ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система багатофакторної індентифікації та автентифікації користувача при роботі з інформацією з обмеженим доступом»

на здобуття освітнього ступеня магістра

зі спеціальності __125 - Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ 61
МАРТИНЕНКО Денис
Керівник: ІВАНЧЕНКО Ігор
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

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

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___125 - Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
___Мартиненку Денису Вікторовичу ___

1. Тема кваліфікаційної роботи: «Система багатофакторної індентифікації та автентифікації користувача при роботі з інформацією з обмеженим доступом».

Керівник кваліфікаційної роботи: ІВАНЧЕНКО Ігор, к.т.н., доцент.

Затверджена наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи: 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об’єкт інформаційної діяльності, інформація з обмеженим доступом, технічні канали витоку інформації, методи ідентифікації та автентифікації користувачів, сучасні механізми багатофакторної автентифікації.

4. Зміст розрахунково-пояснювальної записки:

4.1 Захист інформації на об’єктах інформаційної діяльності.

4.2 Огляд методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

4.3 Розробка та вдосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до ІзОД.

5. Перелік графічного матеріалу: презентаційний матеріал на слайдах.

6. Дата видачі завдання: 15.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Денис МАРТИНЕНКО

Керівник роботи _____ Ігор ІВАНЧЕНКО

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел і додатків. У роботі подано теоретичне обґрунтування, структурні схеми, таблиці порівняння методів автентифікації та презентаційний матеріал у додатках.

Метою кваліфікаційної роботи є удосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом на об’єкті інформаційної діяльності.

У роботі визначено порядок захисту інформації на об’єкті інформаційної діяльності, проаналізовано загрози інформаційній безпеці та технічні канали витоку інформації. Систематизовано методи ідентифікації та автентифікації користувачів, розглянуто парольні, токенові, одноразові, біометричні та криптографічні механізми автентифікації.

Розроблено модель багатофакторної автентифікації, що поєднує фактори знання, володіння, властивості користувача та контекст доступу. Запропоновано політики доступу до інформації з обмеженим доступом, модель оцінки захищеності механізмів MFA та рекомендації щодо практичного впровадження.

Апробація:

Д.В. Мартиненко, І.С. Іванченко, УДОСКОНАЛЕННЯ СИСТЕМИ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА ПРИ РОБОТІ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.56-57. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ІДЕНТИФІКАЦІЯ, АВТЕНТИФІКАЦІЯ, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, ПАРОЛЬ, ТОКЕН, БІОМЕТРІЯ, FIDO2.

ABSTRACT

The qualification thesis consists of an introduction, three chapters, general conclusions, a list of references and appendices. The work includes theoretical justification, structural diagrams, comparison tables and presentation material.

The aim of the qualification thesis is to improve mechanisms of multi-factor identification and authentication of users when working with restricted-access information at an object of information activity.

The thesis defines the procedure for protecting information at an object of information activity, analyzes information security threats and technical leakage channels. Methods of user identification and authentication are systematized, including password, token-based, one-time, biometric and cryptographic mechanisms.

A multi-factor authentication model combining knowledge, possession, inherence and contextual factors is developed. Access policies, a security assessment model and practical implementation recommendations are proposed.

Keywords: INFORMATION PROTECTION SYSTEM, OBJECT OF INFORMATION ACTIVITY, RESTRICTED ACCESS INFORMATION, IDENTIFICATION, AUTHENTICATION, MULTI-FACTOR AUTHENTICATION, PASSWORD, TOKEN, BIOMETRICS, FIDO2.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ОІД – Об’єкт інформаційної діяльності

ІзОД – Інформація з обмеженим доступом

ТЗІ – Технічний захист інформації

ТКВІ – Технічні канали витоку інформації

ІКМ – Інформаційно-комунікаційна мережа

ІС – Інформаційна система

НСД – Несанкціонований доступ

MFA – Multi-Factor Authentication

OTP – One-Time Password

TOTP – Time-Based One-Time Password

FIDO2 – Fast IDentity Online 2

RBAC – Role-Based Access Control

ABAC – Attribute-Based Access Control

CIA – Confidentiality, Integrity, Availability

ВСТУП

На сучасному етапі цифрової трансформації діяльність державних установ, підприємств та організацій тісно пов’язана з обробленням інформації з обмеженим доступом. Така інформація потребує не лише криптографічного захисту каналів передавання та фізичного захисту приміщень, а й надійного підтвердження особи користувача, який отримує доступ до інформаційних ресурсів.

Одним із найпоширеніших шляхів реалізації несанкціонованого доступу є компрометація облікового запису користувача. Пароль може бути підібраний, перехоплений, повторно використаний або добровільно розкритий під впливом соціальної інженерії. Тому використання лише парольної автентифікації не відповідає сучасним вимогам до захисту ІзОД.

Багатофакторна автентифікація дозволяє підвищити стійкість системи доступу за рахунок поєднання декількох незалежних доказів особи: того, що користувач знає, чим володіє, ким є, а також того, у якому контексті він звертається до ресурсу. Водночас надмірне ускладнення автентифікації може знижувати зручність роботи, тому важливим є ризик-орієнтований вибір факторів.

Метою роботи є удосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

Об’єктом дослідження є процес ідентифікації та автентифікації користувачів при доступі до інформаційних ресурсів, що містять інформацію з обмеженим доступом.

