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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби автентифікації користувачів в інформаційно-комунікаційних системах»

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

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

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Андрій СЕРЕДІН
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
СЕРЕДІН Андрій
(прізвище, ім'я)

Керівник д.т.н, професор Галина ГАЙДУР
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Середін Андрій Валерійович
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
Засоби автентифікації користувачів в інформаційно-комунікаційних системах

керівник кваліфікаційної роботи д. т. н., професор, Гайдур Галина
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «_» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2025 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення ESET;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми автентифікації користувачів в інформаційно-комунікаційний системі.
2. Засоби автентифікації в інформаційно-комунікаційний системі, одноразовий код (OTP) та біометричний фактор у вигляди відбитка пальця на базі архітектури ESET

3. Рекомендації що до впровадження засобів автентифікації користувачів в інформаційно-комунікаційний системі

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок організації.	03.03.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз проблеми автентифікації користувачів в інформаційно-комунікаційний системі.		
4.	Засоби автентифікації в інформаційно-комунікаційний системі, одноразовий код (OTP) та біометричний фактор у вигляди відбитка пальця на базі архітектури ESET		
5.	Рекомендації що до впровадження засобів автентифікації користувачів в інформаційно-комунікаційний системі		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Андрій СЕРЕДІН
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

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

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

Направляється здобувач СЕРЕДІН Андрій до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: Засоби автентифікація користувачів в інформаційно-комунікаційних системах

Кваліфікаційна робота і рецензія додаються.
Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) (ім'я, прізвище)

Висновок керівника кваліфікаційної роботи

Здобувач ***СЕРЕДІН Андрій*** обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***СЕРЕДІН Андрій*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***СЕРЕДІН Андрій*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **СЕРЕДІН Андрій** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 56 сторінки, 11 рисунків, 18 джерел.

Об'єкт дослідження – інформаційно-комунікаційні системи.

Предмет дослідження – методи, підходи та засоби автентифікації користувачів, а також конкретні рішення, що застосовуються в таких системах.

Мета роботи – аналіз проблемиавтентифікації користувачів в інформаційно-комунікаційній системі.

Методи дослідження – Методи дослідження – опрацювання наукової літератури, аналіз сучасних стандартів інформаційної безпеки, а також порівняння існуючих підходів та технологій автентифікації користувачів у інформаційно-комунікаційних системах. Проведено огляд та систематизацію методів багатофакторної автентифікації, включно з використанням одноразових кодів (OTP) та біометричних факторів, зокрема відбитків пальців, а також розглянуто архітектуру прикладних рішень на базі системи ESET.

У роботі досліджено актуальні проблеми автентифікації користувачів у інформаційно-комунікаційних системах, визначено мету і завдання забезпечення надійного доступу. Проведено аналіз основних ризиків і загроз, що виникають під час ідентифікації користувачів, та оцінено ефективність сучасних методів автентифікації в умовах зростаючих кіберзагроз. Розглянуто функціональні особливості та складові рішення ESET для багатофакторної автентифікації, що включає як традиційні, так і біометричні фактори.

На основі проведеного дослідження запропоновано рекомендації щодо впровадження багатофакторних засобів автентифікації, які підвищують рівень безпеки інформаційно-комунікаційних систем. Розроблено практичні поради для фахівців з інформаційної безпеки щодо ефективного використання засобів автентифікації, що дозволяє мінімізувати ризики несанкціонованого доступу та захистити критичні дані організації.

Галузь використання – кібербезпека інформаційних ресурсів.

ЗМІСТ

Стор.

ВСТУП

Актуальність дослідження. На разі в сучасному світі де швидкого розвитку набувають інформаційно-комунікаційні технології, та збільшується обсяг інформації яка потребує перевірки, особливої уваги набувають безпечні доступи до систем.

Одним з головних методів захисту інформації є автентифікація та ідентифікація користувачі, яка забезпечує підтвердження особи та запобігає несанкціонованому доступу до інформації.

Якщо взяти до уваги швидке зростання та різноманіття засобів автентифікації, а також потенційні ризики які з'являються під час їх застосування дослідження проблем автентифікації користувачів у інформаційно-комунікаційних системах є надзвичайно важливим та актуальним процесом.

