повинен мати фізичний доступ до каналу зв'язку або мережі. Зловмисник перехоплює канал зв'язку між двома легітимними суб'єктами, наприклад користувач зі своїм пристроєм (ноутбуком, комп'ютером, телефоном) та вебсайт, на який здійснюється авторизація (Рис.1.1) [4].

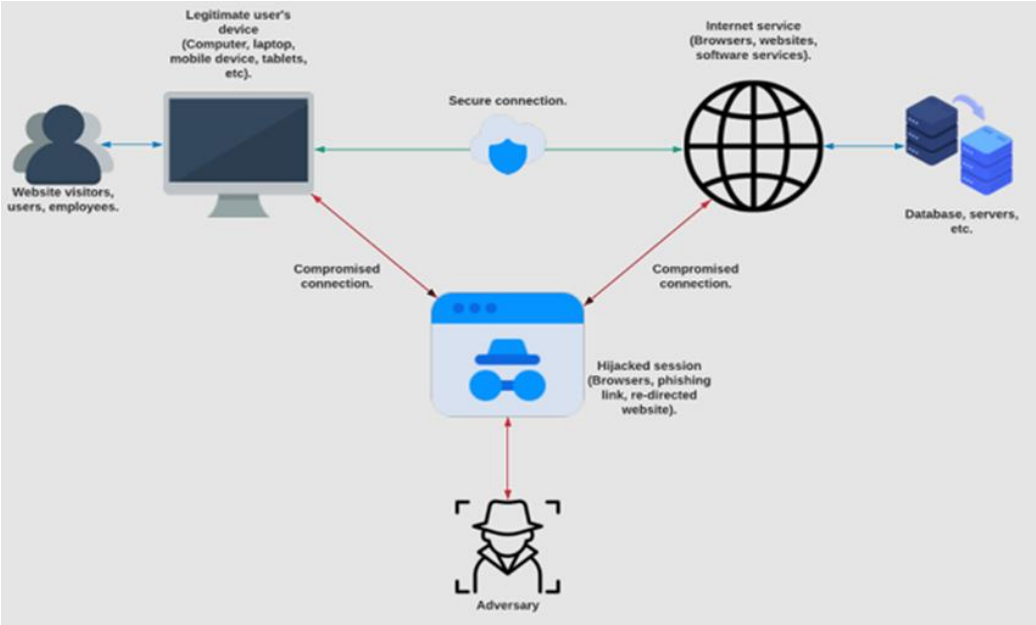

Рис. 1.1. Ілюстрація атаки «Людина посередині»

Соціальна інженерія проти автентифікації - це легкодоступна атака з низькими вимогами до навичок, яку може здійснити навіть зловмисник-початківець. Це метод маніпулювання людською поведінкою, який дозволяє обійти більшість систем захисту інформаційних систем. Соціальна інженерія передбачає різні підходи до викрадення облікових даних легітимного користувача, серед яких найпоширенішими є фішингові атаки. Зловмисники використовують різні соціальні технології, щоб видавати себе за легітимну організацію для створення каналу зв'язку і доставки шкідливих вкладень, часто замаскованих під термінові/важливі файли, зображення або програмне забезпечення зі шкідливим корисним навантаженням [2].

Всі ці загрози призводять до одного результату: отримання несанкціонованого доступу в систему. Коли неавторизовані особи отримують доступ до системи, вони часто націлені на конфіденційні дані, такі як фінансові записи, особиста ідентифікаційна інформація, комерційна таємниця або інтелектуальна власність. Таке вторгнення може призвести до значних фінансових втрат, шкоди репутації компанії та потенційних юридичних наслідків. У деяких випадках зловмисник може не лише викрасти дані, але й пошкодити, знищити або зашифрувати їх.

Ще одним основним ризиком, пов'язаним з несанкціонованим доступом, є потенційна можливість шахрайства. Маючи доступ до конфіденційних даних, кіберзлочинці можуть здійснювати різноманітні шахрайські дії. Це може бути шахрайство з кредитними картками, маніпуляції з банківськими рахунками або навіть створення фіктивних підприємств. Несанкціонований доступ дозволяє злочинцям здійснювати ці шахрайські дії, надаючи їм необхідну інформацію або доступ до фінансових ресурсів. Наприклад, вони можуть використовувати викрадену інформацію про кредитні картки для здійснення незаконних покупок або маніпулювати банківськими системами для незаконного виведення коштів.

У деяких випадках несанкціонований доступ може бути використаний для саботажу організаційних систем або пошкодження веб-сайтів. Це може включати в себе порушення функціонування мережі, впровадження шкідливого

коду на веб-сайт або навіть отримання контролю над системою, що спричиняє широкомасштабний хаос і збої в роботі [5].

1.2 Огляд методів автентифікації

В цьому пункті буде розглянуто найпоширеніші методи автентифікації. Почнемо з однофакторної автентифікації. Однофакторна автентифікація (Single-Factor Authentication, SFA) - це метод автентифікації, який використовує лише один спосіб перевірки особи користувача при спробі доступу. SFA полягає у використанні пароля та імені користувача для підтвердження того, що він є власником облікового запису (Рис.1.2).

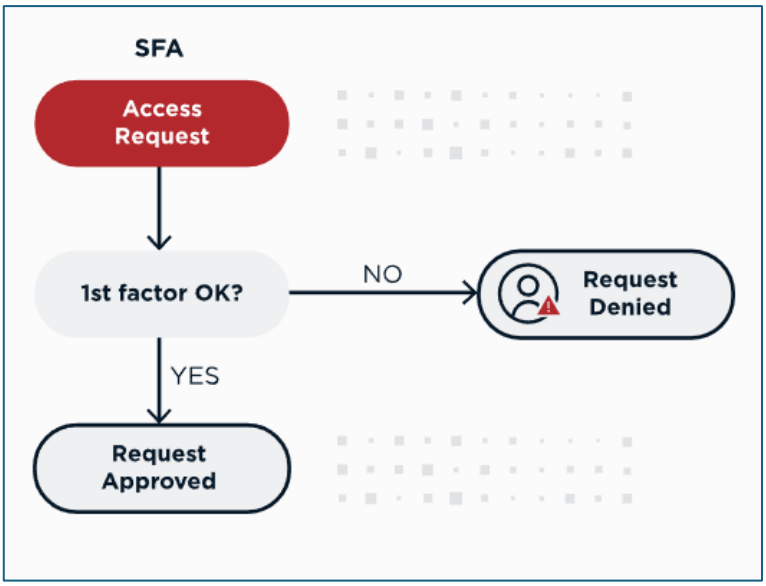

Рис. 1.2. Алгоритм SFA

Розуміючи, що таке SFA і як вона працює, варто глибше розглянути характеристики SFA через найбільш значущі переваги SFA (Рис.1.3):

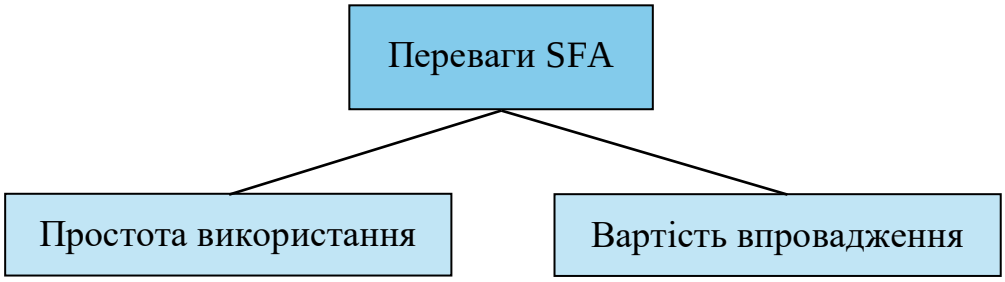

Рис. 1.3. Переваги SFA

Зручність і простота SFA - одна з головних причин, чому цей метод автентифікації став настільки поширеним майже у всіх сферах, від банківської галузі до соціальних мереж. SFA просто працює, і не потрібно докладати жодних зусиль, щоб вона працювала стабільно. Просто введіть ім'я та пароль, і ви в системі.

Вартість впровадження більше стосується підприємств, ніж індивідуальних користувачів. Для компаній, особливо тих, в яких працює велика кількість працівників, впровадження складних заходів багатофакторної автентифікації (Multi-Factor Authentication, MFA) може бути дорогою інвестицією. Натомість SFA є простою і відносно легкою у впровадженні. Крім того, працівники не потребують складних технічних навичок, щоб використовувати її щодня.

Звичайно, окрім переваг цього методу автентифікації, важливо також враховувати ризики SFA. Нижче наведені найбільш суттєві недоліки SFA (Рис.1.4):

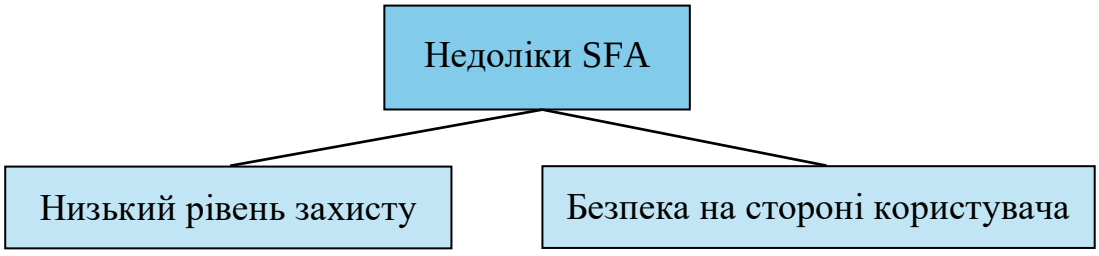

Рис. 1.4. Недоліки SFA

Найочевидніший і найпроблемніший аспект SFA полягає в тому, що вона не забезпечує надійного та надійного захисту. Незалежно від того, який саме однофакторний метод використовується, основна проблема системи полягає в тому, що існує лише один фактор автентифікації.

У SFA користувач є основним фактором, що визначає, наскільки безпечним буде його обліковий запис, виходячи з надійності його пароля. Чим простіший пароль, тим легше хакери можуть його зламати [6].

Що таке двофакторна автентифікація (Two-Factor authentication, 2FA)? Це один із найдієвіших способів захисту облікових записів завдяки використанню одразу двох різних способів підтвердження (Рис.1.5) [7].

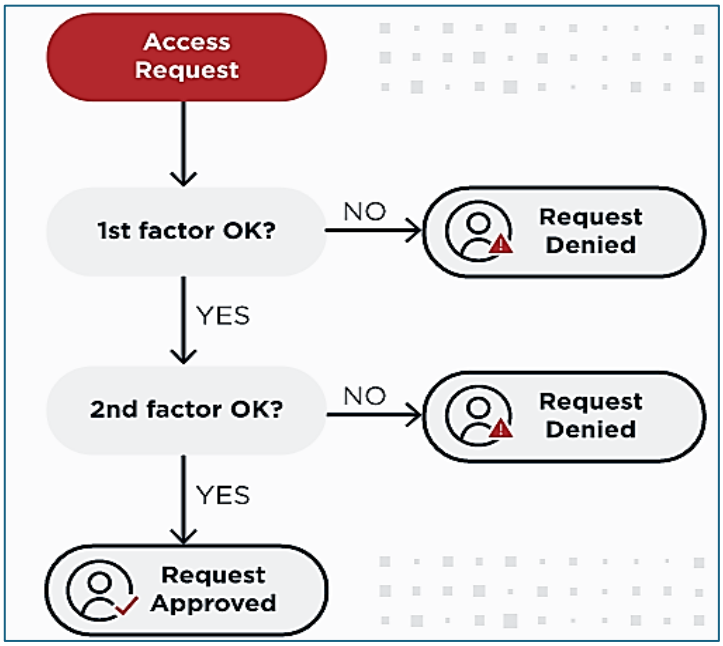

Рис. 1.5. Алгоритм 2FA

Зазвичай, фактори автентифікації, які перевіряються перед наданням доступу, поділяються на три загальні категорії:

– фактор знання (те, що ви знаєте), це може бути пароль, пін-код або відповідь на секретне питання;

– фактор власності (те, що ви маєте), це може бути фізичний токен, такий як мобільний телефон, на якому встановлено спеціальний захищений додаток;

– фактор належності (те, ким ви є), це може бути біометричний фактор, такий як відбиток пальця, розпізнавання обличчя та сітківка ока [8].

В порівнянні з SFA, 2FA має низку переваг (Рис.1.6):

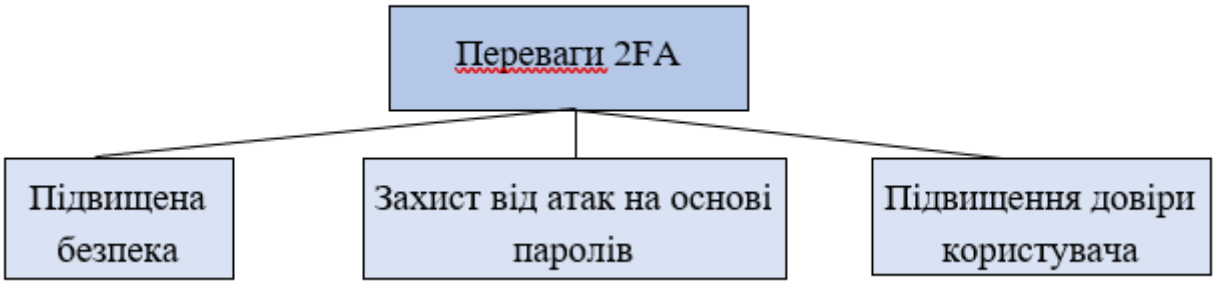

Рис. 1.6. Переваги 2FA

Основною перевагою 2FA є значне підвищення рівня безпеки, який він забезпечує. Вимагаючи декілька типів автентифікації, зловмисникам буде набагато складніше отримати доступ до акаунтів, навіть якщо у них є один фактор у вигляді паролю.

2FA допомагає зменшити ризики, пов'язані зі слабкими або викраденими паролями. Навіть якщо хакер отримає пароль, йому все одно знадобиться додатковий фактор для доступу до облікового запису, що значно знижує ефективність атак на основі паролів.

Впровадження 2FA може підвищити впевненість користувачів у безпеці їхніх облікових записів та особистої інформації, що призведе до підвищення довіри до онлайн-сервісів та платформ.

Але, звичайно, цей метод автентифікації теж недоскональний, через що в ньому присутні декілька недоліків. Розглянемо їх (Рис.1.7):

Одним з основних недоліків 2FA є додаткова складність, яку вони вносять у процес входу в систему. Користувачі повинні пам'ятати та керувати кількома факторами автентифікації, що може викликати невдоволення та забирати багато часу.

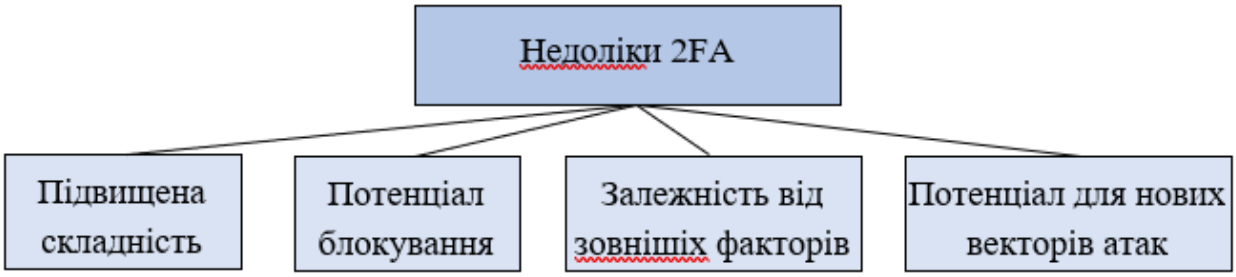

Рис. 1.7. Недоліки 2FA

Якщо користувачі втрачають доступ до одного з факторів автентифікації (наприклад, втрачають смартфон або токен безпеки), вони можуть бути тимчасово заблоковані у своїх облікових записах.

Для отримання кодів автентифікації 2FA часто покладається на зовнішні фактори, такі як мобільний зв'язок або підключення до Інтернету.

Хоча 2FA значно покращує безпеку, він також може створювати нові вектори атак. Наприклад, атаки з підміною SIM-карт (Subscriber Identification Module) націлені на метод автентифікації на основі SMS (Short Message Service), що підкреслює важливість вибору безпечних варіантів додаткових факторів перевірки [9].

Може здатися, що цей опис 2FA трохи схожий на MFA. Так і є, і на те є вагома причина. 2FA - це різновид MFA.

MFA - це багаторівневий метод захисту віртуального та фізичного доступу, коли система вимагає від користувача комбінації двох або більше автентифікаторів для підтвердження особи користувача для входу в систему. MFA підвищує безпеку, оскільки небажані користувачі не зможуть отримати доступ до цілі, навіть якщо один автентифікатор буде скомпрометований [10].

Цей метод має стільки ж категорій автентифікації, скільки і 2FA. Тобто: щось, що ви знаєте; щось, що у вас є; біометричний фактор.

Що ж відрізняє MFA від 2FA? MFA і 2FA використовують додаткові форми автентифікації, щоб захистити обліковий запис. MFA вимагає надання

двох або більше факторів автентифікації, тоді як 2FA вимагає надання тільки двох. Будь-яка 2FA - це завжди MFA, але MFA - не завжди 2FA (Рис.1.8) [11].

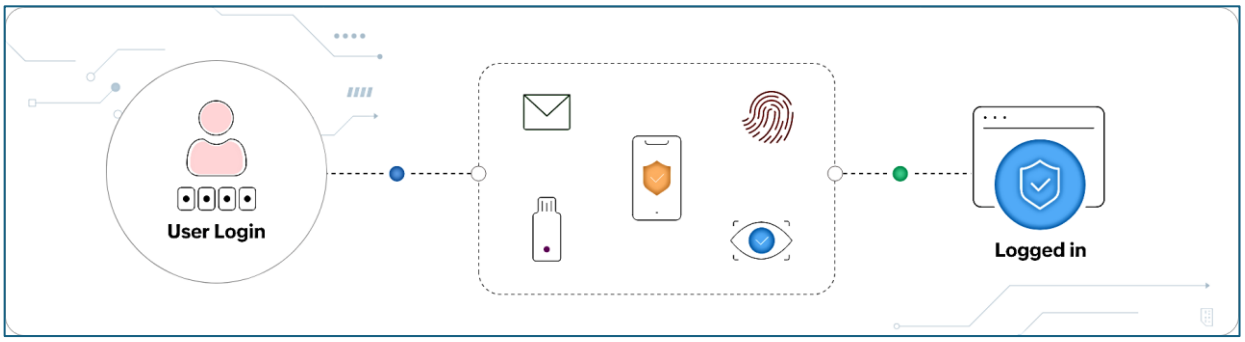

Рис. 1.8. Алгоритм MFA

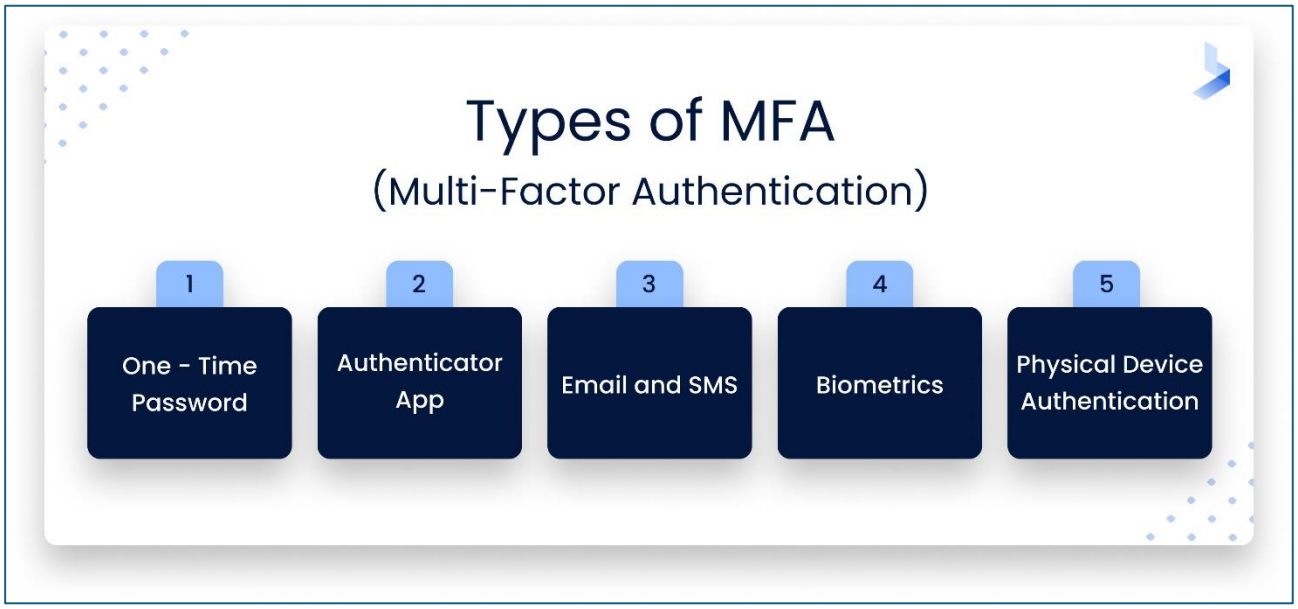

Рис. 1.9. Типи MFA

MFA може бути корисною як для бізнесу, так і для приватних осіб, забезпечуючи багаторівневий підхід до доступу та безпеки. Давайте розглянемо її ключові переваги (Рис.1.10).