Предметом дослідження є механізми, моделі та політики багатофакторної ідентифікації й автентифікації користувачів.

Для досягнення поставленої мети необхідно: проаналізувати загрози інформаційній безпеці та канали витоку інформації; дослідити сучасні технології ідентифікації й автентифікації; розробити архітектуру MFA; сформувати модель оцінки захищеності та практичні рекомендації щодо застосування MFA для доступу до ІзОД.

РОЗДІЛ 1
ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1 Аналіз інформації з обмеженим доступом та режимів її захисту

Інформація з обмеженим доступом є сукупністю відомостей, доступ до яких обмежується відповідно до законодавства, внутрішніх політик власника інформації або умов договору. На об'єкті інформаційної діяльності така інформація може перебувати в паперовій, електронній, аудіовізуальній або комбінованій формі. Вимоги до її захисту визначаються цінністю інформаційного активу, можливими наслідками розголошення та роллю користувача у виробничому процесі.

З практичної точки зору режим захисту ІзОД має включати класифікацію інформаційних ресурсів, призначення відповідальних осіб, визначення правил доступу, технічне розмежування повноважень, криптографічний захист каналів передавання, журналювання подій та регулярний аудит. Без належної ідентифікації користувача всі інші механізми контролю втрачають доказовість, оскільки неможливо встановити, хто саме виконував дію.

У межах цієї роботи під доступом до ІзОД розуміється не лише читання файлів або перегляд сторінок інформаційної системи, а й виконання операцій створення, модифікації, копіювання, експорту, друкування, видалення та передавання даних. Кожна така операція повинна мати власний рівень критичності і може вимагати різної сили автентифікації.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об'єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися

ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов'язків працівника.

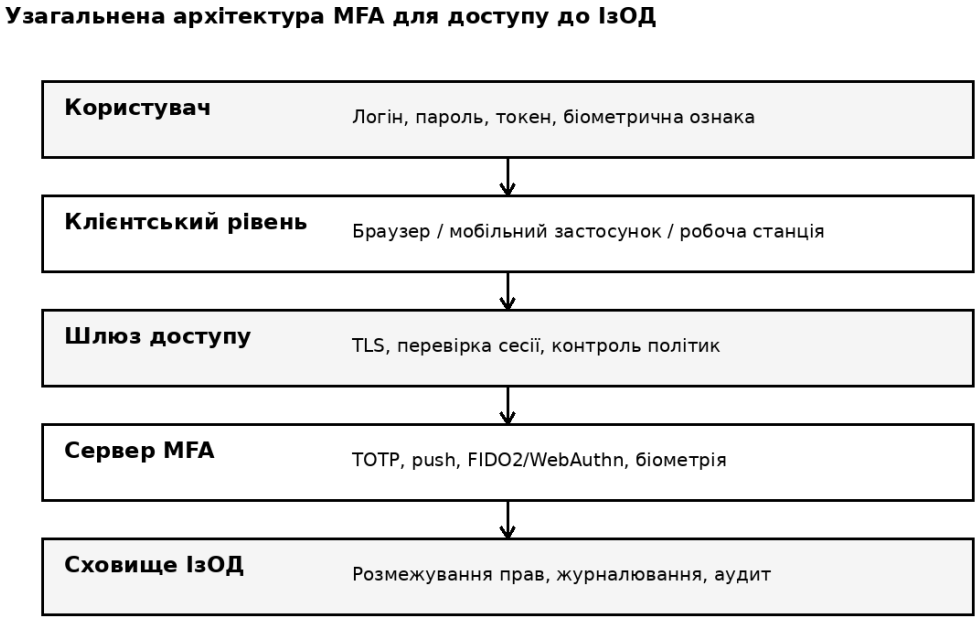

Рис. 1. 1.1 Аналіз інформації з обмеженим доступом та режимів її захисту

1.2 Загрози інформаційній безпеці на об'єкті інформаційної діяльності

Загрози інформаційній безпеці ОІД формуються як зовнішніми, так і внутрішніми факторами. Зовнішній порушник може застосовувати фішинг, підбір паролів, експлуатацію вразливостей веб-застосунків, перехоплення трафіку або шкідливе програмне забезпечення. Внутрішній порушник може мати легітимний доступ до частини ресурсів, але використовувати його з перевищенням повноважень.

Особливу небезпеку для систем автентифікації становлять атаки на облікові дані. До них належать credential stuffing, brute force, password spraying, повторне використання паролів, перехоплення одноразових кодів, підміна веб-сторінок входу та атаки типу "людина посередині". Наявність другого незалежного фактора значно ускладнює реалізацію таких атак, але не усуває потребу в моніторингу ризикової поведінки.

Людський фактор залишається одним із ключових джерел ризику. Користувач може встановити простий пароль, зберегти його у відкритому вигляді, підтвердити push-запит без перевірки контексту або передати свій токен іншій особі. Тому MFA повинна супроводжуватися навчанням користувачів, політикою безпечного поводження з факторами та процедурою реагування на втрату пристрою.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об'єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу.

Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов'язків працівника.

