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: “ ТЕХНОЛОГІЇ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ЯК СПОСІБ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ”

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

_____ Артем ЖУРАВЕЛЬ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

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

Артем ЖУРАВЕЛЬ
Ім’я, ПРІЗВИЩЕ

Керівник: Віталій САВЧЕНКО
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:
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

Журавлю Артему Вадимовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Технології багатофакторної автентифікації як спосіб захисту персональних даних”,
керівник кваліфікаційної роботи САВЧЕНКО Віталій, д.т.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

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

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *багатофакторна автентифікація, Технології багатофакторної автентифікації, захист персональних даних, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати витоки та теоретичні основи автентифікації та захисту персональних даних.
4.2. Дослідити технології багатофакторної автентифікації та приклади їх використання.
4.3. Провести аналіз практичного застосування mfa для захисту персональних даних.

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’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз витоків та теоретичних основ автентифікації та захисту персональних даних.	08.04.2025	
4.	Дослідження технології багатофакторної автентифікації та приклади їх використання.	15.04.2025	
5.	Проведення аналізу практичного застосування mfa для захисту персональних даних.	22.04.2025	
6.	Формулювання висновків за результатами проведеногодослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Артем Журавель
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(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 здобувачка Журавель А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технології багатофакторної автентифікації як спосіб захисту персональних даних"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ЖУРАВЕЛЬ Артем у кваліфікаційній роботі проаналізув особливості витоків та теоретичних основ автентифікації та захисту персональних даних, дослідив технології багатофакторної автентифікації та приклади їх використання, провів аналіз практичного застосування багатофакторної автентифікації для захисту персональних даних, розробив практичні рекомендації за темою дослідження.

ЖУРАВЕЛЬ Артем 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 двох конференціях.

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

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Журавель А.В. 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 ЖУРАВЛЯ Артема
на тему “Технології багатофакторної автентифікації як спосіб захисту персональних даних”

Актуальність. У сучасному цифровому середовищі, де державні установи, комерційні компанії та пересічні користувачі постійно зазнають ризику кіберзагроз, забезпечення інформаційної безпеки набуває пріоритетного значення. В умовах стрімкого розвитку ІТ-сфери, технологічні досягнення, які покращують продуктивність та зручність користування цифровими сервісами, одночасно створюють нові вектори атак та загрози для конфіденційності даних. Одним із ефективних інструментів у протидії несанкціонованому доступу до персональних даних виступає багатофакторна автентифікація, яка підвищує рівень захисту за рахунок використання декількох незалежних факторів перевірки особи.

З огляду на зазначене вивчення технологій багатофакторної автентифікації як способу захисту персональних даних є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено особливості технологій багатофакторної автентифікації як способу захисту персональних даних.
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: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо ефективного використання технологій багатофакторної автентифікації.

Недоліки.

Доцільно було б приділити більше уваги вивченню і класифікації програмних інструментів для впровадження технологій багатофакторної 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 ЖУРАВЕЛЬ Артем заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій багатофакторної автентифікації як спосіб захисту персональних даних. Робота складається зі вступу, трьох розділів, що містять 4 рисунка, висновків і списку використаних джерел із 48 найменувань. Загальний обсяг роботи становить 86 аркушів, з яких 7 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження технологій багатофакторної автентифікації як спосіб захисту персональних даних.

Об'єктом дослідження є процес багатофакторної автентифікації.

Предмет дослідження – особливості застосування технологій багатофакторної автентифікації як спосіб захисту персональних даних.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки.

Як результат у роботі проаналізовано особливості багатофакторної автентифікації, досліджено основні характеристики впровадження технологій багатофакторної автентифікації; вивчено інструменти та методи впровадження багатофакторної автентифікації як спосіб захисту персональних даних, розроблено практичні рекомендації.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті захисту персональних данних.

Ключові слова: БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, ТЕХНОЛОГІЇ БАГАТОВАКТОРНОЇ АВТЕНТИФІКАЦІЇ, ПЕРСОНАЛЬНІ ДАННІ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАННИХ.

ABSTRACT

The qualification work is devoted to the study of multifactor authentication technologies as a way to protect personal data. The work consists of an introduction, three chapters containing 4 figures, conclusions and a list of references of 48 titles. The total volume of the work is 86 pages, of which 7 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to study multifactor authentication technologies as a way to protect personal data.

The object the study is the multifactor authentication process.

The subject of the study is the peculiarities of using multifactor authentication technologies as a way to protect personal data.

Research methods. To solve the above scientific task, the paper uses the methods of analysis and synthesis, comparison, classification, and an expert evaluation.

As a result, the paper analyzes the features of multifactor authentication, examines the main characteristics of the implementation of multifactor authentication technologies; examines the tools and methods of implementing multifactor authentication as a way to protect personal data, and develops practical recommendations.

Field of application. The developed approaches can be used in the planning and implementation of an enterprise information security management system in the context of personal data protection.

Keywords: MULTIFACTOR AUTHENTICATION, MULTIFACTOR AUTHENTICATION TECHNOLOGIES, PERSONAL DATA, PERSONAL DATA PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ..... … 10

ВСТУП 11

РОЗДІЛ 1 ВИТОКИ ТА ТЕОРЕТИЧНІ ОСНОВИ АВТЕНТИФІКАЦІЇ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ 13

1.1 Еволюція технологій MFA 13

1.2 Вплив кібербезпеки на розвиток MFA 15

1.3 Основні етапи та віхи розвитку MFA..... 15

1.4 Ключові терміни і поняття в MFA 17

1.5 Види автентифікації 19

1.6 Моделі доступу та управління правами 23

1.7 Криптографічні основи захисту 27

1.8 Стандарти та найкращі практики автентифікації і захисту даних 31

1.9 Роль автентифікації у забезпеченні захисту персональних даних 37

1.10 Проблеми та виклики реалізації автентифікації і захисту даних 40

Висновки до розділу 1 45

РОЗДІЛ 2 ТЕХНОЛОГІЇ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ПРИКЛАДИ ЇХ ВИКОРИСТАННЯ..... 47

2.1 Сучасні технологій багатофакторної автентифікації 47

2.2 Приклади впровадження MFA в різних сферах 54

2.3 Типові загрози та способи обходу MFA, методи захисту 58

2.4 Методи захисту та найкращі практики MFA 63

Висновки до розділу 2 64

РОЗДІЛ 3 АНАЛІЗ ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ MFA ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ..... 66

3.1 Вибір технології MFA для конкретної системи 68

3.2 Практичне впровадження багатофакторної автентифікації 71

Висновки до розділу 3 78

ВИСНОВКИ …… 80

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ …… 81

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) ……. 87

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
FIDO2	Fast Identity Online 2
GDPR	General Data Protection Regulation
HOTP	HMAC-based One-Time Password
IA	Identification and Authentication
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OTP	One-Time Password
PSD2	Payment Services Directive 2
RSA	Rivest–Shamir–Adleman
SSPR	Self-Service Password Reset
TOTP	Time-based One-Time Password
U2F	Universal 2nd Factor
VPN	Virtual Private Network

ВСТУП

Актуальність теми. У сучасному цифровому середовищі, де державні установи, комерційні компанії та пересічні користувачі постійно зазнають ризику кіберзагроз, забезпечення інформаційної безпеки набуває пріоритетного значення. В умовах стрімкого розвитку IT-сфери, технологічні досягнення, які покращують продуктивність та зручність користування цифровими сервісами, одночасно створюють нові вектори атак та загрози для конфіденційності даних. Одним із ефективних інструментів у протидії несанкціонованому доступу до персональної інформації виступає багатофакторна автентифікація (Multi-Factor Authentication, MFA), яка підвищує рівень захисту за рахунок використання декількох незалежних факторів перевірки особи.

З огляду на зазначене вивчення технологій багатофакторної автентифікації як способу захисту персональних даних є актуальним науковим завданням.

Мета роботи полягає у дослідженні технологій багатофакторної автентифікації як спосіб захисту персональних даних.

Об'єкт дослідження – процес багатофакторної автентифікації.

Предмет дослідження – особливості застосування технологій багатофакторної автентифікації як спосіб захисту персональних даних.

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

1. Проаналізувати витоки та теоретичні основи автентифікації та захисту персональних даних.

2. Дослідити технології багатофакторної автентифікації та приклади їх використання.

3. Провести аналіз практичного застосування mfa для захисту персональних даних.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані при впровадженні технологій багатофакторної автентифікації в інформаційні системи організацій для підвищення рівня захисту персональних даних. Запропоновані підходи дозволяють здійснити обґрунтований вибір типів автентифікаторів та методів їх комбінації відповідно до рівня ризику, технічних можливостей і специфіки бізнес-процесів підприємства.

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

РОЗДІЛ 1 ВИТОКИ ТА ТЕОРЕТИЧНІ ОСНОВИ АВТЕНТИФІКАЦІЇ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Перші приклади MFA можна знайти ще в 1960-х роках. Зокрема, банкомати (ATM), які з'явилися у 1967 році, вимагали дві складові – банківську картку та PIN-код – для підтвердження особи користувача [1]. Таке поєднання *«чогось, що ви маєте»* і *«чогось, що ви знаєте»* стало прообразом сучасної двофакторної автентифікації. Аналогічно, системи "chip-and-PIN" для банківських карток (картка + PIN) теж є раннім прикладом MFA [2].

Сучасна реалізація 2FA з'явилася у середині 1980-х. Компанія RSA у 1986 році першою запропонувала комерційний токен-брелок, що генерував одноразові паролі (RSA SecurID) [3]. Цей пристрій додавав короткий код до паролю користувача і забезпечував додатковий фактор захисту. Протягом наступних 20 років великі корпорації та урядові установи активно використовували такі апаратні токени для захисту внутрішніх систем [3].

Ідея багатофакторної автентифікації була формалізована в 1990-х роках. Наприклад, компанія AT&T запатентувала метод двофакторної автентифікації у 1995 році (патент видано в 1998) [4]. Окремо своє авторство технології заявляв підприємець Кім Дотком (Kim Schmitz), який подав патент у 1998 році та отримав його у 2000-му [6]. Хоча питання першості залишається спірним, очевидно, що концепція «пароль + додатковий фактор» утвердилась до кінця 90-х років.

1.1 Еволюція технологій MFA

1990-ті роки ознаменувалися появою доступних рішень для 2FA на основі фізичних пристроїв. Широко впроваджувалися апаратні токени (такі як RSA SecurID), що генерували одноразові паролі або коди та використовувались у парі з паролем [1]. Смарт-картки з PIN-кодом також застосовувалися для захисту доступу в корпоративному та державному середовищі. Недоліком цих рішень була потреба видавати і носити спеціальні пристрої.

У 2000-х роках із поширенням мобільних телефонів з’явилися м’якші за інтеграцією методи 2FA. Одноразові паролі (OTP) почали надсилатися користувачам через SMS або генеруватися в мобільних додатках-автентикаторах, таких як Google Authenticator [1]. Це зменшило потребу в окремому апаратному токені, адже смартфон став другим фактором, що завжди під рукою. Уже в 2004 році видання *New York Times* відзначало зростання популярності двофакторної автентифікації у банках [5]. Водночас виникли і нові загрози – наприклад, атаки типу SIM-swapping для перехоплення SMS-кодів, які продемонстрували вразливість автентифікації через SMS [1].

У 2010-х роках почали широко застосовувати *«те, ким ви є»* як третій фактор. Смартфони та інші пристрої отримали сканери відбитків пальців, розпізнавання обличчя, райдужки ока тощо, що зробило біометрію масовим явищем [1]. Біометричні фактори (відбитки, обличчя) почали комбінувати з традиційними (паролі, OTP), утворюючи повноцінну багатофакторну автентифікацію [1]. Наприклад, у смартфонах Apple з 2013 року (Touch ID) і 2017 року (Face ID) біометрична автентифікація інтегрована для підтвердження доступу [8]. Біометрія значно підвищила зручність і безпеку, хоча породила дискусії щодо приватності та методів обману цих систем.

Розвиваючись далі, MFA перейшла до адаптивних моделей, де додаткові фактори запитуються лише за підвищеного ризику (з врахуванням геолокації, поведінки, параметрів пристрою) [1]. Паралельно набули розвитку безпарольні технології (FIDO2, WebAuthn), які спираються на крипографічні ключі та біометрію замість традиційних паролів [1]. Таким чином, еволюція MFA триває – від фізичних токенів до смартфонів і біометрії, а зараз до більш непомітних та постійних методів перевірки.

1.2 Вплив кібербезпеки на розвиток MFA

Зростання кіберзагроз суттєво вплинуло на популяризацію багатофакторної автентифікації. У 2010-х роках відбувся вибух випадків витоку даних і зламів облікових записів, що продемонструвало ненадійність одного лише пароля. Дослідження відзначають, що саме масові витоки паролів та їх компрометація зумовили стрімке запровадження 2FA/MFA у багатьох сервісах [4]. Коли зловмисники почали активно експлуатувати викрадені паролі (які користувачі часто повторно використовують), необхідним став додатковий фактор захисту.

Деякі гучні інциденти безпеки напряму спонукали до розвитку MFA. Наприклад, уразливість Heartbleed (2014) призвела до витоку мільйонів паролів і наочно показала вразливість традиційної аутентифікації. Це змусило і бізнес, і громадськість усвідомити проблему, і вже незабаром Білий дім розпочав кампанію “#TurnOn2FA”, закликаючи користувачів масово ввімкнути двофакторний захист [2]. Серія інших атак – злами акаунтів знаменитостей (iCloud), випадки викрадення даних великих компаній (Sony, OPM тощо) – спричинила появу рекомендацій та вимог використовувати MFA всюди, де це можливо [3]. В результаті, до середини 2010-х двофакторна автентифікація перетворилась із “незручної опції” на базовий компонент кібербезпеки для захисту від фішингу, зламу акаунтів та інших атак.

1.3 Основні етапи та віхи розвитку MFA

- **1967:** Перший банкомат (Barclays, Лондон) — поєднання картки та PIN як прототип двофакторної автентифікації [1].
- **1986:** RSA SecurID — запуск першого масового токена OTP; апаратні генератори кодів увійшли в ужиток для корпоративної безпеки [3].
- **1995:** Патент AT&T на 2FA — офіційне визнання технології двофакторної автентифікації (патент США, видано 1998) [4].

- **2000-ні:** Банківські онлайн-сервіси впроваджують 2FA для клієнтів. З початку 2000-х банки почали видавати OTP-токени та надсилати SMS-коди для підтвердження транзакцій; про *«бум»* двофакторної автентифікації повідомляла преса вже у 2004 році [5].
- **2010:** Атака Operation Aurora – злами Gmail китайськими хакерами. Це спонукало Google увести додаткові фактори: наприкінці 2010 року Google запустив додаток Google Authenticator, а з початку 2011-го надав двофакторний логін усім користувачам Google Accounts [3]. Вперше 2FA стала доступною масово для мільйонів користувачів інтернету.
- **2011–2014: Масове впровадження 2FA великими платформами.** Слідом за Google у 2011–2013 роках такі компанії, як *Facebook, Microsoft, Apple, Twitter, Yahoo* та інші, почали пропонувати користувачам опцію двофакторної автентифікації [3]. У 2014 році вийшов стандарт FIDO U2F, що поклав початок безпарольним апаратним ключам. Того ж року сталися інциденти (як-от Heartbleed), які підштовхнули державні органи до активних дій (ініціативи *"Lock Down Your Login"* та ін.).

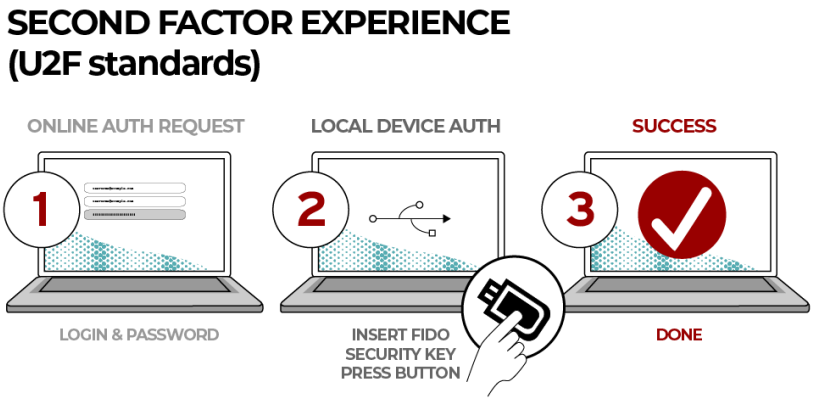

Рис. 1.1. Схема стандарту U2F [3]

- **2015–2017: Регуляторні вимоги.** У відповідь на кіберзагрози з'являються обов'язкові вимоги MFA в різних сферах. Стандарти на кшталт PCI-DSS (платіжні системи) та європейська директива PSD2 (банківські послуги)

зобов’язали використовувати сильну автентифікацію для захисту платежів і даних клієнтів [7]. Федеральна торгова комісія США у 2015 році також включила двофакторну автентифікацію до офіційних рекомендацій з безпеки для бізнесу [3]. Смартфони тим часом масово оснащуються Touch ID/Face ID, що привчає користувачів до біометричної 2FA.

- **2020–2021: Нова реальність та обов’язковий MFA.** Пандемія COVID-19 різко збільшила кількість віддаленого доступу – компанії й заклади освіти вимушено розгорнули MFA для захисту VPN і онлайн-ресурсів [6]. Концепція Zero Trust (нульової довіри) стала державною політикою: згідно з Указом Президента США 14028 (травень 2021), всі федеральні установи зобов’язані впровадити багатофакторну автентифікацію та шифрування до кінця 2024 року [6]. Подібні вимоги висуваються і в інших країнах та галузях.

1.4 Ключові терміни і поняття в MFA

Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [25]. Іншими словами, будь-яка інформація, що стосується конкретної людини (ПІБ, адреса, дата народження, біометричні дані, ідентифікаційний номер тощо), належить до персональних даних. Захист персональних даних означає забезпечення недоторканності приватного життя особи шляхом належної обробки та зберігання таких відомостей, запобігання їх витоку, несанкціонованому використанню чи іншим порушенням прав суб’єкта даних. Законодавство визначає принципи обробки і захисту персональних даних, покладаючи на володільців і розпорядників даних обов’язок гарантувати конфіденційність і цілісність інформації про особу [22].

Ідентифікація, автентифікація та авторизація. Ідентифікація – це процес надання користувачем системі своїх даних для розпізнавання, тобто заявлення певної ідентичності (наприклад, введення логіна або пред’явлення електронного сертифіката) [11]. Автентифікація – це перевірка достовірності

такої заявленої ідентичності, встановлення факту, що суб’єкт є тим, за кого себе видає [11]. За визначенням NIST, автентифікація – це засіб встановлення правильності пред’явленої ідентичності, як правило, шляхом перевірки певних доказів чи автентифікаторів (наприклад, пароля, токена або біометричного шаблону) [11]. Таким чином, під час автентифікації система переконується, що користувач справді володіє відповідними обліковими даними. Авторизація ж – це процес надання автентифікованому користувачу певних прав доступу, визначення того, які дії йому дозволені в системі. Іншими словами, після успішної автентифікації здійснюється контроль доступу – перевірка, чи має даний суб’єкт право доступатися до запитуваних ресурсів або операцій. Наприклад, користувач, пройшовши автентифікацію (ввівши правильний пароль), залежно від своєї ролі, може бути авторизований лише на перегляд певних даних, але не на їх редагування.