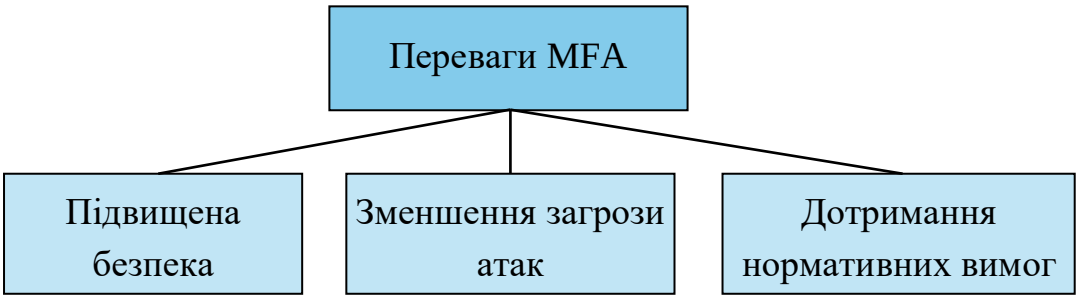

Рис. 1.10. Переваги MFA

MFA виступає в ролі вартового, перешкоджаючи зловмисникам. Навіть якщо їм вдасться дізнатися пароль, вони зіткнуться з додатковими перешкодами, якими є додаткові фактори автентифікації.

Фішингові атаки залишаються поширеною загрозою, яка змушує нічого не підозрюючих користувачів розкривати свої облікові дані за допомогою хитро замаскованих електронних листів і веб-сайтів. Навіть якщо користувач стане жертвою фішингового шахрайства і поділиться своїм паролем, зловмисники не матимуть додаткових факторів автентифікації, що зробить їхні зусилля марними.

Для компаній, що працюють у регульованих галузях, дотримання суворих правил захисту даних не підлягає обговоренню. MFA часто є необхідною умовою для дотримання нормативних вимог.

Хоча багатофакторна автентифікація є потужним захистом від кіберзагроз, вона не позбавлена певних недоліків, які варто розглянути, перш ніж повністю впроваджувати цей захід безпеки (Рис.1.11):

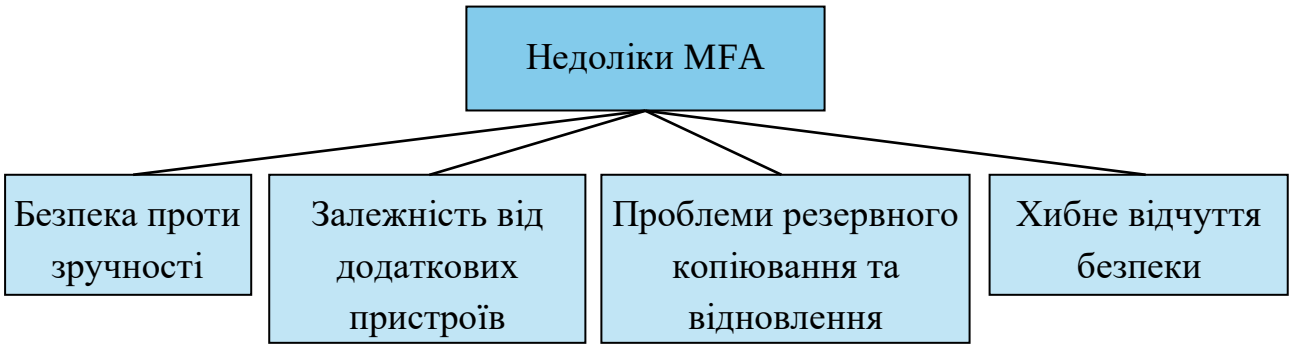

Рис. 1.11. Недоліки MFA

Безсумнівно, першочерговим завданням MFA є посилення безпеки. Однак це часто відбувається за рахунок зручності. Після впровадження MFA вхід у акаунти стає багатоетапним процесом.

MFA часто покладається на «щось, що у вас є», наприклад, смартфон або апаратний токен. Хоча це додає додатковий рівень безпеки, це також створює залежність від цих пристроїв. Якщо смартфон користувача загублений, вкрадений або розрядився, доступ до акаунтів може перетворитися на справжнє випробування.

Наявність плану резервного копіювання є життєво важливою, особливо коли методи MFA пов'язані з фізичними пристроями. Якщо основний пристрій недоступний, надійний метод резервного копіювання має вирішальне значення для відновлення доступу до акаунтів.

Хоча MFA є потужним інструментом, він не захищений від усіх загроз. Досвідчені зловмисники можуть розробити методи обходу певних механізмів MFA або використати вразливості в їхній реалізації [12].

1.3 Аналіз міжнародних стандартів та нормативних вимог щодо MFA

Різні міжнародні стандарти та нормативні документи включають вимоги або рекомендації щодо впровадження безпечної автентифікації з метою підвищення безпеки доступу до критично важливих даних. Буде розглянуто, як принципи MFA інтегруються в провідні стандарти безпеки, зокрема в ISO/IEC 27001:2022, ISO/IEC 27002:2022, PCI DSS v4.0 та NIST SP 800-63.

У стандарті ISO/IEC 27001:2022 в таблиці A.1 з додатку A наголошується впровадження безпечних методів та процедур автентифікації (засіб управління безпекою 8.5).

Стандарт ISO/IEC 27001:2022 визначає структуру, яка необхідна організаціям для проходження сертифікації за цим стандартом. Ця структура складається з пунктів 5-8 та 93 засобів управління [13]. При тому ISO/IEC 27002:2022 містить настанови щодо впровадження будь-якого з 93 засобів

управління безпекою в ISO/IEC 27001 всередині організації. Детальна настанова щодо впровадження безпечної автентифікації відповідно до ISO/IEC 27002:2022:

Для підтвердження заявленої ідентичності користувача, програмного забезпечення, повідомлень та інших об'єктів слід обрати відповідний метод автентифікації.

Надійність автентифікації повинна відповідати ступеню секретності інформації, до якої надається доступ.

Автентифікаційна інформація повинна супроводжуватися додатковими факторами автентифікації для доступу до критично важливих інформаційних систем. Використання комбінації декількох факторів автентифікації, таких як те, що ви знаєте, що ви маєте і хто ви є, зменшує можливості для несанкціонованого доступу.

Інформація про біометричну автентифікацію повинна бути анульована, якщо її коли-небудь скомпрометують.

Процедура входу в систему або додаток повинна бути розроблена таким чином, щоб мінімізувати ризик несанкціонованого доступу. Процедури та технології входу в систему повинні бути реалізовані з урахуванням наступного:

– не відображати конфіденційну інформацію про систему або додаток до успішного завершення процесу входу;

– відображення загального повідомлення, яке попереджає, що доступ до системи, додатку або послуги мають лише авторизовані користувачі;

– не надавати довідкові повідомлення під час процедури входу в систему, які могли б допомогти неавторизованому користувачеві;

– валідація інформації для входу в систему тільки після завершення введення всіх вхідних даних;

– захист від спроб грубого підбору імен користувачів та паролів;

– ведення журналу невдалих та успішних спроб;

– генерування події безпеки при виявленні потенційної спроби або успішного порушення контролю входу в систему;

– відображення або надсилання окремим каналом наступної інформації після завершення успішного входу в систему;

– не відображати пароль відкритим текстом під час його введення;;

– не передавати паролі відкритим текстом через мережу, щоб уникнути їх перехоплення мережевою програмою-сніффером;

– завершення неактивних сеансів після певного періоду бездіяльності, особливо в місцях підвищеного ризику;

– обмеження тривалості з'єднання для забезпечення додаткової безпеки для додатків з високим рівнем ризику та зменшення можливостей для несанкціонованого доступу [14].

Тепер же розглянемо основні положення стандарту PCI DSS v4.0 стосовно багатофакторної автентифікації.

При використанні на додаток до унікальних ідентифікаторів, фактор автентифікації допомагає захистити ідентифікатори користувачів від компрометації, оскільки зловмиснику потрібно мати унікальний ідентифікатор і скомпрометувати пов'язаний з ним фактор (фактори) автентифікації.

Поширеним підходом зловмисників до компрометації системи є використання слабких або неіснуючих факторів автентифікації (наприклад, паролів/парольних фраз). Вимога надійних факторів автентифікації допомагає захиститися від цієї атаки.

Вимога 8.4.1 потребує обов'язкову MFA для будь-якого неконсольного адміністраторського доступу до середовища даних про держателів карток (Cardholder Data Environment, CDE). Тобто, через логічний доступ, що відбувається через мережевий інтерфейс, а не через пряме фізичне з'єднання.

Вимога 8.4.2 потребує наявності MFA для всіх облікових записів, що мають доступ до CDE, а не лише для адміністраторів.

Таким чином, застосування MFA до одного типу доступу не замінює необхідності застосування іншого екземпляра MFA до іншого типу доступу. Якщо особа спочатку підключається до мережі організації через віддалений доступ, а потім пізніше ініціює підключення до CDE з мережі, згідно з цією

вимогою, особа повинна автентифікуватися за допомогою MFA двічі, один раз при підключенні через віддалений доступ до мережі організації, а другий раз при підключенні через неконсольний адміністративного доступу з мережі організації до CDE.

Вимога 8.4.3 вказує, що MFA реалізується для всього віддаленого мережевого доступу, що походить ззовні мережі організації який може отримати доступ до CDE або вплинути на нього наступним чином:

– весь віддалений доступ всього персоналу, як користувачів, так і адміністраторів та адміністраторів, що походить ззовні за межами мережі організації;

– будь-який віддалений доступ третіх осіб та постачальників.

Якщо віддалений доступ здійснюється до частини мережі організації, яка належним чином сегментована від CDE, так що віддалені користувачі не можуть отримати доступ до CDE або впливати на нього, MFA для віддаленого доступу до цієї частини мережі не потрібен. Однак MFA потрібен для будь-якого віддаленого доступу до мереж, що мають доступ до CDE, і рекомендується для будь-якого віддаленого доступу до всіх мереж організації.

Вимога 8.5.1 фокусується на безпечному налаштуванні MFA. Системи MFA повинні бути реалізовані наступним чином:

– система MFA не чутлива до повторних атак. Вона повинна бути розроблена таким чином, щоб запобігти несанкціонованому повторному використанню коду автентифікації;

– системи MFA не можуть бути обійдені жодними користувачами, включаючи адміністративних користувачів, якщо це не задокументовано та дозволено керівництвом на як виняток, на обмежений період часу;

– використовується щонайменше два різних типи автентифікації;

– успішне проходження всіх факторів автентифікації є обов'язковим перед наданням доступу.

Погано налаштовані системи MFA можуть бути оминені зловмисниками. Тому ця вимога стосується конфігурації систем MFA, які забезпечують MFA для

користувачів, які отримують доступ до системних до компонентів системи в CDE [15].

Проаналізувавши вимоги PCI DSS 4.0 щодо MFA, перейдемо до аналізу стандарту NIST SP 800-63, а саме частини 63B, де деталізовані вимоги до методів автентифікації залежно від рівня забезпечення автентифікації [16].

Рівень забезпечення автентифікації (Authentication Assurance Level, AAL) характеризує надійність перевірки автентифікації як порядкову категорію. Більш надійна автентифікація (тобто вищий AAL) вимагає від зловмисників кращих можливостей і більших ресурсів для успішного підриву процесу автентифікації. Автентифікація з вищим AAL може ефективно знизити ризик атак.

NIST SP 800-63B визначає три рівні забезпечення автентифікації: AAL1, AAL2, AAL3.

AAL1 забезпечує базову впевненість у тому, що заявник контролює автентифікатор, прив'язаний до облікового запису абонента, який автентифікується. AAL1 вимагає лише однофакторної автентифікації з використанням широкого спектру доступних технологій автентифікації. Однак рекомендується, щоб додатки, які оцінюються на рівні AAL1, пропонували варіанти багатофакторної автентифікації. Успішна автентифікація вимагає, щоб заявник довів володіння та контроль над автентифікатором.

AAL2 забезпечує високу впевненість у тому, що заявник контролює один або декілька автентифікаторів, прив'язаних до облікового запису абонента, який автентифікується. Необхідно надати докази володіння і контролю над двома різними факторами автентифікації. Додатки, що оцінюються на рівні AAL2, повинні пропонувати варіант автентифікації, стійкий до фішингу.

На рівні AAL2 для автентифікації ПОВИНЕН використовуватися або багатофакторний автентифікатор, або комбінація двох однофакторних автентифікаторів. Багатофакторний автентифікатор вимагає двох факторів для виконання однієї події автентифікації, наприклад, криптографічно захищений пристрій з вбудованим біометричним датчиком, який необхідний для активації пристрою.

AAL3 забезпечує дуже високу впевненість у тому, що заявник контролює один або кілька автентифікаторів, прив'язаних до облікового запису абонента, який автентифікується. Автентифікація на рівні AAL3 базується на доказі володіння ключем за допомогою криптографічного протоколу з відкритим ключем. Для автентифікації за протоколом AAL3 потрібен апаратний автентифікатор з неекспортованим приватним ключем і автентифікатор, стійкий до фішингу. Один і той самий пристрій може відповідати обом вимогам. Для автентифікації за стандартом AAL3 заявники повинні довести володіння та контроль над двома різними факторами автентифікації [17].

1.4 Порівняльний аналіз технологій багатофакторної автентифікації

Звичайні паролі є одними з найменш безпечних методів автентифікації, які розробники можуть вбудовувати у свої програми та веб-сайти. Незважаючи на те, що паролі продовжують широко використовуватися, їх поступово витісняють більш безпечні та зручні для користувача безпарольні технології автентифікаціїї.

У цьому пункті буде розглянуто та порівняно декілька цих технологій з їх перевагами та недоліками.

OTP - це унікальний, динамічно згенерований код, який може бути використаний лише один раз для підтвердження особи користувача при спробі увійти до свого облікового запису.

Основна відмінність між традиційною автентифікацією за допомогою імені користувача та пароля і OTP полягає в тому, що традиційний метод є статичним, тоді як OTP є динамічним. В OTP сервер автентифікації генерує унікальний код для конкретного використання або мети, підвищуючи безпеку, гарантуючи, що його дійсність обмежується єдиним екземпляром.

OTP поєднує в собі два компонента: ключ та рухомий фактор (Рис.1.12). Ключ - секретне значення, яке слугує відправною точкою для генерації цих одноразових паролів. Це конфіденційне унікальне значення, яке надійно зберігається в системі автентифікації.

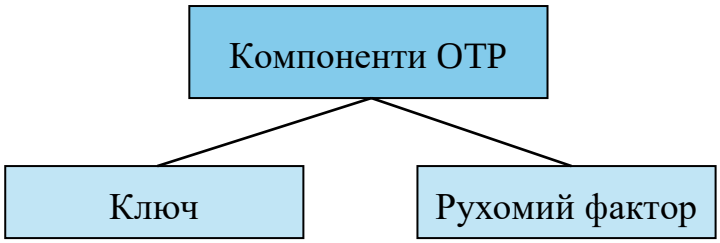

Рис. 1.12. Компоненти OTP

Рухомий фактор - це елемент, який змінюється з кожним поколінням OTP. Він може базуватися на часі (OTP на основі часу) або на лічильнику, який збільшується з кожним використанням (OTP на основі події).

Цей динамічний «рухомий фактор» поєднується з ключовим словом для створення унікального та чутливого до часу OTP для кожної спроби автентифікації; він додає додатковий захист, гарантуючи, що пароль дійсний лише протягом короткого періоду або для певного використання.

Хоча ключ майже завжди є динамічним набором цифр або букв, саме рухомий фактор визначає тип методу OTP, який буде використовуватися. У зв'язку з цим існує два різних типи методів OTP, кожен з яких має свої переваги та поширені випадки використання: одноразовий пароль на основі часу (Time-based One-Time Password Algorithm, TOTP) та одноразовий пароль на основі хешу (HMAC-Based One-Time Password Algorithm, HOTP). У той час як TOTP покладається на поточний час, HOTP - на значення лічильника, яке збільшується з кожним використанням. Обидва методи підвищують безпеку, генеруючи унікальні одноразові паролі, які зловмисникам складно передбачити або повторити.

TOTP - це тип алгоритму, який використовується для генерації одноразових паролів для автентифікації. TOTP додає фактор часу (рухомий фактор) до генерації паролів, роблячи їх дійсними лише протягом короткого і заздалегідь визначеного періоду.

Це гарантує, що TOTP буде дійсним лише протягом короткого періоду (наприклад, 30 секунд), додаючи додатковий рівень безпеки. Навіть якщо зловмисник перехоплює TOTP, він швидко стає недійсним, що знижує ризик несанкціонованого доступу.

HOTP - це ще один алгоритмічний метод генерації одноразових паролів, що використовується в процесах автентифікації. На відміну від TOTP, який покладається на годинник як рушійний фактор, HOTP покладається на значення лічильника, яке збільшується з кожним використанням. Це значення лічильника в поєднанні зі спільним секретним ключем створює унікальний і одноразовий код автентифікації [18].

Fast IDentity Online 2 (FIDO2) - це відкритий стандарт автентифікації, який дозволяє користувачам отримувати доступ до онлайн-сервісів за допомогою фізичного ключа безпеки.

Коли користувач вперше хоче зареєструвати ключ в обліковому записі, ключ безпеки генерує приватний ключ з випадковим числом і використовує функцію безпечного хешування для хешування цього числа, домену веб-сайту, на якому знаходиться користувач, і секретного ключа. З цього приватного ключа генерується відкритий ключ з контрольною сумою, також захищений безпечним хешуванням, і відправляється на сервер разом з числом.

Для входу в систему після реєстрації користувачеві потрібно вставити ключ і натиснути кнопку. Ключ безпеки застосовує той самий процес для генерації того самого приватного ключа і використовує контрольну суму, щоб підтвердити, що випадкове число дійсно надійшло від пристрою. Потім пристрій підписує виклик закритим ключем за допомогою алгоритму цифрового підпису еліптичної кривої (Elliptic Curve Digital Signature Algorithm, ECDSA) і надсилає його на сервер. Сервер перевіряє підпис за допомогою відкритого ключа.

Оскільки для генерації ключа використовується домен веб-сайту, під час фішингової атаки буде згенеровано інший ключ, і контрольна сума буде невірною. Таким чином, зловмисник не може отримати доступ до справжнього підпису.

Це апаратний маркер безпеки, тому навіть якщо комп'ютер заражений шкідливим програмним забезпеченням, зловмисники не зможуть викрасти секретний ключ з нього. Ключ також вимагає фізичного натискання кнопки людиною , тому його не можна активувати віддалено.

Навіть якщо зловмиснику вдасться заразити сервер і викрасти з нього відкритий ключ, він все одно не зможе підписати запит і увійти в систему. Закритий ключ все ще зберігається в ключі безпеки. Механізм відповіді на виклик також запобігає повторним атакам, а підпис на ключі також є одноразовим.