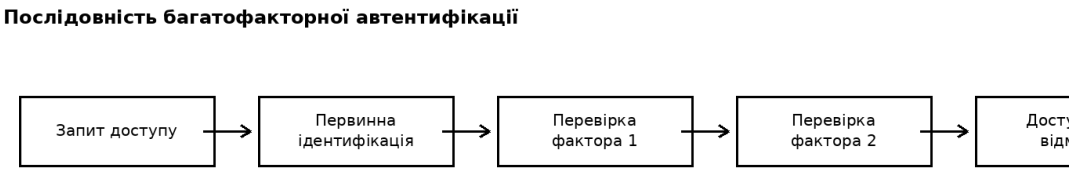

Рис. 2. 1.2 Загрози інформаційній безпеці на об'єкті інформаційної діяльності

1.3 Аналіз технічних каналів витоку інформації

Технічні канали витоку інформації виникають унаслідок фізичних процесів, що супроводжують оброблення, передавання або відображення інформації. До основних груп належать акустичні, віброакустичні, електромагнітні, електричні, оптичні та матеріальні канали. Хоча MFA безпосередньо не усуває такі канали, вона обмежує можливість використання скомпрометованого доступу для отримання інформації з інформаційних систем.

Структура технічного каналу витоку включає джерело небезпечного сигналу, середовище поширення та засіб перехоплення. На ОІД джерелом можуть бути робочі станції, сервери, засоби відображення, кабельні лінії,

мережеве обладнання або користувач, який озвучує чи відображає конфіденційну інформацію. Тому система захисту має поєднувати технічні засоби екранування з контролем доступу.

У контексті автентифікації важливим є канал витоку облікових даних. Пароль, OTP-код, QR-код для прив'язки токена або резервний код можуть бути перехоплені візуально, технічно або через шкідливе ПЗ. Це обґрунтовує необхідність переходу до криптографічних механізмів, де секрет не передається мережею у вигляді коду, придатного для повторного використання.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об'єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов'язків працівника.

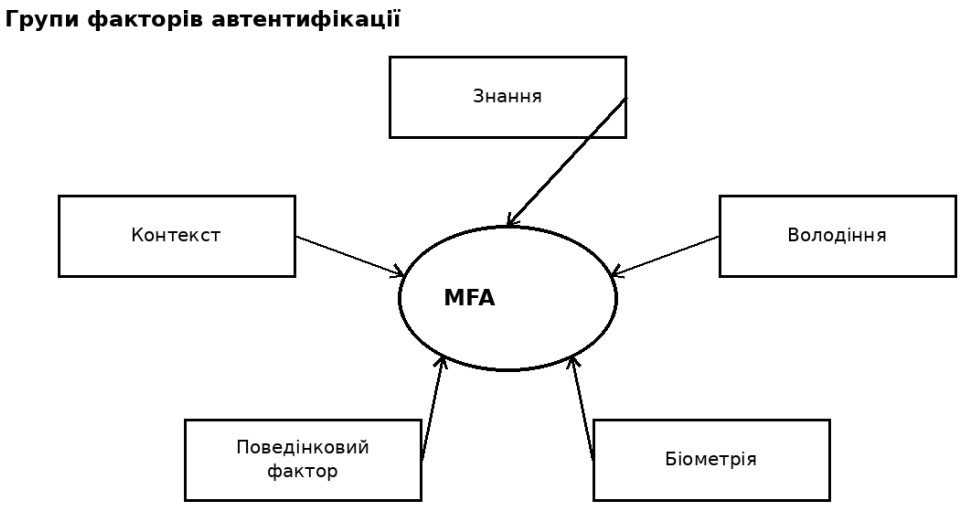

Рис. 3. 1.3 Аналіз технічних каналів витоку інформації

1.4 Організаційно-технічні вимоги до захисту ІзОД

Організаційно-технічні вимоги до захисту ІзОД мають встановлювати мінімально необхідні повноваження користувачів, правила реєстрації та видалення облікових записів, порядок призначення ролей, регламент зміни паролів і порядок відновлення доступу. Особливо важливо, щоб процедура відновлення доступу не була слабшим місцем, ніж основний механізм автентифікації.

Технічні вимоги до MFA повинні передбачати захищене зберігання секретів, шифрування каналів передавання, прив’язку фактора до конкретного користувача, контроль життєвого циклу токенів, журналювання подій, виявлення аномалій та блокування доступу при перевищенні порогу ризику. Для критичних операцій доцільно застосовувати step-up автентифікацію.

Ефективність MFA визначається не тільки кількістю факторів, але й їх незалежністю. Наприклад, пароль і відповідь на контрольне питання належать до одного класу “знання” і не забезпечують істинної багатофакторності. Надійніша

схема має поєднувати пароль з апаратним ключем, TOTP-токеном, смарт-картою або біометричним підтвердженням.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

Рис. 4. 1.4 Організаційно-технічні вимоги до захисту ІзОД

Висновки до розділу

У розділі систематизовано основні положення, що визначають порядок побудови захисту інформації та автентифікації користувачів. Показано, що ефективний доступ до ІзОД має ґрунтуватися на поєднанні організаційних регламентів, технічних засобів, криптографічних механізмів, журналювання та ризик-орієнтованого вибору факторів автентифікації.

РОЗДІЛ 2
ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

2.1 Процес ідентифікації, автентифікації та авторизації

Ідентифікація полягає у заявленні суб'єктом свого ідентифікатора, наприклад імені користувача, номера облікового запису або сертифіката. Автентифікація підтверджує, що суб'єкт дійсно володіє правом використовувати цей ідентифікатор. Авторизація визначає, які дії дозволено виконувати після успішної автентифікації.