У контексті захисту інформації автентифікація та авторизація тісно пов’язані, але виконують різні функції. Автентифікація встановлює **хто** звертається до системи, а авторизація визначає **що** цей суб’єкт може робити. Обидва етапи є частинами єдиного механізму управління доступом (Access Control) і разом з принципом обліку (відстеження дій користувачів) утворюють основу політики безпеки інформаційних систем [11]. В українській термінології автентифікацію інколи також називають авторизацією доступу або розпізнаванням користувача, хоча слід розрізняти ці поняття: перше – підтвердження особи, друге – надання прав.

Автентифікатор – це той фактор або дані, за допомогою яких здійснюється автентифікація суб’єкта. Автентифікаторами можуть бути різноманітні засоби: пароль чи інший секрет (те, що відомо користувачу), апаратний токен або картка (те, що користувач має), біометричні характеристики (те, ким користувач є) [11]. В подальших розділах детально розглянуто види автентифікаторів та способи їх комбінування.

Конфіденційність, цілісність, доступність. Ці три властивості становлять класичну тріаду безпеки CIA (Confidentiality, Integrity, Availability).

Конфіденційність означає, що дані захищені від несанкціонованого доступу чи розкриття; цілісність – що дані захищені від несанкціонованої модифікації або знищення; доступність – що авторизовані користувачі мають своєчасний та безперебійний доступ до інформації. У контексті захисту персональних даних конфіденційність виступає на перший план, адже персональні відомості є чутливими і підлягають обмеженню кола осіб, що можуть їх бачити чи обробляти. Автентифікація користувачів є безпосередньо пов'язаною з забезпеченням конфіденційності: тільки успішно автентифіковані та належним чином авторизовані суб'єкти мають отримати доступ до персональних даних. Відповідно, порушення автентифікації (наприклад, компрометація пароля) ставить під загрозу конфіденційність і цілісність даних – зловмисник може не лише прочитати чужі дані, а й змінити або викрасти їх. Тому автентифікація є фундаментом, на якому будується захист інформації в системі [11].

1.5 Види автентифікації

Існує кілька підходів до автентифікації, які різняться типом автентифікаторів та рівнем надійності. Класично виділяють три категорії факторів автентифікації: знання, володіння та характеристика користувача [11]. На основі цих факторів розрізняють такі основні види автентифікації:

- **Автентифікація за знанням (текстовий пароль, PIN-код, секретні питання).** Це найбільш розповсюджений і традиційний спосіб – користувач повідомляє системі деякий секрет, який відомий лише йому. Паролі – приклад автентифікатора типу "те, що знає користувач". При цьому безпека залежить від складності пароля та його конфіденційності. Недолік паролів полягає в тому, що люди схильні обирати прості або однакові паролі для різних сервісів, що підвищує ризики компрометації [17]. Крім того, паролі можуть бути викрадені шляхом фішингу чи зламування баз даних. Стандарти радять застосовувати стійкі паролі (значну довжину, різноманітні символи) та не використовувати ті, що були скомпрометовані раніше [19]. Однак навіть складний пароль

залишається єдиним фактором, який може бути підглянутий або вгаданий, тому нині паролям рекомендують доповнення іншими факторами автентифікації.

- **Автентифікація за володінням (апаратні токени, смарт-карти, мобільні пристрої).** У цьому випадку користувач доводить свою особу тим, що має певний фізичний предмет чи пристрій. Наприклад, це може бути електронний токен генерування одноразових паролів (OTP), USB-ключ безпеки, смарт-карта з чипом, корпоративний бейдж із RFID, або навіть зареєстрований смартфон з додатком-аутентифікатором. При доступі до системи користувач вводить динамічний код з токена або підключає картку – система перевіряє валідність цього об’єкта. Такі методи менш залежні від пам’яті користувача (не треба запам’ятовувати секрет), проте вразливі до втрати чи крадіжки пристрою. Якщо токен потрапить до рук зловмисника, той зможе автентифікуватися від імені власника. Тому важливо поєднувати фактор володіння з іншими – наприклад, захищати токен PIN-кодом (двохфакторна схема: маєш токен + знаєш PIN). Стандарти автентифікації високого рівня вимагають, щоб апаратні автентифікатори були стійкими до підробки та копіювання, а передача даних з них – захищеною криптографічно [13].
- **Автентифікація за характеристиками (біометрична).** Цей вид автентифікації ґрунтується на унікальних фізичних або поведінкових характеристиках особи: відбитки пальців, рисунок райдужної оболонки ока, риси обличчя (розпізнавання обличчя), голос, підпис, навіть манера введення тексту чи ходьба [21]. Біометричні технології набули широкого поширення – від розблокування смартфонів відбитком чи обличчям до систем контролю доступу на підприємствах. Їх перевага – зручність для користувача (не треба запам’ятовувати чи носити з собою, “пароль завжди з вами”) і досить високий рівень надійності: біометричні характеристики складно вкрасти або підробити [21]. Водночас біометрія має низку специфічних викликів і ризиків. По-перше, будь-яка система біоавтентифікації оперує цифровими шаблонами (відбитками) цих характеристик, які зберігаються в базі; компрометація біометричних шаблонів створює серйозний ризик, адже на відміну від пароля, відбиток пальця

чи рисунок обличчя неможливо змінити – витік таких даних має незворотні наслідки для приватності [21]. По-друге, є імовірність помилок: хибні відмови (система не впізнала власника) чи хибні прийняття (впустила чужого). Якість біометрії залежить від алгоритмів і умов – вологі пальці, слабке освітлення тощо можуть завадити розпізнаванню [13]. По-третє, виникають питання етики і законності: використання біометрії повинно відповідати законодавству про захист персональних даних, отримувати згоду суб'єктів, гарантувати, що дані не будуть використані не за призначенням (наприклад, для стеження) [21]. З цих причин біометрія часто поєднується із іншими факторами (наприклад, смартфон розблоковується одночасно відбитком і PIN-кодом) та потребує альтернативних способів входу на випадок відмови біометричного (резервний пароль тощо) [13]. Не зважаючи на недоліки, біометрична автентифікація відіграє зростаючу роль у підвищенні зручності та безпеки, особливо в комплексі з традиційними методами.

Окрім наведених, можна згадати додаткові фактори, які іноді виділяють окремо: "те, що ви робите" – поведінкові шаблони (динамічна автентифікація за моделлю поведінки користувача в системі), та "те, де ви є" – автентифікація за місцеположенням або часом (напр. дозволити вхід тільки з визначеного пристрою або мережі, у робочі години). Такі фактори зазвичай застосовуються для адаптивної (risk-based) автентифікації: система аналізує контекст входу і при підозрілій активності може вимагати додаткове підтвердження. Наприклад, якщо спробу входу зафіксовано з незвичного географічного регіону чи в нетиповий час, користувачу надсилається запит підтвердити особу додатково (OTP-кодом, біометрією тощо) [13]. Такий підхід підвищує безпеку без постійного навантаження на користувача – додаткові кроки ввімкнено лише за ризикових умов.

Однофакторна vs багатофакторна автентифікація. Якщо при вході використовується лише один фактор (скажімо, тільки пароль або тільки відбиток пальця), то це однофакторна автентифікація (SFA). Її надійність обмежена стійкістю одного автентифікатора. Для значного посилення захисту нині

повсюдно впроваджується двохфакторна або ширше багатофакторна автентифікація (MFA) – комбінування щонайменше двох незалежних факторів з різних категорій [13]. Найпоширеніший приклад – це пароль + одноразовий код з телефону: зломщик, перехопивши чи вгадавши лише пароль, все одно не зможе увійти без доступу до другого фактору (телефону). Статистика демонструє колосальну ефективність MFA: за оцінками корпорації Microsoft, підключення двохфакторної автентифікації здатне блокувати до ~99% масових атак на облікові записи [19]. Впровадження MFA зараз розглядається як обов'язкове для критичних систем і конфіденційних даних. Деякі стандарти безпеки прямо вимагають MFA для адміністраторів та віддаленого доступу. Наприклад, рекомендації NIST визначають три рівні впевненості у автентифікації (Authenticator Assurance Levels, AAL1–AAL3), де на найвищому рівні AAL3 потрібні щонайменше два різних фактори, зокрема апаратний криптографічний токен плюс додатковий фактор [10]. Організації, що впровадили багатофакторну автентифікацію, суттєво знижують ризик викрадення персональних даних навіть у разі компрометації частини автентифікаційної інформації (наприклад, якщо пароль утече, залишиться другий фактор).

Серед сучасних тенденцій – відмова від паролів як таких, тобто перехід до методів автентифікації без введення користувачем секретного слова. Це так звана passwordless-аутентифікація. Вона все одно базується на описаних вище факторах – просто для користувача прибирається необхідність пам'ятати пароль. Наприклад, технологія FIDO2/WebAuthn дозволяє автентифікуватися на сайтах за допомогою апаратного ключа безпеки або біометрії пристрою: браузер виконує криптографічний протокол за участі апаратного автентифікатора і генерує підпис (що доводить особу), користувачу досить лише підтвердити дію на своєму пристрої (доторкнутися до USB-ключа або пройти біометрію) [19]. Таким чином усувається ризик фішингу пароля та використання вразливих або повторних паролів. Багато великих постачальників (Microsoft, Google, Apple) просувають підходи passwordless, інтегруючи подібні методи (наприклад, Microsoft Hello на Windows використовує TPM-модуль комп'ютера і

біометрію/ПІН замість пароля, що відповідає концепції passwordless). Очікується, що в найближчі роки такі схеми доповнять або й замінять класичні паролі для більшості користувачів, підвищивши одночасно і безпеку, і зручність. Втім, повна відмова від паролів ще потребує вирішення питань сумісності зі старими системами і виховання довіри у користувачів до нових технологій автентифікації.

1.6 Моделі доступу та управління правами

Автентифікація користувача – необхідна передумова, щоб система знала хто звернувся за доступом. Наступний крок – вирішити, що саме цьому користувачу дозволено робити. Це завдання вирішує модель контролю доступу (access control model), яка визначає правила, за якими призначаються та перевіряються права доступу суб'єктів до ресурсів системи. У теорії інформаційної безпеки напрацьовано кілька базових моделей доступу: дискреційна (DAC), обов'язкова (MAC), рольова (RBAC), а також більш сучасні варіанти на основі атрибутів (ABAC) тощо. Розглянемо їх принципи.

Дискреційна модель доступу (DAC, Discretionary Access Control). При DAC власник ресурсу самостійно визначає, хто має доступ до його даних і що саме дозволено робити [15]. Ця модель надає максимальну гнучкість і "дискрецію" власникам об'єктів. Наприклад, у файловій системі Windows або Unix власник файлу може виставити для нього права (читати/писати/виконувати) для інших користувачів або груп на власний розсуд. "Дискреційність" означає, що кінцеве рішення про надання доступу приймається суб'єктом, який контролює ресурс, а не централізованою політикою. DAC є найбільш поширеною у цивільних системах завдяки простоті та прозорості: вона інтуїтивна, дозволяє гнучко змінювати права відповідно до потреб бізнесу, полегшує спільну роботу (власник може поділитися файлом із колегою, надавши йому доступ) [15]. Однак недоліком є слабший контроль і потенційні уразливості: користувач може випадково чи навмисно відкрити доступ стороннім, складніше забезпечити єдину

політику безпеки по всій організації. Безпека при DAC залежить від сумлінності кожного власника ресурсу, тому зростає ризик несанкціонованого доступу через людський фактор [15]. До того ж, DAC у чистому вигляді не запобігає поширеним атакам внутрішніх порушників: користувач із доступом до об'єкту може переприсвоїти права іншому або скопіювати інформацію і розповсюдити її, чого не контролює центральна політика. Через це у середовищах з високими вимогами до безпеки (наприклад, військових) дискреційна модель вважається недостатньою.

Обов'язкова модель доступу (MAC, Mandatory Access Control). На відміну від DAC, обов'язкова (або мандатна) модель передбачає централізовану політику керування доступом, де рішення про доступ визначаються суворими правилами, встановленими адміністратором, і не можуть змінюватися користувачами [15]. Класичний приклад MAC – багаторівнева модель з мітками секретності в урядових системах (такими як модель Белла-Лападули для конфіденційності). Кожному об'єкту (файлу, запису) присвоюється певний гриф доступу (наприклад, "Таємно", "Цілком таємно"), а кожному суб'єкту – рівень допуску (наприклад, персонал з відповідним рівнем секретності). Правила MAC зазвичай влаштовані так: суб'єкт може читати інформацію не вище свого рівня (заборона "читання вниз" – щоб секретні дані не потрапили тим, хто не має допуску), і може записувати інформацію не нижче свого рівня (щоб не "знизити секретність" даних при записі). Характерна ознака MAC – жорстка фіксація політики: користувачі не можуть самостійно змінити права або поділитися ресурсом, усе визначає адміністратор і система згідно з заданими правилами [15]. Це забезпечує високий рівень контролю і зменшує ризик довільного витоку інформації. MAC ідеальна для середовищ, де потрібна максимальна безпека – збройні сили, урядові організації, критична інфраструктура [15]. Її переваги: висока безпека та централізований захист – унеможливлює ситуацію, коли недосвідчений співробітник випадково виставив неправильні права. Недоліки: ригідність та складність управління – щоб політика підходила під всі випадки, її треба ретельно продумати; важко адаптуватися під зміни, гнучкість мінімальна

[15]. У сучасних корпоративних системах чистий MAC застосовується рідко (хіба що в спеціальних системах): він може гальмувати робочі процеси. Проте елементи MAC присутні, наприклад, у системах з матричним контролем доступу або помітковим доступом (коли ресурсам присвоюються теги, і доступ вирішується на їх основі). Загалом MAC гарантує, що користувач не зможе обійти обмеження, навіть якщо формально має права власника якогось об'єкту – його дії все одно обмежені глобальними правилами безпеки.

Дискреційна та обов'язкова моделі – це дві крайнощі спектру: DAC дає свободу ціною потенційної ризикованості, MAC забезпечує контроль ціною гнучкості [15]. У реальних системах часто використовується комбінований підхід: критично важливі ресурси захищено MAC-політиками, а менш чутливі – DAC для зручності. Існують також гібридні моделі (напр. рольово-дискреційна), що намагаються поєднати плюси обох підходів [15].

Рольова модель доступу (RBAC, Role-Based Access Control). Рольова модель стала проміжним рішенням, що отримало широке визнання в корпоративному секторі. При RBAC права доступу призначаються ролям, а не безпосередньо користувачам [26]. Роль – це певна сукупність привілеїв, яка відповідає посаді або функції в організації. Наприклад, роль "Менеджер відділу" може мати права читати та редагувати документи свого відділу, затверджувати заявки, але не мати доступу до IT-адміністрування. Користувачі призначаються на ролі відповідно до своїх службових обов'язків, і через роль успадковують усі потрібні дозволи. Такий підхід значно спрощує адміністрування: замість керування правами кожного окремого співробітника, достатньо настроїти набір типових ролей і стежити, щоб кожен мав правильну роль. RBAC також сприяє реалізації принципу найменших привілеїв – користувач отримує тільки ті права, що необхідні для його ролі. У великих організаціях ролі часто ієрархічні (вищі ролі успадковують дозволи нижчих) [26], що відображає структуру підпорядкування. Рольова модель вважається більш централізованою, ніж DAC, але більш гнучкою, ніж чистий MAC. Адміністратори визначають набір ролей і їх привілеї – тобто політика доступу певною мірою централізована, користувачі

самі не обирають права, але система все ж більш динамічна: при зміні функцій працівника достатньо змінити його роль. Сьогодні RBAC є дефакто стандартом у системах управління доступом на підприємствах. Більшість СУБД, операційних систем та застосунків підтримують рольове розподілення прав. Стандарт RBAC був формалізований NIST у 1992 р. і нині має різні варіації (статичний RBAC, динамічний з активацією ролей тощо).

Модель на основі атрибутів (ABAC, Attribute-Based Access Control). Рольова модель не завжди достатньо гнучка, особливо якщо контекст прийняття рішень складний. ABAC – більш загальний підхід, при якому рішення про доступ ґрунтуються на наборі атрибутів суб'єкта, об'єкта та навколишнього середовища за заздалегідь визначеними правилами. Атрибути – це властивості, наприклад: для користувача – його відділ, посада, рівень допуску, для даних – рівень чутливості, для середовища – час доби, тип запиту тощо. Політика ABAC може звучати так: "дозволити співробітникам з атрибутом Department=Sales читати об'єкти з атрибутом Type=ClientData лише в робочі години". Таким чином, ABAC охоплює і ролі (роль – теж атрибут), і мітки MAC (рівень секретності – атрибут). Це надзвичайно потужна та гнучка модель, яка реалізована, зокрема, у стандартах XACML (eXtensible Access Control Markup Language) від OASIS [26]. ABAC дозволяє динамічно змінювати правила без необхідності перерозподілу прав вручну: достатньо змінити атрибут чи правило. В контексті захисту персональних даних ABAC корисна, бо можна врахувати статус суб'єкта (наприклад, "чинний клієнт" чи "колишній клієнт") або категорію даних (наприклад, "медичні дані – доступ тільки медикам із ліцензією"). Недолік ABAC – складність реалізації: потребує потужної системи прийняття рішень (PDP), визначення усіх релевантних атрибутів і підтримки їх актуальності. Втім, багато сучасних систем (хмарні рішення, системи керування доступом у великих організаціях) поступово впроваджують політики, близькі до ABAC, для більшого контролю.

Інші моделі та концепції. Окрім наведених, існують спеціалізовані моделі контролю доступу, такі як модель на основі правил (Rule-Based Access Control),

де рішення приймаються на основі набору умов (дещо подібно до бранчів ABAC, іноді Rule-BAC розглядають як частковий випадок ABAC). Також є модель на основі володіння (Capability-Based), де суб'єкти отримують незвідні маркери-дозволи ("capability") для доступу до об'єктів; вона використовується в деяких ОС і прикладних системах.

Сьогодні все більшого значення набуває концепція "нульової довіри" (Zero Trust), яка не є моделлю контролю доступу у традиційному сенсі, але задає філософію: жодному суб'єкту чи мережевому вузлу не довіряти за замовчуванням, кожен доступ має бути автентифіковано і авторизовано наново незалежно від попередніх сесій чи розташування в мережі. Реалізація принципів Zero Trust часто включає сувору автентифікацію та авторизацію при кожному зверненні до ресурсу, мікросегментацію мережі, моніторинг аномалій тощо. Таким чином, роль автентифікації ще більше підвищується – вона має бути неперервною і контекстною.

Отже, моделі контролю доступу забезпечують авторизаційну складову захисту даних. Вибір моделі залежить від балансу між безпекою та гнучкістю, а на практиці часто поєднуються елементи різних підходів. Головне – щоб після встановлення особи (автентифікації) система правильно застосувала політику доступу, яка мінімізує ризик несанкціонованих дій з персональними даними, дотримуючись принципів, закріплених у стандартах і законодавстві.