Один і той самий пристрій універсальної двофакторної аутентифікації (Universal Second Factor, U2F) можна використовувати для автентифікації для декількох сервісів. Ніхто не зможе дізнатися, що це був один і той самий пристрій, навіть якщо він мав доступ до обох баз даних.

Якщо USB-токен (Universal Serial Bus) загублено або викрадено, на ньому не зберігається жодної інформації про користувача. Їх також не можна клонувати, оскільки приватна інформація на ключі не може бути витягнута.

Однак недоліками є те, що придбання спеціального ключа безпеки коштує грошей, на відміну від TOTP та HOTP, які є безкоштовним.

Доведеться носити ключ із собою, і є ймовірність, що він буде загублений, тому потрібно мати додатковий ключ у надійному місці, щоб не втратити доступ до свого акаунта.

Крім цього, ця технологія ще дуже свіжа і багато сервісів просто не підтримують її [19].

Біометрична автентифікація - це метод, який підтверджує особу користувача за допомогою його унікальних біологічних особливостей, таких як відбитки пальців, голос, сітківка ока тощо. Системи біометричної автентифікації зберігають цю інформацію, щоб підтвердити особу користувача, коли він отримує доступ до свого облікового запису.

Існує чимало варіантів беометричної автентифікації. Найпоширеніші з них - це розпізнавання обличчя, відбитків пальців та сітківки ока.

Системи розпізнавання обличчя використовують унікальні риси обличчя людини для її ідентифікації. Використовується в різних сферах, наприклад, у смартфонах, при оплаті кредитними картками та в правоохоронних органах;

Автентифікація за відбитками пальців використовує унікальний відбиток пальця людини для підтвердження її особи за допомогою такого пристрою, як токен автентифікації FIDO2. Її можна використовувати для захисту всього, від мобільних пристроїв до автомобілів і навіть будівель, що робить її найпоширенішою технологією біометричної автентифікації;

Розпізнавання сітківки ока використовує унікальний візерунок райдужної оболонки або сітківки ока для ідентифікації людини. Оскільки цей тип біометричної автентифікації складніше реалізувати, він менш поширений, ніж інші типи біометричної автентифікації. Для забезпечення точності сканування райдужної оболонки ока потрібне джерело інфрачервоного світла, камера, яка може бачити інфрачервоне випромінювання, і мінімальне світлове забруднення;

Переваги біометричної автентифікації (Рис.1.13):

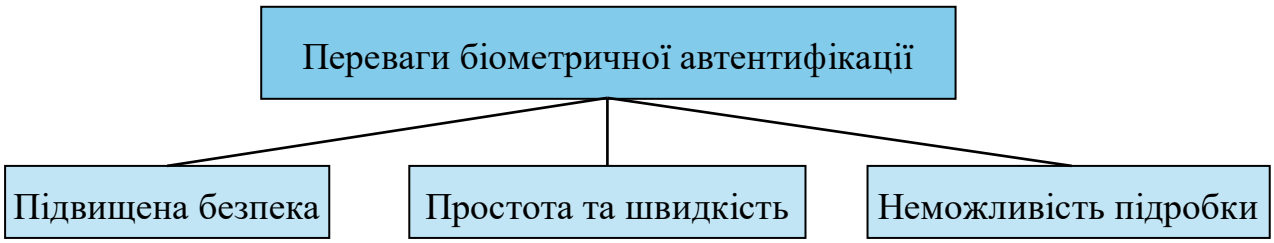

Рис. 1.13. Переваги біометричної автентифікації

Біометрична автентифікація дає відповіді на питання «що людина має і ким вона є» і допомагає підтвердити особу. Її складне програмне забезпечення дозволяє провайдерам знати, що людина є тією, за кого вона себе видає, завдяки відчутним, реальним рисам. Навіть якщо кіберзловмисник знає пароль користувача, він не зможе підробити біометричні дані.

Використовуючи біометрію для розблокування облікового запису, користувач скорочує кількість разів, коли йому доводиться входити в систему, використовуючи довгий пароль.

Біометричні дані майже неможливо підробити. Їх важко скопіювати і вкрасти. Дуже малоймовірно, що хакер зможе отримати доступ до чогось, що захищене біометричними даними.

Але, технології беометричної автентифікації далеко не ідеальні, тому мають декілька недоліків (Рис.1.14):

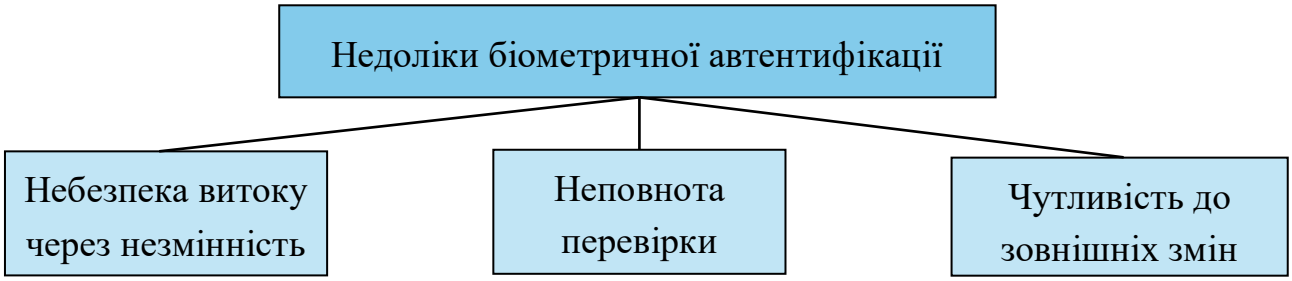

Рис. 1.14. Недоліки біометричної автентифікації

Біометрія все ще може бути зламана. Компанії та уряди, які збирають та зберігають персональні дані користувачів, перебувають під постійною загрозою з боку хакерів. Якщо ж ці компанії стають жертвами витоку даних, біометричні дані є незамінними для хакерів.

Де б не зберігалися біометричні дані, вони повинні зберігатися надійно. Біометричні дані не можна скинути, як пароль.

Найпоширеніші методи біометричної автентифікації покладаються на часткову інформацію для підтвердження особи користувача. Наприклад, під час реєстрації вашого відбитка пальця, система зчитує дані з усього відбитка і перетворює їх на дані. Однак під час наступних автентифікацій для підтвердження особи будуть потрібні лише часткові дані відбитків пальців.

Коли користувач реєструється для розпізнавання обличчя, він реєструє певний кут і вираз свого обличчя. Однак, оскільки система має дані лише з процесу реєстрації, щоразу, коли користувач носить окуляри, макіяж або навіть

посміхається, системі розпізнавання обличчя важко розпізнати користувача, що може ускладнити процес входу в систему.

Вибір технології автентифікації залежить від того, чи надається перевага зручності над безпекою та складністю налаштування [20].

Коротке порівняння технологій автентифікації наведено у таблиці 1.1.

Таблиця 1.1.

Порівняння технологій автентифікації

Технологія автентифікації	Переваги	Недоліки
TOTP	Короткий термін дії коду зменшує ризик отримання несанкціонованого доступу	Може бути незручним для користувача через повторне введення коду після закінчення часу
HOTP	Зручний для користувача	Менш надійний, бо немає прив’язки до часу
FIDO2	Висока крипто- та фішингостійкість	Обмежена підтримка, не безкоштовна, можна втратити доступ при втраті ключа
Біометрія	Висока надійність, зручність використання	Неможливо змінити біометричні дані у разі витоку, імовірність помилкового розпізнавання

Висновки до розділу 1

Здійснено аналіз сучасних методів автентифікації користувачів в інформаційних системах, акцентувавши увагу на їх типових загрозах та ризиках. Розглянуто вектори атак на автентифікацію, серед яких найпоширенішими є соціальна інженерія, атаки грубого перебору, та атаки «людина посередині».

Особливу увагу приділено принципам функціонування однофакторної, двофакторної та багатофакторної автентифікації, їх перевагам та недолікам.

Було ретельно проаналізовано міжнародні стандарти та нормативні документи, які містять вимоги щодо MFA, таких як ISO/IEC 27001:2022 та ISO/IEC 27002:2022, PCI DSS v4.0 та NIST SP 800-63B. Зазначені документи підтверджують необхідність використання багатофакторної автентифікації як ключовий засіб для зменшення ймовірності несанкціонованого доступу до критичних інформаційних ресурсів.

Проведено порівняльну характеристику технологій TOTP, HOTP, FIDO2 та біометричної автентифікації, що дозволило обґрунтувати переваги й обмеження кожного з підходів з точки зору рівня захисту, криптостійкості, стійкості до фішингових атак, а також зручності використання.

Розділ 2 МОДЕЛЮВАННЯ МЕТОДИКИ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

2.1 Вимоги до інтеграції MFA в систему управління інформаційною безпекою

Простота використання є одним з найважливіших факторів при виборі рішення MFA. Якщо кінцеві користувачі не зможуть легко отримати доступ до своїх корпоративних облікових записів, виявиться значне падіння продуктивності та велику кількість звернень до служби підтримки, оскільки люди звертатимуться за допомогою до IT-відділу.

Найкращий спосіб уникнути цієї проблеми - знайти рішення MFA, яке пропонує широкий спектр варіантів автентифікації. Найпоширенішим типом MFA є OTP, але існує також багато інших методів автентифікації.

Користувачі повинні мати можливість, наприклад, обирати між отриманням push-повідомлень на свої смартфони через мобільний додаток або використанням U2F-ключів та біометричної автентифікації.

Створення облікового запису і вибір бажаних опцій MFA не повинно викликати труднощі у користувачів. Сучасні, прості у використанні додатки та інтуїтивно зрозумілі користувацькі інтерфейси матимуть велике значення.

Звичайно, при використанні багатофакторної автентифікації неминуче, що в той чи інший момент користувач буде заблокований у своїх акаунтах. Наприклад, якщо він використовує смартфон для отримання SMS-кодів, він може легко загубитися або бути викраденим, що не дозволить користувачеві отримати коди верифікації. Це може бути серйозною проблемою для користувачів і IT-команд, особливо у випадку з базовими або безкоштовними рішеннями MFA, які не пропонують централізованого адміністрування.

Сервіси MFA пом'якшують цю проблему, дозволяючи користувачам мати два пристрої для автентифікації в будь-який момент часу: основний і резервний. Якщо один з них буде викрадено, другий можна використовувати для

забезпечення доступу до акаунтів. Обране рішення також повинно дозволяти адміністраторам легко скидати доступ до акаунтів з консолі управління, щоб користувачі могли швидко відновити доступ до своїх облікових записів у разі потреби.

Для вибору правильного рішення дуже важливо визначити, які саме облікові записи та сервіси потрібно захистити за допомогою багатофакторної автентифікації. Потрібно захистити лише одну програму чи всі облікові записи користувачів? Як щодо локальних додатків або користувацьких додатків, які організація розробила власними силами?

Рекомендується шукати рішення, яке дозволить легко впровадити багатофакторну автентифікацію для всіх програм і служб користувачів. Хоча деякі безкоштовні або платні рішення MFA можуть забезпечувати захист лише для декількох додатків і охоплювати лише кілька сценаріїв використання, важливо, щоб кожен обліковий запис був захищений, а ще краще, якщо є центральне місце адміністратора для управління всіма підключеними додатками та користувачами.

Найкращі рішення MFA забезпечують автентифікацію для широкого спектру сценаріїв використання та додатків, тож не доведеться обирати, які програми треба захистити, а які залишити незахищеними. Вони адмініструють захист будь-якої системи, яка вимагає від користувачів входу в систему, і навіть можуть увімкнути MFA при вході на локальні пристрої в автономному режимі для Windows і MacOS.

Також може знадобитися захист для кастомних додатків або комбінації хмарних і локальних додатків, тому важливо знайти рішення, яке впорається з цими специфічними випадками використання. Звичайно, не кожна організація потребуватиме всіх цих функцій, і базовий MFA може забезпечити адекватний захист, якщо в них лише невелика кількість сценаріїв використання і вузькі вимоги до безпеки.

Процес розгортання MFA може бути складним при неправильному виборі рішення, з трудомісткими конфігураціями, необхідними для підключення

користувачів до різних додатків. Це може бути ще складніше, якщо мережеве середовище складається з локальних, хмарних і користувацьких додатків. Але є кілька ключових особливостей, на які варто звернути увагу, щоб значно спростити процес приєднання користувачів.

Рекомендується шукати рішення, які дозволяють користувачам самостійно реєструватися, що заощадить адміністраторам багато часу, коли справа доходить до адаптації. Кінцеві користувачі повинні мати можливість самостійно налаштовувати бажані методи автентифікації та пристрої, щоб адміністраторам не доводилося мати справу з таким рівнем деталізації.

Багато великих організацій вже мають служби каталогів користувачів, такі як Microsoft Azure Active Directory. Тому треба обрати рішення, яке інтегрується з каталогом для полегшення керування та автоматичної реєстрації користувачів. Це означає, що рішення автоматично реєструватиме нових користувачів і автоматично відкликатиме доступ, коли користувачів буде видалено з оригінальної служби каталогів.

Обране рішення має інтегруватися з широким спектром додатків і сервісів як для автентифікації доступу користувачів, так і для полегшення керування мережею безпеки.

Тому треба обрати рішення, яке підтримує кастомні інтеграції з додатками та сервісами. Зазвичай це означає, що вони зможуть інтегруватися з будь-якими додатками, які використовують стандарти Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS) або Security Assertion Markup Language (SAML), а деякі рішення також забезпечують попередньо створені інтеграції з певними корпоративними додатками.

Крім того, ці рішення повинні тісно інтегруватися з іншими продуктами безпеки. Це гарантує, що буде легше керувати своїми службами безпеки, а також вийде мати доступ до більш спрощених звітів та аналітики.

Однією з головних переваг впровадження рішення з багатофакторною автентифікацією є те, що воно надає адміністраторам набагато більше контролю над доступом до корпоративних даних і додатків. Це також є ключовим

принципом Нульової довіри (Zero Trust) - ідеального рівня безпеки, який гарантує, що доступ користувачів постійно перевіряється, і що доступ надається лише за необхідності.

З цієї причини при виборі рішення для MFA надзвичайно важливими є можливості адміністрування та доступні політики, яке дозволяє налаштовувати політики на рівні додатків і груп, а також на глобальному рівні.

Політики на рівні додатків і груп дозволяють застосовувати додаткові засоби захисту для певних додатків, які можуть бути дуже чутливими, або для груп користувачів з високим рівнем ризику, наприклад, керівників вищої ланки.

Глобальні політики можуть допомогти забезпечити базовий рівень безпеки доступу в організації, дозволяючи адміністраторам налаштовувати політики, які визначають, як поводитися з незареєстрованими користувачами в системі, які пристрої, браузери та мережі можуть отримати доступ до корпоративних облікових записів, а також які фактори можна використовувати для перевірки особистих даних.

Найкраще обрати варіант рішення, де присутній високий рівень документації щодо конфігурацій політик. Іноді детальні конфігурації можуть бути надто складними, тому слід переконатися, що є достатньо довідкових матеріалів, які допоможуть розібратися з інструментами та політиками адміністрування.

Ще одна ключова перевага MFA полягає в тому, що він дає змогу набагато краще контролювати і розуміти ландшафт безпеки організації. Це не тільки корисно для вдосконалення процесів безпеки, але також може продемонструвати інструменти безпеки, які організація має для захисту доступу до облікових записів для цілей відповідності та аудиту.

Саме тому, доступні звіти та аналітика є одним з головних аспектів, на які звертається увага при розгляді переваг і недоліків рішення MFA. Звіти повинні бути легко доступні в консолі адміністратора. Випробовуючи рішення, треба звернути увагу на обсяг інформації, що відображається, а також на можливість легко генерувати, планувати та отримувати доступ до звітів. Звіти має бути легко

знайти і легко експортувати, що дозволить бачити всю необхідну інформацію з першого погляду, як тільки вона знадобиться.

Найкращі постачальники послуг автентифікації також надають звіти, які детально описують, коли і де відбуваються спроби автентифікації, з інформацією про пристрої та операційні системи, що використовуються. Це може бути надзвичайно корисно для виявлення зловмисних входів і відкликання доступу до незахищених або скомпрометованих пристроїв.

Ціна буде ключовим фактором для будь-якої організації при виборі рішення MFA. Якщо розбити це питання на складові, то існує низка «безкоштовних» постачальників MFA, які стверджують, що їхнє налаштування нічого не коштує. Такі сервіси, як Microsoft Authenticatior, включені в деякі бізнес-плани, і тому можуть здатися найбільш економічно вигідним варіантом для розгортання MFA.

Але ці рішення не надають багатьох функцій, наприклад, охоплення широкого спектру сценаріїв використання MFA, надання звітів та аналітики, інтеграції з користувацькими програмами або адміністративних елементів керування та політик. Деякі постачальники MFA можуть також мати нижчі початкові витрати, але в подальшому стягувати додаткові платежі, наприклад, додаткові витрати на захист певних додатків.

Варто також згадати, що деякі рішення можуть заявляти про свою дешевизну, але насправді вимагатимуть більших витрат у вигляді накладних витрат на адміністрування або залучення зовнішніх підрядників. Слабкі рішення MFA можуть зайняти багато часу на налаштування та управління, особливо якщо вони не пропонують вичерпної документації з підтримки в Інтернеті. Через це витрати на налаштування та підтримку часто набагато нижчі у випадку з готовим платним рішенням, ніж у випадку з «безкоштовним» сервісом [21].

Таблиця 2.1

Вимоги до інтеграції MFA в СУІБ

Вимога	Опис
Зручна автентифікація	Рішення має бути простим у використанні, підтримувати різні методи MFA (OTP, push, U2F, біометрія) та дозволяти швидке відновлення доступу
Широке охоплення випадків використання автентифікації	Рішення повинно підтримувати захист як для хмарних, так і локальних додатків, включаючи кастомні додатки
Просте розгортання та підключення користувачів	Рішення має інтегруватися з каталогом (наприклад, Microsoft Azure Active Directory) для полегшення керування, автоматичної реєстрації користувачів і автоматичного відкликання доступу, коли користувачів буде видалено з оригінальної служби каталогів
Інтеграції з додатками та сервісами	Рішення повинно мати підтримку стандартів (LDAP, RADIUS, SAML) та тісно інтегруватися з сервісами безпеки.
Адміністрування та політики	Система має надавати гнучкі налаштування політик на глобальному рівні, рівні груп та додатків, а також містити зручну документацію для адміністраторів
Звітність та аналітика	Повинна бути доступна детальна звітність про спроби автентифікації: спроби входу, пристрої, операційні системи
Загальна вартість володіння	При виборі слід враховувати не лише стартову ціну, а й приховані витрати на налаштування, підтримку, інтеграції та обслуговування. Деякі безкоштовні рішення можуть бути дорожчими в довгостроковій перспективі

2.2 Методика розробки і впровадження MFA в систему управління інформаційною безпекою

На етапі аналізу здійснюється комплексне вивчення поточного стану систем автентифікації та ризиків безпеки в організації. Дослідженням існуючих механізмів автентифікації, виявленням вразливостей (наприклад, слабкі паролі,

відсутність контролю доступу на критичних ділянках, випадки компрометації облікових записів) і визначенням потенційних загроз несанкціонованого доступу займаються фахівці служби інформаційної безпеки спільно з IT-аналітиками.

Проводиться аналіз вимог нормативних актів і стандартів, релевантних для галузі. В межах цього етапу визначаються критичні ресурси й інформаційні системи, що потребують посиленого захисту (наприклад, системи дистанційного доступу, фінансові або персональні дані), та оцінюється потенційний вплив впровадження MFA на існуючу інфраструктуру й бізнес-процеси.

Попередньо оцінюються витрати на реалізацію різних варіантів MFA, включно з вартістю необхідного обладнання або ліцензій, трудовими ресурсами на інтеграцію та супровід, можливими витратами на навчання персоналу. Такий аналіз дозволяє керівництву розуміти економічну доцільність проєкту і спланувати бюджет.

Результатом етапу аналізу є сформоване бачення поточних проблем автентифікації та чітко окреслена потреба у MFA як в одному з ключових засобів зниження ризиків [22].