Ці процеси часто об'єднують у модель AAA: authentication, authorization, accounting. Останній елемент - облік або підзвітність - забезпечує реєстрацію подій доступу, що є важливою умовою розслідування інцидентів. Для роботи з ІзОД журналювання повинно бути незмінним, захищеним від редагування та пов'язаним із перевіреним ідентифікатором користувача.

У системах доступу до ІзОД автентифікація має виконуватися до надання доступу до ресурсу, а також повторно під час виконання критичних операцій. Повторне підтвердження особи доцільне при зміні контексту: новий пристрій, нестандартна IP-адреса, нічний час, підвищення привілеїв або спроба експорту значного обсягу даних.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об'єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

Матриця рішень для вибору фактора автентифікації

Ризик	Фактор 1	Фактор 2	Додатковий контроль
Низький	Пароль	TOTP	Журналювання
Середній	Пароль	Push	Контроль пристрою
Високий	Пароль	FIDO2/біометрія	Адаптивна перевірка
Критичний	FIDO2	Біометрія	Дозвіл адміністратора

Рис. 5. 2.1 Процес ідентифікації, автентифікації та авторизації

2.2 Парольні та одноразові механізми автентифікації

Паролі залишаються найпоширенішим засобом автентифікації через простоту реалізації та низьку вартість. Водночас пароль є найбільш уразливим фактором, оскільки залежить від поведінки користувача. Основними вимогами до парольної політики є достатня довжина, відсутність типових словникових

конструкцій, захист від повторного використання та обмеження кількості невдалих спроб входу.

Одноразові паролі усувають ризик повторного використання перехопленого коду, але не є універсальним вирішенням проблеми. SMS OTP залежить від оператора мобільного зв'язку та вразливий до SIM-swap. TOTP базується на спільному секреті та часовому інтервалі, тому потребує захисту секрету під час реєстрації та резервного відновлення.

Для підвищення стійкості одноразових паролів слід обмежувати час дії коду, кількість спроб введення, прив'язувати код до конкретної операції та використовувати захищений канал відображення. У критичних системах OTP доцільно розглядати як проміжний рівень захисту, а не як найсильніший механізм MFA.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об'єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і

забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

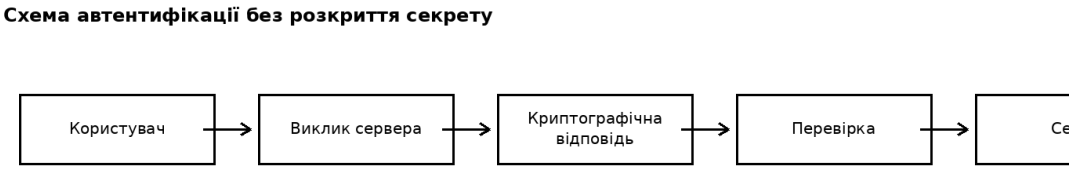

Рис. 6. 2.2 Парольні та одноразові механізми автентифікації

2.3 Токени, смарт-карти та криптографічні протоколи

Фактор володіння реалізується через апаратні або програмні засоби, які користувач має при собі. До них належать USB-токени, смарт-карти, мобільні застосунки, апаратні OTP-генератори та FIDO2-ключі. Основною перевагою є те, що зловмисник повинен не лише знати пароль, а й отримати контроль над фізичним або логічним носієм другого фактора.

Сучасним напрямом є використання FIDO2/WebAuthn, де автентифікація базується на асиметричній криптографії. Під час реєстрації створюється пара ключів, відкритий ключ передається серверу, а приватний залишається на пристрої користувача. Під час входу користувач підписує виклик сервера, не розкриваючи секрет.

Криптографічні протоколи мають перевагу над кодовими схемами, оскільки протидіють повторному використанню перехоплених даних. Водночас вони потребують захисту пристрою, на якому зберігається приватний ключ, правильного управління реєстрацією ключів та процедури відкликання у разі втрати пристрою.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

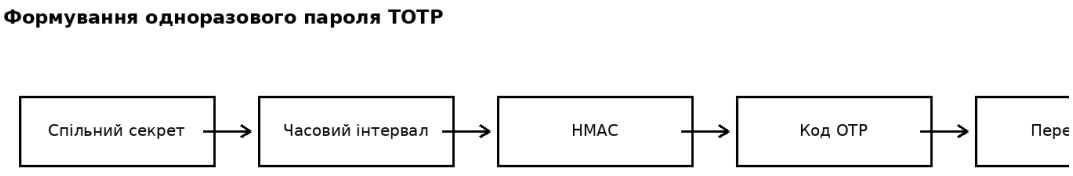

Рис. 7. 2.3 Токени, смарт-карти та криптографічні протоколи

2.4 Біометричні та поведінкові методи автентифікації

Біометрична автентифікація використовує фізіологічні або поведінкові характеристики користувача: відбиток пальця, геометрію обличчя, райдужну оболонку ока, голос, динаміку підпису чи особливості набору тексту. Її перевага полягає у зручності та складності передачі біометричного фактора іншій особі.

Біометрія має специфічні ризики. На відміну від пароля, біометричну ознаку неможливо повністю змінити після компрометації. Тому в системах доступу до ІзОД доцільно зберігати не первинні зображення, а захищені шаблони, застосовувати перевірку живості та комбінувати біометрію з іншим фактором.