1.7 Криптографічні основи захисту

Криптографія є невід'ємним елементом сучасних механізмів автентифікації та захисту даних. Під криптографією розуміють науку про перетворення даних з метою приховування їх змісту, підтвердження достовірності або забезпечення інших властивостей безпеки. Криптографічні методи забезпечують технічні засоби реалізації конфіденційності, цілісності, автентичності даних, у тому числі електронного підпису і засобів автентифікації користувачів [11]. Сучасна криптографія виходить далеко за рамки простого

шифрування для секретності – вона включає алгоритми хешування, цифрового підпису, протоколи обміну ключами, а також широке застосування у системах автентифікації (наприклад, зберігання паролів в хеш-формі, протоколи взаємної автентифікації за допомогою сертифікатів тощо).

Розглянемо основні криптографічні механізми і те, як вони сприяють захисту персональних даних:

- **Шифрування даних**. Це процес перетворення відкритих (зрозумілих) даних у зашифрований вигляд за допомогою криптографічного ключа. Розрізняють симетричне шифрування (один і той самий ключ використовується для шифрування і дешифрування) та асиметричне шифрування (пара ключів – відкритий для шифрування, приватний для дешифрування) [11]. Шифрування гарантує конфіденційність персональних даних: навіть якщо зловмисник перехопить чи викраде зашифрований файл або базу, без ключа він не зможе прочитати інформацію. Регуляторні стандарти (в тому числі GDPR) прямо згадують шифрування як один із заходів захисту, доречний для персональних даних [9]. Симетричні алгоритми (AES, DES/3DES, Twofish тощо) дуже швидкі і підходять для шифрування великих обсягів даних (наприклад, всієї БД). Асиметричні алгоритми (RSA, ECC) значно повільніші [11], зате вирішують проблему розподілу ключів – їх часто застосовують для безпечного обміну симетричними ключами та для цифрових підписів. У автентифікації шифрування використовується, наприклад, у протоколах TLS при передачі пароля на сервер – щоб пароль не був видимий у мережі. Крім того, сховища паролів на сервері часто шифруються, щоб у разі компрометації БД зловмисник не отримав усі дані у відкритому вигляді.
- **Хешування та зберігання паролів**. Криптографічні хеш-функції (SHA-2, SHA-3, Bcrypt, Argon2 тощо) перетворюють довільний вхід (наприклад, пароль) у фіксований рядок біт певної довжини, причому односторонньо – за хешем практично неможливо відновити початкове значення. Правильна практика зберігання паролів передбачає, що замість самого пароля в базі зберігається лише його криптографічний хеш (часто ще й із додаванням випадкової «солі» для

уникнення атак підбору). У випадку витоку хеш-значень, паролі все ще потрібно зламувати брутфорсом. Це значно підвищує стійкість системи: як відзначає Verizon у своїх звітах, незважаючи на мільярди скомпрометованих записів, багато паролів були захищені хешуванням і солінням, що ускладнює їх зловживання [17]. Сучасні вимоги (зокрема, NIST 800-63B) рекомендують використовувати «повільні» хеш-функції для паролів (наприклад, Argon2, Bcrypt), які утруднюють масовий перебір. Таким чином, криптографія забезпечує захист автентифікаційних даних при зберіганні.

- **Цифровий підпис і сертифікати**. Цифровий підпис – це криптографічний механізм перевірки цілісності та автентичності даних. Він створюється за допомогою приватного ключа і може бути перевірений будь-ким, хто має відповідний відкритий ключ, не розкриваючи при цьому сам приватний ключ. У контексті автентифікації цифрові сертифікати (які містять відкритий ключ суб'єкта, підписаний центром сертифікації) дозволяють реалізувати автентифікацію на основі сертифікатів. Наприклад, протокол TLS підтримує автентифікацію клієнта: клієнт пред'являє свій сертифікат і підписує випадкове повідомлення серверу своїм приватним ключем; сервер перевіряє підпис і таким чином переконується в особі клієнта. Така криптографічна автентифікація значно сильніша за парольну, оскільки зламати її, не маючи приватного ключа, практично неможливо. Багато корпоративних систем використовують смарт-карти або токени з сертифікатами для входу співробітників – це приклад двофакторної схеми (у токені зберігається приватний ключ, захищений PIN-кодом). Цифрові підписи також забезпечують незаперечність (користувач не може заперечити, що саме він увійшов або здійснив ту чи іншу дію, якщо вона підписана його ключем). У контексті захисту персональних даних сертифікати важливі для забезпечення шифрування каналів зв'язку (сертифікат сервера у TLS) та для побудови довірчих відносин між суб'єктами (взаємна автентифікація систем).

- **Протоколи автентифікації**. Криптографія дозволяє будувати протоколи, в яких жодна зі сторін не передає свій секрет відкритим текстом, що запобігає

перехопленню автентифікаційних даних. Класичний приклад – протокол challenge-response: сервер надсилає випадковий виклик (challenge), клієнт обчислює певну функцію від виклику і свого секрету (наприклад, хеш з'єднання "пароль+виклик") і надсилає результат як відповідь. Сервер, маючи еталонний хеш пароля, може перевірити, чи відповідь правильна, і при цьому сам пароль не передавався. Так працює, зокрема, протокол автентифікації NTLM в Windows. Ще досконаліші протоколи – одноразові паролі (One-Time Password, OTP). Наприклад, алгоритми HOTP/TOTP (стандарт OATH) генерують новий пароль кожні 30 секунд на основі секретного ключа і лічильника/часу; сервер, знаючи той самий секрет, може згенерувати і звірити OTP. Одноразові паролі неможливо повторно використати, тому перехопивши OTP, зловмисник уже не зможе увійти вдруге. NIST відзначає, що криптографічні методи дозволяють створити аутентифікацію без передачі постійного пароля – шляхом доказу володіння ключем [11]. Саме так діють апаратні токени і клієнтські сертифікати.

- **Криптографічні ключі та керування ними**. Надійність криптографічних механізмів залежить від безпеки ключів. Тому важливо впроваджувати правильне управління ключами: генерацію крипостійких випадкових ключів, їх безпечне зберігання (наприклад, у апаратних модулях безпеки – HSM), ротацію та знищення ключів при необхідності. Стандарти (як-от ISO/IEC 27002) встановлюють вимоги щодо політик управління ключами, розподілу ролей при роботі з ключами, резервного копіювання ключових матеріалів тощо. Для автентифікації це означає, що приватні ключі користувачів мають бути захищені (на смарт-карті або хоча б зашифровані в сховищі), паролі – зберігатися тільки в хешованому вигляді, ключі шифрування баз даних персональних даних – обмежено доступні і теж захищені. Компрометація ключів рівнозначна компрометації всієї системи безпеки, тому питання криптографії нерозривно пов'язані з питаннями управління доступом: хто може отримати ключ, той може обійти авторизаційні обмеження.

Тому, можна зробити висновок, що криптографічні засоби відіграють подвійну роль: захищають дані як такі (шифруванням) та підтримують механізми

автентифікації і контролю доступу. Без сучасної криптографії неможливо уявити безпечний веб-вхід (TLS), зберігання паролів, двофакторну автентифікацію, електронний цифровий підпис тощо. Як зазначено в NIST SP 800-12, криптографія є фундаментом розвинених методів автентифікації: дозволяє проводити автентифікацію шляхом демонстрації володіння ключем замість передачі пароля, реалізовувати одноразові паролі та інші протоколи [11]. Усе це значно підвищує стійкість системи до атак, зменшуючи залежність від людського фактора. Разом з тим, впровадження криптографії потребує правильного управління і відповідності стандартам (наприклад, використання тільки схвалених алгоритмів шифрування – AES, RSA, SHA-3 і т.д., згідно з рекомендаціями NIST, ISO або державних регуляторів).

1.8 Стандарти та найкращі практики автентифікації і захисту даних

У сфері кібербезпеки накопичено значну кількість міжнародних стандартів, рекомендацій і нормативних вимог, що визначають еталонні підходи до автентифікації та захисту персональних даних. Дотримання цих стандартів є важливою умовою побудови надійної системи безпеки, а також часто – законодавчою вимогою або умовою сертифікації. Розглянемо основні стандарти і практики, що мають відношення до теми.

Стандарти ISO/IEC серії 27000. Міжнародна організація зі стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC) розробила низку стандартів для управління інформаційною безпекою. Базовим є стандарт ISO/IEC 27001 – «Система управління інформаційною безпекою (СУІБ) – Вимоги». Він задає рамкові вимоги до впровадження комплексної системи захисту інформації в організації. Додаток А ISO 27001 містить перелік контрольних заходів, серед яких є цілий розділ, присвячений контролю доступу. У версії ISO 27001:2013 це був розділ A.9 «Control of Access», у новій ISO/IEC 27001:2022 – пункт 8.5 «Secure authentication» і суміжні пункти про управління доступом. Вимоги цих пунктів, детально роз’яснені у стандарті рекомендацій ISO/IEC 27002,

включають: наявність формальної політики управління доступом; реєстрацію та видалення користувачів; управління привілейованим доступом; безпечні методи автентифікації та управління автентифікаційною інформацією; використання криптографії для захисту даних тощо [13]. Зокрема, ISO 27002:2022 наголошує, що автентифікація повинна здійснюватися із застосуванням відповідних технологій і процедур, а якщо використовуються паролі – вони мають передаватися і зберігатися в зашифрованому вигляді; для чутливих систем треба впроваджувати багатофакторну автентифікацію (наприклад, токени, сертифікати або біометрію замість лише пароля) [13]. Наводиться рекомендація: комбінувати кілька факторів – "те, що знаєш, маєш і ким є" – адже це значно знижує шанси зловмисного проникнення [13]. Також стандарт радить застосовувати додаткові фактори у специфічних випадках (напр., при доступі з незвичних місць або до критично важливих ресурсів) та враховувати обмеження біометрії (наприклад, мати запасний метод на випадок, якщо відбиток не зчитується) [13]. Таким чином, ISO 27001/27002 встановлюють базовий рівень вимог до автентифікації: від процедур управління обліковими записами до технічної реалізації. Сертифікація за ISO/IEC 27001 підтверджує, що організація впровадила ці контролі належним чином.

Окремо варто згадати ISO/IEC 27701:2019 – розширення до 27001, яке додає компоненти системи управління конфіденційністю інформації (Privacy Information Management System) для відповідності вимогам захисту персональних даних (GDPR тощо) [14]. ISO 27701 містить конкретні контролі щодо обробки персональних даних, в тому числі стосовно автентифікації та управління доступом до таких даних. Впровадження ISO 27701 демонструє, що організація забезпечила належні політики і механізми захисту ПД і може слугувати доказом відповідності GDPR [14]. Фактично, ISO 27701 на міжнародному рівні уніфікує практики приватності, дозволяючи пройти сертифікацію і довести партнерам та регуляторам, що конфіденційна інформація захищена за найвищими стандартами. В контексті автентифікації стандарт 27701 підсилює вимоги 27001/27002 акцентом на доступ до персональних даних:

рекомендується принцип need-to-know, суворий контроль облікових записів, обмеження доступу навіть для IT-адміністраторів (наприклад, використання розподілу ролей, щоб одна особа не мала повного доступу до всіх персональних даних без потреби). Отже, стандарти ISO створюють цілісну систему правил, якої повинна дотримуватися організація, щоб гарантувати належну автентифікацію і захист даних.

Рекомендації NIST (США). Національний інститут стандартів і технологій США (NIST) видає спеціальні публікації (SP), багато з яких стали міжнародно визнаними керівництвами. У сфері цифрової автентифікації ключовим є документ NIST SP 800-63B “Digital Identity Guidelines: Authentication & Lifecycle Management” (редакція 2017 року) [10]. Цей гайдлайн встановлює вимоги до різних рівнів довіри автентифікації (AAL) в федеральних інформаційних системах США, але його широко використовують і в приватному секторі. NIST 800-63B описує прийнятні типи автентифікаторів для кожного рівня – від паролів та SMS-OTP (мінімальний рівень) до багатофакторних криптографічних токенів (вищий рівень) [10]. Зокрема, цей стандарт містить сучасні вимоги до паролів: мінімальна довжина 8 символів, перевірка відсутності пароля в списках скомпрометованих, відміна практики частого примусового змінювання паролів (оскільки це знижує їх якість) – на користь використання багатофакторної автентифікації та моніторингу аномалій [19]. NIST також дає поради щодо блокування облікових записів при численних невдалих спробах, вимоги до інтерфейсу вводу пароля (наприклад, відображати індикатор надійності пароля користувачу). Окремий розділ присвячено життєвому циклу автентифікаторів – реєстрації, відновленню при втраті, скасуванню (revocation) тощо, а також стійкості автентифікаторів до загроз (фішингу, перехоплення, підбору) та відповідним мірам протидії [10]. NIST SP 800-63B фактично задає детальний набір технічних вимог і рекомендацій, який можна використовувати як чекліст при побудові системи автентифікації. Наприклад, він рекомендує відмовитися від SMS як другого фактору, якщо є можливість – через уразливість

до перехоплення (SIM swap), і переходити на криптографічні апаратні ключі або одноразові коди в додатках.

Інший важливий документ – NIST SP 800-53 “Security and Privacy Controls for Federal Information Systems”. Це об’ємний каталог контролів безпеки, серед яких сімейства IA (Identification and Authentication) та AC (Access Control) описують конкретні вимоги: наприклад, контроль IA-2 вимагає багатофакторної автентифікації для адміністраторів і віддаленого доступу, IA-5 – зберігати паролі в хешованому вигляді, IA-8 – використовувати у разі потреби автентифікацію за сертифікатами. Ці контролі перекликаються з ISO, але більш деталізовані. NIST SP 800-53 використовується в США на рівні держави, але багато приватних компаній також беруть його за основу для внутрішніх політик.

Також NIST видає спеціальні документи по криптографії (наприклад, FIPS 140-3 щодо модулів безпеки, SP 800-131A щодо використання криптоалгоритмів), які задають стандарти, яких треба дотримуватися. Для захисту персональних даних важливо застосовувати лише криптографічні алгоритми, що не мають відомих вразливостей і схвалені експертним співтовариством (AES, RSA, SHA-256 тощо), уникати застарілих (MD5, SHA-1, DES). Це також фіксується у стандартах: GDPR, наприклад, не диктує конкретні алгоритми, але вимагає “state-of-the-art” заходів, тобто актуальних, а не застарілих.

Регламенти захисту даних (GDPR та ін.). В правовому полі головним міжнародним актом є Регламент (ЄС) 2016/679 (GDPR) – загальний регламент про захист даних, чинний з 2018 року для країн ЄС та компаній, що працюють з даними громадян ЄС. GDPR встановлює принципи обробки персональних даних (законність, прозорість, мінімізація даних, цілісність і конфіденційність тощо) і визначає обов’язки контролерів та процесорів даних щодо забезпечення безпеки. Стаття 32 GDPR вимагає від контролера і процесора впровадити “відповідні технічні та організаційні заходи безпеки” з урахуванням ризиків – зокрема, згадуються псевдонімізація та шифрування персональних даних, здатність забезпечити конфіденційність, цілісність, доступність і стійкість систем [9], а

також можливість вчасно відновити доступність даних у разі інциденту [9]. Тобто GDPR прямо не диктує “використовуйте двофакторну автентифікацію” чи щось подібне, але очевидно, що для забезпечення конфіденційності і відповідності ризику необхідно застосовувати належні методи автентифікації. Регулятори GDPR при розгляді інцидентів часто оцінюють, чи мала компанія впроваджену MFA для доступу до чутливих даних; якщо ні – це розцінюється як недостатній захід безпеки. Були випадки накладення значних штрафів, коли витік персональних даних стався через слабкий пароль або брак другого фактору для адміністратора – такі інциденти трактуються як недотримання ст.32 (не забезпечено належного рівня захисту). Відтак, міжнародна практика дедалі більше зміщується до того, що багатофакторна автентифікація для доступу до персональних даних – це стандарт де-факто.

В Україні діє згаданий Закон “Про захист персональних даних” №2297-VI. Хоча він і не містить детальних технічних вимог щодо автентифікації, загальні положення зобов’язують володільців і розпорядників даних вживати необхідних заходів для захисту персональних даних від несанкціонованого доступу (ст.24 закону). Орган, відповідальний за нагляд (Уповноважений ВРУ з прав людини), у своїх рекомендаціях теж наголошує на необхідності обмеження кола осіб, що мають доступ до ПД, використання засобів захисту інформації тощо. Відповідно, дотримання ISO 27001 чи подібних стандартів можна розглядати як виконання вимог закону. Слід зазначити, що в Україні, окрім профільного закону про ПД, є також Закон “Про кібербезпеку” 2017 року, який зобов’язує об’єкти критичної інфраструктури дотримуватися певних стандартів захисту інформації, хоча він більше стосується загалом кіберзахисту, а не конкретно персональних даних. Проте для державних інформаційних систем діють ще Державні будівельні норми та стандарти (наприклад, ДСТУ з технічного захисту інформації), які, як правило, передбачають наявність підсистеми розмежування доступу, реєстрації та блокування, використання сертифікованих криптозасобів тощо. Таким чином, на національному рівні також встановлено нормативні вимоги, що імпліцитно включають належну автентифікацію.

Корпоративні політики та рекомендації виробників. Великі IT-компанії та консорціуми також публікують найкращі практики. Наприклад, Microsoft постійно випускає матеріали на тему відмови від паролів, впровадження MFA, захисту облікових записів у хмарних сервісах. Представники Microsoft Security підкреслюють, що організації марно витрачають зусилля на політики типу “міняти паролі щомісяця” або вимагати складних символів, замість того щоб зосередитися на впровадженні багатофакторної автентифікації та інтелектуальних систем захисту від входу з викраденими паролями [19]. Вони зазначають: “коли йдеться про довжину і складність, ваш пароль переважно не має значення; важливо впроваджувати речі, які реально допомагають – MFA, виявлення аномалій” [19]. Такі повідомлення ще раз акцентують, що пароль сам по собі більше не забезпечує прийнятного рівня захисту в сучасних умовах.

Компанія Cisco, один з лідерів у сфері мережевої безпеки, також просуває концепцію Zero Trust та рішення типу Cisco Duo, що спрощують впровадження MFA. У матеріалах Cisco підкреслюється, що 2FA/MFA наразі відіграють критичну роль у захисті цифрових середовищ, але це лише частина комплексного підходу; потрібно також централізовано керувати ідентифікаціями і правами (IAM), підвищувати обізнаність користувачів щодо загроз фішингу тощо [20]. Cisco застерігає, що хоча MFA суттєво підсилює безпеку, вона не є панацеєю – з’являються нові техніки обходу, як-то “MFA fatigue” (зловмисник масово шле push-запити на смартфон, поки змучений користувач випадково не підтвердить) або комбіновані фішингові атаки, тому треба постійно вдосконалювати стратегії кіберзахисту [20]. Ці практичні рекомендації виробників доповнюють стандарти, надаючи актуальні поради з урахуванням нових тенденцій атак.

Спеціалізовані стандарти. У певних галузях діють свої нормативи. Наприклад, для індустрії платіжних карт – стандарт PCI DSS вимагає багатофакторної автентифікації для адміністративного доступу до систем, що обробляють дані карт, і регламентує політики паролів. У сфері охорони здоров’я США – HIPAA Security Rule вимагає впровадження механізмів, що забезпечують унікальну ідентифікацію користувачів і контроль доступу до медичних даних

(часто це реалізується теж через ролі і двофакторну автентифікацію для доступу поза межами захищеної мережі). Державні органи, як правило, мають власні нормативні документи з захисту інформації, які багато в чому дублюють ISO/NIST, але адаптовані під місцеві вимоги. В Україні, наприклад, діють нормативні документи Держспецзв'язку (Технічні вимоги з ТЗІ), де явно прописано необхідність розмежування доступу, реєстрації дій, використання сертифікованих криптозасобів для шифрування та ЕЦП в державних інформаційних системах. Це все формує комплекс стандартів і норм, яким повинні слідувати організації, обробляючи персональні дані.