Наступним кроком є визначення вимог до впровадження MFA з урахуванням результатів аналізу. На цьому етапі формулюються як технічні, так і організаційні вимоги, які повинна задовольняти система MFA в межах організаційного середовища.

Під час визначення вимог залучаються експерти підрозділу інформаційної безпеки, представники IT-відділу (системні архітектори, адміністратори), а також керівники бізнес-напрямів або уповноважені менеджери, чиї підрозділи будуть охоплені новими заходами автентифікації. Такий склад учасників гарантує врахування різних аспектів:

– безпекових (необхідний рівень захищеності, відповідність організаційним політикам і стандартам);

– технічних (сумісність MFA-рішення з існуючими системами, вимоги до продуктивності та масштабованості, підтримка сучасних протоколів автентифікації);

– організаційних (зручність використання для персоналу, наявність процедур відновлення доступу у разі втрати другого фактора);

– фінансових (допустимі витрати на впровадження та підтримку рішення).

Вимоги фіксуються у вигляді технічного завдання або специфікації. Визначається, скільки факторів автентифікації буде застосовано (двофакторна чи багатофакторна схема), які саме фактори дозволені (апаратні токени, одноразові паролі TOTP через мобільний додаток, біометричні ідентифікатори, SMS-коди, push-сповіщення тощо), яким чином MFA інтегруватиметься із наявними системами управління доступом (Active Directory, корпоративна SSO-платформа тощо) та які політики застосування будуть встановлені (для яких категорій користувачів MFA є обов'язковою, чи будуть винятки для окремих сервісів) [22].

Визначення вимог також охоплює розроблення плану управління користувацьким досвідом:

– як мінімізувати незручності для співробітників при впровадженні MFA;

– як забезпечити доступність підтримки;

– які навчальні матеріали та інструкції потрібно підготувати.

На цій стадії ключову роль відіграє узгодження вимог з керівництвом організації, яке затверджує основні очікування від впровадження MFA, зважаючи на стратегічні цілі безпеки та бізнесу.

Після того, як вимоги сформульовано, здійснюється прийняття рішення щодо впровадження конкретного рішення MFA. Цей етап передбачає оцінку можливих варіантів і вибір оптимального шляху реалізації, виходячи з узгоджених вимог та обмежень. Як правило, на цьому етапі формується робоча група, до якої входять представник керівництва (директор з інформаційної безпеки), фахівці інформаційної безпеки, IT-архітектори, а також представник фінансового підрозділу для оцінки бюджету [23].

Учасники цієї групи аналізують кілька альтернативних сценаріїв впровадження MFA, наприклад, придбання й впровадження готового комерційного продукту MFA, використання хмарного рішення, або розробка внутрішнього модуля автентифікації власними силами. Кожен варіант порівнюється за критеріями відповідності вимогам, рівня безпеки, вартості та складності впровадження, сумісності з наявною інфраструктурою.

На основі раніше проведеного аналізу витрат розраховується очікувана сукупна вартість володіння для кожного варіанту (включаючи початкові витрати і довгострокові витрати на підтримку). Керівництво оцінює, якою мірою обране рішення зменшить ризик витоку даних чи несанкціонованого доступу і чи виправдані витрати в порівнянні з потенційними збитками від кібератак. На підставі цих оцінок затверджується придбання певного програмно-апаратного комплексу MFA або вибір хмарного сервісу з відповідними характеристиками. Рішення оформлюється офіційно у вигляді наказу керівництва чи протоколу засідання комітету з інформаційної безпеки, що санкціонує початок робіт з впровадження обраного MFA-рішення та виділення необхідних ресурсів [22].

Після прийняття управлінського рішення настає етап вибору моделі та детального планування впровадження MFA. Під моделлю розуміється конкретна архітектура і підхід до інтеграції багатофакторної автентифікації в існуючу систему безпеки. На цьому етапі IT-спеціалісти та архітектори систем, співпрацюючи зі службою інформаційної безпеки, розробляють детальний проєкт рішення. Спочатку проводиться уточнення технічних параметрів обраного MFA-рішення, в якому визначаються підтримувані платформи та протоколи (наприклад, чи сумісне рішення з мобільними пристроями всіх співробітників, чи підтримує воно стандартні API для інтеграції зі сторонніми застосунками), вимоги до інфраструктури (сервери автентифікації, мережеві налаштування, канали зв’язку для доставки кодів або push-повідомлень), способи відмовостійкості (наявність офлайн-методів генерування кодів на випадок відсутності зв’язку тощо).

Інтеграція MFA планується таким чином, щоб мінімізувати вплив на наявні системи. Визначаються точки інтеграції (VPN-шлюзи, веб-портали, бази даних, служби каталогів), для кожної з яких розробляється сценарій застосування MFA.

Особлива увага приділяється моделі взаємодії з користувачами, де вирішується, як саме користувачі будуть проходити другий фактор, скільки спроб буде дозволено, як часто потрібна повторна автентифікація тощо. Все це повинно відповідати як вимогам безпеки, так і принципам зручності.

На етапі проєктування розробляються проєкти оновлених політик безпеки, де MFA стає обов'язковою для певних дій або ролей. Готуються інструкції для користувачів та адміністраторів щодо використання нової системи, планується програма навчання для персоналу [22].

Важливо передбачити і механізми реагування на інциденти, пов'язані з MFA. Може статися ситуація, що співробітник втратив токен або смартфон і треба визначити, як проводитиметься процедура відновлення доступу. На основі таких даних складається детальний проєктний план впровадження MFA, де зазначені етапи робіт, відповідальні особи, строки виконання та ключові контрольні точки.

Після завершення стадії проєктування проводиться тестування обраного рішення MFA у контрольованому середовищі. Метою тестування є перевірка працездатності та ефективності системи до її повномасштабного розгортання. Спочатку можуть бути розгорнуті тестові сервери MFA або використано ізольоване середовище. Вибирається обмежена група користувачів або тестових облікових записів, для яких активується новий метод автентифікації. Такий пілотний запуск дозволяє оцінити, чи успішно відбувається двофакторна автентифікація при вході в різні системи, чи коректно генеруються та передаються коди, чи спрацьовують усі політики.

Під час перевірки сумісності MFA-рішення перевіряється, чи не виникає конфліктів з існуючим програмним забезпеченням, чи витримує система очікуване навантаження та оцінюється швидкодія з затримками при здійсненні автентифікації [22].

Також проводиться тестування зручності для користувачів. Обрані співробітники проходять процедуру MFA і надають зворотний зв’язок щодо зрозумілості інтерфейсів та можливих труднощів. Паралельно, служба інформаційної безпеки може моделювати різні сценарії атак для перевірки надійності.

У результатах тестування ретельно аналізуються виявлені помилки чи недоліки, після чого вносяться необхідні корективи у конфігурацію або навіть у вимоги. Тестування повторюється до досягнення впевненості, що система MFA функціонує надійно і відповідає як критеріям безпеки, так і потребам користувачів.

У разі успішного завершення тестової фази переходять до глобального впровадження MFA у середовищі організації. Глобальне впровадження здійснюється поетапно. Спочатку MFA вмикають для критичних систем та облікових записів з найвищими привілеями, потім для великих груп співробітників, і зрештою для всіх інших [23].

Такий фазований підхід дозволяє краще керувати навантаженням на службу підтримки і врахувати досвід перших хвиль користувачів. Перед початком розгортання усім співробітникам заздалегідь повідомляють про заплановані зміни. Проводяться комунікаційні заходи у вигляді розсилки інформаційних листів, оголошення на внутрішньому порталі.

Для навчання персоналу готуються покрокові інструкції щодо налаштування другого фактора і практичного використання. Як показує практика, підготовленість користувачів і їх розуміння важливості MFA значно підвищують успішність впровадження. Тому на цьому етапі приділяється увага підвищенню обізнаності. Пояснюються можливі загрози автентифікації і як MFA їх нейтралізує та наголошується на відповідальності кожного співробітника за безпеку своїх облікових записів.

Технічна реалізація глобального впровадження полягає в активації MFA згідно плану, в якому адміністратори налаштовують відповідні політики у системах, розгортають необхідні серверні компоненти в продуктивному

середовищі та розсилають користувачам посилання або токени для реєстрації другого фактора.

У цей період значно зростає навантаження на службу підтримки. Фахівці допомагають користувачам налаштувати додатки на телефонах, відповідають на запитання, оперативно вирішують інциденти [23].

Для контролю процесу впровадження створюється механізм зворотного зв'язку, в якому користувачі можуть повідомляти про проблеми. Ці звернення швидко опрацьовуються, щоб жоден співробітник не залишився відрізаним від роботи через технічні труднощі. Усі кроки цього етапу документуються. Це не лише дозволяє відстежувати прогрес, але й формує базу знань для подальшої експлуатації системи.

На фінальному етапі здійснюється постійний моніторинг функціонування системи багатофакторної автентифікації, оцінка її ефективності та внесення поліпшень за потреби. Служба інформаційної безпеки разом з IT-відділом відстежують всі спроби автентифікації, особливо важливі події, аналізують статистика використання MFA. Такий моніторинг дозволяє виявляти підозрілу активність і своєчасно реагувати на неї.

Експлуатація включає постійне адміністрування системи MFA, а саме: ведення довідника користувачів і їхніх привілеїв доступу, додавання нових користувачів, видалення або зміна прав звільнених співробітників, заміна або перевидача засобів автентифікації.

Хоча основне навчання було проведено на етапі впровадження, під час експлуатації регулярно нагадуються правила безпечної роботи, новим співробітникам надається інструктаж з MFA, а служба підтримки продовжує оперативно реагувати на запити користувачів, пов'язані з автентифікацією [22].

Керівництво періодично переглядає політику MFA, враховує зміни у загрозах та технологіях і приймає рішення щодо подальшої оптимізації системи. Таким чином, експлуатаційний етап плавно переходить у підтримку сталого високого рівня безпеки, де MFA стає невід'ємною частиною корпоративної культури безпеки, а процес її вдосконалення інтегрується в загальну СУІБ

організації. Це забезпечує, що впроваджена багатофакторна автентифікація постійно адаптується до нових викликів і потреб бізнесу, зберігаючи свою ефективність у запобіганні несанкціонованому доступу [22].

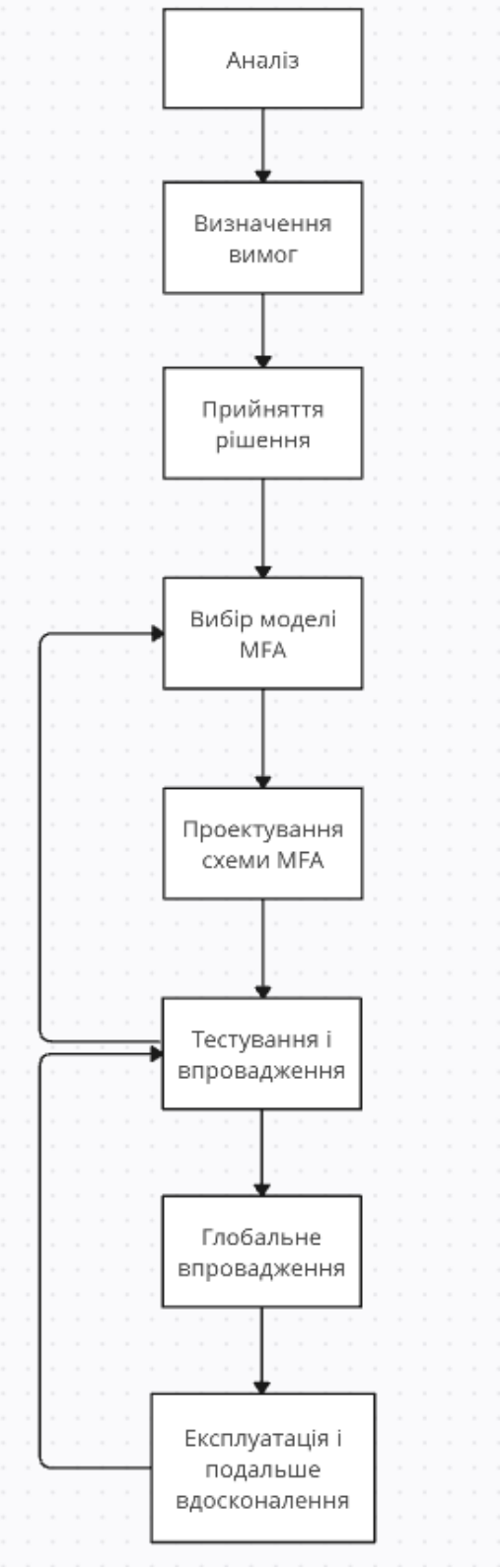

Рис. 2.1. Етапи методики розробки і впровадження MFA

2.3 Критерії впливу MFA на продуктивність і безпеку систем

Критерії впливу MFA на продуктивність і безпеку інформаційних систем здійснюється на основі кількісних і якісних ключових критеріїв ефективності (KPI).

Визначені кількісні критерії впливу MFA на безпеку системи представлені в табл. 2.2, а кількісні критерії впливу MFA на продуктивність системи в табл. 2.3.

Таблиця 2.2

Критерії впливу MFA на безпеку інформаційної системи

Критерій / KPI	Опис
Кількість інцидентів несанкціонованого доступу	Порівняння кількості несанкціонованого доступу до і після впровадження MFA
Кількість компрометованих облікових записів	Кількість зламаних акаунтів або використаних викрадених паролів
Скорочення часу виявлення інциденту (MTTD)	Скільки часу проходить до виявлення атаки
Зниження впливу фішингових атак	Відсоток успішних фішингових спроб до/після MFA
Кількість успішних спроб входу з невідомих пристроїв або локацій	Зменшення таких входів означає кращу безпеку
Зменшення привілеїв lateral movement	Чи вдалося зупинити зловмисника на ранній стадії атаки після початкового проникнення в систему

Зниження кількості інцидентів несанкціонованого доступу визначається шляхом порівняння кількості підтверджених порушень до і після впровадження MFA. Це дозволяє оцінити безпосередній вплив технології на здатність запобігати несанкціонованому доступу до ресурсів системи [24].

Зменшення кількості компрометованих облікових записів означає скорочення випадків, коли зловмисники змогли отримати доступ до користувацьких акаунтів шляхом використання викрадених, зламаних або ненадійних паролів. Завдяки впровадженню другого фактора автентифікації,

навіть за наявності доступу до основного пароля, вхід до акаунта стає неможливим без підтвердження додатковим засобом. Це суттєво обмежує ефективність атак, спрямованих на компрометацію облікових даних [25].

Скорочення часу виявлення інциденту (Mean Time to Detect, MTTD) - середній час, що минає з моменту початку атаки до її виявлення аналітиками з безпеки або автоматизованими системами. Використання MFA, як правило, супроводжується посиленим моніторингом і реєстрацією подій, що дозволяє оперативніше виявляти спроби несанкціонованого доступу, наприклад, при невдалій верифікації другого фактора [26].

Зниження ефективності фішингових атак вимірюється як частка успішних фішингових спроб отримати доступ до системи до та після впровадження MFA. Враховуючи, що більшість фішингових кампаній орієнтуються на викрадення паролів, використання MFA значно зменшує шанси успішного проникнення [27].

Зменшення кількості успішних входів з невідомих пристроїв або геолокацій демонструє здатність системи розпізнавати та блокувати підозрілу активність, що відбувається з нетипових середовищ. Адаптивні механізми MFA можуть вимагати додаткової перевірки або повністю блокувати спробу входу, якщо вона виконується з незвичної IP-адреси або нового пристрою, що не асоціюється з користувачем [25].

Обмеження можливостей lateral movement (горизонтального переміщення в мережі) визначається як здатність зупинити зловмисника на ранньому етапі атаки після початкового проникнення в систему. Впровадження MFA не дає зловмисникам змоги переміщатися мережею, підвищувати привілеї, розгортати шкідливе програмне забезпечення та викрадати дані [28].

Таблиця 2.3

Критерії впливу MFA на продуктивність (операційну ефективність) системи

Критерій / KPI	Опис
Середній час входу в систему (Avg Login Time)	Час, який користувач витрачає на автентифікацію

Продовження таблиці 2.3

Критерій / KPI	Опис
Кількість звернень до служби підтримки через проблеми MFA	Визначає складність використання MFA
Простій або затримки в роботі	Чи викликало MFA затримки у процесах чи доступі до систем
Кількість користувачів, які відмовились через незручність	Ознака низької прийнятності MFA
Сумісність з мобільними/застарілими пристроями	Впливає на доступність і зручність використання
Середній час на вирішення проблем з автентифікацією	Важливий для IT-підтримки та юзабіліті

Середній час входу в систему (Average Login Time) є базовим показником, що характеризує, скільки часу користувач витрачає на проходження процедури автентифікації. Включення додаткового фактора, як правило, подовжує цей процес. Показник дозволяє оцінити вплив MFA на швидкість початку роботи співробітника з корпоративними ресурсами [29].

Кількість звернень до служби підтримки через проблеми з MFA відображає ступінь технічної складності та зручності запропонованого рішення. Збільшення цього показника після впровадження свідчить про необхідність додаткового навчання персоналу або про недосконаліть впровадженого рішення. Такі звернення, як правило, пов’язані з труднощами при генерації коду або втраті доступу до пристрою, який використовується у процесі проходження додаткового фактору.

Простій або затримки в роботі, викликані складністю чи помилками в MFA, є важливим показником впливу на бізнес-процеси. Якщо користувачі не можуть вчасно отримати доступ до системи через проблеми з автентифікацією, це може призводити до уповільнення роботи підрозділів або до зупинки критичних процесів. Високе значення цього показника потребує перегляду процедур або технічного вдосконалення системи MFA.

Кількість користувачів, які відмовилися від використання MFA через незручність, свідчить про рівень прийнятності впровадженого рішення в колективі. Відмова може бути як активною (запит на вимкнення MFA), так і пасивною (припинення користування сервісом), що прямо вказує на низьку юзабіліті та відсутність мотивації користувача дотримуватися нових вимог безпеки [25].

Сумісність MFA з мобільними та застарілими пристроями є технічним параметром, що впливає на доступність автентифікації для різних категорій користувачів. У разі несумісності (наприклад, старі версії ОС) користувачі можуть бути частково або повністю обмежені в можливості проходження автентифікації, що призводить до зниження ефективності роботи та збільшення звернень до підтримки [30] [31].

Середній час на вирішення проблем з автентифікацією демонструє навантаження на IT-службу та ефективність внутрішніх процедур реагування. Чим довше триває вирішення проблем із MFA (наприклад, відновлення доступу після втрати доступа до пристрою з другим фактором), тим більшим є ризик простоїв та зниження загальної продуктивності організації [25].

Додатково з кількісними критеріями впливу в KPI використовуються якісні методи оцінювання, які представлені в табл. 2.4.:

Таблиця 2.4

Якісні критерії оцінювання впливу MFA на продуктивність і безпеку системи

Критерій / KPI	Опис
Опитування користувачів	Визначає рівень задоволення, зручність, сприйняття безпеки кінцевими користувачами
Аудити та Penetration Testing	Визначає чи вдалося обійти MFA
Аналіз логів	Визначає кількість заблокованих несанкціонованих спроб доступу

Одним із головних методів якісного оцінювання впливу MFA на продуктивність і безпеку систем є проведення опитувань кінцевих користувачів, що дає змогу визначити рівень їхнього задоволення від взаємодії з новою системою автентифікації. У процесі аналізу особливу увагу приділяють аспектам зручності використання при щоденному доступі, а також рівню довіри до запропонованих механізмів безпеки. Збір таких даних дає змогу оцінити загальну прийнятність обраної моделі автентифікації.

Наступний метод до якісного оцінювання впливу MFA є проведення аудитів інформаційної безпеки включно з тестуванням на проникнення.

В межах проведення аудиту проводиться перевірка відповідності процесів і технічних рішень вимогам політик безпеки, внутрішніх регламентів та міжнародних стандартів (наприклад, ISO/IEC 27001). Аудит включає аналіз процедур автентифікації, політик доступу, реєстраційних процесів, управління ідентифікаторами та обробки інцидентів. Зокрема, перевіряється, чи належним чином реалізовані механізми захисту другого фактора, чи виконується журналювання подій, і чи існує контроль за своєчасним відкликанням прав доступу при зміні ролі користувача. Результати аудиту дозволяють виявити організаційні або процедурні недоліки, які не обов’язково виявляються технічними засобами.