Поведінкові фактори можуть використовуватися як додатковий контекст. Наприклад, система аналізує швидкість введення тексту, типову геолокацію, пристрій, час активності або шаблони взаємодії. Такий підхід добре підходить для ризик-орієнтованої автентифікації, але не повинен бути єдиним фактором у критичних сценаріях.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

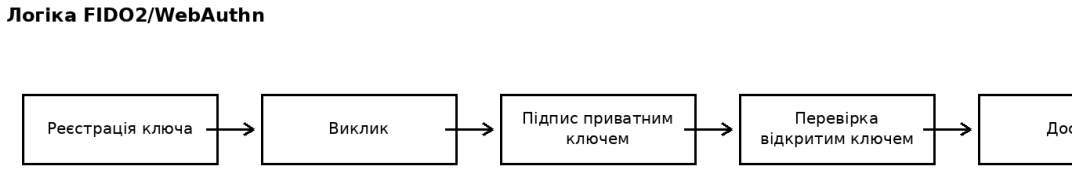

Рис. 8. 2.4 Біометричні та поведінкові методи автентифікації

2.5 Вимоги до організації процесів автентифікації

Організація процесів автентифікації повинна відповідати принципу мінімальних привілеїв, розмежуванню ролей і політиці життєвого циклу облікового запису. Кожен користувач має отримувати доступ лише до тих ресурсів, які необхідні для виконання службових обов’язків. Надання, зміна та відкликання доступу мають бути документованими.

Важливо забезпечити баланс між безпекою та зручністю. Надто складна схема входу може спонукати користувачів шукати обхідні шляхи: записувати резервні коди, передавати токени колегам або підтверджувати запити без перевірки. Тому MFA має застосовуватися диференційовано: сильніше для ІзОД і критичних операцій, простіше для низькоризикових дій.

Процедури відновлення доступу, заміни токена, реєстрації нового пристрою та скидання пароля мають бути захищені не слабше за основну автентифікацію. Інакше зловмисник може обійти MFA через службу підтримки або компрометацію резервного каналу.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

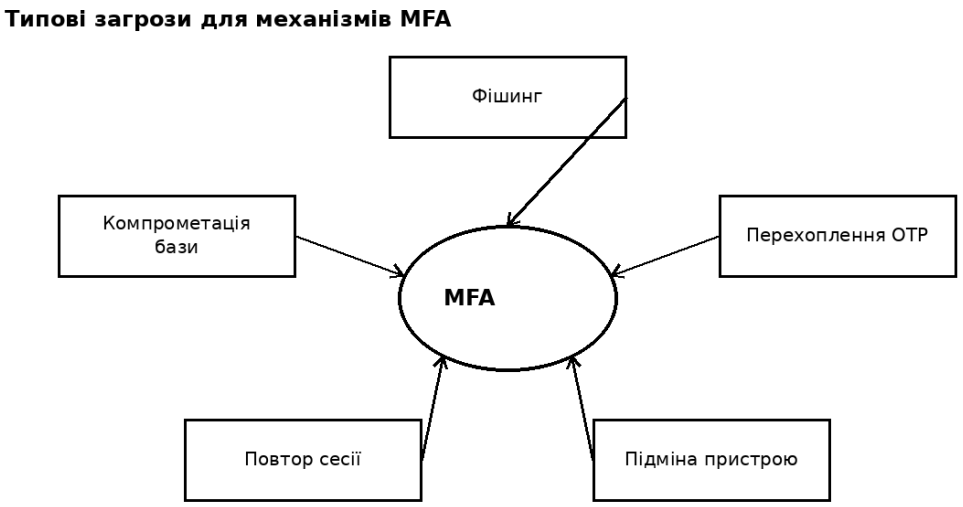

Рис. 9. 2.5 Вимоги до організації процесів автентифікації

Таблиця 10. Узагальнення характеристик для підрозділу

Параметр	**Зміст**	**Ризик**	**Контроль**
Фактор	Незалежність від пароля	Середній	MFA
Сесія	Обмежений строк дії	Високий	Повторна перевірка
Журнал	Фіксація подій	Середній	Аудит

Висновки до розділу

У розділі систематизовано основні положення, що визначають порядок побудови захисту інформації та автентифікації користувачів. Показано, що ефективний доступ до ІзОД має ґрунтуватися на поєднанні організаційних регламентів, технічних засобів, криптографічних механізмів, журналювання та ризик-орієнтованого вибору факторів автентифікації.

РОЗДІЛ 3
РОЗРОБКА МЕХАНІЗМІВ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

3.1 Вимоги до механізму MFA для доступу до ІзОД

Механізм MFA для доступу до ІзОД має забезпечувати достатню криптографічну стійкість, незалежність факторів, контроль життєвого циклу облікових записів, можливість аудиту та адаптацію до рівня ризику. Він повинен підтримувати інтеграцію з каталогом користувачів, системою керування ролями та журналом подій безпеки.

Базовими функціональними вимогами є реєстрація користувачів, прив’язка другого фактора, перевірка фактора при вході, step-up автентифікація для критичних дій, блокування при підозрілих подіях, керування резервними кодами та відкликання факторів. Нефункціональні вимоги включають продуктивність, масштабованість, відмовостійкість і зручність використання.