1.9 Роль автентифікації у забезпеченні захисту персональних даних

Автентифікація відіграє центральну роль у системі захисту інформації: саме вона є «першою лінією оборони» проти несанкціонованого доступу [11]. Якщо уявити багатоешелонну оборону даних (мережевий захист, шифрування, моніторинг), то автентифікація – це перший шлюз, який відсіює сторонніх. Жодні заходи захисту персональних даних не будуть ефективними, якщо зловмисник може видавати себе за законного користувача або співробітника і тим самим обходити ці заходи. Тому стійкість автентифікації прямо визначає, наскільки система вцілому здатна протистояти спробам викрадення чи компрометації персональних даних.

Головна функція автентифікації – забезпечення конфіденційності. Лише пройшовши перевірку достовірності, суб'єкт може отримати доступ до конфіденційних записів. У разі слабкої автентифікації чужа особа може проникнути під чужими обліковими даними і прочитати персональну інформацію, що є прямим порушенням конфіденційності. Аналіз інцидентів показує, що більшість витоків даних трапляються саме через компрометацію облікових записів. Наприклад, було встановлено, що в 4 із 5 випадків зламів систем охорони здоров'я зловмисники використали викрадені або слабкі паролі

для доступу до записів пацієнтів [17]. Таким чином, міцна автентифікація – перший бар’єр для захисту приватності клієнтів, пацієнтів, користувачів.

Друга важлива роль – забезпечення цілісності та контроль дій. Завдяки автентифікації кожна дія в системі може бути прив’язана до певного суб’єкта. Це створює основу для відстеження та аудиту (хто переглядав або змінював ті чи інші персональні дані). Якщо користувач не автентифікований або автентифікований неналежним чином, неможливо гарантувати, що саме уповноважена особа виконувала дії. У випадку інциденту (скажімо, виявлено несанкціоновану зміну даних) аудит логів допоможе тільки якщо облікові записи надійно прив’язані до реальних осіб. В іншому разі запобігти шахрайському редагуванню чи видаленню даних і знайти винного буде складно. Тому автентифікація забезпечує відповідальність (accountability): користувачі знають, що їх дії фіксуються під їхнім іменем, що дисциплінує і служить стримуючим фактором для зловживань [11]. Особливо це важливо при роботі з персональними даними, де кожен доступ має бути обґрунтований – система може логувати, хто і коли переглядав запис суб’єкта даних, щоб у разі скарги довести законність або виявити порушення.

Авторизація (контроль доступу) теж спирається на автентифікацію. Поки суб’єкт не встановлений, не можна ефективно застосувати політики доступу. Через це будь-який недолік автентифікації підриває усю модель контролю доступу. Навіть найдосконаліша рольова політика (RBAC) марна, якщо зловмисник входить під обліковим записом адміністратора – він отримає всі права цієї ролі. Тобто авторизація настільки ж надійна, наскільки надійна автентифікація.

Окрім безпосереднього захисту від зовнішніх атак, сильна автентифікація допомагає і у захисті від внутрішніх загроз. Наприклад, обмеження доступу працівників до персональних даних інших підрозділів через єдиний вхід та ролі знижує ризик зловживань (цікавість, промислове шпигунство). Якщо співробітник залишить своє робоче місце, система повинна вимагати повторної автентифікації (ре-логін) після певного часу неактивності – це не дасть іншому

підглянути дані на чужому комп'ютері. Такі механізми, знову ж таки, базуються на автентифікації (наприклад, блокування екрану і повторний ввід пароля).

Відповідність законодавству. Роль автентифікації проявляється і в юридичній площині. Законодавство (GDPR, закон України про ПД) вимагає допускати до персональних даних лише осіб, які мають відповідні повноваження, і лише в обсязі, необхідному для виконання завдань. Належні процеси автентифікації і управління обліковими записами – спосіб виконати цю вимогу. Наприклад, GDPR також говорить про псевдонімізацію – якщо дані знеособлені (відокремлені від ідентифікаторів суб'єктів), то доступ до зв'язку "ідентифікатор – особа" має мати дуже обмежене коло людей. Це технічно реалізується через окремі облікові записи для доступу до таблиці відповідності псевдонімів, з MFA і журналюванням. Отже, законодавчі принципи повинні імплементуватися через налаштування системи автентифікації/авторизації. Організації, які недбало ставляться до цього, можуть не лише втратити дані, а й отримати штраф.

В контексті кіберстійкості (resilience) можна відзначити, що автентифікація захищає від значної кількості атак на інформаційні системи. За даними звітів, використання MFA могло б запобігти левовій частці компрометацій облікових записів і, як наслідок, зупинити розвиток багатьох атак на ранньому етапі [18]. В той же час, відсутність надійної автентифікації часто робить даремними інші вкладення в безпеку. Наприклад, організація може мати дорогі міжмережеві екрани, системи виявлення атак, але якщо адміністратор використовує пароль "12345" і його зламано – зловмисник в обхід усього потрапляє всередину, як законний користувач.

Окремо варто згадати роль автентифікації у забезпеченні довіри користувачів до системи. Якщо клієнти знають, що їхні дані захищені (скажімо, банк сповіщає, що в додатку для входу застосовується двофакторна автентифікація, а дані профілю шифруються), це підвищує рівень довіри до компанії. Навпаки, випадки, коли дані викрадалися через банальну відсутність другого фактору, підривають репутацію. У світі, де приватність стає цінністю,

наявність сильних механізмів автентифікації – конкурентна перевага для компанії.

1.10 Проблеми та виклики реалізації автентифікації і захисту даних

Попри наявність більш зрілих технологій і стандартів, на практиці забезпечення надійної автентифікації та захисту персональних даних стикається з низкою проблем і викликів. Розглянемо основні з них:

1. Людський фактор і слабкі паролі. Найбільш вразливою ланкою залишаються самі користувачі. Багато людей обирають надто прості й передбачувані паролі або використовують один пароль для різних сервісів. За даними Verizon DBIR, 60–80% зламів пов'язані саме з використанням вразливих облікових даних [17]. Скільки б не навчали працівників, у великій організації завжди знайдеться хтось зі словом "password123" або "Qwerty" як паролем. До того ж, люди схильні повідомляти паролі шахраям під впливом соціальної інженерії (фішингові листи, дзвінки від нібито служби підтримки тощо). Таким чином, проблема паролів залишається основною: користувачі часто є "слабкою ланкою", через яку зловмисники здобувають доступ. Це підтверджується тим, що фішинг фігурує у понад 90% інцидентів, пов'язаних із викраденням облікових даних [18]. Навіть добре технічно захищені системи можуть пасти жертвою, якщо співробітник клікне на підробну сторінку і введе там свій логін/пароль.

Для вирішення цієї проблеми впроваджуються два підходи: підвищення вимог до паролів (мінімальна довжина, заборона типових шаблонів, перевірка щодо відомих витоків) та додавання інших факторів (MFA). Однак у реальності зустрічається супротив користувачів складним вимогам. Занадто складна політика паролів часто призводить до того, що люди записують їх на папірцях або забувають, а часте примусове змінювання – до використання однотипних паролів з невеличкими змінами (що теж небезпечно). NIST у своїх нових рекомендаціях навіть зазначив, що часте експірування паролів – зайва практика, яка може шкодити [19]. Отже, баланс між безпекою і зручністю тут складний.

Багато організацій досі залежать від паролів як головного методу автентифікації, і тому вразливі до людських помилок. Поступовий вихід – це масовий перехід на безпарольні технології або принаймні MFA, але це вимагає ресурсів і часу.

2. Низькі темпи впровадження багатофакторної автентифікації. Хоча MFA визнано ефективним засобом, дослідження показують, що рівень його добровільного використання кінцевими користувачами залишається низьким [24]. Багато сервісів (пошти, соціальні мережі) пропонують двофакторну автентифікацію, але включають її за замовчуванням одиниці. За оцінками станом на 2023 рік, лише близько ~30–35% користувачів інтернет-сервісів активували 2FA на своїх облікових записах [24]. У корпоративному середовищі впровадження MFA теж не завжди повне: великі компанії зазвичай мають, а от в малих бізнесах MFA може не використовуватися взагалі, якщо немає вимоги чи тиску згори [47]. Причини – інерція і зручність. Користувачі не люблять додаткових кроків при вході; адміністрації компаній побоюються збільшення навантаження на підтримку (наприклад, більше звернень у разі втрати телефона для OTP); деякі застарілі системи не підтримують MFA і потребують модернізації. Навіть коли MFA впроваджується, часто обирають менш безпечні варіанти (наприклад, SMS-коди), бо вони простіші у реалізації, хоча і відомо про їхні уразливості (перехоплення SMS, дублювання SIM-карт). У результаті зловмисники все ще мають широкий простір для атак на паролі.

3. Атаки соціальної інженерії та фішинг 2.0. З розвитком захисних технологій атакувальники теж удосконалюються. З’явилися фішингові набори, здатні обходити двофакторну автентифікацію. Наприклад, фішингові сайти, що проксіюють реальний сайт: користувач вводить OTP, який миттєво використовують на реальному сайті, обходячи MFA. Також відзначається сплеск атак типу MFA fatigue – коли зловмисник отримав пароль і намагається увійти, а користувачу на телефон йде безліч push-повідомл зловмисники все ще мають широкий простір для експлуатації людського фактору. Наразі бачимо появу «фішингу 2.0» – вдосконалених атак соціальної інженерії, здатних обходити навіть додаткові заходи. Наприклад, фішингові сайти можуть у реальному часі

ретранслювати введені користувачем дані на справжній сайт (так звані атаки “phishing proxy”), примушуючи користувача вводити і одноразовий код, і таким чином одночасно обходячи двофакторний захист. Поширилися також атаки типу MFA fatigue (бомбардування запитами) – зловмисник, дізнавшись пароль, багаторазово ініціює запити авторизації на пристрій користувача (наприклад, push-повідомлення додатку) доти, доки стомлений або неуважний користувач не натисне “Дозволити” помилков [20]. Такі інциденти вже мали місце в практиці, що змушує впроваджувати додаткові заходи – наприклад, обмежувати частоту запитів або навчати користувачів ніколи не підтверджувати несподівані запити. У відповідь на ці виклики індустрія просуває стійкі до фішингу методи автентифікації (phishing-resistant MFA) – зокрема, апаратні FIDO2-ключі, які неможливо обманути проксі-сайтом. Однак перехід на них лише набирає обертів.

4. Атаки зі збором даних облікових записів (credential stuffing). Мільярди паролів, викрадених з одних сервісів, зловмисники масово випробовують на інших. Багато користувачів мають звичку повторно використовувати той самий пароль всюди – цим і користуються атаки типу credential stuffing. Наприклад, якщо утекли логіни/паролі від якоїсь соцмережі, зловмисники можуть автоматизовано перевірити їх на сайтах інтернет-банкінгу чи корпоративних VPN. У звітах вказується, що в веб-атаках до 77% випадків зловмисники отримують доступ саме шляхом використання вкрадених раніше облікових даних [16]. Захиститися від цього складно простими засобами – потрібні або MFA, або моніторинг підозрілих входів (наприклад, виявлення логінів з незвичайних локацій чи пристроїв), або ж примусова зміна паролів при відомості про витік. Організаціям доводиться відстежувати повідомлення про великі витоки у світі та звіряти, чи їхні користувачі не використовують ті самі паролі. Це створює додаткове навантаження і потребує інструментів кіберрозвідки.

5. Проблеми сумісності і легасі-систем. Часто впровадженню сучасних механізмів автентифікації заважає наявність застарілих систем, які не підтримують, скажімо, протоколів типу OAuth2/OIDC чи SAML для єдиного

входу, або не мають модулів під MFA. Перехід на нові системи може бути дорогим або й неможливим через критичність легасі. Така ситуація типова для великих організацій з “зоопарком” систем. У результаті безпека всієї інфраструктури визначається “найслабшою ланкою” – якщо одна з ключових систем не може запровадити MFA, то вона стане улюбленою мішенню. Ще одна сумісністна проблема – управління обліковими записами між різними платформами. Ідеально, коли діє єдина централізована служба каталогу (напр. Active Directory) і всі автентифікації проходять через неї з єдиними політиками. Але на практиці буває розрізненість: окремо облікові записи в корпоративній мережі, окремо – в хмарних сервісах, окремо – в якихось спеціалізованих БД. Це ускладнює забезпечення єдиних високих вимог (потрібні різні рішення MFA, кілька точок адміністрування облікових записів, тощо) і збільшує ризик людських помилок при керуванні доступами (наприклад, звільнили працівника – обліковку в домені видалили, а в іншій системі забули вимкнути). Вирішенням є впровадження систем федерації ідентичності та єдиного входу (SSO), але це теж проектна задача з немалими затратами.

6. Баланс безпека vs зручність vs вартість. Кожен додатковий рівень захисту – це потенційна незручність для користувачів і додаткові витрати для організації. Наприклад, апаратні токени потребують закупівлі і роздачі кожному співробітнику, їхньої підтримки (замінити при втраті, тощо). Біометрія – питання конфіденційності і також вартості обладнання (сканери, сенсори). Багато компаній, особливо малого і середнього бізнесу, зважують: чи дійсно їм потрібен такий “складний” захист, чи можна обійтись паролем і економити час/кошти. До інциденту зазвичай переважає бажання спростити. Користувачі теж надають перевагу менш обтяжливому входу: тому, наприклад, складні вимоги до пароля чи часта його зміна часто саботуються (люди починають записувати паролі на стікерах, що зводить нанівець усю політику). Тож впроваджуючи заходи безпеки, доводиться шукати компроміс. Одне з рішень – risk-based автентифікація, коли користувачу незвично проходити 2FA на кожен вхід, але якщо система визначає спробу входу як низькоризикову (звичний пристрій, IP, час), то може і не вимагати

OTP. Однак реалізація таких динамічних підходів потребує зрілості систем. У будь-якому разі, питання зручності залишається викликом: як зробити сильну автентифікацію не надто обтяжливою для легітимних користувачів. Це особливо актуально для сервісів з мільйонами кінцевих клієнтів, де надто строгі вимоги можуть відштовхнути частину аудиторії.

7. Захист біометричних даних та приватність. Як вже зазначалось, біометрія приносить нові ризики: компрометація бази біометричних шаблонів є надзвичайно критичним інцидентом, адже ці дані унікальні і незмінн [21]. Компаніям, що впроваджують біометричну автентифікацію, доводиться інвестувати у дуже сильний захист відповідних баз даних (шифрування, розподіл на сегменти, апаратні модулі безпеки). Також в деяких країнах діють суворі закони щодо біометричних даних (наприклад, в штаті Іллінойс, США – закон BIPA накладає великі штрафи за неправомірне зберігання біометрії). Тому для багатьох організацій простіше уникати біометричної автентифікації, ніж брати на себе відповідальність за ці дані. В контексті персональних даних це дилема: біометрія може суттєво підвищити захищеність доступу, але сама по собі є дуже чутливими персональними даними. Цей виклик частково знімається, коли біометрія використовується на стороні клієнта (наприклад, відбиток зберігається тільки в смартфоні користувача для розблокування криптоключа, а серверу надсилається лише підпис, але не біометричний шаблон). Саме така архітектура в FIDO2/WebAuthn – сервер не зберігає біометрії, а довіряє пристрою користувача. Це хороше вирішення проблеми приватності, але потребує, щоб усі клієнти мали відповідні пристрої і програмне забезпечення, що поки не завжди так (особливо в корпоративному середовищі з ПК без датчиків).

8. Управління життєвим циклом доступів та внутрішні загрози. Забезпечити надійну автентифікацію – не тільки про технології на вході, а й про правильне адміністрування облікових записів. Поширений виклик – несвоєчасне відключення доступів. Наприклад, звільнений співробітник, контрактор або студент у вузі може зберігати обліковку, якщо процеси її деактивації не налагоджені. Такі «привидні» акаунти становлять ризик, бо можуть бути

використані злочинцем (особливо якщо це був акаунт з привілеями). Так само проблема надлишкових привілеїв: коли користувач міняє посаду, йому часто додають нові права, але старі не відбирають – з часом він накопичує доступ туди, куди вже не повинен мати. Це нівелює принцип найменших привілеїв. Для боротьби з цим великі організації впроваджують системи IAM (Identity & Access Management) і регулярно проводять перевірку доступів, але для менших це може бути складно. Відсутність належного управління доступами усередині організації підриває всі зусилля: навіть з MFA, але з сотнями «мертвих душ» у системі, ризик витоку даних високий. Також є проблема внутрішніх зловживань: авторизований користувач може перевищити свої повноваження (наприклад, медпрацівник цікавиться записами відомого пацієнта без виробничої потреби). Тут рішення лежать поза суто автентифікацією – потрібен моніторинг дій, розмежування обов'язків, можливість виявляти аномальні дії легітимних користувачів. Але ці завдання теж впираються в коректну автентифікацію: треба точно знати, **хто** виконав дію, щоб застосовувати санкції чи контрзаходи.

Висновки до розділу 1

У даному розділі було здійснено комплексний огляд теоретичних засад автентифікації та захисту персональних даних. Проаналізовано сутність ключових понять – ідентифікації, автентифікації, авторизації – та їхню роль у системі безпеки. Встановлено, що автентифікація є фундаментальною передумовою контролю доступу і забезпечення конфіденційності інформації: без надійного встановлення особи користувача неможливо гарантувати захист персональних даних від потрапляння в чужі руки. Розглянуто основні види автентифікації (за знанням, володінням, біометричними характеристиками) і відзначено переваги багатофакторних схем над традиційними паролям. Сучасні тенденції, такі як відмова від постійних паролів на користь криптографічних токенів чи біометрії, свідчать про прагнення підвищити і безпеку, і зручність для користувачів.

Особливу увагу приділено криптографічним механізмам, що лежать в основі захисту даних: шифруванню як засобу забезпечення конфіденційності, хешуванню паролів для унеможливлення їх розголошення, цифровим підписам і сертифікатам для реалізації сильних методів автентифікації та цілісност. Акцентовано, що надійна криптографія є обов'язковим атрибутом систем, які обробляють персональні дані, відповідно до міжнародних стандартів і вимог GDP .

Зіставлення міжнародних стандартів (ISO/IEC 27001, NIST SP 800-63B тощо) та українських нормативів показало зближення підходів: Україна імплементує положення GDPR у національне законодавств, що означає підвищення вимог до контролю доступу, обов'язкове повідомлення про витоки, суттєві штрафи за нехтування захистом. Таким чином, українським організаціям доведеться відповідати тим самим високим критеріям, які вже діють у ЄС. Втім, багато прогресивних компаній не чекають законодавчого примусу і вже застосовують у себе ISO 27001 та інші найкращі практики – від політик складних паролів і двофакторної автентифікації до регулярних аудитів безпеки.