За допомогою тестування на проникнення здійснюється моделювання дій потенційного зловмисника з метою обходу чинної системи автентифікації. Таке тестування дозволяє ідентифікувати вразливості як у конфігурації MFA, так і у супутній інфраструктурі, зокрема у випадках некоректної інтеграції з зовнішніми сервісами або недостатнього захисту додаткових факторів. Результати тесту на проникнення мають практичне значення для подальшого вдосконалення політик контролю доступу та вибору найбільш стійких до компрометації механізмів [24].

Доповненням до зазначених методів є аналітична обробка логів. Основна мета цього аналізу полягає у виявленні та класифікації несанкціонованих спроб доступу, які були успішно заблоковані завдяки впровадженню MFA [32].

MFA істотно посилює безпеку корпоративних систем. Основна перевага - різке зниження ймовірності несанкціонованого доступу до облікових записів навіть у випадку компрометації паролів. Він, безумовно, є найкращим захистом від більшості атак, пов'язаних з паролями, включаючи грубий перебір. При чому аналіз, проведений Microsoft, свідчить про те, що він зупинив би 99,9% компрометацій облікових записів [33].

Згідно зі звітами, майже половина компаній, що зазнали витоку даних у 2023 році, не мала впровадженої базової MFA, що підкреслює, наскільки відсутність додаткових факторів підвищує вразливість систем [34]. Навіть якщо користувач стає жертвою фішингового шахрайства і ділиться своїм паролем, зловмисники не матимуть додаткових факторів автентифікації, що робить їхні зусилля марними [12].

Як наслідок, впровадження MFA суттєво знижує ризик успішних кібератак. Наприклад, після запровадження апаратних ключів MFA у Google, жоден з понад 85 тисяч співробітників компанії не став жертвою успішної фішингової атаки на облікові записи [35]. Такі показники підтверджують, що багатофакторна автентифікація підвищує загальний рівень захищеності корпоративних систем від несанкціонованого доступу.

Водночас MFA - не панацея від усіх загроз. Кіберзлочинці постійно вдосконалюють методи обходу MFA, наприклад, атака типу «MFA fatigue» (масове надсилання запитів підтвердження для вимотування користувача). Вона може призвести до того, що користувачі ігноруватимуть, відключатимуть або навіть помилково схвалюватимуть зловмисні запити. Жертвами таких атак стали такі великі корпорації, як Uber і Cisco [34].

Успішність цих атак є ще одним нагадуванням про те, наскільки добре соціальна інженерія продовжує знаходити способи обійти загальновизнану технологію безпеки - не ламаючи її, а вивчаючи, як вона працює настільки добре, що можна маніпулювати нею, щоб обвести навколо пальця законних користувачів.

Ці маніпуляції призвели до появи кількох досить ефективних форм компрометації MFA - наприклад, перехоплення MFA, коли зловмисники компрометують електронні поштові скриньки, смартфони або інші канали для перехоплення одноразових кодів автентифікації MFA [36].

Попри ці складні вектори атак, MFA значно підвищує рівень безпеки порівняно з однофакторною схемою. Однак її варто застосовувати у поєднанні з іншими засобами захисту і постійно вдосконалювати механізми безпеки. Іншими словами, багатофакторна автентифікація має бути частиною комплексної стратегії кібербезпеки.

Впровадження MFA неминуче впливає на користувацький досвід, часто створюючи додаткові кроки при вході в систему. З точки зору безпеки, користувачі отримують більше захисту, але виникає компроміс між безпекою та зручністю [12].

Додаткова перевірка (наприклад, введення одноразового коду з телефону або підтвердження push-сповіщення) може сприйматися як зайва затримка або ускладнення, особливо якщо входити до системи потрібно часто. Багато користувачів відчувають невдоволення через необхідність виконувати кілька дій замість однієї, що потенційно знижує задоволеність і продуктивність роботи [37].

Дослідження HYPR показало, що 62% компаній відзначили погіршення користувацького досвіду після впровадження суворішої автентифікації, що призводило до опору з боку співробітників [38] [39].

Такі реакції не дивні, адже зміна усталеної процедури входу часто зустрічає психологічний супротив: користувачі можуть вважати MFA незручним та надмірно обтяжливим, не до кінця розуміючи його переваги [12].

Окрім суб’єктивного дискомфорту, існують і конкретні проблеми: якщо користувач втрачає пристрій (телефон або токен), що використовується як другий фактор, це може тимчасово унеможливити доступ до робочих ресурсів, поки не буде застосовано резервний метод або доки не втрутиться адміністратор [33].

Деякі користувачі визнають переваги MFA з точки зору безпеки, більшість з них все ще стикаються з проблемами початкової конфігурації, розуміння дизайну системи, обмеженої сумісності пристроїв та компромісів щодо ризиків, що призводить до відмови від використання MFA [40].

Втім, є і позитивні аспекти для користувачів. Зростає усвідомлення важливості захисту даних, і багато співробітників згодом відчувають більше довіри до системи, яка забезпечена додатковим захистом. Звіт JumpCloud про IT-тренди 2024 року показав, що більше половини опитаних позитивно ставляться до онлайн-платформ, що впроваджують MFA [41].

Одним з вимірюваних наслідків впровадження MFA є збільшення часу, необхідного для отримання доступу до системи. Якщо автентифікація з одним паролем займає лише кілька секунд, то багатофакторна - через додатковий крок - може тривати значно довше.

За деякими оцінками, навіть при використанні відносно швидких методів (наприклад, push-сповіщень) загальний процес входу може займати близько хвилини. У випадку ж факторів, що доставляються повільніше (SMS або електронна пошта), час очікування коду інколи сягає кількох хвилин.

Така затримка не лише викликає невдоволення користувачів, але й перериває робочий процес: працівникам доводиться відволікатися від виконання завдань, чекаючи підтвердження входу, що негативно впливає на продуктивність. Якщо сесії часто розриваються або система вимагає повторної автентифікації після короткого періоду неактивності, ці часові втрати множаться і можуть перетворити MFA на фактор постійної фрустрації [37].

З точки зору загальної продуктивності організації, такі затримки на кожному вході можуть накопичуватися. Уявімо, що співробітник виконує автентифікацію з MFA 5-10 разів на день: додаткові хвилини на кожен сеанс складаються у години втраченого робочого часу на місяць. Для пом’якшення цього ефекту компанії застосовують різні підходи. Один з них - SSO, коли користувач проходить багатофакторну перевірку один раз, а далі отримує доступ до кількох систем без повторного введення кодів [42]. Також поширена практика

запам’ятовування пристрою на певний період - система не вимагає повторної MFA при кожному вході з відомого середовища протягом, наприклад, 30 днів.

Висновки до розділу 2

У цьому розділі було проаналізовано вимоги до вибору та інтеграції рішень MFA у систему управління інформаційною безпекою організації з урахуванням таких критично важливих аспектів, як: зручна автентифікація, широке охоплення випадків використання автентифікації, просте розгортання та підключення користувачів, інтеграції з додатками та сервісами, адміністрування та політики, звітність та аналітика і загальна вартість володіння.

Сформовано покрокову методику розробки і впровадження MFA, що охоплює етапи оцінки стану інформаційної системи, залучення зацікавлених сторін, вибору MFA-рішення, розробки політик щодо MFA, технічної інтеграції, навчання користувачів, зворотного зв’язку та повного розгортання і подальшого моніторингу.

На основі кількісних та якісних критерій оцінено вплив MFA на безпеку та продуктивність систем. Встановлено, що впровадження другого фактора автентифікації суттєво знижує ризики компрометації облікових даних, зменшує кількість інцидентів несанкціонованого доступу та підвищує рівень захисту від фішингових атак. Водночас проаналізовано потенційні негативні наслідки - зниження зручності користувачів, збільшення часу автентифікації, навантаження на службу підтримки.

Таким чином, запропонована методика розробки та впровадження MFA дозволяє збалансувати вимоги безпеки та зручності, забезпечуючи підвищення стійкості інформаційної системи організації до сучасних загроз. Отримані результати слугують основою для подальшої практичної реалізації системи MFA в корпоративному середовищі.

Розділ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ MFA ТА РЕКОМЕНДАЦІЇ ПО ВПРОВАДЖЕННЮ В СУІБ ОРГАНІЗАЦІЇ

3.1. Вибір програмного та апаратного забезпечення для впровадження MFA

Після аналізу старої політики ІБ компанії Creatio, було визначено критичну необхідність впровадження MFA у СУІБ цієї компанії. Було здійснено аналіз наявної ІТ-інфраструктури, зокрема апаратне та програмне забезпечення, яке використовується для бізнес-процесів компанії.

Creatio спеціалізується на розробці безкодових платформ для автоматизації бізнес-процесів та управління взаємовідносинами з клієнтами (Customer Relationship Management, CRM) [43]. Компанія пропонує інструменти, що дозволяють бізнес-користувачам швидко створювати та налаштовувати корпоративні додатки (для маркетингу, продажів, обслуговування клієнтів тощо) без глибоких знань програмування. Основна ідея - дати можливість організаціям за лічені дні автоматизувати робочі процеси й взаємодію з клієнтами за допомогою візуальних дизайнерів та функцій штучного інтелекту.

На базі проаналізованої інформації, для інтеграції MFA було обрано хмарне рішення Auth0. Платформа управління ідентифікацією та доступом (Identity And Access Management, IAM) Auth0 підтримує різні типи додатків і фреймворків. Незалежно від того, чи є додаток звичайним веб-додатком, мобільним додатком або міжмашинним додатком, Auth0 надає конфігурації для найбільш безпечного надання авторизації або робочого процесу для кожного з них.

Окрім підтримки безпечних протоколів, платформа автентифікації Auth0 дозволяє налаштовувати служби входу індивідуально для кожної організації, її технологій та клієнтської бази. За допомогою інформаційної панелі Auth0 та API (Application Programming Interface) управління можна створити власний екземпляр Auth0 для автентифікації та авторизації клієнтів організації.

Auth0 пропонує кілька варіантів захисту від атак, наприклад, виявлення ботів у поєднанні з Google reCAPTCHA Enterprise для запобігання кібератакам. Навіть якщо використовується власна сторінка для входу, Auth0 пропонує інші варіанти захисту, які організації можуть ввімкнути на інформаційній панелі Auth0:

– виявлення зламаних паролів, які є заходом захисту від зловмисників з викраденими обліковими даними.

– захист від перебору грубою силою, який захищає цільовий обліковий запис користувача, обмежуючи кількість спроб входу, що автоматично блокує зловмисний IP і надсилає сповіщення обліковому запису користувача, який було позначено як зловмисник.

– дроселювання підозрілих IP-адрес, яке працює там, де зупиняється захист від перебору грубою силою, блокуючи трафік з будь-якої IP-адреси, яка намагається здійснити швидку реєстрацію або вхід [44].

Це рішення створене для додавання служб автентифікації та авторизації до додатків організації, завдяки якому можна уникнути витрат, часу та ризиків, пов'язаних з розробкою власного рішення для автентифікації та авторизації користувачів [45].

Для створення додатку, який у подальшому буде розгорнутий на базі Auth0, було використано JavaScript фреймворк Next.js. Next.js - це фронтенд-фреймворк, який базується на можливостях React, універсальної бібліотеки JavaScript, що використовується для створення користувацьких інтерфейсів. Відмінною рисою Next.js є його здатність спрощувати складні аспекти веб-розробки, надаючи комплексний набір інструментів та функцій [46].

В якості додаткових методів автентифікації було обрано TOTP з додатку Google Authenticator та push-повідомлення з Auth0 Guardian.

TOTP було обрано як другий фактор автентифікації через його високу сумісність із різними платформами, незалежність від підключення до інтернету та підтримку з боку Auth0 без необхідності у додатковому обладнанні.

Як альтернативу TOTP, було обрано механізм push-сповіщень. Push-аутентифікація полягає в надсиланні сповіщення на мобільний пристрій користувача, яке він підтверджує одним дотиком, що забезпечує високий рівень зручності для користувача, зменшуючи потребу вручну вводити код, а також дозволяє реалізувати додаткові механізми перевірки.

На випадки, якщо користувач не зможе отримати доступ до пристрою або облікового запису, що використовується для авторизації за допомогою MFA, він може використати код відновлення для автентифікації. Код відновлення - це унікальний код, згенерований Auth0, який дозволяє користувачеві відновити доступ до облікового запису [47].

Google Authenticator - це мобільний додаток для забезпечення безпеки, який надає додатковий тип підтвердження для веб-сайтів та онлайн-сервісів, що використовують MFA для перевірки особи користувача перед наданням йому доступу до захищених ресурсів [48].

Цей додаток надає код для кожного сайту або сервісу, який користувач зареєстрував в автентифікаторі. Кожний код - це шестизначне число, яке оновлюється кожні 30 секунд. Як додатковий шар захисту, у додатку можна підключити біометричний сканер, щоб навіть при втраті фізичного пристрою ніхто не зміг отримати доступ до кодів.

Auth0 Guardian - теж мобільний додаток для забезпечення безпеки, який під час підтвердження користувача дозволяє проходити MFA за допомогою push-сповіщень або TOTP [49].

OAuth - це стандарт для авторизації на основі токенів [50], який використовує платформа Auth0. Він розроблений для того, щоб дозволити веб-сайту або додатку отримувати доступ до ресурсів, розміщених на інших веб-додатках, від імені користувача [51]. OAuth дозволяє стороннім сервісам, таким як Facebook і Google, використовувати інформацію про обліковий запис кінцевого користувача, не розкриваючи облікові дані користувача третій стороні. Він діє як посередник від імені кінцевого користувача, надаючи сторонньому

сервісу токен доступу, який дозволяє передавати певну інформацію про обліковий запис. Процес отримання токена називається потоком авторизації [50].

Ідентифікаційні токени використовуються для кешування інформації про профіль користувача та надання її клієнтському додатку, забезпечуючи тим самим кращу продуктивність і зручність роботи. Додаток отримує ідентифікаційний токен після успішної автентифікації користувача, потім споживає його і витягує з нього інформацію про користувача, яку потім може використовувати для персоналізації взаємодії з користувачем [52].

Токени доступу використовуються, щоб дозволити програмі отримати доступ до API. Додаток отримує токен доступу після того, як користувач успішно пройшов автентифікацію та авторизувався, а потім передає його як обліковий запис під час виклику цільового API. Переданий токен інформує API, що власник токена має право доступу до API та виконання певних дій, визначених областю дії, яка була надана під час авторизації [53].

Обидва токени є веб-токенами JSON (JavaScript Object Notation) і тому мають термін дії, вказаний за допомогою вимоги exp, а також заходи безпеки, такі як підписи. Зазвичай користувачеві потрібен новий токен доступу, коли він отримує доступ до ресурсу вперше або після закінчення терміну дії попереднього токена доступу.

Токен оновлення - це артефакт облікових даних, який OAuth може використовувати для отримання нового токена доступу без взаємодії з користувачем. Це дозволяє серверу авторизації скоротити термін дії токенів доступу з метою безпеки, не залучаючи користувача, коли термін дії токена доступу закінчується [54].

3.2 Налаштування та тестування MFA

Для налаштування та тестування MFA було використано звичайний веб-додаток, написаний на JavaScript фреймворку Next.js. Цей додаток було додано в інформаційну панель Auth0.

Для зв'язку з Auth0 треба отримати ключі додатку. Знадобляться деякі дані про програму, а саме: AUTH0_ISSUER_BASE_URL, AUTH0_CLIENT_ID, AUTH0_CLIENT_SECRET. Ці дані розміщені у файлі «.env.local» (Рис.3.1).

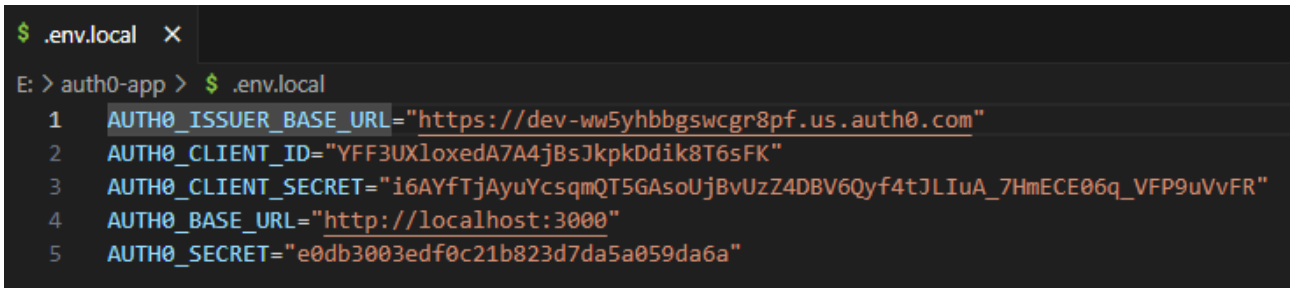

Рис. 3.1. Файл «.env.local»

AUTH0_ISSUER_BASE_URL - це базовий URL (Uniform Resource Locator).

AUTH0_CLIENT_ID - це ідентифікатор клієнта програми Auth0 [55].

AUTH0_CLIENT_SECRET - це симетричний метод автентифікації. При автентифікації за допомогою секретного ключа клієнта використовується секретний ключ Auth0, згенерований при створенні додатку [56].

Після отримання ключів додатку треба налаштувати адресу зворотного виклику. Адреса зворотного виклику - це адреса у додатку, на яку Auth0 перенаправляє користувача після його автентифікації. Адресу зворотного виклику для додатку потрібно додати до поля «Дозволені адреси зворотного виклику» у налаштуваннях додатку. Якщо це поле не встановлено, користувач не зможе увійти в додаток і отримає помилку.

Адреса виходу - це адреса у додатку, до якої Auth0 може повернутися після того, як користувач вийшов з сервера авторизації. Вона вказується в параметрі запиту returnTo. Адресу виходу для додатку слід додати до поля «Дозволені адреси виходу» у налаштуваннях додатку. Якщо це поле не встановлено, користувач не зможе вийти з програми і отримає помилку [55].

Після налаштування додатку у інформаційній панелі, перейдемо до безпосереднього запуску додатку. Процес запуску додатку та отримання доступу відбувається наступним чином:

– додаток запускається на локальному пристрої на 3000-му TCP порті через команду «npm run dev» у терміналі;

– для переходу на головну сторінку у браузері потрібно перейти на localhost:3000;

– відбувається ідентифікація, автентифікація та авторизація, які проходять через сервер Auth0;

– сервер перевіряє введені дані, після чого все повертається назад у локальний клієнт.

У процесі реєстрації облікового запису користувач повинен створити новий акаунт використавши пошту як логін та створити надійний пароль, або ж зареєструватися використовуючи сервіси Google, Facebook чи GitHub.

Пароль обов'язково повинен складатися з щонайменше 8 символів, включаючи принаймні 3 з наступних 4 типів символів: літера нижнього регістра (a-z), літера вищого регістра (A-Z), цифра (0-9), спеціальний символ (наприклад, !@#$%^&*). Не більше 2 однакових символів підряд (наприклад, 111 не допускається) [57].

Після реєстрації користувачу буде запропоновано підключити додатковий метод автентифікації на вибір (з тих, які були підключені у інформаційній панелі). Користувач сканує код швидкого реагування (QR-код) або вводить секретний ключ в додатку на телефоні.

Після прив'язки додатку з телефона користувачу буде надано одноразовий резервний код на випадок, якщо доступ до фізичного пристрою з додатком буде втрачено, щоб в нього все ще була можливість отримати доступ до облікового запису.

Надалі користувач буде проходити авторизацію використовуючи логін з паролем, або через сервіс, який було використано для реєстрації і обов'язково проходити додатковий етап автентифікації.

А тепер розглянемо більш поглиблено процес авторизації у разі вибору TOTP. Цей процес складається з наступних кроків:

– перехід на головну сторінку;

– після натискання кнопки Login відбувається перенаправлення на захищену сторінку авторизації, яка розміщена вже на стороні Auth0;

– користувач проходить етап ідентифікації та автентифікації;

– користувач вводить TOTP з додатку;

– сервер Auth0, використовуючи OAuth 2.0, перевіряє вказані дані та після успішної перевірки видає токени (ідентифікаційний токен, токен доступу, токен оновлення);

– користувача успішно авторизовано в обліковий запис.