Для системи, що обробляє ІзОД, рекомендовано мінімізувати використання SMS OTP і надавати перевагу TOTP, апаратним токенам, смарт-картам або FIDO2. У разі застосування біометрії необхідно забезпечити локальну перевірку шаблону або захищене зберігання біометричних даних.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації

користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов'язків працівника.

Матриця рішень для вибору фактора автентифікації

Ризик	Фактор 1	Фактор 2	Додатковий контроль
Низький	Пароль	TOTP	Журналювання
Середній	Пароль	Push	Контроль пристрою
Високий	Пароль	FIDO2/біометрія	Адаптивна перевірка
Критичний	FIDO2	Біометрія	Дозвіл адміністратора

Рис. 11. 3.1 Вимоги до механізму MFA для доступу до ІзОД

Таблиця 12. Узагальнення характеристик для підрозділу

Параметр	**Зміст**	**Ризик**	**Контроль**
Фактор	Незалежність від пароля	Середній	MFA
Сесія	Обмежений строк дії	Високий	Повторна перевірка
Журнал	Фіксація подій	Середній	Аудит

3.2 Архітектура системи багатофакторної автентифікації

Запропонована архітектура складається з клієнтського рівня, шлюзу доступу, сервера MFA, сервера політик, каталогу користувачів, сховища журналів і захищеного ресурсу з ІзОД. Клієнт ініціює запит доступу, шлюз перевіряє сесію, сервер MFA підтверджує фактори, а сервер політик приймає рішення на основі ролі, ресурсу та контексту.

Алгоритм роботи передбачає послідовні етапи: введення ідентифікатора, перевірка основного фактора, оцінка контекстного ризику, вибір другого фактора, перевірка другого фактора, прийняття рішення, створення сесії з обмеженим строком дії та запис події до журналу. При підвищеному ризику система запитує додаткове підтвердження або блокує доступ.

Для підвищення стійкості сесія користувача повинна мати обмежений строк дії, бути прив’язаною до пристрою і не повинна зберігати секрети у відкритому вигляді. При зміні IP-адреси, браузера, пристрою або поведінкового профілю система має виконувати повторну перевірку.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість

централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов'язків працівника.

3.3 Модель оцінки захищеності механізмів MFA

Оцінка захищеності механізму MFA може бути подана як інтегральний показник, що враховує криптографічну стійкість факторів, незалежність факторів, ризик перехоплення, ризик соціальної інженерії, складність відновлення доступу та зручність для користувача. Такий підхід дозволяє порівнювати різні схеми автентифікації.

Для умовного оцінювання вводиться шкала від 0 до 1, де 1 відповідає найвищому рівню захисту. Схема "пароль + SMS OTP" отримує нижчий бал через ризики перехоплення SMS та SIM-swap. Схема "пароль + TOTP" є стійкішою, але залежить від захисту спільного секрету. Схема "пароль + FIDO2" має високий рівень захисту, оскільки приватний ключ не передається мережею.

Інтегральний показник не повинен розглядатися як абсолютна гарантія безпеки. Він є інструментом прийняття рішень для вибору архітектури доступу. Остаточна оцінка має враховувати загальний ландшафт загроз, тип ІзОД, можливості порушника та вимоги до зручності експлуатації.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об'єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації

користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов'язків працівника.

Таблиця 13. Узагальнення характеристик для підрозділу

Параметр	**Зміст**	**Ризик**	**Контроль**
Фактор	Незалежність від пароля	Середній	MFA
Сесія	Обмежений строк дії	Високий	Повторна перевірка
Журнал	Фіксація подій	Середній	Аудит

3.4 Політики доступу та алгоритм прийняття рішення

Політика доступу визначає, який набір факторів необхідний для конкретного ресурсу або операції. Для читання загальних внутрішніх документів може бути достатньо парольної автентифікації з TOTP. Для доступу до ІзОД доцільно застосовувати пароль і FIDO2 або пароль і біометричний фактор. Для адміністративних операцій необхідне посилене підтвердження та додатковий контроль.

Алгоритм прийняття рішення має враховувати роль користувача, рівень критичності ресурсу, тип операції, пристрій, місцезнаходження, час, історію входів та результати попередніх перевірок. Якщо сукупний ризик нижче порогу, доступ надається. Якщо ризик середній, виконується step-up автентифікація.

Якщо ризик високий, доступ блокується і формується повідомлення адміністратору.

Для запобігання втомі від push-підтверджень необхідно відображати користувачу контекст запиту: ресурс, дію, час, IP-адресу, пристрій і географічний регіон. Користувач повинен мати можливість позначити запит як підозрілий, що автоматично ініціює блокування сесії та зміну облікових параметрів.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу. Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

Таблиця 14. Узагальнення характеристик для підрозділу

Параметр	**Зміст**	**Ризик**	**Контроль**
Фактор	Незалежність від пароля	Середній	MFA

Сесія	Обмежений строк дії	Високий	Повторна перевірка
Журнал	Фіксація подій	Середній	Аудит

3.5 Практичні рекомендації щодо впровадження

Впровадження MFA слід виконувати поетапно. На першому етапі проводиться інвентаризація інформаційних ресурсів і класифікація ІзОД. На другому етапі визначаються ролі користувачів і рівні ризику операцій. На третьому етапі обираються фактори автентифікації, готуються політики доступу та проводиться пілотне впровадження.