Розглянуто сучасні проблеми та загрози в сфері автентифікації: людський фактор (схильність до слабких паролів, піддавання фішингу), технічні обмеження легасі-систем, новітні методи атак на MFA, складність балансування безпеки і зручності. Для ефективного захисту персональних даних одних тільки технологій недостатньо – потрібна комплексна система заходів: технічних, організаційних та навчальних. З одного боку, впровадження багаторівневої автентифікації (MFA) суттєво знижує ризик компрометації облікових записі, з іншого – необхідно постійно підвищувати обізнаність користувачів, відпрацьовувати процедури реагування на інциденти, переглядати права доступу. Лише за такої комплексної стратегії можна протистояти як зовнішнім зловмисникам, так і потенційним внутрішнім порушникам.

РОЗДІЛ 2 ТЕХНОЛОГІЇ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ПРИКЛАДИ ЇХ ВИКОРИСТАННЯ

2.1 Сучасні технологій багатофакторної автентифікації

Сучасні рішення для багатофакторної автентифікації реалізують наведені принципи за допомогою різноманітних технологій. Розглянемо основні типи MFA-технологій, що нині використовуються.

1. Одноразові паролі (OTP) та токени генерації кодів. Один із найпоширеніших підходів – це використання одноразових паролів (One-Time Password, OTP), які генеруються для кожної сесії входу або транзакції. Одноразові паролі можуть доставлятися користувачу різними каналами: через SMS-повідомлення, електронну пошту, спеціальний мобільний додаток-генератор або апаратний токен. Принцип роботи OTP простий: генерується випадковий або псевдовипадковий код, дійсний лише один раз (або впродовж короткого проміжку часу), який користувач вводить як другий фактор. Після використання код стає недійсним.

Існують стандартизовані алгоритми для генерації OTP. Зокрема, алгоритм HOTP (HMAC-Based One-Time Password) генерує паролі на основі лічильника подій, а TOTP (Time-Based One-Time Password) – на основі часу. Обидва алгоритми визначені відкритими стандартами (RFC 4226 для HOTP та RFC 6238 для TOTP) і широко впроваджені в практиці. Найвідомішим прикладом є додатки-аутентифікатори (Google Authenticator, Microsoft Authenticator, Authy тощо), які реалізують TOTP: додаток та сервер мають спільний секретний ключ (seed), на основі якого та поточного часу (зазвичай з кроком 30 секунд) обчислюється 6- або 8-значний одноразовий код. Код відображається користувачу, який вводить його в систему, доводячи тим самим, що володіє пристроєм з коректним секретним ключем. З точки зору класифікації, такий OTP-код підтверджує фактор “щось, що ви маєте” – пристрій або додаток-генератор кодів [10]. Важливо, що OTP має короткий строк життя (для TOTP зазвичай 30

або 60 секунд) і не може бути використаний повторно, що зменшує ризики перехоплення.

Окрім програмних генераторів OTP на смартфоні, використовуються і апаратні токени. Класичний приклад – токени RSA SecurID або інші апаратні брелоки, які показують на дисплеї змінний код кожні N секунд. Такі пристрої мають вбудований секрет і годинник, генеруючи тимчасові коди аналогічно до TOTP. Деякі апаратні OTP-токени працюють за принципом HOTP – показують код при натисканні кнопки, синхронізований з лічильником на сервері. Існують також кредитні картки з дисплеєм, що генерують OTP, та інші варіації. Усі вони реалізують той самий підхід: фактор володіння, який надає одноразовий секрет для автентифікації.

Одноразові паролі через SMS були довгий час фактичним стандартом для онлайн-банкінгу та двофакторної автентифікації в соцмережах. SMS-OTP прості у впровадженні (не вимагають встановлення додатків – потрібен лише телефон) і зрозумілі користувачам. Однак, з безпекової точки зору, SMS – не ідеальний канал: повідомлення можна перехопити або перенаправити через атаки типу SIM- swap (перереєстрація номера на SIM-карті зловмисника) чи вразливості в мережах операторів. Через це регулятори та експерти все більше не рекомендують покладатися на SMS як на другий фактор. Наприклад, Європейське агентство з кібербезпеки (ENISA) радить по можливості уникати SMS і голосових дзвінків для автентифікації, віддаючи перевагу фішингостійким методам (апаратним токенам, смарт-картам, FIDO2-ключам) [27]. Попри ці застереження, OTP через SMS та електронну пошту все ще широко застосовуються, особливо в споживчих сервісах, як компроміс між безпекою та зручністю.

2. Токени та пристрої апаратної автентифікації (U2F, FIDO2). Новітнім розвитком фактору “володіння” є стандарти універсальних апаратних автентикаторів – таких як U2F та FIDO2/WebAuthn. U2F (Universal 2nd Factor) – це відкрита специфікація, розроблена FIDO Alliance у співпраці з технологічними компаніями, що дозволяє використовувати окремий фізичний ключ безпеки як

другий фактор автентифікації. Ключ U2F – зазвичай компактний USB-пристрій (або з підтримкою NFC/Bluetooth для мобільних), який зберігає криптографічний секрет. При реєстрації на вебсайті ключ генерує пару ключів (приватний та публічний) і передає публічний ключ серверу. При подальшому вході користувач спочатку вводить свій пароль, а потім вставляє U2F-ключ і натискає кнопку на ньому. Браузер надсилає ключу криптографічний виклик від сервера, який ключ підписує своїм приватним ключем (операція можлива лише при фізичному натисканні кнопки користувачем – це запобігає невидимому використанню). Сервер перевіряє підпис за допомогою раніше збереженого публічного ключа і таким чином підтверджує фактор володіння – користувач має при собі зареєстрований пристрій. За рахунок використання криптографії, U2F-автентифікація не вразлива до підробки одноразових кодів чи перехоплення – ключ не передає жодних статичних секретів, тільки підписує виклики, прив'язані до конкретного домену сайту. Це робить U2F дуже стійким до фішингу та атак типу "людина посередині". Перевага також у тому, що один апаратний ключ U2F можна використовувати для багатьох сервісів – кожен сервіс отримує свій унікальний публічний ключ, тож компрометація одного акаунту не вплине на інші. FIDO Alliance зазначає, що U2F дозволяє суттєво спростити паролі (аж до 4-значного ПІНу) без втрати безпеки, адже основний захист надає апаратний фактор [28].

Наступним кроком еволюції U2F став стандарт FIDO2 (включно з протоколом WebAuthn). FIDO2 – це спільна ініціатива FIDO Alliance та W3C, яка дозволяє як двофакторну, так і бездпарольну автентифікацію, використовуючи або зовнішні ключі безпеки, або вбудовані апаратні модулі пристроїв (наприклад, Trusted Platform Module в ноутбуці чи Secure Enclave в телефоні) [28]. Основні компоненти – це веб-API WebAuthn, який підтримують сучасні браузери, та протоколи CTAP2/CTAP1 для взаємодії з зовнішніми автентикаторами. WebAuthn дозволяє вебсайту (через браузер) звернутися до автентикатора на пристрої користувача з запитом автентифікації. Це може бути зовнішній USB/NFC ключ або вбудований, наприклад, модуль біометрії ноутбука. При реєстрації

створюється пара ключів аналогічно до U2F. При вході користувач може взагалі не вводити пароль: замість цього сервер посилає виклик на автентикатор (через браузер), користувач розблоковує автентикатор локальним методом (PIN, відбиток пальця тощо), і автентикатор підписує виклик приватним ключем. Таким чином досягається passwordless-автентифікація – користувач доводить свою особу володінням пристрою *і* фактично ще одним фактором (PIN або біометрія для розблокування пристрою). Отже, FIDO2 може працювати як двофакторна схема (якщо застосовується разом з паролем) або як самодостатня багатофакторна схема без пароля (пристрій + біометрія/PIN) [28].

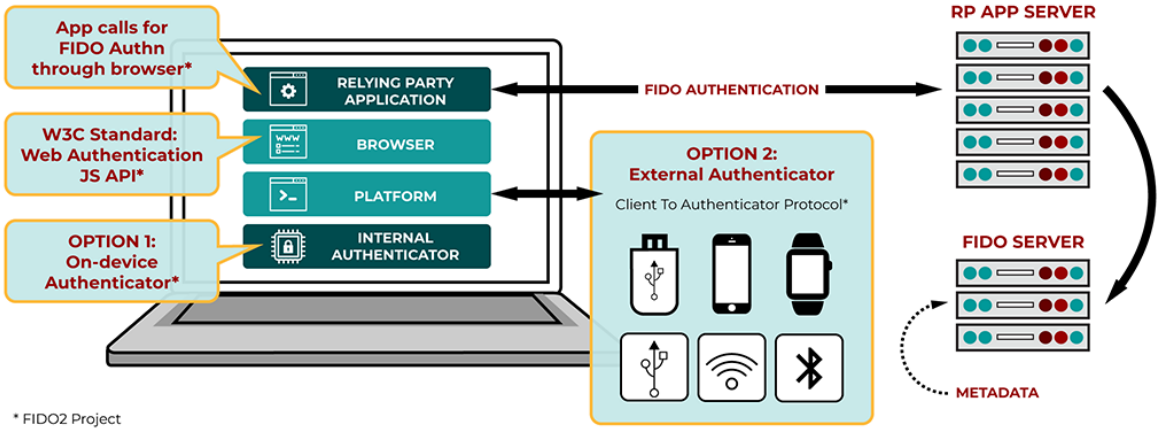

Рис. 2.1. Проєкт FIDO2 [28]

Усі провідні платформи – Windows, Android, iOS, macOS, веб-браузери – підтримують FIDO2, що дозволяє використовувати його практично скрізь.

Важливо відзначити, що FIDO2/WebAuthn є фішингостійким методом автентифікації. Оскільки криптографічний виклик містить інформацію про домен, з якого він надійшов, апаратний ключ підпише лише той виклик, який прийшов від справжнього сайту. Якщо користувача заманять на фішинговий сайт, ключ відмовиться підписувати “чужий” домен, і автентифікація провалиться. Це суттєва відмінність від OTP-кодів або SMS, які користувач може несвідомо ввести на підробленому сайті. Завдяки цьому властивості техгіганти розглядають FIDO2 як шлях до майбутнього без паролів. У травні 2022 року Apple, Google та Microsoft спільно оголосили про підтримку єдиного стандарту безпарольного входу (FIDO “passkeys”) на всіх основних платформах [29]. Це означає, що найближчим часом користувачі зможуть входити на вебсайти, підтверджуючи

вхід лише на своєму телефоні (через Face ID, Touch ID або PIN), без введення парольної фрази [29]. На практиці телефон генерує та зберігає FIDO2 ключ (passkey), синхронізує його через хмару для резервування, і стає головним засобом автентифікації користувача. Така схема поєднує простоту для користувача (не треба запам'ятовувати паролі) та безпеку (зломщику потрібно фізично заволодіти пристроєм користувача + обійти локальний захист пристрою).

3. Біометричні методи автентифікації. Біометрія належить до фактору "що ви є" і все ширше використовується як складова MFA. Поширеними прикладами є відбитки пальців (сканери відбитків на смартфонах, ноутбуках), розпізнавання обличчя (Face ID на iPhone, Windows Hello Face на Windows 10/11), сканування райдужки ока, розпізнавання голосу. Біометричні дані зручні для користувача – не потрібно нічого запам'ятовувати чи носити з собою, достатньо самого себе. Однак у контексті багатофакторної автентифікації біометрія зазвичай не використовується ізольовано, а поєднується з іншим фактором. Це пов'язано з особливостями біометрії: її не можна легко змінити чи відкликати у разі компрометації (на відміну від пароля або токена), і існують способи обманути деякі біометричні системи (наприклад, використання високоякісного зображення обличчя або підробленого відбитка). Тому біометрію часто застосовують як активатор іншого фактора.

Прикладом є сучасні смартфони: з метою зручності користувачі розблоковують телефон відбитком або обличчям, що слугує біометричним фактором, але сам телефон при цьому виступає фактором володіння у схемі MFA для доступу до сервісів. Тобто, коли користувач підтверджує вхід натисканням "Підтвердити" в додатку, справжня автентифікація відбувається за рахунок криптографічного ключа на пристрої (фактор володіння), а відбиток лише дає змогу використати цей ключ (локальна перевірка). Така комбінація двох факторів (пристрій + біометрія) вбудована в один автентикатор відповідає поняттю мультифакторного автентикатора за NIST [10]. Наприклад, апаратний FIDO2-ключ може бути мультифакторним: його приватний ключ захищений PIN-кодом

або відбитком – для виконання криптографічної операції потрібно ввести щось, що знаєте, або притаманне вам. Таким чином досягається два фактори (володіння ключем і знання PIN/наявність біометрії) в одному компактному пристрої.

У деяких сценаріях біометрію використовують і як окремий другий фактор, особливо всередині організацій. Наприклад, система може вимагати окрім пароля ще й прикладення пальця до сканера. Але на відміну від OTP чи токенів, чисто біометричний другий фактор менш розповсюджений через складність інтеграції та апаратні вимоги. Частіше біометрія інтегрована в інші рішення (смартфон, смарт-карта тощо).

Також розвиваються поведінкові біометричні фактори (діяльнісні ознаки) – про них детальніше йтиметься в розділі про перспективи. Це, наприклад, ритм введення пароля, звички руху мишкою, манера тримати смартфон. Вони можуть додавати непомітний для користувача шар перевірки (фактор “те, як ви робите”). Наразі поведінкові фактори зазвичай використовуються для *додаткового моніторингу* (continuous authentication), а не як явний фактор, який потрібно підтвердити при вході.

4. Автентифікація на основі пуш-сповіщень (push-based MFA). Окремо варто виділити метод, коли другий фактор підтверджується через пуш-сповіщення на мобільному пристрої. Сценарій виглядає так: після введення користувачем пароля, на його телефон приходить повідомлення від додатку-аутентифікатора (наприклад, Microsoft Authenticator, Duo Mobile, Okta Verify тощо) зі запитом підтвердити вхід. Користувач одним дотиком (натискання “Approve/Дозволити”) підтверджує спробу входу. В цей момент додаток формує криптографічну відповідь серверу, аналогічно до одноразового паролю, але це відбувається “за лаштунками” і непомітно для користувача. Push-автентифікація зручна тим, що не вимагає ручного введення кодів. Користувачеві достатньо мати при собі телефон і розблокувати екран для підтвердження. Реалізація найчастіше ґрунтується на тому, що додаток має криптографічний ключ, спільний з сервером (або зареєстрований публічний ключ), і при підтвердженні підписує nonce

(одноразову випадкову послідовність) – це доводить, що користувач володіє зареєстрованим пристроєм.

Push-based MFA набуло значної популярності у корпоративному середовищі та сервісах для кінцевих користувачів, оскільки спрощує UX (user experience). Приміром, Google при автентифікації у власні сервіси на Android запитує підтвердити “Чи ви зараз намагаєтесь увійти?” натисканням кнопки. Банківські застосунки теж впроваджують підтвердження транзакцій через push. Однак цей метод має і вразливі місця, про які йтиметься далі (атаки типу “MFA fatigue”). З точки зору факторів, push-метод покладається на **володіння** довіреним пристроєм (з додатком), але для безпечності його часто поєднують з локальним розблокуванням додатку (наприклад, запитати у користувача біометрію або PIN перед підтвердженням) – щоб у разі втрати телефону зловмисник не зміг схвалити запит.

5. Безпарольна автентифікація (passwordless) як різновид MFA. Концепція “безпечного майбутнього без паролів” тісно пов’язана з багатофакторною автентифікацією. Passwordless не означає відмову від другого фактору – радше навпаки, це перенесення акценту з знання (пароля) на інші фактори (володіння та притаманність). Багато passwordless-рішень фактично є двофакторними схемами, але без традиційного пароля. Наприклад, система одноразового посилання на email: користувач вводить лише адресу пошти, і отримує лист з унікальним посиланням для входу. Перейшовши за посиланням (що підтверджує володіння поштовою скринькою), він потрапляє в акаунт. Тут роль “пароля” грає доступ до email (який сам повинен бути захищений). Інший приклад – входи через мобільний додаток за QR-кодом або підтвердженням: вебсайт показує QR-код, користувач сканує його телефоном у своєму додатку, і тим самим автентифікується (як це реалізовано, наприклад, у Telegram, WhatsApp Web тощо). Усі ці методи все одно спираються на фактор володіння (пристроєм чи адресою) і часто додатково захищені притаманністю (розблокувати телефон для сканування QR). Тобто, фактично безпарольні методи включають MFA “під капотом”, але прибирають обтяжливу для користувача частину – паролі.

Найперспективнішим напрямком безпарольної автентифікації є вже згаданий стандарт FIDO2/WebAuthn, зокрема механізм Passkeys. Passkey – це запис (пара ключів) у пристрої користувача, який повністю замінює пароль. Для входу користувач використовує тіло/біометрію або PIN для розблокування свого пристрою, а той виконує криптографічну автентифікацію із сервісом. По суті, пароль замінено зв'язкою "пристрій + локальний метод розблокування", яка сама є мультифакторною (володіння + знання або володіння + притаманність). Як вже згадувалося, великі платформи анонсували підтримку passkeys синхронізованих через хмару, що дозволить користувачам легко переходити на безпарольний вхід [29].

2.2 Приклади впровадження MFA в різних сферах

Державний сектор. Урядові та державні установи у всьому світі активно впроваджують MFA для захисту доступу до чутливих даних і систем. Зокрема, у США після низки кібератак було видано низку нормативних актів, що вимагають обов'язкового використання багатофакторної автентифікації. У травні 2021 року Указ Президента США №14028 "Про вдосконалення кібербезпеки нації" прямо зобов'язав федеральні органи протягом визначеного періоду часу впровадити багатофакторну автентифікацію на всіх рівнях доступу [30]. Виконання цього указу означає, що всі працівники федеральних агентств повинні використовувати MFA (наприклад, апаратні смарт-карти PIV з PIN-кодом або інші засоби) для доступу до урядових мереж і додатків. В Європейському Союзі дія Директиви NIS також стимулює державні структури та операторів критичної інфраструктури впроваджувати "сильні" методи автентифікації. Наприклад, агенції ЄС (ENISA та CERT-EU) в своїх спільних рекомендаціях зазначають необхідність захищати всі віддалені доступи за допомогою MFA [27]. На практиці багато країн вводять двофакторну автентифікацію для доступу громадян до електронних послуг держави (через BankID, MobileID, Дія.Підпис тощо). Таким чином, в держсекторі MFA стала стандартом де-факто для захисту

як внутрішніх урядових систем (входу службовців), так і зовнішніх сервісів для громадян.

Бізнес і корпоративний сектор. Комерційні компанії, особливо великі, усе більше інтегрують MFA в свої системи безпеки. Це стосується як доступу співробітників до корпоративних ресурсів (VPN, електронна пошта, хмарні сервіси), так і захисту клієнтських акаунтів. Практично всі великі IT-компанії зобов'язали своїх працівників використовувати 2FA/MFA. Показовим прикладом є компанія Google: ще у 2017 році Google роздав всім 85 тисячам своїх співробітників апаратні ключі безпеки (YubiKey) і зробив їх використання обов'язковим для входу в корпоративні облікові записи. Результат – жоден з цих акаунтів не був успішно фішингований чи зламаний в наступні роки [31] . За словами представників компанії, після впровадження апаратної MFA вони не зафіксували *жодного* випадку компрометації облікового запису співробітника шляхом крадіжки пароля [31]. Цей кейс часто наводять як доказ ефективності сучасних MFA-рішень. Інші корпорації, як-от Microsoft, також активно впроваджують MFA: Microsoft з 2019 року ввімкнув за замовчуванням політику Security Defaults для всіх нових орендарів Azure AD, яка вимагає MFA від користувачів та адміністраторів. Багато компаній переходять на безпарольні рішення для своїх працівників – наприклад, впроваджують входи за допомогою Windows Hello for Business (ключі FIDO2 на базі TPM в ноутбуках).