Якщо розглянути отримання доступу через push-сповіщення, то все відбувається майже так само, як з TOTP. Але замість того, щоб заходити в додаток та вводити код, користувачу прийде сповіщення, де він зможе натиснути на підтвердження чи відмову запиту на авторизацію у обліковий запис (Рис.3.2).

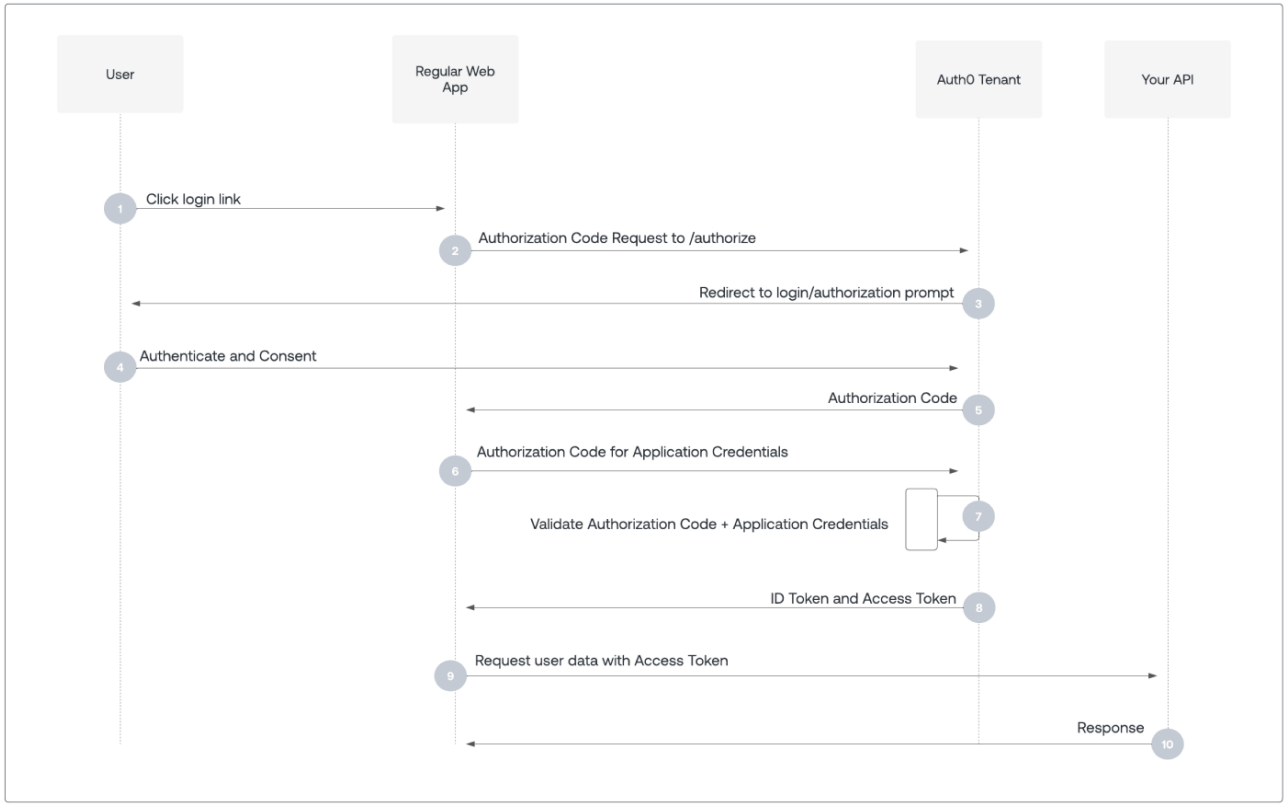

Рис. 3.2. Процес отримання доступу в Auth0

Перед початком впровадження проаналізовано можливі підходи інтеграції Auth0 з Creatio. Обидві системи підтримують протокол автентифікації OpenID Connect. Auth0, у свою чергу, може виконувати роль постачальника ідентичностей (Identity Provider, IdP) для сторонніх додатків за допомогою протоколу OpenID. З огляду на рекомендації щодо MFA в Creatio, було вирішено реалізувати інтеграцію Auth0 за допомогою OpenID Connect.

OpenID Connect - це відкритий стандартний протокол автентифікації, побудований на основі фреймворку авторизації OAuth 2.0. Він дозволяє розробникам автентифікувати користувачів на веб-сайтах, в мобільних додатках і додатках без необхідності володіти та керувати обліковими даними до паролів [58].

Першим кроком стало створення додатку в консолі Auth0, який буде відповідати за автентифікацію користувачів Creatio. У налаштуваннях Auth0 створено новий клієнт типу Regular Web Application та згенеровано унікальні облікові дані – Client ID і Client Secret. Ці облікові дані будуть використовуватися Creatio для встановлення з'єднання з Auth0. В полі налаштувань Allowed Callback URLs на стороні Auth0 вказано URL сторони Creatio, куди провайдер буде переспрямовувати користувача після успішної автентифікації. Для інтеграції OpenID Connect таким URL є спеціальна кінцева точка Creatio: creatio.com/ServiceModel/AuthService.svc/OpenIdCallback. Creatio.com - це базова адреса веб-додатку Creatio. Також налаштовано Allowed Logout URLs із значенням creatio.com /ServiceModel/AuthService.svc/OpenIdLogoutCallback, щоб забезпечити коректне завершення сеансу.

Наступним важливим налаштуванням на стороні Auth0 стала активація та конфігурація MFA. У розділі Security > Multi-factor Auth на панелі Auth0 було увімкнено функцію багатофакторної автентифікації для відповідного застосунку. Для пілотного впровадження було обрано метод TOTP як базовий, а також за потреби - push-сповіщення з Auth0 Guardian для більш зручного досвіду.

Для забезпечення коректної взаємодії з Creatio, на стороні Auth0 також було перевірено спеціальний документ виявлення службових кінцевих точок

(Endpoint Discovery Document), де містяться всі необхідні кінцеві точки: авторизації, отримання токена, ключів для перевірки підпису токенів тощо. Auth0 автоматично надає цей документ за URL виду creatio.com.auth0.com/.well-known/openid-configuration

Наступний етап – конфігурація Creatio для довіреної автентифікації через Auth0. У системі Creatio було створено спеціальний інтерфейс для налаштування SSO-провайдерів. Використовуючи панель адміністрування у розділі Single Sign-On (SSO) configuration, було додано нового провайдера. Оскільки Auth0 не входить до списку шаблонів за замовчуванням, налаштування виконано у режимі кастомної інтеграції OpenID Connect.

В полі конфігурації провайдера Creatio послідовно заповнено такі параметри, отримані з Auth0: Client ID, Client Secret, URL провайдера, Discovery URL, End session endpoint, Display name.

Після заповнення цих полів конфігурацію збережено. Creatio автоматично встановлює зв’язок із Auth0 для перевірки даних; зокрема, відбувається спроба завантажити OpenID-конфігурацію з наданого URL. У разі успіху провайдера додано до списку доступних. На цьому етапі, було увімкнуто функцію Just-In-Time Provisioning (JIT) - автоматичного створення облікових записів користувачів у Creatio при першому вході, щоб не створювати вручну кожного користувача в системі [59].

Після успішного налаштування підключення Auth0 постало завдання зробити так, щоб усі користувачі компанії при вході обов’язково проходили через новий механізм автентифікації. У нашому випадку, оскільки планується повний перехід на використання Auth0, ми визначили створеного провайдера як провайдера за замовчуванням для автентифікації. Через системне налаштування у параметрі DefaultSsoProvider встановлено значення, що відповідає провайдеру Auth0. Після цього, потік входу виглядає так: користувач переходить на сторінку Creatio, натискає «Вхід», система перенаправляє його на хмарний сервіс Auth0, де той вводить свої облікові дані та проходить додаткову перевірку MFA. Auth0 перевіряє правильність пароля і другого фактора. Тільки після успішного

проходження MFA користувача авторизовано. Далі Auth0 формує для Creatio відповідь і впускає користувача в систему.

Після налаштування інтеграції були проведені ретельні випробування. Спочатку розгорнули локальне середовище Creatio з налаштованим HTTPS-доменом. На етапі тестування перевіряли кілька сценаріїв:

– вхід існуючого у системі Creatio користувача;

– вхід нового користувача, якого немає у системі (для перевірки JIT provisioning);

– помилковий ввод пароля або MFA-коду;

– повторний вхід після виходу.

Всі ці кейси успішно відпрацювали. Зокрема, для нового користувача спершу було створено обліковий запис у Auth0 і надано з ним QR-кодом для налаштування TOTP-додатку. При першому вході цей користувач був перенаправлений на Auth0, де виконав реєстрацію MFA. Надалі цей другий фактор буде вимагатися автоматично. Після введення правильного коду користувач отримав доступ до Creatio. Повторні входи цього користувача також вимагали TOTP-коду. Таким чином, локальні випробування підтвердили працездатність інтеграції.

Аналіз логів автентифікації дає змогу виявити помилки конфігурації, оцінити коректність роботи механізму входу, підвищити рівень безпеки та виявити аномалії [60].

Ці логи містять записи про всі спроби входу (успішні й неуспішні), що дає можливість виявляти несанкціоновані спроби доступу, атаки підбором паролів, чи були облікові дані певного користувача використані у масштабному публічному витоку даних тощо.

Всі події, які виконувалися під час тестування MFA записувалися у інформаційній панелі Auth0. У процесі тестування відбулися наступні події:

– неправильне налаштування адреси зворотного зв’язку;

– неправильно введені логін або пароль;

– неправильно введений код з додатку;

– відхилення запиту на авторизацію при проходженні другого фактору;

– блокування доступу до облікового запису з певної IP-адреси через велику кількість спроб авторизації;

– перевищення ліміту запитів до API;

– невдала реєстрація;

– додаткова вимога у підтвердженні фактора автентифікації (у випадку спрацювання оцінки ризику адаптивної MFA);

– успішна реєстрація;

– успішно пройдена MFA;

– успішна авторизація;

– успішний обмін авторизаційного коду на токен доступу;

– успішний вихід із системи.

Неправильно налаштована адреса зворотного зв’язку (Callback URL mismatch) з кодом «f» виникає, коли запит автентифікації не відповідає жодному з дозволених у налаштуваннях Auth0. Якщо адресу зворотного зв’язку неправильно вказано в конфігурації, користувач побачить повідомлення про помилку і не зможе увійти у додаток.

Якщо були неправильно введені логін або пароль, Auth0 реєструє подію Failed Login. Коди подій: «fp» (Failed Login - Incorrect Password) або «fu» (Failed Login - Invalid Email/Username). Ця подія означає, що автентифікація першого фактору не була пройдена. З погляду безпеки така подія вказує на невдалу спробу входу і може сигналізувати про атаку підбором пароля.

При введенні неправильного одноразового паролю Auth0 реєструє подію OTP Auth Failed з кодом «gd_auth_failed». Це означає, що перевірка другого фактора не пройдена через неправильно введений код. Така подія підвищує безпеку - вона вказує, що на другому етапі вхід заблокований - і за необхідності система може вводити обмеження на кількість спроб.

Відхилення запиту на авторизацію при проходженні другого фактору виникає, коли користувач відхиляє запит на проходження багатофакторної

автентифікації, наприклад, у мобільному застосунку (якщо користувач обрав push-сповіщення як додатковий фактор). У такому випадку, Auth0 реєструє подію OTP Auth Rejected з кодом «gd_auth_rejected». Це вказує на те, що автентифікація була навмисно зірвана користувачем. Така поведінка потенційно є індикатором атаки - наприклад, користувач отримав неочікуваний запит і відхилив його. Це може бути сигналом спроби несанкціонованого входу, коли зловмисник вже ввів правильний логін з паролем, але не має доступу до другого фактора.

Подію блокування доступу до облікового запису з певної IP-адреси через велику кількість спроб авторизації Auth0 реєструє під назвою Blocked Account з кодом «limit_wc». Вона вказує на те, що подальші спроби блокуються з цієї IP-адреси для цього користувача, оскільки ця адреса досягла максимальної кількості невдалих спроб входу за короткий час. У більшості випадків це результат спрацювання механізмів захисту від атаки грубого перебору.

Перевищення ліміту запитів до API (Rate Limit On API) може виникнути при багаторазових вводах TOTP коду протягом короткого інтервалу часу, наприклад, у разі надмірних спробах обходу MFA. Така подія свідчить про належно налаштовану політику rate limiting, яка захищає API від потенційного перевантаження. Це також є механізмом захисту від грубого перебору TOTP кодів. Auth0 фіксує цю подію з кодом «api_limit».

Подія невдалої реєстрації (Failed Signup) з кодом «fs» фіксується в Auth0 у разі, якщо спроба створення нового облікового запису завершилася помилкою. Це може статися через кілька причин: email-адреса вже використовується, порушення валідаційних правил (наприклад, слабкий пароль), або збій підключення до зовнішнього сервіса автентифікації (наприклад, Google, Facebook).

Потреба у підтвердженні додаткового фактора автентифікації свідчить про спрацювання оцінки ризику адаптивної MFA. Ця подія виникає з кодом «mfar» (MFA Required) і може свідчити про те, що авторизація відбувається з незвичної IP-адреси, геолокації, або невідомого пристрою.

Подія успішної реєстрації нового користувача (Success Signup) в Auth0 фіксується з кодом «ss», що вказує на створення нового облікового запису через форму реєстрації або зовнішній сервіс автентифікації.

Успішне проходження MFA (OTP Auth Succeed) Auth0 фіксує подію як «gd_auth_succeed». Це означає, що мультифакторна аутентифікація пройдена і користувач повністю підтверджений, після чого його буде авторизовано у його обліковий запис.

Подія успішної авторизації (Success Login) в Auth0 реєструється з кодом «s», яка відбувається при умові, якщо було правильно введено логін з паролем та було пройдено додатковий фактор автентифікації. Це підтверджує, що вказані облікові дані відповідають записам у системі.

Подія з кодом «seacft» у системі журналювання Auth0 позначає успішний обмін авторизаційного коду на токен доступу (Success Exchange). Така подія свідчить про те, що після успішної автентифікації користувача та повернення авторизаційного коду, клієнт ініціював запит до сервера авторизації для обміну цього коду на токен доступу, і цей обмін пройшов успішно.

Коли користувач виходить із системи, Auth0 записує подію успішного виходу із системи (Success Logout) з кодом «slo», що означає, що сесію користувача було закрито і використання старого токена більше неможливе [61].

Перевірка стійкості MFA до атак проводиться з метою оцінки надійності впровадженого механізму захисту в реальних умовах експлуатації. У ході перевірки аналізуються можливі вектори атак. Метою є виявлення слабких місць, які можуть бути використані зловмисниками для обходу другого фактора або компрометації облікового запису. Таке тестування дозволяє не лише підтвердити ефективність наявних захисних механізмів, але й виявити сценарії, при яких навіть багатофакторна автентифікація може бути обійдена. У результаті проведеної перевірки формується цілісне уявлення про рівень стійкості системи до реальних загроз, що у свою чергу є основою для подальших покращень.

Фішинг - поширений тип кібератаки, спрямований на приватних осіб через електронну пошту, текстові повідомлення, телефонні дзвінки та інші форми

комунікації. Фішингова атака має на меті обманом змусити одержувача виконати бажані дії зловмисника, наприклад, розкрити фінансову інформацію, облікові дані для входу в систему або іншу конфіденційну інформацію. По суті, ці загрози експлуатують людську психологію, а не технічні вразливості [62].

Більш складний тип фішингу називається MITM. Це тип кібератаки, при якій зловмисник таємно перехоплює і передає повідомлення між двома сторонами, які вважають, що спілкуються безпосередньо один з одним. [63] [64].

Атака грубого перебору - це тип кібератаки, в якій зловмисники намагаються отримати несанкціонований доступ до облікового запису або зашифрованих даних методом проб і помилок, використовуючи кілька облікових даних для входу або ключів шифрування, поки не знайдуть правильний пароль [65].

Симуляцію MITM було здійснено з використанням програмного комплексу Burp Suite для перевірки стійкості TOTP та push-сповіщень проти неї.

Burp Suite - це набір інструментів для тестування на проникнення веб-додатків. Він був розроблений PortSwigger, провідною компанією у світі веб-безпеки. Burp Suite оптимізований і розроблений для задоволення потреб професійних пентестерів і є найбільш широко використовуваним інструментом у своїй галузі. Це модульний інструмент, який дозволяє проводити як ручні, так і автоматизовані тести, допомагаючи пентестерам ефективно виявляти вразливості у веб-додатках.

Головною особливістю Burp Suite є проксі-сервер. Проксі дозволяє Burp діяти як посередник між клієнтом (веб-браузером) і сервером, на якому розміщено веб-додаток. Розмістившись між цими двома компонентами, Burp зможе перехоплювати всі обміни та запити між веб-браузером і сервером. Таким чином, пентестер зможе детально проаналізувати запити і, за бажанням, змінити їх.

Для модифікації запитів проксі перехоплює запити один за одним і дозволяє пентестеру вибрати, пропустити їх або відхилити. Якщо він пропускає їх, він може змінити їх перед передачею на сервер.

Проксі також дозволяє переглядати історію запитів в реальному часі без необхідності передавати їх вручну на сервер. Насправді, це найбільш часто використовуваний режим роботи проксі-сервера [66].

Сертифікат Burp створений для того, щоб під час роботи Burp Suite можна було отримати доступ до URL-адреси на протоколі HTTPS (Hyper Text Transfer Protocol Secure), яка захищена сертифікатом TLS (Transport Layer Security).

Однією з ключових функцій TLS є перевірка автентичності веб-серверів, з якими взаємодіє браузер. Цей процес автентифікації допомагає запобігти, наприклад, маскуванню шахрайського веб-сайту під легітимний. Він також шифрує дані, що передаються, і здійснює перевірку цілісності для захисту від атак типу MITM. Щоб перехопити трафік між браузером і цільовим веб-сервером, Burp Suite повинен розірвати це TLS-з'єднання. В результаті, якщо буде спроба отримати доступ до HTTPS URL-адреси під час роботи Burp, браузер виявить, що він не зв'язується безпосередньо з автентичним веб-сервером, і покаже попередження про безпеку.

Щоб запобігти цій проблемі, Burp генерує власний TLS-сертифікат для кожного хоста, підписаний власним центром сертифікації (ЦС). Цей сертифікат ЦС генерується під час першого запуску Burp і зберігається локально. Щоб найбільш ефективно використовувати Burp Proxy з HTTPS-сайтами, потрібно встановити цей сертифікат як довірений корінь у сховище довіри браузера. Потім Burp буде використовувати цей сертифікат ЦС для створення і підписання TLS-сертифіката для кожного хоста, який відвідується, що дозволить переглядати HTTPS-адреси як зазвичай. Після цього можна використовувати Burp Suite для перегляду і редагування запитів і відповідей, надісланих по HTTPS, так само, як і для будь-яких інших HTTP-повідомлень [67].

Від атаки MITM зберігається загроза, що логін і пароль від облікового запису легко компрометуються і зчитуються зловмисником. TOTP хоч і мають обмежений час дії, його застосування не виключає можливості компрометації за умови миттєвого перехоплення, через що їх використання є все ще безпечнішим за використання логіну з паролем, але не запобігає такому виду атаки.

На відміну від TOTP, push-автентифікація забезпечує вищу стійкість до атак MITM, оскільки підтвердження здійснюється на окремому довіреному пристрої. Але все залежить від обізнаності користувача. У випадку, якщо він на фішинговому сайті ввів свої облікові дані, їх буде скомпрометовано і використано на справжньому сайті. Після чого користувачеві відправиться запит на авторизацію. Технічно обійти такий механізм без активної участі користувача неможливо.

Для перевірки стійкості пароля було використано утиліту John The Ripper. Це безкоштовне програмне забезпечення з відкритим вихідним кодом, яке використовується хакерами, як етичними, так і не дуже, для злому паролів. Вона підтримує три види атак на паролі: грубий перебір, атака за словником та атака за маскою.