Після пілотного впровадження необхідно оцінити кількість відмов, час входу, кількість звернень до служби підтримки, частоту помилкових спрацювань і рівень прийняття користувачами. За результатами оцінки політики коригуються. Лише після цього MFA масштабується на всі ресурси, що містять ІзОД.

Обов’язковими є резервні процедури: втрата токена, зміна телефону, компрометація пароля, підозра на фішинг, відпустка або звільнення працівника. Всі такі події мають фіксуватися в журналі безпеки, а доступ має переглядатися регулярно.

Додатково слід враховувати, що практична реалізація розглянутих положень залежить від організаційної структури об’єкта, складу користувачів, рівня критичності інформаційних ресурсів та доступності технічної інфраструктури. Тому рішення з автентифікації не повинні впроваджуватися ізольовано, а мають бути узгоджені з політикою інформаційної безпеки, моделлю загроз, планом реагування на інциденти та процедурою аудиту.

Для забезпечення керованості системи доцільно формувати формалізовані регламенти, у яких визначаються відповідальні особи, порядок реєстрації користувачів, правила використання факторів, процедура втрати або заміни автентифікаційного засобу, а також порядок тимчасового блокування доступу.

Наявність таких регламентів підвищує відтворюваність процесів і зменшує залежність безпеки від випадкових рішень адміністратора.

З позиції технічного проектування важливо передбачити масштабованість, сумісність із наявними інформаційними системами, можливість централізованого журналювання та інтеграцію з каталогами користувачів. Це дозволяє реалізувати єдину політику доступу для різних класів ресурсів і забезпечити оперативну зміну прав при зміні функціональних обов’язків працівника.

Висновки до розділу

У розділі систематизовано основні положення, що визначають порядок побудови захисту інформації та автентифікації користувачів. Показано, що ефективний доступ до ІзОД має ґрунтуватися на поєднанні організаційних регламентів, технічних засобів, криптографічних механізмів, журналювання та ризик-орієнтованого вибору факторів автентифікації.

ВИСНОВКИ

1. У кваліфікаційній роботі вирішено актуальне завдання удосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при роботі з інформацією з обмеженим доступом. Показано, що парольна автентифікація не забезпечує достатнього рівня стійкості до сучасних загроз, а тому має доповнюватися незалежними факторами підтвердження особи.

2. У першому розділі проаналізовано особливості захисту інформації на об’єктах інформаційної діяльності, визначено основні загрози інформаційній безпеці та технічні канали витоку інформації. Обґрунтовано, що контроль доступу до ІзОД є невід’ємним елементом комплексної системи захисту інформації.

3. У другому розділі систематизовано технології ідентифікації та автентифікації користувачів. Розглянуто парольні механізми, одноразові коди, токени, смарт-карти, біометричні та криптографічні методи. Визначено переваги FIDO2/WebAuthn як сучасного підходу, що не передбачає передавання секрету мережею.

4. У третьому розділі розроблено архітектуру системи MFA для доступу до ІзОД, модель оцінки захищеності механізмів автентифікації, політики доступу та алгоритм прийняття рішення. Запропонована система враховує роль користувача, критичність ресурсу, тип операції та контекст доступу.

5. Практичне значення результатів полягає у можливості використання запропонованої архітектури та політик під час проектування або модернізації систем доступу на об’єктах інформаційної діяльності, де обробляється інформація з обмеженим доступом. Подальші дослідження доцільно спрямувати на експериментальну перевірку моделі в реальному середовищі та інтеграцію з SIEM/SOAR-системами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію».

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах».

3. Закон України «Про захист персональних даних».

4. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист приватності. Системи керування інформаційною безпекою.

5. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.

6. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

7. ISO/IEC 9798-1:2010. Information technology — Security techniques — Entity authentication — Part 1: General.

8. ISO/IEC 9798-2:2019. Entity authentication mechanisms using symmetric encipherment algorithms.

9. ISO/IEC 9798-3:2019. Entity authentication mechanisms using digital signature techniques.

10. ISO/IEC 9798-4:1999. Entity authentication mechanisms using a cryptographic check function.

11. ISO/IEC 9798-5:2009. Entity authentication mechanisms using zero-knowledge techniques.

12. NIST SP 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management.

13. NIST SP 800-207. Zero Trust Architecture.

14. NIST Cybersecurity Framework 2.0.

15. FIDO Alliance. FIDO2: WebAuthn and CTAP Specifications.

16. W3C. Web Authentication: An API for accessing Public Key Credentials.

17. IETF RFC 6238. TOTP: Time-Based One-Time Password Algorithm.

18. IETF RFC 4226. HOTP: An HMAC-Based One-Time Password Algorithm.

19. IETF RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3.

20. OWASP. Authentication Cheat Sheet.

21. OWASP. Multifactor Authentication Cheat Sheet.

22. ENISA. Digital Identity and Trust Services Guidelines.

23. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems.

24. Bishop M. Computer Security: Art and Science.

25. Stallings W. Cryptography and Network Security: Principles and Practice.

26. Конахович Г.Ф., Корченко О.Г. Захист інформації в телекомунікаційних системах.

27. Хорошко В.О., Чекатков А.А. Методи та засоби захисту інформації.

28. Ленков С.В., Перегудов Д.А., Хорошко В.О. Методи і засоби захисту інформації.