Використання MFA в бізнесі продиктоване не лише турботою про безпеку, а й вимогами кіберстрахування та відповідності стандартам (компаніям може бути відмовлено у виплатах після інциденту, якщо не було належного захисту облікових записів). За оцінками опитувань, на кінець 2024 року близько 83% організацій впровадили вимогу MFA для доступу співробітників до ключових IT-ресурсів [32]. При цьому великий бізнес робить це значно частіше, ніж малий: серед компаній з понад 10 тисячами працівників MFA використовують 87%, а серед малих фірм (до 25 співробітників) – лише 27% [32]. Це свідчить про те, що більші організації краще розуміють важливість і мають ресурси для

впровадження багатофакторного захисту, тоді як малий бізнес часто залишається уразливим (про проблеми впровадження – далі).

Банківська і фінансова сфера. Банки були одними з піонерів застосування двофакторної автентифікації, адже захист коштів клієнтів безпосередньо залежить від надійності автентифікації. Ще з 2000-х років банки видавали клієнтам апаратні OTP-токени для підтвердження транзакцій (наприклад, пристрої типу Vasco, OTP-калькулятори тощо). Надалі багато хто перейшов на SMS-коди (мобільний телефон майже є у кожного клієнта). Регулятори фінансового сектору також вимагають MFA. В ЄС з 2019 року набрали чинності вимоги PSD2 щодо так званої сильної автентифікації клієнта (Strong Customer Authentication, SCA). SCA – це обов'язкова двофакторна автентифікація для майже всіх електронних платежів: клієнт має підтвердити платіж двома з трьох факторів (знання, володіння, притаманність) [33]. Банки реалізують це по-різному – хтось продовжує надсилати SMS + вимагає вводити постійний пароль, інші перейшли на push-підтвердження в мобільному додатку або скан відбитка в додатку. Для карткових платежів онлайн впроваджується протокол EMV 3-D Secure версії 2, який підтримує різні способи SCA і фактично зобов'язує e-commerce платіжні сторінки запитувати у покупця другий фактор. Таким чином, у банківській сфері на сьогодні двофакторна автентифікація стала нормативною вимогою. Як результат – скоротилися шахрайства з платежами, хоча й з'явилися нові види атак на саму MFA (соціальна інженерія клієнтів для отримання кодів, malware на смартфонах для перехоплення SMS тощо – про це у відповідному розділі).

Крім клієнтської автентифікації, банки захищають і доступ до адміністративних IT-систем. Стандарти безпеки, такі як PCI DSS (для платіжних карт), прямо вимагають від фінансових установ використовувати MFA для будь-якого адміністративного доступу до систем, що обробляють дані карт. Остання версія PCI DSS 4.0 розширила цю вимогу: тепер MFA має застосовуватися для *всіх* акаунтів з доступом до середовища карткових даних, а не тільки для адміністраторів [34]. Тобто фактично кожен співробітник банку чи

процесингового центру, що працює з платіжною інформацією, мусить проходити багатофакторну автентифікацію.

Охорона здоров'я. Медична галузь також стикається з ростом кібератак, особливо з поширенням електронних медичних записів та дистанційних сервісів. Медичні дані пацієнтів є конфіденційними і захищеними законом (наприклад, HIPAA в США, GDPR – у Європі). У зв'язку з цим регулятори охорони здоров'я дедалі частіше рекомендують чи навіть зобов'язують використовувати MFA для доступу до електронних медичних інформаційних систем, щоб запобігти несанкціонованому доступу при компрометації пароля. Наприклад, Управління з прав цивільних прав (OCR) при Міністерстві охорони здоров'я і соціальних служб США у 2023 році внесло пропозицію змін до правил HIPAA, які б вимагали від постачальників медичних послуг впровадження багатофакторної автентифікації для доступу до електронних медичних записів та іншої чутливої інформації [35]. Така вимога була продиктована різким зростанням кіберінцидентів у лікарнях, зокрема атак з використанням викрадених облікових даних. Якщо ця норма буде прийнята, всі лікарні, страхові компанії та інші суб'єкти, підпорядковані HIPAA, повинні будуть технічно забезпечити MFA для лікарів, медперсоналу і партнерів, що підключаються до систем з медданими.

Наразі багато медичних установ впроваджують MFA добровільно. Зазвичай це відбувається через видачу працівникам апаратних бейджів/карт з RFID або смарт-карток, які використовуються спільно з PIN-кодом для входу в комп'ютери та медичні системи (що є двофакторною схемою). Інші підходи – це надсилання кодів на телефони лікарів при віддаленому доступі до систем (наприклад, VPN доступ в лікарняну мережу), або використання біометричних зчитувачів. Деякі країни впровадили національні медичні ідентифікатори з двофакторним захистом – наприклад, в Естонії лікарі використовують електронну ID-карту (з чипом та PIN) для доступу до медичних реєстрів.

Інші сфери. У сфері електронної комерції MFA використовується для захисту акаунтів покупців (наприклад, при вході на Amazon є опція OTP), а також майданчики впроваджують двофакторну перевірку для продавців (щоб захистити

фінансові налаштування). Соціальні мережі та електронна пошта – теж критичні сервіси, де MFA може запобігти захопленню акаунтів. Facebook, Twitter, Instagram, Gmail, Outlook та інші пропонують користувачам ввімкнути 2FA (SMS, додаток або ключ безпеки). Статистика кілька років тому показувала, що відсоток користувачів, які добровільно вмикають MFA, був невисоким (близько 10% на Gmail станом на 2018 рік). Проте останнім часом платформи почали примусово підключати двофакторовий захист: Google оголосив у 2021 році, що автоматично ввімкнув 2-Step Verification для понад 150 мільйонів акаунтів, які раніше його не мали, аби підвищити рівень безпеки екосистеми[36]. В бізнес-сервісах (GitHub, GitLab, Salesforce тощо) MFA також стає умовою використання – GitHub повідомив, що з кінця 2023 року вимагатиме 2FA для всіх розробників, які вносять код [37].

2.3 Типові загрози та способи обходу MFA, методи захисту

Хоча багатофакторна автентифікація значно зміцнює безпеку, жоден захисний механізм не є абсолютним. Зловмисники адаптуються і розробляють атаки, націлені на обхід або злам саме MFA-рішень. Розглянемо основні загрози та методи атак на MFA, а також відповідні засоби протидії цим загрозам.

Фішинг та атаки “людина посередині” (MitM) проти MFA. Звичайний фішинг (коли жертва вводить свій пароль на підробленому сайті) малоефективний проти облікових записів з MFA, адже окрім пароля треба ще перехопити одноразовий код чи інший другий фактор. Тому зловмисники вдосконалили тактику: вони проводять фішинг у реальному часі із залученням проксі-сервера. Схема така: жертва переходить на фейковий сайт (дуже схожий на справжній), вводить там логін і пароль, а фішинговий інструмент миттєво пересилає ці дані на справжній сайт і отримує запит другого фактора. Далі жертві *на тому ж підробленому сайті* показується сторінка введення коду 2FA (наприклад, “введіть 6-значний код з SMS”). Жертва вводить OTP, зловмисник передає його на справжній сайт – і тим самим входить в акаунт, обійшовши MFA.

Такі атаки називають **proxy phishing** або атакою посередника (**MITM/AITM** – Adversary-in-the-Middle). В останні роки з'явилися готові фреймворки для автоматизації цього процесу, наприклад **Evilginx2, Modlishka, Muraena** тощо, які значно полегшують проведення подібних атак навіть не дуже технічно підкованим злочинцям. У 2022 році сталася серія фішингових нападів на відомі компанії (Twilio, Cloudflare та інші) з використанням проксі-фішингу: зловмисники розсилали СМС зі шкідливими посиланнями, а співробітники, які перейшли і ввели свої 2FA-коди на фальшивих сторінках, фактично віддали доступ зловмисникам. Це продемонструвало, що **методи на основі OTP (особливо SMS, TOTP)** вразливі до добре організованого фішингу.

Ще складніший варіант – **перехоплення сесійного cookie** після MFA. У випадку проксі-атаки зловмисник, увійшовши на справжній сайт, може витягнути сесійну кукі, яка підтверджує авторизацію, і зберегти її. Потім він може використати цю кукі (наприклад, імпортувати в браузер) щоб отримати доступ до акаунту вже *без повторної автентифікації*. Це дозволяє обійти навіть такі MFA, як push, бо жертва вже схвалила одну сесію, і атакувальник просто її **перехопив**. Саме таким чином діяли деякі хакерські групи: Microsoft у 2022 описала кампанію, де злочинці масово застосовували спеціалізовані фішингові комплекти для крадіжки сесій після MFA – так звані **AiTM-attacks (Adversary-in-the-middle)** [38].

Як захищатися? Основний захід – фішингостійкі методи MFA, тобто такі, що не можна легко передати зловмиснику. Апаратні FIDO2-ключі – найкращий приклад: через прив'язку до домену проксі-схема не спрацює (підроблений домен не отримає підпис). Інший підхід – прив'язка сесії до клієнта (наприклад, браузер видає сесійний токен, прив'язаний до криптографічного контексту, який важко відтворити на іншій машині). Також все більшої уваги надається контролю за логінами: навіть якщо cookie викрадено, систему моніторингу можуть насторожити аномалії (наприклад, різке переміщення сесії на іншу IP-адресу чи геолокацію). Від користувацького боку – рекомендується ніколи не вводити 2FA-коди на підозрілих сайтах і уважно стежити за URL (але це класична порада, яка,

на жаль, часто ігнорується). В цілому, усвідомивши проблему, великі компанії почали переходити на безфішингові MFA. Зокрема, Офіс управління та бюджету США (OMB) у меморандумі M-22-09 зобов'язав федеральні агентства забезпечити для публічних сервісів можливість використання користувачами факторів, стійких до фішингу (наприклад, WebAuthn) [39]. ENISA так само радить перейти на апаратні токени та FIDO2, а SMS і OTP вважає менш надійними [27].

Атаки типу "MFA fatigue" (втомлення від MFA). Це відносно новий метод, націлений на push-базовану автентифікацію. Якщо зловмисник здобув пароль користувача, але натрапляє на другий фактор у вигляді підтвердження на телефоні, він може вдатися до спаму запитами: автоматично десятки разів поспіль ініціювати вхід, щоб телефон жертви безперервно отримував запити схвалити вхід. Ідея в тому, що користувач або помилково, або через роздратування може зрештою натиснути "Approve" просто щоб зупинити надоїдливі нотифікації. Такі атаки отримали назву "prompt bombing" або MFA fatigue. У вересні 2022 року гучна атака на компанію Uber була здійснена саме таким способом: злочинці спершу викрали пароль одного з співробітників, а далі засипали його телефон запитами на підтвердження входу в VPN. Паралельно вони зв'язалися з ним у WhatsApp, представившись IT-відділом Uber, і вмовили нарешті підтвердити один з тих запитів під приводом "щоб їх вимкнути". Співробітник погодився – і нападники проникли всередину мереж Uber, спричинивши серйозний інцидент [38]. Подібні випадки сталися і в інших компаніях, що свідчить: якщо push-сповіщення не захищені додатково, людський фактор знову можна експлуатувати. З точки зору користувача, нескінченні запити виглядають як збій системи, і він може несвідомо натиснути "Так" просто щоб це припинилось – чим і користуються зловмисники.

Контрзаходи: постачальники рішень вже відреагували. По-перше, впроваджується так зване "number matching": замість простого "Approve/Deny" користувачу показується число на пристрої, яке він має ввести у телефоні для підтвердження. Це ускладнює автоматичний бомбінг – користувач не зможе

помилково прийняти запит, не глянувши на екран. Microsoft Authenticator у 2023 зробив number matching обов'язковим для всіх, щоб закрити вектор MFA fatigue. По-друге, вводять обмеження частоти запитів: після певної кількості невдалих запитів акаунт блокується або принаймні сповіщається адміністратор. Але тут треба обережно, щоб не створити можливість DoS (зловмисник навмисно заблокує легітимного користувача, кілька разів невірно запитавши код). Кращий підхід – сповіщати користувача: якщо він отримує вал запитів, яких не ініціював, йому слід терміново змінити пароль і повідомити безпеку. Компанії навчають персонал: правило "якщо ви раптом отримуєте багато несподіваних запитів MFA – одразу інформуйте IT, це ознака атаки".

Крім того, деякі реалізації push вводять додатковий фактор напрямку зв'язку: наприклад, при спробі входу на екрані браузера показується код, який треба вибрати у телефоні. Це захищає від віддаленого спаму, бо зловмисник не знає, який код показано жертві. В цілому, хоча атаки MFA fatigue були успішними проти деяких компаній, вони легко ускладнюються технічними оновленнями, і цей вектор, ймовірно, втратить ефективність по мірі оновлення систем.

Соціальна інженерія та обхід через підтримку. Зрештою, найбільш "універсальний" шлях – спробувати змусити саму жертву або адміністратора відключити MFA. Зловмисники можуть видавати себе за користувача і дзвонити в службу підтримки, просячи "відключити 2FA, бо телефон загубився", або навпаки – видаючи себе за підтримку, дзвонити користувачу і випитувати коди. Були випадки, коли шахраї телефонували працівникам компаній, представлялися IT-адмінами і під приводом "усунення проблеми" випитували код з SMS, або надсилали посилання для скидання MFA. Такі методи не технічні, але інколи спрацьовують, особливо якщо внутрішні процеси по reset MFA недостатньо захищені. Тому організаціям важливо продумати процедури: наприклад, щоб відновити доступ при втраті другого фактора, користувач має особисто підтвердити особу за низкою питань або через керівника, а не просто по дзвінку. І навчити співробітників: ніколи не повідомляти коди перевірки чи не схвалювати запити входу, яких ви самі не ініціювали.

Технічні експлойти факторів. В деяких випадках зловмисники можуть атакувати сам механізм другого фактора. Наприклад, якщо використовується TOTP-додаток, можна спробувати інфікувати смартфон шкідливим ПЗ, щоб перехоплювати коди до того, як користувач їх введе. Існують мобільні трояни, що спеціалізуються на крадіжці SMS-кодів – такі часто б'ють по банківських клієнтах (трояни типу Cerberus, EventBot тощо). Деякі навіть намагаються викрасти секретний ключ TOTP з пам'яті телефону (якщо додаток не захищений належно) – тоді можна синхронно генерувати коди. Це доволі складний шлях, але високоорганізовані групи можуть його застосувати. Інший напрям – атаки на алгоритми або реалізації. В історії були випадки скомпрометованих генераторів OTP (наприклад, злам RSA SecurID у 2011, коли зловмисники викрали внутрішні дані, що дозволило їм клонувати токени деяких клієнтів). Також можуть бути помилки в програмному коді серверу перевірки 2FA, що дозволять, скажімо, завжди проходити при введенні певного фіктивного коду. Це дуже індивідуальні випадки, але їх потрібно враховувати: MFA не скасовує необхідності тестування безпеки компонентів автентифікації.

Фактор "біометрія" також має свої загрози. Біометричні системи можуть бути обмануті: є випадки, коли високоякісні відбитки або модель обличчя (наприклад, роздруківка 3D-маски) розблоковували пристрій. Відбитки можна "зняти" з предметів і виготовити латексний муляж. Голосові автовідповідачі можуть вводитись в оману синтезованим голосом. Це все реальні ризики, хоча сучасні системи впроваджують захист від підробки (liveness detection) – наприклад, камера перевіряє рух очей або реагує на інфрачервоне випромінення, щоб відрізнити живу людину від фотографії. Для критичних сценаріїв рекомендується комбінувати біометрію з іншим фактором, щоб навіть якщо одну систему обійшли, залишився бар'єр.

2.4 Методи захисту та найкращі практики MFA

Враховуючи наведені загрози, індустрія виробила такі рекомендації:

Використовувати фішингостійкі MFA там, де це можливо. До них належать апаратні криптографічні автентифікатори: FIDO2, смарт-карти, TPM-базовані рішення. Вони практично усувають ризик проксі-фішингу. Наприклад, федеральні установи США переходять на апаратні PIV-картки, а великі IT-компанії – на ключі YubiKey. Якщо дозволити користувачам вибір, варто заохочувати саме ці методи (скажімо, давати бонуси чи спрощувати процес для тих, хто обрав ключ, і трохи ускладнювати для тих, хто на SMS).

Менш безпечні фактори – під особливий контроль. Якщо SMS або одноразові коди все ж використовуються (не можна від них одразу відмовитись через користувацьку базу), потрібно моніторити їх використання. Наприклад, запровадити обмеження на кількість запитів OTP, навчити службу підтримки перевіряти підозрілі ситуації (часті звернення про “не приходить SMS” можуть свідчити про атаку на телеком). Корисно впроваджувати додаткові перевірки: наприклад, банківські системи SCA вимагають не просто OTP, а OTP, прив’язаний до суми і рахунку платежу (динамічний зв’язок) – так званий Transaction signing. Це реалізовано у європейських банках згідно PSD2: код генерується пристроєм на основі деталей транзакції, тому навіть якщо його перехопити, він не валідний для іншої операції.

Механізми резервного доступу – безпечні і обмежені. Потрібно передбачити, як користувач увійде, якщо втрачено другий фактор: чи будуть резервні одноразові коди, чи процедура через підтримку. Ці резервні методи повинні бути не легше зламати, ніж основний MFA. Поганою практикою було б дозволити “тимчасово відключити 2FA по email” – адже email може бути скомпрометовано. Краще видавати заздалегідь набір статичних паролів для одноразового використання, які користувач тримає в безпечному місці. Або мати сувору верифікацію особи при запиті на скидання MFA (паспорт, особисте спілкування з адміном тощо).

Адаптивна аутентифікація. По можливості системи повинні оцінювати ризики кожної спроби входу і відповідно реагувати. Наприклад, якщо користувач завжди входить з Києва, а раптом його пароль правильно вводять з Бразилії – вимагати не два, а три фактори (якщо таке налаштовано) або блокувати спробу. Або якщо обліковий запис адміністратора – завжди застосовувати найсильніший метод (апаратний ключ), незалежно від того, що іншим дозволено SMS. Багато компаній практикують модель нульової довіри (Zero Trust), де MFA запитується не тільки при логіні, а й при доступі до чутливих операцій, або періодично перепідтверджується протягом сесії.

Моніторинг аномалій MFA. Як згадувалось, слід відстежувати підозрілі ситуації: велика кількість відхилених запитів MFA, часті звернення до адміністратора з проханням скинути 2FA, логіни з нових пристроїв. Сучасні системи управління ідентичностями (IAM) надають журнали таких подій, їх аналіз може виявити спроби атаки ще до компрометації.

Навчання та політики. Техніка ефективна лише разом з правильною поведінкою людей. Політики безпеки мають чітко регламентувати: нікому не повідомляти коди, ніколи не схвалювати неініційовані запити. Корисно розсилати нагадування, проводити тренінги з соціальної інженерії, навіть імітувати фішингові атаки, щоб перевірити пильність. Користувач повинен розуміти: якщо на телефоні з’явився запит на вхід, а він сам цього не робив – значить, пароль вже викрадено, і треба негайно змінювати його та інформувати службу безпеки. Така обізнаність закриває останній “людський” вектор.