На сам перед зі зростанням розвитку технологій з'являються і нові методи несанкціонованого доступу до інформації, через це важливо розуміти як захистити свою інформацію, з цим якраз таки й допомагає автентифікація та її різновиди від банальних паролей до більш розвинутих методів таких як сканування відбитків пальців або ж сітчатки ока.

Автентифікація допомагає як і звичайним людям в повсякденному житті, так і великим компаніям для забезпечення безпеки даних так облегшення класифікацій доступу, наприклад доступ до певної інформації можуть мати лише високопоставлені члени компанії, а до більш доступної яка не може сильно нашкодити вже всі працівники, наприклад така як місце розташування або бейдж який дозволяє попасти на робоче місце

Мета і завдання дослідження. Метою цієї роботи є аналіз проблеми автентифікації користувачів в інформаційно-комунікаційній системі, розгляд існуючих рішень та розробка рекомендацій щодо впровадження ефективних засобів автентифікації.

Для досягнення мети поставлені такі завдання:

1) дослідити поняття автентифікації користувачів;

2) проаналізувати ризики та загрози, пов’язані з ідентифікацією користувачів;
3) розглянути основні підходи до засобів автентифікації;
4) здійснити аналіз існуючих рішень засобів автентифікації;
5) обрати і описати архітектуру конкретного рішення;
6) розробити рекомендації щодо впровадження засобів автентифікації.

Об’єкт і предмет дослідження. Об’єктом дослідження є інформаційно-комунікаційні системи, які потребують контролю доступу та захисту інформації. Предметом дослідження є методи, підходи та засоби автентифікації користувачів, а також конкретні рішення, що застосовуються в таких системах.

1 АНАЛІЗ ПРОБЛЕМИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

1.1. Поняття автентифікації користувачів

Автентифікація користувачів це механізм систем інформаційної безпеки, призначенням якого є достовірне підтвердження особи користувача, який хоче отримати доступ до певного ресурсу, суть процесу полягає в тому щоб порівняти реальні данні автентифікації з тими які використовує користувач, це і забезпечує основний захист від не санкціонованого доступу до інформації.

В сучасному світі автентифікація з просто контролю доступу до інформації перетворилась на дуже складну багатошарову систему, яка включає в себе велике різноманіття методів підтвердження особи, з часом ці система пройшла довгий шлях від звичайних паролей типу (12435) до більш складних комбінованих рішень, які поєднують в собі криптографічні методи, біометричні технології та апаратні засоби захисту [1].

Автентифікація зазвичай використовує декілька ключових функцій які допомагають підтвердити особу суб’єкту, а саме :

Ідентифікація та автентифікація суб’єкту:

Ідентифікація та автентифікація є над важливими в процесі підтвердження особі користувача в системі, ці два терміни часто використовуються разом, але мають різні значення та виконуються різні функції.

Ідентифікація це перший етап який перевіряє достовірність ідентифікаційних даних введених в систему, після того, як суб'єкт ввів данні до системи вона повинна переконатися чи є ці данні достовірними за це якраз таки і відповідає наступний крок автентифікація за допомогою нього система перевіряє чи є данні які користувач ввів на етапі ідентифікації достовірними [1].

Запобігання несанкціонованого проникнення:

Процес який має на меті запобігання несанкціонованого проникнення осіб або програм які не повинні мати доступ до певної інформації, це допомагає мінімізувати ризики компрометації та захистити данні та систему від втручання.

Най поширенішим рішенням є парольна автентифікація яка полягає в веденні секретного коду тобто паролю який повинен знати лише користувач, цей метод має свої обмеження такі як вразливість до атак методом підбору паролей або ж фішинг. Тому на разі бажано використовувати багатофакторну автентифікацію (MFA) яка полягає в декількох незалежних між собою методах підтвердження особи користувача, а саме пароль, сканування відбитка пальця, посилання на пошту з секретним кодом, або ж (Face id) сканування обличчя, ці методи допомагають навіть коли один з них був скомпрометований тому, що вони не залежні один від одного [1].

Забезпечення звітування дій користувача:

Цей етап також має важливе значення, а саме процес фіксує всі дій користувача в системі на основі яких можна буде провести подальший аналіз який допоможе виявити порушення або шахрайські дії, цей етап має кілька основних аспектів.