Різниця цих атак в тому, що атака за словником використовує слова зі словника або іншої бібліотеки термінів для створення варіацій можливих паролів (наприклад, «Summer2025») [68]. Атаку за маскою можна використовувати для прискорення пошуку пароля, якщо відомі певні характеристики пароля (наприклад, його довжина). Маска складається з постійної та змінної частин [69]. А грубий перебір перебирає всі можливі комбінації, що є набагато довшим.

За умови відсутності вразливостей у механізмах зберігання паролів, їх збігів із відомими словниковими шаблонами, а також доступу до скомпрометованих або криптографічно слабких хешів, реалізація атаки грубого перебору стає практично неможливою навіть при використанні потужних обчислювальних систем. Забезпечення належного рівня складності, зокрема шляхом використання паролів довжиною не менше 12 символів, які містять літери різного регістру, цифри та спеціальні символи, істотно ускладнює можливість успішного підбору та підвищує загальний рівень стійкості.

Проти атаки грубого перебору обидва методи автентифікації є надійними. Завдяки вбудованим механізмам захисту проти цієї атаки у Auth0, при перебиранні пароля зловмиснику буде заблоковано IP-адресу після 10 спроб вводу паролю за короткий термін часу. Навіть у випадку, якщо зловмисник знає

пароль, перебрати TOTP код з додатку є майже неможливим через велику кількість шестизначних комбінацій цифр.

Що стосується push-методу автентифікації, то він є ще більш стійким до грубого перебору, адже сам механізм не передбачає можливості введення коду. Запит на підтвердження доступу надсилається на прив’язаний пристрій користувача, де підтвердження здійснюється вручну.

3.3 Оцінка ефективності впровадження

Оцінка ефективності впровадження MFA відбувається за KPI. Для визначення впливу MFA на безпеку інформаційної системи Creatio використовувалися наступні кількісні KPI: кількість інцидентів несанкціонованого доступу, кількість компрометованих облікових записів, час на виявлення інциденту, кількість реалізацій фішингових атак, кількість успішних спроб входу з невідомих пристроїв або локацій та кількість зменшення привілеїв (lateral movement). Статистика кількості інцидентів до впровадження MFA була проведена на базі аналізу логів та звітів з безпеки в період за 1 місяць березня.

До впровадження механізмів MFA в інформаційній системі компанії Creatio рівень інформаційної безпеки залишався вразливим до низки сучасних загроз, зумовлених використанням лише базового методу автентифікації за логіном і паролем. Аналіз засвідчив, що в середньому щомісяця фіксувалося 10 інцидентів несанкціонованого доступу до облікових записів. Основними причинами таких інцидентів були повторне використання паролів на різних платформах, слабка складність паролів та наявність облікових даних у відкритих базах після попередніх витоків.

Впродовж тестового періоду MFA, завдяки запровадженню другого фактора автентифікації у вигляді TOTP або push-повідомлень, було виявлено зменшення кількості інцидентів несанкціонованого доступу до 8. Основною

причиною вдалих спроб залишилась та ж сама проблема з використанням слабких паролів.

Кількість компрометованих облікових записів до впровадження MFA склала 17, з яких 6 стосувалися користувачів з розширеними адміністративними або технічними правами доступу. У більшості випадків компрометація відбувалася через фішинг і використання слабких паролів. Відсутність додаткових рівнів автентифікації дозволяла зловмиснику, маючи лише логін і пароль, одразу отримувати повний доступ до функціоналу системи.

Після впровадження багатофакторної автентифікації кількість випадків компрометації облікових записів у системі Creatio зменшилася до 14 в місяць. Навіть у ситуаціях, коли логіни та паролі користувачів були скомпрометовані, завдяки обов'язковому другому фактору автентифікації, деякі з спроб авторизації не завершилися успіхом. Таким чином, впровадження MFA продемонструвало свою часткову ефективність у запобіганні компрометації облікових даних.

Середній час виявлення інциденту до впровадження багатофакторної автентифікації був неприйнятно високим. За підсумками аналізу, значення MTTD становило приблизно 8 годин. Причиною такої затримки виявлення була відсутність автоматизованих систем сповіщення про підозрілі активності. Виявлення інцидентів зазвичай відбувалося або під час планових перевірок журналів активності, або після звернень користувачів, які помічали несанкціоновані дії у своїх облікових записах. Така затримка у виявленні значно ускладнювала процес реагування та локалізації загроз, а також збільшувала потенційний масштаб завданої шкоди.

Після впровадження багатофакторної автентифікації MTTD у системі Creatio скоротився з 9 годин до приблизно 6 годин. Таке покращення стало можливим завдяки впровадженню централізованого журналювання подій автентифікації в Auth0, автоматичному створенню інцидентів у разі невдалих спроб. Завдяки цим записам, адміністратори безпеки отримували актуальну

інформацію про потенційні загрози в режимі реального часу, що дозволило швидше локалізовувати та перевіряти підозрілі події.

Фішингові атаки фіксувалися в середньому 13 разів на місяць, причому в кожному другому випадку користувачі, не розпізнавши шахрайство, самостійно вводили свої облікові дані на фальшивих ресурсах. Відсутність другого етапу перевірки дозволяла зловмиснику одразу після компрометації облікових даних отримати повноцінний доступ без додаткових бар'єрів.

Після впровадження MFA в системі Creatio було зафіксовано зниження кількості успішних фішингових атак до 11 разів. В усіх випадках несанкціонований доступ стався виключно внаслідок людського фактору, коли користувачі вводили свій TOTP-код на підробленому ресурсі, що дозволило зловмиснику використати цей код у межах 30-секундного вікна дії і коли користувачі помилково підтверджували вхід до облікового запису через push-сповіщення. Таким чином, впровадження MFA забезпечило часткове зниження ефективності фішингових методів, але недостатній рівень обізнаності користувачів все ще залишається проблемою.

Ще однією серйозною проблемою була кількість успішних спроб входу з невідомих пристроїв або нетипових локацій, яка в середньому складала 12 випадків на місяць. Оскільки система не мала механізмів адаптивної автентифікації, жодна з цих спроб не блокувалася автоматично. Такі входи часто залишалися поза увагою адміністратора безпеки, оскільки не супроводжувалися явними сповіщеннями.

Після впровадження адаптивного MFA з використанням платформи Auth0 ситуація трошки покращилася: протягом тестового періоду було зареєстровано 9 подібних спроб, кожна з яких була виконана користувачами системи зі включеним стороннім VPN. Але усі такі входи були автоматично позначені як ризиковані, що активувало вимогу обов'язкового проходження другого фактора автентифікації.

Особливо тривожною була ситуація з lateral movement - переміщенням зловмисника мережею після первинного проникнення. Було зафіксовано 9

випадків, коли зловмисник після отримання доступу до облікового запису без додаткового підтвердження особи зумів переміститься до внутрішніх адміністративних панелей. У 3-х з цих випадків спостерігалася ескалація прав доступу, що дозволила зловмисникам модифікувати об’єкти в CRM-системі та зчитувати лог-файли серверів.

Після впровадження багатофакторної автентифікації ситуація з lateral movement зазнала покращення. Якщо у період до впровадження MFA було зафіксовано 9 випадків, коли зловмисник зміг переміститься між сегментами системи, то після впровадження додаткового фактора 7 спроб завершились успішно.

Сукупність наведених даних вказує на те, що без впровадження MFA інформаційна система Creatio функціонувала в умовах підвищеного ризику, при цьому вона не мала ефективних механізмів стримування чи виявлення проти ключових векторів атак. Це зумовило необхідність запровадження багаторівневої моделі автентифікації, яка дозволила покращити видимість подій безпеки та підвищити загальний рівень кіберзахисту компанії. Порівняльна статистика впливу MFA на безпеку наведена у табл. 3.1.

Таблиця 3.1

Вплив MFA на безпеку до та після її інтеграції

Критерій / KPI	До впровадження MFA	Після впровадження MFA	Степінь впливу (%)
Кількість інцидентів несанкціонованого доступу	10 випадків	8 випадків	+20%
Кількість компрометованих облікових записів	17 випадків	14 випадків	+17%

Продовження таблиці 3.1

Критерій / KPI	До впровадження MFA	Після впровадження MFA	Степінь впливу (%)
Час виявлення інциденту (MTTD)	8 годин	6 годин	+25%
Вплив фішингових атак	13 випадків	11 випадків	+15%
Кількість успішних спроб входу з невідомих пристроїв або локацій	12 випадків	9 випадків	+25%
Зменшення привілеїв lateral movement	9 випадків	7 випадків	+22%

Для визначення впливу MFA на продуктивність інформаційної системи Creatio використовувалися такі кількісні KPI: середній час входу в систему, кількість звернень до служби підтримки через проблеми MFA, простій або затримки в роботі, кількість користувачів, які відмовились через незручність, сумісність MFA з мобільними/застарілими пристроями та середній час на вирішення проблем з автентифікацією.

Середній час входу в систему до впровадження MFA займав небагато часу - в середньому 27 секунд. Це пояснювалося використанням SFA: користувач вводив логін та пароль, після чого одразу отримував доступ до робочого середовища. Незважаючи на оперативність такого процесу, саме спрощеність і відсутність додаткових факторів стали однією з причин високого ризику несанкціонованого доступу.

Після впровадження MFA середній час входу очікувано збільшився. Вхід з використанням TOTP займав 30 секунд, а з використанням push-сповіщень - 32, залежно від швидкості реакції користувача та стабільності інтернет-з’єднання на мобільному пристрої.

Кількість звернень до служби підтримки через проблеми з автентифікацією до впровадження MFA залишалася незначною. У середньому

фіксувалося 6 звернення на місяць, що були пов’язані переважно з втратою або скиданням пароля.

Ця кількість збільшилася після впровадження. Це було пов’язано з адаптацією користувачів до нової процедури. Було зафіксовано 7 звернень, які стосувалися труднощів із налаштуванням додатка Google Authenticator, втратою доступу до прив’язаного мобільного пристрою або проблемами з отриманням push-сповіщень.

До впровадження MFA затримки в роботі та простої виникали у випадках, пов’язаних із непередбачуваними блокуваннями доступу до облікових записів. Всього було зафіксовано 4 такі випадки.

Після впровадження випадки простою або затримок в роботі стали відбуватися частіше. 3 випадки через втрату мобільного пристрою користувачем і скидання додаткового фактору у його обліковому записі, 2 випадка - через тимчасову недоступність push-сервісу. В кожному з цих випадків простій не перевищував 10 хвилин.

До впровадження MFA кількість користувачів, які відмовились від використання системи через незручність автентифікації, була відсутньою через простоту процесу входу.

За результатами внутрішнього моніторингу та опитувань, після впровадення MFA один користувач висловив бажання повернутись до попередньої схеми автентифікації, аргументуючи це додатковими складнощами для авторизації у обліковий запис.

До впровадження MFA було зафіксовано 8 випадків несумісності з мобільними та застарілими пристроями. Зокрема, деякі з користувачів не змогли увійти до системи з пристрою на базі Android 4.4 через відсутність підтримки сучасних TLS-протоколів, необхідних для захищеного з'єднання. Інші випадки стосувалися смартфона з iOS 9, де веб-форма входу відображалась некоректно через несумісність з JavaScript-компонентами, що унеможливлювало введення облікових даних. Ще один випадок був пов'язаний із корпоративним ноутбуком

на Windows 7, де через обмеження політик безпеки та відсутність оновлень браузера виникали труднощі з доступом до системи.

Після впровадження MFA кількість випадків несумісності із мобільними та застарілими пристроями збільшилася до 10. У цих випадках користувачі мали проблеми з встановленням додатку Google Authenticator на старих смартфонах, де виникали збої при запуску програми. Інші випадки були пов'язані із використанням iPhone із застарілою версією iOS, яка не підтримувала push-сповіщення через Auth0 Guardian.

Середній час на вирішення проблем з автентифікацією був коротким і складав до 5 хвилин. Через відсутність складної процедури автентифікації більшість проблем вирішувалась шляхом скидання пароля або технічної підтримки користувача в рамках стандартного дзвінка або внутрішньої заявки.

Після впровадження MFA цей час збільшився в середньому до 6 хвилин. Всі випадки стосувалися втрати доступу до мобільного пристрою або необхідності повторного налаштування MFA.

Впровадження MFA не спричинило істотного уповільнення бізнес-процесів. Тимчасове зростання кількості звернень до служби підтримки було очікуваним і контрольованим, а всі проблеми з автентифікацією вирішувались у межах допустимого часу. Рівень прийнятності MFA серед користувачів залишився високим: випадків масової відмови або системної недоступності не зафіксовано. Порівняльна статистика впливу MFA на ефективність системи наведена у табл. 3.2.

Таблиця 3.2

Вплив MFA на продуктивність до та після її інтеграції

Критерій / KPI	До впровадження MFA	Після впровадження MFA	Степінь впливу (%)
Середній час входу в систему	27 секунд	32 секунд (TOTP) 30 секунд (push-сповіщення)	-18% (TOTP) -11% (push-сповіщення)

Продовження таблиці 3.2

Критерій / KPI	До впровадження MFA	Після впровадження MFA	Степінь впливу (%)
Кількість звернень до служби підтримки через проблеми MFA	6 випадків	7 випадків	-16%
Простій або затримки в роботі	4 випадки	5 випадків	-25%
Кількість користувачів, які відмовились через незручність	Відсутні	1 випадок	-100%
Сумісність з мобільними/застарілими пристроями	8 випадків	10 випадків	-25%
Середній час на вирішення проблем з автентифікацією	До 5 хвилин	До 6 хвилин	-20%

Для якісного визначення впливу впровадження MFA на безпеку та продуктивність системи використовуються наступні якісні KPI: результати опитування користувачів, аудити, тестування на проникнення та аналіз логів.

Оцінка за результатами опитування користувачів показала загалом позитивне сприйняття запровадженого механізму автентифікації. Звичайно, всім користувачам було набагато простіше користуватися системою до впровадження завдяки використанню тільки логіну і паролю. За результатами опитування, більшість оцінили MFA як зручну або повністю прийнятну та відзначили, що відчувають підвищений рівень захищеності облікових записів після впровадження другого фактора. Мала частина опитуваних висловили бажання повернутись до попередньої однофакторної моделі, що може свідчити про необхідність покращення програми навчання щодо основ MFA.

Результат аналізу попередніх аудитів безпеки інформаційної системи Creatio, які було проведено до впровадження MFA, виявив низку критичних

вразливостей у процедурі автентифікації компанії. Зафіксовано значну кількість випадків обходу механізму автентифікації.

Повторний аудит після впровадження MFA засвідчив зниження ризиків пов’язаних із автентифікацією. Зафіксовано наявність обмежень на кількість спроб входу, реєстрацію спроб аномальної активності, ізоляцію ненадійних сесій. Загальний вплив впровадження MFA на безпеку, за аудиторською оцінкою, значно покращив ситуацію з безпекою інформаційної системи.

До впровадження MFA в системі Creatio було проведено тестування на проникнення з метою оцінки рівня стійкості однофакторної моделі автентифікації до типових векторів атак. Результати виявили критичну вразливість системи: у 100% змодельованих сценаріїв наявність лише логіна та пароля дозволяла отримати повний доступ до облікового запису користувача, за умови, що ці дані були отримані або підібрані.

Після впровадження, тестування на проникнення проводилось повторно для оцінки стійкості MFA до атак. За результатами тестування стійкості MFA до атак типу MITM, було встановлено, що 1 з 2 методів автентифікації мають уразливість до обходу при сприятливих умовах для зловмисника. У результаті Push-сповіщення виявилися стійкими до цієї атаки, тому що навіть при наявності логіну та пароля зловмисник не зможе перехопити це сповіщення на пристрої користувача. Але під час тестування вдалося обійти захист TOTP-методу, що свідчить про необхідність покращення методів захисту від цієї атаки та впровадження додаткових фішингостійких методів автентифікації.

У випадку з використанням атаки типу грубого перебору, можна впевнено сказати, що обидва методи автентифікації є майже на 100% надійними від цієї атаки. Якщо розглянути спрообу обходу захисту TOTP, зловмисник має дуже низький шанс (0,00003%) вгадати 1 шестизначний код з 1000000 можливих. При використанні push-сповіщень обійти захист цього методу виявилося повністю неможливим.

До впровадження MFA, можливості аналізу логів у системі Creatio були обмеженими. Облік подій автентифікації вівся у вигляді стандартних логів про

вхід і вихід користувачів, без детального розподілу за причинами помилок чи ризиковими активностями. Відсутність спеціалізованих механізмів контролю унеможливлювала оперативне виявлення аномальної поведінки або підозрілих спроб входу.

Після впровадження MFA на базі Auth0 ситуація принципово змінилась. Інформаційна панель Auth0 надала можливість детально відстежувати події автентифікації. Завдяки цьому служба безпеки отримала змогу оперативно аналізувати ризики, будувати шаблони поведінки користувачів і впроваджувати додаткові політики захисту. Таким чином, після інтеграції MFA механізми логування трансформувались із базового моніторингу в повноцінний інструмент контролю та профілактики інцидентів, що значно підвищило рівень ситуаційної обізнаності й швидкість реагування на загрози.

Результати якісного визначення впливу MFA на інформаційну систему Creatio надано у табл. 3.3.

Таблиця 3.3

Якісне визначення впливу MFA на безпеку та продуктивність системи

Критерій / KPI	До впровадження MFA	Після впровадження MFA
Результати опитування користувачів	Користувачів повністю влаштовувало використання тільки логіну та пароля	Більшість користувачів показала загалом позитивне сприйняття запровадженого механізму автентифікації
Аудити	Результат зафіксував значну кількість випадків обходу механізму автентифікації	Результат зафіксував зниження ризиків пов’язаних із автентифікацією, що свідчить про значне покращення ситуації з безпекою інформаційної системи
Penetration Testing	Критична вразливість системи. наявність лише логіна та пароля дозволяла отримати повний доступ до облікового запису користувача	1 з 2 методів автентифікації вразливі до атаки типу MITM, що свідчить про потребу у додаткових механізмах захисту та додаткових методах автентифікації

Продовження таблиці 3.3

Критерій / KPI	До впровадження MFA	Після впровадження MFA
Аналіз логів	Можливості аналізу логів у системі Creatio були обмеженими. Логування велося у вигляді стандартних записів про вхід і вихід користувачів	Інформаційна панель Auth0 надала можливість детально відстежувати події автентифікації, завдяки чому служба безпеки отримала змогу аналізувати детальні записи пов'язаних з авторизацією та оперативно реагувати на підозрілу активність

3.4 Рекомендації щодо подальшого вдосконалення MFA в організації

З метою підвищення загальної ефективності впровадженого рішення багатофакторної автентифікації, а також мінімізації залишкових ризиків, пов'язаних із людським фактором, доцільно реалізувати системну програму навчання з обізнаності користувачів. Практика тестування та аналіз інцидентів, зафіксованих після впровадження MFA, свідчить про те, що навіть наявність другого фактора автентифікації не є абсолютною гарантією захисту, якщо користувач не усвідомлює основ фішингових атак, принципу дії токенів TOTP або механізму push-сповіщень. У виявлених випадках компрометація облікових даних або проходження авторизації зловмисником стали можливими саме через необачність користувача: введення коду TOTP на фішинговому сайті або помилкове схвалення push-запиту.

У зв'язку з цим, компанії рекомендується впровадити обов'язковий навчальний модуль для всіх нових співробітників під час онбордингу, в якому розглядатимуться основи кібергігієни, принципи роботи багатофакторної автентифікації, а також типові приклади фішингових сценаріїв. Такий курс має включати не лише теоретичні знання, а й практичне моделювання ситуацій, в яких користувач навчається розпізнавати підозрілі посилання, фальшиві форми

автентифікації, неприродні шаблони комунікації та незвичні запити на авторизацію.

Для діючих працівників доцільним є проведення щоквартальних або піврічних оновлювальних тренінгів з фокусом на нові методи атак, адаптацію до оновлень у політиках безпеки та закріплення знань щодо правильного використання MFA. Особливу увагу слід приділити тренуванню навичок дій у разі втрати пристрою для генерації токенів, виявлення підозрілих дій у системі, а також алгоритмам звернення до служби підтримки. Для контролю рівня засвоєння знань рекомендовано впровадити регулярне тестування або симуляцію фішингових атак з наступним аналізом результатів [22].