29. Поповський В.В. Основи криптографічного захисту інформації.

30. Туровський О.Л. Технічні системи захисту інформації.

31. Методичні рекомендації з організації контролю доступу до інформаційних ресурсів об’єкта інформаційної діяльності.

ДОДАТКИ

Система багатофакторної ідентифікації та автентифікації користувача при роботі з інформацією з обмеженим доступом

- Магістерська робота: Денис МАРТИНЕНКО
- Спеціальність 125 «Кібербезпека та захист інформації»
- Керівник: Іванченко Ігор, к.т.н., доцент
- Фокус: MFA, ІзОД, ОІД, контроль доступу

Актуальність теми

- Інформація з обмеженим доступом потребує підтвердження особи користувача з високим рівнем довіри.
- Парольна автентифікація є недостатньою через фішинг, повторне використання паролів і витоки баз даних.
- MFA поєднує незалежні фактори і зменшує ймовірність несанкціонованого доступу.
- Захист має враховувати технічні канали витоку, людський фактор і ризик компрометації сесії.

Мета, об’єкт і предмет

- Мета: удосконалення механізмів MFA при роботі з ІзОД.
- Об’єкт: процес ідентифікації та автентифікації користувачів в ІКМ.
- Предмет: моделі, методи та засоби багатофакторної автентифікації.
- Практична спрямованість: побудова політики доступу до ресурсів ОІД.

Завдання роботи

- Проаналізувати загрози та канали витоку інформації на ОІД.
- Дослідити сучасні методи ідентифікації та автентифікації.
- Сформувати вимоги до MFA для доступу до ІзОД.
- Розробити модель оцінки захищеності та практичну архітектуру MFA.

Структура роботи

- Розділ 1: захист інформації на об’єктах інформаційної діяльності.
- Розділ 2: технології ідентифікації та автентифікації користувачів.
- Розділ 3: розробка механізмів багатофакторної автентифікації.
- Додатки містять презентаційний матеріал.

Інформація з обмеженим доступом

- ІзОД включає конфіденційну, службову та іншу інформацію, доступ до якої обмежується власником або законом.
- Для ІзОД критичними є конфіденційність, цілісність, доступність та підзвітність дій користувача.
- Контроль доступу має бути пов’язаний із роллю, контекстом і рівнем ризику операції.

Загрози несанкціонованого доступу

- Основні загрози: фішинг, підбір паролів, крадіжка токенів, повтор сесій, соціальна інженерія.
- Компрометація одного фактора не повинна автоматично призводити до доступу.
- Журналювання і аудит мають фіксувати успішні та неуспішні спроби доступу.

Канали витоку інформації

- На ОІД можливі акустичні, електромагнітні, електричні, оптичні та матеріальні канали витоку.
- MFA не замінює ТЗІ, але зменшує ризик доступу до інформаційних ресурсів через облікові записи.
- Захист доступу має поєднувати організаційні, технічні та криптографічні заходи.

Класифікація факторів MFA

- Фактор знання: пароль, PIN, контрольна фраза.
- Фактор володіння: апаратний токен, смартфон, смарт-карта, FIDO2-ключ.
- Фактор властивості: біометричні ознаки користувача.
- Контекст: пристрій, геолокація, час, поведінковий профіль.

Паролі та одноразові коди

- Пароль залишається базовим фактором, але є найуразливішим до фішингу і повторного використання.
- OTP/TOTP підвищує безпеку, але потребує захисту спільного секрету.
- SMS OTP менш стійкий через ризики SIM-swap та перехоплення повідомлень.

Біометрія та FIDO2

- Біометрія підвищує зручність, але потребує захищеного зберігання шаблонів.
- FIDO2/WebAuthn забезпечує автентифікацію на основі асиметричної криптографії.
- Приватний ключ не передається мережею, що знижує ризик перехоплення секрету.

Модель оцінки захищеності

- Оцінювання враховує стійкість факторів, незалежність факторів, ризик перехоплення та зручність використання.
- Для критичних операцій необхідний вищий рівень довіри та додаткові перевірки.
- Ризик-орієнтована MFA дає змогу підсилювати автентифікацію лише у небезпечних сценаріях.

Запропонована архітектура

- Користувач проходить первинну ідентифікацію, а потім підтверджує доступ другим незалежним фактором.
- Сервер MFA перевіряє фактори, контекст доступу та політику ролей.
- Рішення інтегрується з журналюванням, аудитом і системою керування доступом.

Політика доступу

- Для низькоризикових дій достатньо пароль + TOTP.
- Для доступу до ІзОД рекомендовано пароль + FIDO2 або пароль + біометрія.
- Для адміністративних операцій застосовується MFA, обмеження сесії та обов’язковий аудит.

Практичне значення

- Запропонований підхід може застосовуватися для ОІД, де обробляється ІзОД.
- MFA зменшує ризик несанкціонованого доступу навіть за компрометації одного фактора.
- Модель дозволяє обирати фактори відповідно до рівня ризику і критичності ресурсу.

Висновки

- Проаналізовано загрози, канали витоку та вимоги до захисту ІзОД.
- Систематизовано методи ідентифікації та автентифікації користувачів.
- Розроблено архітектуру та модель застосування MFA для ОІД.
- Мету роботи досягнуто: механізми MFA обґрунтовано і практично структуровано.