Висновки до розділу 2

У данному розділі було проведено комплексний аналіз сучасних технологій багатофакторної автентифікації (MFA) та окреслено ключові напрямки їх впровадження в різних сферах діяльності. Розглянуто основні типи MFA-рішень — одноразові паролі (OTP), апаратні токени (U2F, FIDO2), біометричні засоби, push-сповіщення, а також концепцію безпарольної автентифікації. Детально

охарактеризовано принципи їх роботи, переваги та недоліки з точки зору безпеки та користувацького досвіду.

У межах підрозділів було проаналізовано практичні приклади впровадження MFA у державному секторі, корпоративному середовищі, банківській справі, медицині та інших критичних галузях. Доведено, що найбільш ефективні та фішингостійкі рішення (зокрема FIDO2/WebAuthn) набувають статусу нових стандартів безпеки у провідних організаціях. Окрему увагу приділено існуючим загрозам, які виникають навіть у системах з MFA: проксі-фішинг, атаки типу "MFA fatigue", соціальна інженерія, експлойти факторів. Проаналізовано сучасні методи захисту від зазначених атак, зокрема використання фішингостійких методів, адаптивної автентифікації та політик безпеки.

РОЗДІЛ 3. АНАЛІЗ ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ MFA ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Мультифакторна автентифікація (MFA) є одним із ключових механізмів забезпечення безпеки доступу до інформаційних систем та персональних даних. Суть MFA полягає у тому, що для підтвердження особи користувача використовується більше ніж один автентифікаційний фактор. Зазвичай фактори автентифікації поділяють на три основні категорії: знання (те, що знає користувач – пароль, PIN-код), володіння (те, що користувач має – токен, смартфон) та властивість (те, чим користувач є – біометричні дані). Комбінація факторів із різних категорій значно ускладнює несанкціонований доступ: зловмиснику недостатньо, наприклад, тільки перехопити пароль, щоб проникнути в обліковий запис. За даними досліджень, впровадження MFA дозволяє запобігти переважній більшості атак, пов’язаних з компрометацією облікових записів. Зокрема, корпорація Microsoft повідомляє, що 99,9% успішних злому облікових записів стаються на акаунтах без ввімкненої MFA [40]. Подібні оцінки наводилися й раніше: за словами директора з безпеки Microsoft А. Вайнерта, обліковий запис із ввімкненою MFA в середньому у 99,9% випадків менш схильний до злому. Статистика Verizon також підтверджує актуальність проблеми: до 74% всіх випадків компрометації даних у 2022 році причетний людський фактор – зокрема, фішингові атаки та використання вкрадених паролів [44].

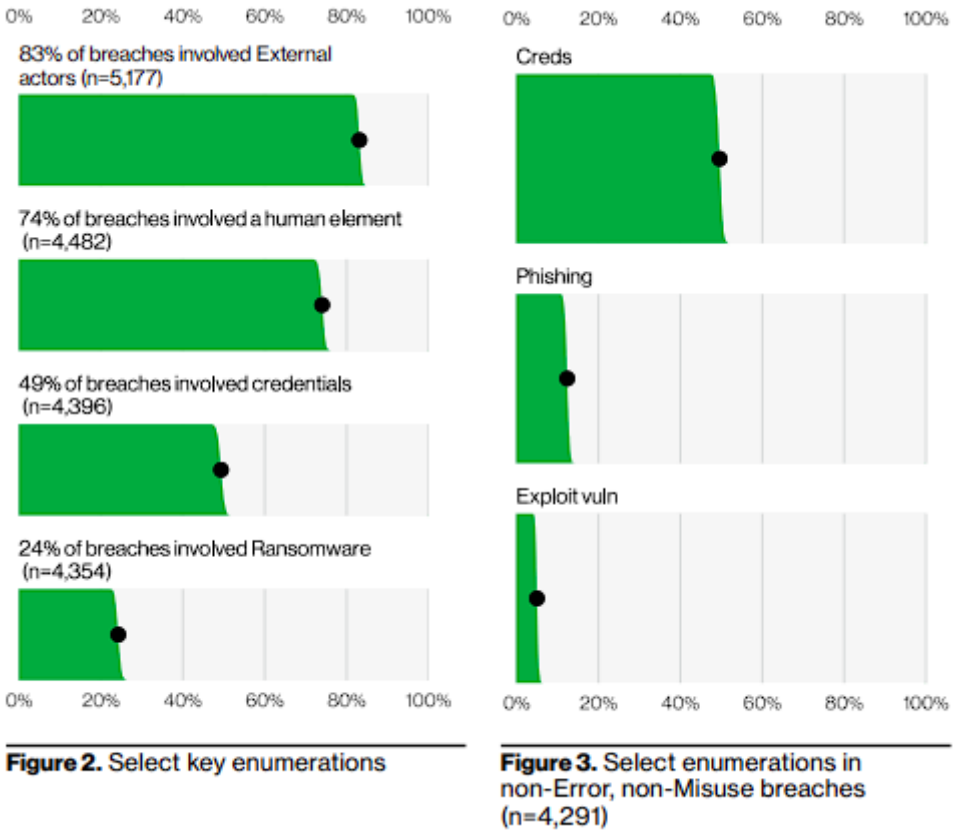

Рис. 3.1. Статистика Verizon щодо випадків компрометації даних

Отже, багато урядових та галузевих стандартів нині вимагають обов'язкового застосування MFA для захисту персональних даних. Наприклад, в ЄС діє вимога нормативу PSD2 щодо сильної автентифікації клієнтів (Strong Customer Authentication, SCA), яка зобов'язує банки застосовувати щонайменше два фактори при доступі до рахунків і здійсненні електронних платежів. У США указом Президента №14028 (2021) передбачено перехід федеральних установ на модель Zero Trust із обов'язковим впровадженням MFA до кінця 2024 року. Отже, питання вибору належної технології MFA, практичної реалізації та оцінки її ефективності є вкрай актуальними. У цьому розділі проведено аналіз підходів до вибору багатофакторної автентифікації для конкретних систем, розглянуто практичне впровадження MFA на прикладі платформи Microsoft Azure, виконано порівняльний аналіз ефективності MFA у банківській сфері та оцінено безпеку й зручність використання MFA з точки зору кінцевого користувача.

3.1. Вибір технології MFA для конкретної системи

При впровадженні багатофакторної автентифікації у конкретній інформаційній системі важливо обрати оптимальну технологію MFA, яка відповідатиме вимогам безпеки цієї системи та умовам її експлуатації. Існує широкий спектр доступних методів MFA, що різняться за принципом дії, рівнем захищеності та зручністю для користувачів. До найбільш поширених належать одноразові паролі OTP (One-Time Password), що генеруються апаратними або програмними токенами, пуш-сповіщення в мобільному додатку, SMS-коди, голосові дзвінки з кодом, біометрична автентифікація (відбиток пальця, розпізнавання обличчя), апаратні криптографічні ключі (наприклад, ключі безпеки FIDO2) тощо [42]. Кожна технологія має свої переваги та недоліки, тому вибір слід здійснювати на основі кількох критеріїв: рівень безпеки, стійкість до типових атак, сумісність із інфраструктурою системи, зручність та досвід користувача, а також вартість і складність розгортання.

Безпекові характеристики різних методів MFA можуть суттєво відрізнятися. Так, простіші рішення на кшталт SMS-кодів або кодів із мобільного додатка-аутентифікатора забезпечують базовий рівень захисту, проте мають вразливості. Зокрема, одноразові паролі, надіслані через SMS, можуть бути перехоплені зловмисником шляхом атаки типу SIM-swapping або інших методів компрометації телефонного номера. Національний інститут стандартів і технологій США (NIST) у своїх рекомендаціях прямо застерігає щодо використання загальнодоступної телефонної мережі (PSTN) для передачі секретів MFA, позначаючи SMS як «обмежений» (restricted) канал через підвищені ризики перехоплення. Тобто, якщо є можливість, слід відмовитися від SMS як другого фактору на користь більш захищених методів – апаратних криптотокенів чи одноразових кодів у спеціальних додатках. Аналогічно, голосові виклики з кодом по телефону не гарантують належної стійкості, оскільки можуть бути переадресовані або перехоплені. Більш сучасні методи MFA пропонують вищий рівень захисту. Наприклад, апаратні токени з

підтримкою FIDO2 (апаратні ключі безпеки) та криптографічні смарт-картки забезпечують фішингостійку автентифікацію – зловмисник не зможе скопіювати ключ або обманом змусити користувача розкрити секрет, адже підтвердження операції виконується апаратно і прив'язане до легітимного сайту. Пуш-сповіщення в додатку (наприклад, Microsoft Authenticator, Google Authenticator) є компромісом між зручністю та безпекою: вони зручні для користувача (достатньо одним тапом підтвердити вхід), але можуть стати об'єктом атаки методом виснаження (MFA fatigue) – коли користувача завалюють запитами на підтвердження зловмисного входу, сподіваючись, що він помилково натисне «Дозволити». Новіші реалізації додають захист від цього, наприклад, номерні матчинг (number matching) – вимогу ввести число з екрану на телефоні, що знижує ймовірність автоматичного підтвердження.

Для конкретної системи вибір MFA має базуватися на моделі загроз та сценаріях використання. Якщо йдеться про корпоративну систему з високими привілейованими доступами, варто обирати максимально стійкі до фішингу та перехоплення рішення (апаратні ключі, смарт-картки, апаратні OTP-токени).

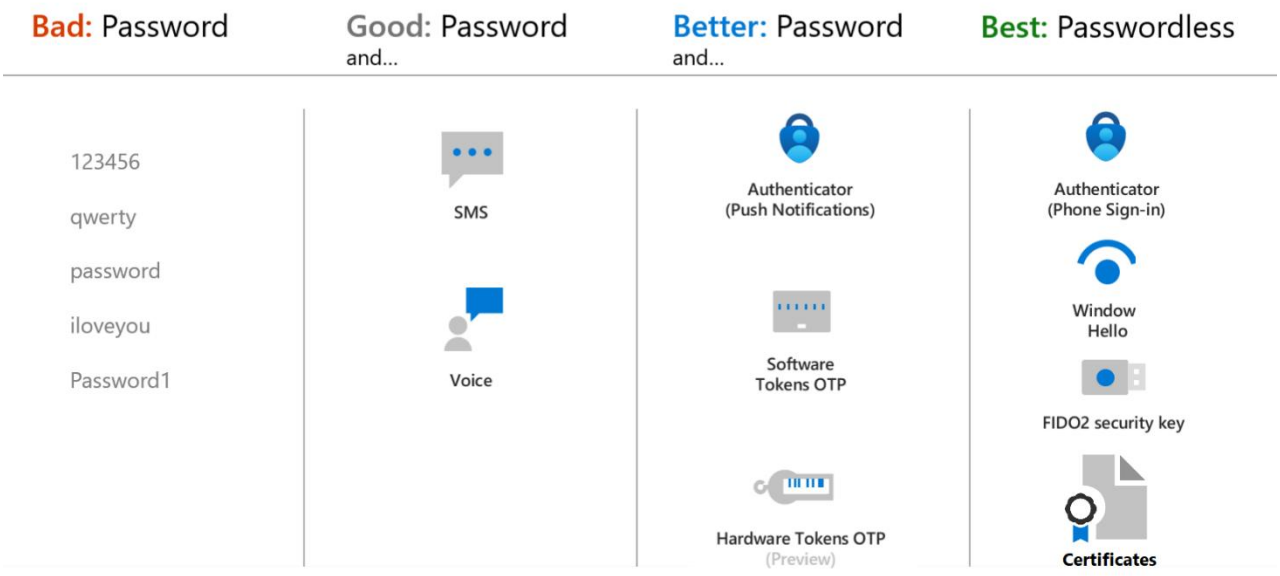

Рис. 3.2. Порівняння надійності методів автентифікації [41]

За даними Microsoft: паролі самі по собі вважаються "поганим" методом, комбінація пароля з SMS або голосовим підтвердженням – "добрим", пароля з пуш-сповіщенням або OTP – "кращим", а найвищий рівень безпеки забезпечують безпарольні методи (апаратні ключі, Windows Hello, сертифікати) [41]. Для масового веб-сервісу, розрахованого на широке коло користувачів, критичним є баланс між безпекою та зручністю: надто складна MFA (наприклад, вимога мати спеціальний апаратний токен) може відштовхнути частину користувачів. У таких випадках доцільно пропонувати декілька опцій MFA на вибір – скажімо, мобільний додаток-аутентифікатор або SMS (з можливістю згодом перейти на безпечніший метод). Відповідно до рекомендацій Microsoft, слід дозволяти користувачам реєструвати кілька методів MFA для резервування [42]. Якщо основний метод недоступний (наприклад, загублено телефон з додатком), користувач зможе пройти автентифікацію запасним методом (наприклад, за допомогою резервного коду чи SMS) [42].

Не менш важливо враховувати сумісність MFA-рішення з існуючою IT-інфраструктурою. Наприклад, у середовищі Microsoft Active Directory зручним є використання Azure MFA або сторонніх рішень, інтегрованих через протоколи OATH, RADIUS тощо. Для веб-додатків часто застосовують стандарти OAuth2/OpenID Connect або SAML2 для підключення MFA через єдиний вхід (SSO). Також слід зважати на регуляторні вимоги та галузеві стандарти. У банківських і платіжних системах діють строгі норми (PSD2 в Європі, стандарт PCI DSS для платіжних карток тощо), які фактично визначають мінімальний набір факторів: пароль + одноразовий код або аналогічна комбінація. Якщо система повинна відповідати таким вимогам, вибір MFA звужується до рішень, схвалених регуляторами (як правило, це OTP через SMS/додаток або апаратні пристрої). Натомість для внутрішньої корпоративної системи можна більш вільно обрати метод, орієнтуючись на зручність для співробітників (наприклад, використати вже наявні у всіх смартфони з додатком Authenticator замість закупівлі апаратних токенів).

Зручність і досвід користувачів (UX) при виборі технології MFA мають велике значення. Практика показує, що добровільне впровадження MFA користувачами йде повільно – за даними Google, станом на 2018 рік менше 10% активних акаунтів Google мали ввімкнену двоетапну перевірку [45]. Багато користувачів уважають додаткові кроки автентифікації обтяжливими. Тому при проєктуванні варто обирати методи, що мінімізують незручності: наприклад, пуш-сповіщення замість ручного введення коду, можливість запам’ятати довірений пристрій на 30 днів, використання біометрії для швидкого підтвердження і т.д. Проведені опитування демонструють, що користувачі схильні миритися з MFA, якщо її застосування обмежене ризикованими операціями. Так, за даними дослідження PYMNTS.com, 83% клієнтів банків погоджуються на додаткову автентифікацію для високоризикових дій (наприклад, вхід з нового пристрою чи підтвердження великого платежу), хоча для повсякденних входів цей показник менший (близько 62%) [47]. Отже, у критичних системах безпека повинна мати пріоритет над абсолютною зручністю, але сучасні технології дозволяють значною мірою поєднати їх. Зокрема, концепція “passwordless” (безпарольної автентифікації) передбачає, що користувач узагалі не вводить пароль – автентифікація відбувається за допомогою пристрою (наприклад, смартфона) та біометрії або ПІНу, які разом реалізують два фактори одночасно [41]. Прикладом є технології Windows Hello, Apple ID з Face ID/Touch ID, апаратні ключі безпеки з відбитком пальця тощо. Такі рішення підвищують і безпеку, і зручність, оскільки позбавляють користувача від необхідності запам’ятовувати паролі, зменшують ризик фішингу та забезпечують швидку автентифікацію.

3.2. Практичне впровадження багатофакторної автентифікації

Для ілюстрації процесу впровадження багатофакторної автентифікації розглянемо реальний сценарій – активацію MFA в хмарній інфраструктурі Microsoft Azure (служба каталогів Azure Active Directory, нині відома як Entra ID).

Microsoft Azure є однією з найбільших хмарних платформ, яку використовують підприємства для розгортання IT-сервісів, тому питання захисту облікових записів у Azure AD є критично важливим. За замовчуванням автентифікація користувачів Azure здійснюється за паролем, проте адміністратор може ввімкнути Azure AD Multi-Factor Authentication для підвищення безпеки. Microsoft надає вбудовані засоби MFA, які інтегровані з усіма сервісами платформи і підтримують різні методи автентифікації.

Методи MFA в Microsoft Azure AD. Azure Active Directory підтримує кілька типів додаткових автентифікаторів, які користувач може використовувати як другий фактор при вході [42].

До них відносяться: мобільний додаток Microsoft Authenticator (генерація одноразових кодів або push-підтвердження), FIDO2-сумісні апаратні ключі безпеки, технологія Windows Hello for Business (біометрія або PIN, прив'язані до пристрою), одноразові паролі за алгоритмом OATH (програмні токени, апаратні токени), а також традиційні SMS і голосові виклики. Ви можете контролювати методи автентифікації, доступні у вашому клієнті. Наприклад, ви можете заблокувати деякі з найменш безпечних методів, наприклад SMS [42]. Приклад методів автентифікації наведено в таблиці 3.1 [42]. А чи використовуються первинні і вторинні методи автентифікації в певних методах наведено в таблиці 3.2 [41].

Таблиця 3.1.

Огляд методів автентифікації та їх керування в системах MFA

Метод автентифікації	Чим керується	Що охоплює
Microsoft Authenticator	Параметри MFA або політика методів автентифікації	Безпарольний вхід із телефону за допомогою автентифікатора можна охопити користувачами та групами
Ключ безпеки FIDO2	Політика методів автентифікації	Можна охопити користувачів і групи

Продовження таблиці 3.1.

Програмні або апаратні токени OATH	Налаштування багатофакторної автентифікації	-
SMS verification	1.Налаштування багатофакторної автентифікації 2.Керуйте входом через SMS для первинної автентифікації в політиці автентифікації	Вхід через SMS можна охопити користувачами та групами.
Voice calls	Політика методів автентифікації	-

Таблиця 3.2.

Категоризація методів автентифікації за типом використання: первинна vs. вторинна

Метод	Первинна автентифікація	Вторинна автентифікація
Windows Hello для бізнесу	Так	MFA
Microsoft Authenticator push	Ні	MFA та SSPR
Microsoft Authenticator без пароля	Так	Ні

Продовження таблиці 3.2.

Ключ доступу Microsoft Authenticator	Так	MFA
Authenticator Lite	Ні	MFA
Ключ доступу (FIDO2)	Так	MFA
Аутентифікація на основі сертифіката (CBA)	Так	MFA
Апаратні маркери OATH (попередній перегляд)	Ні	MFA та SSPR
Програмні маркери OATH	Ні	MFA та SSPR
Методи зовнішньої автентифікації (попередній перегляд)	Ні	MFA
Тимчасовий пропуск (TAP)	Так	MFA
Текст	Так	MFA та SSPR
Голосовий дзвінок	Ні	MFA та SSPR
QR-код (попередній перегляд)	Так	Ні
Пароль	Так	Ні

В сучасних реалізаціях Azure особливий акцент робиться на безпарольних методах – корпорація Microsoft рекомендує, по можливості, переходити на автентифікацію без пароля, використовуючи лише надійні фактори (наприклад, біометричний вхід через Windows Hello або ключі безпеки) [41]. Незважаючи на це, платформа зберігає підтримку й інших методів для сумісності та зручності користувачів. Важливою рекомендацією від Azure AD є налаштування для

користувачів декількох методів MFA – наприклад, зареєструвати в системі і мобільний додаток, і номер телефону – щоби забезпечити стійкість (resiliency) автентифікації на випадок недоступності одного з методів [41].