Реалізація вказаних заходів дозволить суттєво підвищити рівень обізнаності працівників, зменшити кількість інцидентів, пов’язаних із людським фактором, та забезпечити більш повноцінне функціонування механізмів MFA як частини комплексної системи захисту інформаційних активів компанії.

Інтеграція біометричних механізмів, таких як розпізнавання обличчя або відбитка пальця, може суттєво підвищити як рівень захисту, так і зручність для користувачів. Цей метод практично не підробити та він не потребує введення даних вручну, що зменшить ризик фішингових атак та сприяє пришвидшенню процедури входу [20].

Можна розглянути впровадження підтримки стандарту FIDO2, який використовує автентифікацію без використання паролів. Така модель передбачає використання апаратних ключів на окремому захищеному пристрої, що практично виключає можливість фішингових атак і водночас підвищує зручність для користувачів [19].

Для зменшення ризику реалізації атаки MITM слід використовувати надійне WEP/WPA-шифрування (Wired Equivalent Privacy/Wi-Fi Protected Access) на точках доступу, який буде запобігати приєднанню небажаних користувачів до мережі, просто перебуваючи поруч. Слабкий механізм шифрування може дозволити зловмиснику проникнути в мережу грубим перебором і почати атаку MITM.

Важливо переконатися, що стандартний логін для входу в роутер змінено. Не лише пароль до Wi-Fi (Wireless Fidelity), але й облікові дані для входу в роутер. Якщо зловмисник дізнається облікові дані для входу до роутера, він може змінити DNS-сервери на свої шкідливі. Або, що ще гірше, заразити роутер шкідливим програмним забезпеченням.

Віртуальну приватну мережу (Virtual Private Network, VPN) можна використовувати для створення безпечного середовища для конфіденційної інформації в локальній мережі. Вони використовують шифрування на основі ключів для створення підмережі для безпечного зв'язку. Таким чином, навіть якщо зловмисник потрапить у загальну мережу, він не зможе розшифрувати трафік у VPN [70].

Для запобігання випадків несанкціонованого доступу до системи та компрометації облікових записів, слід впровадити політику безпечних паролів та забезпечувати її виконання. Паролі повинні бути довжиною від 12 символів. При створенні пароля обов’язково повинні використовуватися літери верхнього та нижнього регістру, цифри та спеціальні символи. Паролі повинні оновлюватися кожні 90 днів [71].

Обов’язково слід впровадити принцип Least Privilege оскільки він обмежує доступ користувачів, процесів та сервісів лише тими правами, які необхідні їм для виконання конкретних функцій. Це значно зменшує площу атаки системи, ускладнює зловмисникам можливість вертикального або горизонтального переміщення після компрометації облікового запису та знижує ризик випадкових або навмисних дій користувачів, що можуть завдати шкоди [72].

У перспективі також доцільно реалізувати централізовану систему аналітики з автоматичними сповіщеннями про підозрілу активність, що дозволить своєчасно реагувати на потенційні загрози без потреби в постійному ручному моніторингу логів. З цією метою рекомендується інтеграція SIEM-системи (Security information and event management) у Auth0, що дозволить автоматизувати виявлення інцидентів завдяки кореляційним правилам та покращити загальну реакцію на інциденти [32].

І насамкінець, слід повністю перейти на обов’язкову MFA для покращення всієї ситуації з безпекою, що дозволить подолати початковий опір і довести рівень впровадження до значно вищих значень протягом наступних місяців.

Висновки до розділу 3

У результаті практичної реалізації MFA було реалізовано повноцінне впровадження MFA на базі хмарної платформи Auth0 у середовищі корпоративної системи Creatio. Проведено вибір відповідного технічного рішення з урахуванням специфіки інформаційної інфраструктури компанії, типів клієнтських додатків та вимог до безпеки доступу. Впроваджені механізми автентифікації на основі TOTP та push-сповіщень забезпечили надійний контроль доступу до облікових записів, при цьому залишаючись адаптивними до мобільних і десктопних платформ.

Аналіз логів і проведення тестування на проникнення дозволили сформулювати висновки щодо відносної стійкості різних методів MFA та продемонструвати їхню ефективність або неспроможність забезпечувати повний захист. Зокрема, push-аутентифікація виявилась повністю захищеною від спроб перехоплення або повторного використання, тоді як TOTP лишається потенційно вразливим у разі фішингових сценаріїв за активної участі користувача.

Результати впровадження MFA підтвердили підвищення рівня інформаційної безпеки. Також було враховано фактори, що впливають на продуктивність системи.

Таким чином, реалізована методика впровадження MFA підтвердила свою технічну життєздатність, масштабованість і здатність інтегруватися у середовище корпоративного ПЗ. Водночас встановлено, що подальше покращення можливе шляхом впровадження системного проведення навчання обізнаності персоналу, впровадженням фішингостійких методів автентифікації, впровадження додаткових механізмів захисту від атаки MITM, а також впровадженням додаткових механізмів контролю та моніторингу.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було проведено комплексний аналіз сучасних методів автентифікації користувачів в інформаційних системах, окреслено основні загрози, що супроводжують процеси автентифікації, і детально розглянуто технології MFA.

Наукова новизна дослідження полягає в узагальненні підходів до інтеграції багатофакторної автентифікації в існуючі СУІБ з урахуванням організаційно-технічних особливостей сучасної IT-інфраструктури, у створенні методики розробки і впровадження MFA, яка враховує ризик-орієнтований підхід, специфіку ролей користувачів і критичність інформаційних ресурсів та у визначенні критеріїв оцінки ефективності впровадження MFA, зокрема показників зменшення кількості інцидентів доступу, підвищення рівня довіри до аутентифікації та покращення відповідності політикам безпеки.

Проаналізовано нормативні вимоги провідних міжнародних стандартів - ISO/IEC 27001:2022, ISO/IEC 27002:2022, PCI DSS v4.0, NIST SP 800-63, NIST SP 800-63B - що підтвердило необхідність впровадження MFA як ключового елементу системи управління інформаційною безпекою.

Проаналізовано ключові вимоги щодо впровадження MFA у СУІБ організації. Створено методику розробки і впровадження MFA, що охоплює як технічні, так і організаційні аспекти. Визначено критерії (KPI) впливу впровадження на продуктивність і безпеку інформаційної системи.

Реалізовано практичну інтеграцію багатофакторної автентифікації в тестове середовище компанії Creatio з використанням платформи Auth0. Налаштовано веб-додаток, зібрано та проаналізовано логи автентифікації. Проведено тестування стійкості обраного рішення до атак MITM і грубого перебору. Оцінено вплив MFA на безпеку та продуктивність за визначеними KPI. Для подальшого покращення стану безпеки ІС надано відповідні рекомендації.

Таким чином, результати дослідження доводять доцільність та ефективність впровадження багатофакторної автентифікації в сучасних

корпоративних системах. Запропонована методика дозволяє знизити ризик несанкціонованого доступу та може бути адаптована до різних організаційних середовищ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Singh S., Kaur M. Information Security Threats and Mitigation Strategies: A Systematic Review. SSRN Electronic Journal. 2024. URL: https://doi.org/10.2139/ssrn.4482653 (дата звернення: 15.04.2025).

2. A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure / S. P. Otta et al. Future Internet. 2023. Vol. 15, no. 4. P. 146. URL: https://doi.org/10.3390/fi15040146 (дата звернення: 15.04.2025).

3. Martinez J. 11 Common Authentication Vulnerabilities You Need to Know | StrongDM. StrongDM: Your Partner in Zero Trust Privileged Access. URL: https://www.strongdm.com/blog/authentication-vulnerabilities (дата звернення: 15.04.2025).

4. A review of multi-factor authentication in the Internet of Healthcare Things / T. Suleski et al. DIGITAL HEALTH. 2023. Vol. 9. P. 205520762311771. URL: https://doi.org/10.1177/20552076231177144 (дата звернення: 18.04.2025).

5. Premsai R. Cybersecurity Risks in Identity And Access Management Using An Adaptive trust Authenticate Protocol. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. 2024. Vol. 08, no. 12. P. 1–5. URL: https://doi.org/10.55041/ijsrem25645 (дата звернення: 18.04.2025).

6. Single-Factor Authentication Explained: Pros & Cons | Hideez. Passwordless Workforce Identity Solutions | Hideez. URL: https://hideez.com/en-ua/blogs/news/single-factor-authentication (дата звернення: 19.04.2025).

7. Що таке двофакторна автентифікація і як вона працює | Центр з надання кіберзахисту. URL: https://cip.gov.ua/ua/faqs/sho-take-dvofaktorna-avtentifikaciya-i-yak-vona-pracyuye (дата звернення: 19.04.2025).

8. What is Two-factor Authentication (2FA)? How does it work? | Fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/two-factor-authentication (дата звернення: 19.04.2025).

9. Marketing I. Pros and Cons of Multi Factor Authentication | InstaSafe. Zero Trust Blog. URL: https://instasafe.com/blog/pros-and-cons-of-multi-factor-authentication/ (дата звернення: 19.04.2025).

10. Zaky K., Saxe D. H. Multi-factor Authentication. IDPro Body of Knowledge. 2022. Vol. 1, no. 10. URL: https://doi.org/10.55621/idpro.92 (дата звернення: 19.04.2025).

11. Blog I. What are the Key Differences between 2FA and MFA?. Incognia | The Next Generation of Identity (дата звернення: 19.04.2025).

12. Pros and Cons of Enabling Multi-Factor Authentication | Omnidefend. URL: https://www.omnidefend.com/pros-and-cons-of-enabling-multi-factor-authentication/ (дата звернення: 19.04.2025).

13. ISO/IEC 27001:2022. Information technology - Security techniques - Information security management systems – Requirements (дата звернення: 20.04.2025).

14. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls (дата звернення: 20.04.2025).

15. PCI Security Standards Council. Payment Card Industry Data Security Standard. Version 4.0 (дата звернення: 21.04.2025).

16. National Institute of Standards and Technology. NIST Special Publication 800-63. Digital Identity Guidelines (дата звернення: 21.04.2025).

17. National Institute of Standards and Technology. NIST SP 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management (дата звернення: 22.04.2025).

18. OTP vs TOTP vs HOTP: Which One Should You Choose? | SuperTokens Blog. URL: https://supertokens.com/blog/otp-vs-totp-vs-hotp (дата звернення: 23.04.2025).

19. 2FA with FIDO, U2F, OTP, HOTP, TOTP | DEV Community. URL: https://dev.to/pssingh21/2fa-with-fido-u2f-otp-hotp-totp-46ia (дата звернення: 23.04.2025).

20. Tejas B. Sawant, Waman R. Parulekar, Tejas V. Joshi. A Study on Biometric Authentication Systems, Privacy Concerns and Mitigation Strategies. International Journal of Scientific Research in Science and Technology. 2023. P. 199–205. URL: https://doi.org/10.32628/ijsrst52310413 (дата звернення: 23.04.2025).

21. 7 Tips for Choosing the Right Multi-Factor Authentication (MFA) Solution | Expert Insights. URL: https://expertinsights.com/user-auth/7-tips-for-choosing-the-right-multi-factor-authentication-mfa-solution (дата звернення: 01.05.2025).

22. What is MFA Implementation? | Palo Alto Networks Cyberpedia. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-mfa-implementation (дата звернення: 01.05.2025).

23. Deploying an Effective MFA Setup | InstaSafe. URL: https://instasafe.com/blog/deploying-an-effective-mfa-setup/ (дата звернення: 01.05.2025).

24. Hossain M. A., Raza M. A. EXPLORING THE EFFECTIVENESS OF MULTIFACTOR AUTHENTICATION IN PREVENTING UNAUTHORIZED ACCESS TO ONLINE BANKING SYSTEMS. SSRN Electronic Journal. 2025. URL: https://doi.org/10.2139/ssrn.5207142 (дата звернення: 01.05.2025).

25. Authentication Metrics to Track and Why They Matter | Beyond Identity. URL: https://www.beyondidentity.com/resource/authentication-metrics-to-track-and-why-they-matter (дата звернення: 02.05.2025).

26. A Guide to Selecting KPIs for Effective Security Architecture | Aquia. URL: https://www.aquia.us/blog/a-guide-to-selecting-kpis-for-effective-security-architecture (дата звернення: 02.05.2025).

27. 9 Cybersecurity Metrics & KPIs to Track | SecurityScorecard Blog. URL: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/ (дата звернення: 02.05.2025).

28. How to Prevent Lateral Movement with MFA | ISDecisions. URL: https://www.isdecisions.com/en/blog/mfa/how-to-prevent-lateral-movement-with-mfa (дата звернення: 02.05.2025)

29. Legacy Systems Create a Challenge for Multi-Factor Authentication | Carrier Management. URL: https://www.carriermanagement.com/features/2022/07/11/238087.htm?bypass=a35506137235139e52e9e99e94b2d52b (дата звернення: 02.05.2025).

30. How to Implement MFA for Legacy Applications | Strata Identity. URL: https://www.strata.io/blog/app-identity-modernization/how-to-implement-mfa-for-legacy-applications/ (дата звернення: 02.05.2025).

31. Multi-Factor Authentication Solutions | Frontegg Guides. URL: https://frontegg.com/guides/multi-factor-authentication-solutions (дата звернення: 02.05.2025).

32. Integrating Duo MFA Authentication Logs with Your SIEM Stack Using Copilot | SOCFortress on Medium. URL: https://socfortress.medium.com/integrating-duo-mfa-authentication-logs-with-your-siem-stack-using-copilot-7422637921d9 (дата звернення: 03.05.2025).

33. Multifactor Authentication Cheat Sheet | OWASP Cheat Sheet Series. URL: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet (дата звернення: 03.05.2025).

34. Understanding MFA Phishing Protection Measures and Key Statistics | Keepnet Labs. URL: https://keepnetlabs.com/blog/understanding-mfa-phishing-protection-measures-and-key-statistics (дата звернення: 03.05.2025).

35. Google Case Study | FIDO Alliance. URL: https://fidoalliance.org/google-case-study/ (дата звернення: 03.05.2025).

36. Multi-Factor Authentication is Not 99 Percent Effective | Cybersecurity Ventures. URL: https://cybersecurityventures.com/multi-factor-authentication-is-not-99-percent-effective/ (дата звернення: 03.05.2025).

37. Multi-Factor Authentication Sucks | Okta Developer Blog. URL: https://developer.okta.com/blog/2019/12/19/multi-factor-authentication-sucks (дата звернення: 03.05.2025).

38. A Single Solution for Today’s Top MFA and SSO Challenges | Cyolo White Paper. URL: https://cyolo.io/white-papers/a-single-solution-for-todays-top-mfa-and-sso-challenges (дата звернення: 03.05.2025).

39. State of Authentication in Finance Industry 2022 | HubSpot / Silverfort. URL: https://2670073.fs1.hubspotusercontent-na1.net/hubfs/2670073/DL%20Assets/State-of-Authentication-in-Finance-Industry-2022.pdf (дата звернення: 03.05.2025).

40. Sanchari D., Binxing W., Jean C. MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content. 2019. P. 23-35. URL: http://doi.org/10.48550/arXiv.1908.05902 (дата звернення: 03.05.2025).

41. Multi-Factor Authentication Statistics You Should Know | JumpCloud. URL: https://jumpcloud.com/blog/multi-factor-authentication-statistic (дата звернення: 03.05.2025).

42. SSO Service | Hideez. URL: https://hideez.com/en-ua/pages/sso-service (дата звернення: 03.05.2025).

43. About company | Creatio. URL: https://www.creatio.com/company/about (дата звернення: 06.05.2025).

44. Introduction to Auth0 | Auth0 Docs. URL: https://auth0.com/docs/get-started/identity-fundamentals/introduction-to-auth0 (дата звернення: 06.05.2025).

45. Auth0 Overview | Auth0 Docs. URL: https://auth0.com/docs/get-started/auth0-overview (дата звернення: 06.05.2025).

46. What is Next.js | Sanity Glossary. URL: https://www.sanity.io/glossary/next-js (дата звернення: 06.05.2025).

47. Configure Recovery Codes for MFA | Auth0 Docs. URL: https://auth0.com/docs/secure/multi-factor-authentication/configure-recovery-codes-for-mfa (дата звернення: 06.05.2025).

48. Mazin Adnan Abbas. Secure authentication scheme to thwart known authentication attacks using Mobile Device. Mustansiriyah Journal of Pure and

Applied Sciences. 2024. Vol. 2, no. 1. P. 46–61. URL: https://doi.org/10.47831/mjpas.v2i1.99 (дата звернення: 06.05.2025).

49. Auth0 Guardian | Auth0 Docs. URL: https://auth0.com/docs/secure/multi-factor-authentication/auth0-guardian (дата звернення: 06.05.2025).

50. Oauth | TechTarget. URL: https://www.techtarget.com/searchapparchitecture/definition/OAuth (дата звернення: 06.05.2025).

51. What is OAuth 2 | Auth0 Intro to IAM. URL: https://auth0.com/intro-to-iam/what-is-oauth-2 (дата звернення: 06.05.2025).

52. ID Tokens | Auth0 Docs. URL: https://auth0.com/docs/secure/tokens/id-tokens (дата звернення: 06.05.2025).

53. Access Tokens | Auth0 Docs. URL: https://auth0.com/docs/secure/tokens/access-tokens (дата звернення: 06.05.2025).

54. Refresh Tokens | Auth0 Docs. URL: https://auth0.com/docs/secure/tokens/refresh-tokens (дата звернення: 06.05.2025).

55. Webapp Quickstart: Next.js | Auth0 Docs. URL: https://auth0.com/docs/quickstart/webapp/nextjs (дата звернення: 07.05.2025).

56. Application Credentials | Auth0 Docs. URL: https://auth0.com/docs/secure/application-credentials (дата звернення: 07.05.2025).

57. Password Strength | Auth0 Docs. URL: https://auth0.com/docs/authenticate/database-connections/password-strength (дата звернення: 07.05.2025).

58. OpenID Connect vs OAuth 2.0 | SuperTokens Blog. URL: https://supertokens.com/blog/openid-connect-vs-oauth2#whats-openid-connect (дата звернення: 08.05.2025).

59. JIT Provisioning Defined | JumpCloud Blog. URL: https://jumpcloud.com/blog/jit-provisioning-defined (дата звернення: 08.05.2025).

60. Logs | Auth0 Docs. URL: https://auth0.com/docs/deploy-monitor/logs (дата звернення: 08.05.2025).

61. Log Event Type Codes | Auth0 Docs. URL: https://auth0.com/docs/deploy-monitor/logs/log-event-type-codes (дата звернення: 08.05.2025).

62. Phishing | Proofpoint. URL: https://www.proofpoint.com/us/threat-reference/phishing (дата звернення: 09.05.2025).

63. Man-in-the-middle phishing | Bolster Blog. URL: https://bolster.ai/blog/man-in-the-middle-phishing (дата звернення: 09.05.2025).

64. Man-in-the-middle attack (MitM) | TechTarget. URL: https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM (дата звернення: 09.05.2025).

65. Brute-force attack | IBM Think. URL: https://www.ibm.com/think/topics/brute-force-attack (дата звернення: 09.05.2025).

66. Introduction to Burp Suite | Vaadata Blog. URL: https://www.vaadata.com/blog/introduction-to-burp-suite-the-tool-dedicated-to-web-application-security/ (дата звернення: 09.05.2025).

67. Burp Suite – Certificate in External Browser | PortSwigger Documentation. URL: https://portswigger.net/burp/documentation/desktop/external-browser-config/certificate (дата звернення: 09.05.2025).

68. John the Ripper | Bugcrowd Glossary. URL: https://www.bugcrowd.com/glossary/john-the-ripper/ (дата звернення: 09.05.2025).

69. Mask attack | Elcomsoft. URL: https://www.elcomsoft.jp/help/en/edfb/mask-attack.html (дата звернення: 09.05.2025).

70. Man-in-the-Middle Attacks | Rapid7 Fundamentals. URL: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/ (дата звернення: 10.05.2025).

71. Password Policy Compliance Checklist | Syteca Blog. URL: https://www.syteca.com/en/blog/password-policy-compliance-checklist (дата звернення: 11.05.2025).

72. What is the Principle of Least Privilege | Palo Alto Networks Cyberpedia. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege (дата звернення: 11.05.2025).