Налаштування політик MFA (Conditional Access). В Microsoft Azure MFA може бути ввімкнена для всіх користувачів відразу або вибірково, з використанням механізму умовного доступу (Conditional Access). Conditional Access – це функціонал Azure AD, який дозволяє створювати правила, що визначають вимоги до автентифікації в залежності від певних умов: приналежності користувача до групи, типу застосунку, з якого здійснюється вхід, розташування (IP-адреси), оцінки ризику входу тощо [43]. Практичний підхід впровадження MFA в Azure зазвичай такий:

- Адміністратор створює політику Conditional Access, що вимагає виконання MFA. Спочатку можна застосувати її до обмеженої групи користувачів (наприклад, IT-відділу або тестової групи) для перевірки роботи [43].
- Умови політики налаштовуються відповідно до потреб – наприклад, “вимагати MFA для всіх спроб входу користувачів ззовні корпоративної мережі” або “для всіх користувачів групи Адміністратори” [43]. Також можна задати виключення (наприклад, не вимагати MFA від сервісних облікових записів, які не підтримують інтерактивний вхід).
- Користувачі, на яких поширюється політика, повинні зареєструвати принаймні один другий фактор. Azure AD надає зручний портал реєстрації методів безпеки, де користувач додає, приміром, свій телефонний номер для SMS або прив’язує додаток Authenticator.
- Після ввімкнення політики, при наступному вході користувач (що підпадає під умови) після введення пароля отримує вимогу пройти додаткову перевірку – залежно від налаштованого методу, це може бути введення коду з додатка, підтвердження push-повідомлення або введення коду з SMS [41]. Лише за успішного виконання додаткового кроку вхід буде завершено.
- Адміністратор може контролювати стан MFA через відповідні звіти та панелі в Azure Portal. Зокрема, відстежувати, скільки користувачів

зареєстрували фактори, чи були блокування через невдалу MFA, які методи застосовуються найчастіше тощо.

Microsoft Azure також пропонує вбудовані “Security Defaults” – це стандартні налаштування безпеки, які зокрема включають вимогу MFA для всіх користувачів-адміністраторів та для привілейованих операцій. З 2020 року Security Defaults стали доступними для ввімкнення у всіх нових тенантах Azure AD, що спрощує базовий захист для організацій, які не мають ресурсу на гнучке налаштування політик. Цей крок пов’язаний з тим, що понад 99,9% скомпрометованих на Azure AD облікових записів не використовували MFA [40], тож Microsoft намагається максимально спростити увімкнення багатофакторного захисту.

Реєстрація та користувацький досвід. На боці користувача процес підключення MFA в Azure виглядає наступним чином: при першому вході після ввімкнення політики MFA система перенаправляє користувача на сторінку додаткової інформації безпеки. Користувачу пропонується обрати доступний метод – наприклад, «Mobile App» або «Phone». Якщо обрано Mobile App, користувач сканує QR-код у додатку Microsoft Authenticator, тим самим зв’язуючи додаток зі своїм обліковим записом (генерується секрет для TOTP і пуш-сповіщень). Далі користувач підтверджує працездатність – вводить код із додатка або підтверджує сповіщення. Якщо обрано Phone (SMS/voice), то вводиться номер, на який надходить код підтвердження. Після успішної реєстрації при кожному вході (згідно з політикою) користувач проходитиме двокрокову перевірку. В Azure передбачена можливість запам’ятати пристрій на 14 днів, щоб не вводити код при кожному вході з цього браузера. Загалом, досвід користувача у MFA від Azure можна вважати доволі зручним: інтеграція з мобільним додатком дає змогу підтверджувати вхід у один дотик, а у разі відсутності смартфона завжди є опція запасного коду.

Інтеграція MFA з додатками. Після ввімкнення MFA на рівні Azure AD, ця вимога автоматично поширюється на всі додатки, що використовують Azure AD для автентифікації (наприклад, Microsoft 365, Exchange Online, SharePoint,

Azure Portal тощо). Для власних корпоративних застосунків, інтегрованих через SSO з Azure AD, MFA теж буде застосовуватися без потреби додаткових налаштувань у самих додатках. Це є однією з переваг використання хмарного каталогу: достатньо раз налаштувати політику безпеки, і вона централізовано захищає всі пов'язані служби. На практиці, впровадження MFA в Azure часто починають з найбільш критичних облікових записів – адміністратори та користувачі з доступом до конфіденційних даних. Згідно зі статистикою Microsoft, увімкнення MFA для адміністраторів вже істотно підвищує загальний рівень захищеності середовища [40]. Далі поступово охоплюють і решту співробітників. Azure AD надає інструменти для кампанії реєстрації MFA – можна автоматично розіслати користувачам запрошення налаштувати Authenticator, відстежувати прогрес та надсилати нагадування. Це дозволяє організації впровадити MFA поетапно і з мінімальним хаосом.

Аспекти безпеки MFA в Azure. Впровадивши MFA, адміністратор має також подбати про деякі додаткові налаштування. По-перше, важливо вимкнути застарілі протоколи автентифікації, які можуть обходити MFA (так звані «legacy authentication», наприклад, протокол IMAP/POP3 без підтримки сучасних методів OAuth) [46]. Microsoft наголошує, що блокування застарілої автентифікації в комбінації з MFA значно скорочує поверхню атаки на хмарні акаунти [23]. По-друге, варто налаштувати політики збільшення стійкості: резервні адміністраторські облікові записи без MFA (для екстрених випадків), контроль оновлення номерів телефону або пристроїв користувачів, механізми відновлення доступу якщо MFA-фактор загублено. Azure AD передбачає особливу роль Authentication Policy Administrator, яка дозволяє керувати такими аспектами, не маючи повних прав адміністратора каталогу [43].

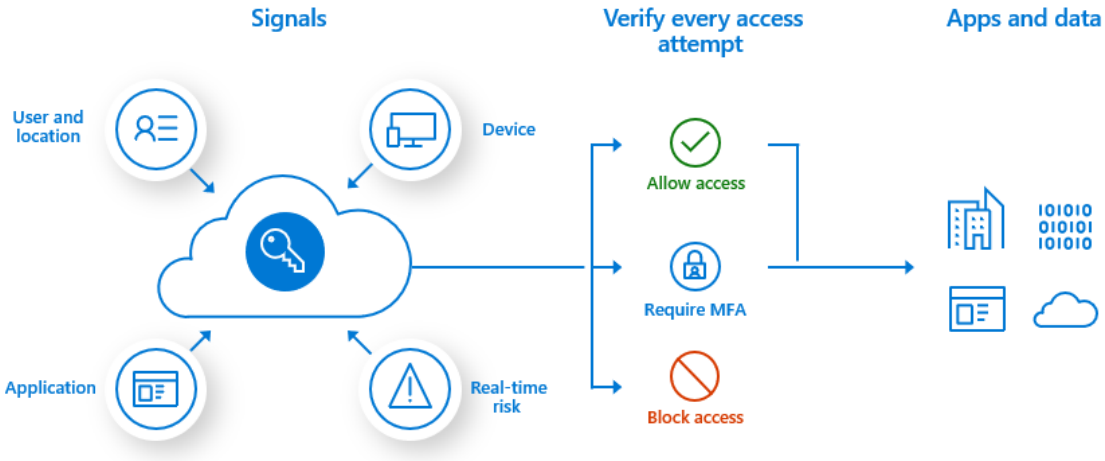

Рис. 3.3. Графік Політики умовного доступу [42]

Підсумовуючи, впровадження MFA на прикладі Microsoft Azure демонструє, що сучасні хмарні платформи надають усі необхідні засоби для посилення автентифікації. Адміністратор може досить гнучко налаштувати політики MFA під потреби організації, а користувачі отримують зручні та зрозумілі механізми підтвердження входу. Як свідчить досвід Google і Microsoft, примусове ввімкнення MFA навіть для частини користувачів дає відчутний ефект: після авто-підключення двофакторної перевірки для ~150 млн акаунтів Google, кількість компрометацій їхніх обліковок знизилася на 50% порівняно з користувачами без MFA [48]. Це підтверджує, що практична реалізація MFA є дієвим кроком до захисту персональних даних в системі.

Висновки до розділу 3.

У данному розділі дипломної роботи було здійснено комплексний аналіз вибору, впровадження та оцінки ефективності багатофакторної автентифікації (MFA) як засобу захисту персональних даних. Досліджено широкий спектр сучасних технологій MFA, розкрито їхні сильні та слабкі сторони з урахуванням безпекових характеристик, юзабіліті та відповідності нормативним вимогам.

На основі аналізу встановлено, що апаратні методи автентифікації (FIDO2, смарт-картки) забезпечують найвищий рівень захисту від фішингу та атак перехоплення, однак їх застосування є доцільним передусім у середовищах із підвищеними вимогами до безпеки. Натомість мобільні застосунки з push-підтвердженням і TOTP забезпечують добрий баланс між захищеністю та зручністю для користувачів, особливо у масових сервісах.

Практична реалізація MFA на прикладі Microsoft Azure підтвердила, що сучасні платформи дозволяють гнучко налаштовувати політики доступу, забезпечувати високу масштабованість рішення та інтеграцію з широким спектром сервісів. Упровадження Conditional Access, підтримка різних методів автентифікації, можливість безпарольного входу та централізований моніторинг дозволяють ефективно управляти доступом і знижувати ризики компрометації облікових записів.

ВИСНОВКИ

У межах виконаної кваліфікаційної роботи було здійснено комплексне дослідження MFA як ефективного інструменту захисту персональних даних в умовах зростаючих кіберзагроз. У роботі висвітлено історичні витоки та теоретичні засади автентифікації, класифіковано сучасні методи MFA, розглянуто стандарти та нормативні вимоги, що регламентують застосування технологій захисту даних, а також виявлено ключові проблеми та виклики, пов’язані з їх впровадженням.

На основі системного аналізу сучасних MFA-технологій — таких як OTP, апаратні токени, біометричні засоби, push-сповіщення та безпарольні методи (FIDO2, Windows Hello) — встановлено, що найбільшу стійкість до фішингових атак та перехоплення демонструють фішингостійкі рішення на основі апаратних ключів. Водночас, для широкого кола користувачів доцільно впроваджувати гнучкі сценарії автентифікації із можливістю обрати зручні методи підтвердження особи.

У роботі проаналізовано успішні приклади впровадження MFA в різних сферах: корпоративному секторі, банківській галузі, охороні здоров’я та публічному адмініструванні. Доведено, що впровадження MFA у поєднанні з умовним доступом (Conditional Access) і централізованим моніторингом забезпечує значне зниження ризику компрометації облікових записів.

Було проведено практичне моделювання впровадження MFA на базі хмарного сервісу Microsoft Azure, що засвідчило можливості платформи щодо масштабування, налаштування політик доступу, підтримки безпарольних методів і підвищення рівня захисту без погіршення користувацького досвіду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is the Evolution of Multi Factor Authentication. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-the-evolution-of-multi-factor-authentication.

2. The Evolution of Two-Factor Authentication and Its Role in Preventing Fraud. Bluefin. URL: https://www.bluefin.com/bluefin-news/evolution-two-factor-idrole-preventing-fraud.

3. Now you can use a key to get into your Google account. New Atlas. URL: https://newatlas.com/google-security-key/34348/.

4. Passwords have a long history – how much do you know…?. Cisco Newsroom. URL: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2022/m11/security-timeline.html.

5. History of Online Security, from CAPTCHA to Multi-Factor Authentication. Beyond Identity. URL: https://www.beyondidentity.com/resource/history-of-online-security-from-captcha-to-multi-factor-authentication.

6. What Is Multi-Factor Authentication? MFA Defined: Then, Now, and Tomorrow. HID Global. URL: https://blog.hidglobal.com/what-multi-factor-authentication-mfa-defined-then-now-and-tomorrow.

7. A review of the evolution of multi-factor authentication (MFA). TypingDNA Blog. URL: https://blog.typingdna.com/evolution-of-multi-factor-authentication/.

8. History of Authentication: From Zero to Hero. ASEE Cybersecurity Education Committee. URL: https://cybersecurity.asee.io/blog/history-of-authentication/.

9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the EU. URL: https://gdpr-info.eu/art-32-gdpr/.

10. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication & Lifecycle Management. Gaithersburg, MD: NIST, June 2017. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf.

11. NIST Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook. Gaithersburg, MD: NIST, 1995. URL: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter16.html.

12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. 30 p.

13. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. Geneva: ISO, 2022. URL: https://preteshbiswas.com/2023/01/09/iso-270012022-a-9-8-5-secure-authentication/.

14. ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and 27002 for privacy information management – Requirements and guidelines. Geneva: ISO, 2019. URL: https://www.isms.online/iso-27701/.

15. Mandatory & Discretionary Access Control: Which to Choose?. Ping Identity Blog. URL: https://www.pingidentity.com/en/resources/blog/post/access-control.html.

16. Data Breach Investigations Report 2024. Verizon Enterprise. URL: https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breachinvestigations-report.pdf.

17. Майкл Хеллер. Verizon DBIR 2017: Basic cybersecurity focus misplaced. TechTarget SearchSecurity. URL: https://www.techtarget.com/searchsecurity/news/450417928/Verizon-DBIR-2017-Basic-cybersecurity-focus-misplaced.

18. Stop the Pwnage: 81% of Hacking Incidents Used Stolen or Weak Passwords. Duo Security (Cisco). URL: https://duo.com/decipher/stop-the-pwnage-81-of-hacking-incidents-used-stolen-or-weak-passwords.

19. Alex Weinert. Your Pa$$word doesn't matter. Microsoft Entra Blog. URL: https://techcommunity.microsoft.com/blog/microsoft-entra-blog/your-paword-doesnt-matter/731984.

20. What Is Two-Factor Authentication (2FA)? Cisco. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-two-factor-authentication.html.

21. Arielle Miller. Unlocking the Future: The Power and Security of Biometric Authentication. AgileBlue. URL: https://agileblue.com/unlocking-the-future-the-power-and-security-of-biometric-authentication/.

22. Data Protected – Ukraine. Linklaters. URL: https://www.linklaters.com/en/insights/data-protected/data-protected---ukraine.

23. Kwee Nguyen. Basic cyber hygiene prevents 98% of attacks. Microsoft Security Blog. URL: https://techcommunity.microsoft.com/blog/microsoft-securityblog/basic-cyber-hygiene-prevents-98-of-attacks/3926856.

24. Nanda A., Jongkil J.J., Syed. W.A.S., Nosoushi. M., Doss R. Examining usable security features and user perceptions of Physical Authentication Devices. ScienceDirect. URL: https://www.sciencedirect.com/science/article/pii/S0167404823005746.

25. Уповноважений ВРУ з прав людини. Захист персональних даних – FAQ: Що таке персональні дані?. URL: https://ombudsman.gov.ua/zahistpersonalnih-danih-faq.

26. Mirren McDade. Multi-Factor Authentication (MFA) Statistics You Need To Know In 2025. ExpertSights. URL: https://expertinsights.com/user-auth/multi-factor-authentication-statistics.

27. ENISA Guidelines for Identity Protection and Phishing Resistant MFA. Thales Group CPL. URL: https://cpl.thalesgroup.com/sites/default/files/content/solution_briefs/field_document/2022-11/guidelines-for-identity-protection-and-phishing-resistant-sb.pdf.

28. User Authentication Specifications Overview. FIDO Alliance. URL: https://fidoalliance.org/specifications/.

29. Apple, Google, and Microsoft team up to support passwordless FIDO logins. The Verge. URL: https://www.theverge.com/2022/5/5/23057646/applegoogle-microsoft-passwordless-sign-in-fido.

30. Executive Order on Improving the Nation's Cybersecurity – Key Points. CISA. URL: https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity.

31. Leswing, K. None of Google's 85,000 employees have been phished since using security keys. Business Insider. URL: https://www.businessinsider.com/none-of-googles-employees-get-phished-because-of-yubikey-security-key-2018-7.

32. 2025 MFA Statistics & Trends to Know. JumpCloud. URL: https://jumpcloud.com/blog/multi-factor-authentication-statistics.

33. Strong customer authentication: Securing digital transactions. Okta. URL: https://www.okta.com/identity-101/strong-customer-authentication/.

34. PCI Security Standards Council (2022). Payment Card Industry Data Security Standard, Version 4.0. Onespan. URL: https://www.onespan.com/blog/new-mfa-requirements-in-PCI-DSS-4.0.

35. Burt J. HHS Proposes Mandating MFA, Data Encryption in HIPAA. MSSP Alert. URL: https://www.msspalert.com/news/hhs-proposes-mandating-mfa-data-encryption-in-hipaa.

36. Greig J. By end of 2021, Google plans to auto-enroll 150 million users in two-step verification and require 2 million YouTube creators to turn it on. ZDNET. URL: https://www.zdnet.com/article/by-end-of-2021-google-plans-to-auto-enroll-150-million-users-in-two-step-verification-and-require-2-million-youtube-creators-to-turn-it-on/.

37. Юлія Сабадишина. GitHub вимагатиме двофакторну автентифікацію від усіх розробників, які пишуть туди код. Dou. URL: https://dou.ua/lenta/news/github-and-f2/.

38. De Simone S. Multi-Factor Authentication Fatigue Key Factor in Uber Breach. InfoQ. URL: https://www.infoq.com/news/2022/09/Uber-breach-mfa-fatigue/.

39. Shalanda D. Young. Delivering a Digital-First Public Experience. BidenWhitehouse. URL: https://bidenwhitehouse.archives.gov/omb/management/ofcio/delivering-a-digital-first-public-experience/.

40. Security at your organization: Multifactor authentication statistics. Microsoft Partner Center. Partner Center. URL: https://learn.microsoft.com/en-us/partner-center/security/security-at-your-organization.

41. What authentication and verification methods are available in Microsoft Entra ID?. Microsoft Entra Docs. URL: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods.

42. Plan a Microsoft Entra multifactor authentication deployment. Microsoft Entra Docs. URL: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-getstarted.

43. Tutorial: Secure user sign-in events with Microsoft Entra multifactor authentication. Microsoft Entra Docs. URL: https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa.

44. Data Breach Investigations Report 2023. Verizon Enterprise. URL: https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf.

45. Honorof M. Only 10 Percent of Google Accounts Use 2FA. TomsGuide. URL: https://www.tomsguide.com/us/google-2fa-activate-now,news-26479.html.

46. Maynes M. One simple action you can take to prevent 99.9 percent of attacks on your accounts. Microsoft SecurityBlog. URL: https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/.

47. Consumer Behaviors and Perceived Security Across Devices. PYMNTS. URL: https://www.pymnts.com/wp-content/uploads/2023/04/PYMNTS-Consumer-Behaviors-and-Perceived-Security-Across-Devices-April-2023.pdf.

48. Guemmy K. Making you safer with 2SV. Google Blog. URL: https://blog.google/technology/safety-security/reducing-account-hijacking/.