Аудит та журналювання аспект який веде звід про дії в системі такі як час входу в систему час знаходження які файли було відкрито або змінено.

Моніторинг та аналіз поведінки на разі багато сучасних систем ведуть моніторинг дій користувача на приклад час знаходження на сайти або ж швидкість орієнтування в системі, саме це іноді допомагає виявити несанкціоновані дії так як поведінка не збігається з звичайною.

Ролі та обмежений доступ допомагають побудувати чітку ієрархію в якій певні користувачі мають доступ лише до певної інформації, це дуже сильно зменшує коло пошуку в разі несанкціонованого доступу до певного типу інформації [1].

Аналізування інцидентів цей аспект дозволяє швидко провести розслідування та виявити хто саме був порушником в системі, це дуже важливо для реагування та запобігання подібних випадків в майбутньому [1].

На разі методи захисту інформації стають все більш розвинутими та часто використовують в своїх системах штучний інтелект який допомагає в багатьох етапах перевірки даних.

1.2. Аналіз ризиків та загрози ідентифікації користувачів

Ідентифікація користувачів у інформаційно-комунікаційних системах супроводжується різноманітними ризиками і загрозами, які можуть призвести до несанкціонованого доступу, втрати або компрометації інформації. Аналіз цих ризиків є важливим етапом при розробці та впровадженні засобів автентифікації [2].

Основними загрозами ідентифікації користувача є:

Прехоплення облікових даних завдяки вразливості типу людина по середині (Man-in-the-Middle), фішинг, де зловмисник отримує доступ до паролей чи токенів користувача.

Повторно використаня паролів або слабкі паролі, постійне використання одно і того паролю збільшують ризик злому, так само як і використання занадто простих паролей. Паролі повинні мати складну структури по типу (fFd23@ls@65) де використовуються як і знаки так і букви з цифрами бажано не використовувати повторювання символів в паролі [2].

Соціальна інженерія або ж маніпуляція з користувачем а саме розмова або ж текст який підштовхує на те щоб ви розкрили свої данні такі як паролі чи засекречена інформація, це метод який в першу чергу розрахований на те щоб дізнатися данні на пряму від користувача, через це системного захисту від нього не існує.

Крадіжка або втрата апаратних засобів, на приклад крадіжка телефону щоб отримати доступ до інформації власника або ж компанії в якій він працює.

Вразливості в системах біометричного сканування, наприклад підробка відбитків пальців чи використання фото для підтвердження користувача [2].

Не правильне налаштування систем автентифікації яке може призвести до пропуску певних етапів перевірки або недостатньої складності механізмів перевірки [2].

Таблиця 1.1.

Аналіз ризиків та загрози ідентифікації користувачів

Тип загрози	Опис загрози	Рівень загрози (1-низький, 5-високий)
Прехоплення облікових даних	Зловмисники можуть перехопити дані (паролі, токени) через вразливість типу 'людина посередині' або фішинг.	4
Повторно використаня паролів або слабкі паролі	Використання одного паролю або простих паролів збільшує ризик злому.	4
Соціальна інженерія або ж маніпуляція з користувачем	Маніпуляція користувачем для отримання його даних без технічного захисту.	5
Крадіжка або втрата апаратних засобів	Крадіжка мобільних пристроїв чи інших засобів автентифікації може дати доступ до інформації.	4
Вразливості в системах біометричного сканування	Підробка біометричних даних (відбитки пальців, фото) для обману системи автентифікації.	3

Не правильне налаштування систем автентифікації	Помилки в налаштуванні системи можуть призвести до ослаблення безпеки і пропуску важливих етапів.	3

Всі перераховані загрози можуть стати причиною порушення цілісності інформації та її доступності.

Для того що мінімізувати такі загрози потрібно застосовувати багатошарові методи захисту інформації, постійно оновлювати програмне забезпечення до нових версій або ж використовувати більш надійні рішення, регулярно проводити аудити на як навчають користувачів безпечної поведінки та захисту своєї інформації, використовувати сучасні технології автентифікації які стійкі до атак [2].

1.3. Аналіз підходів до автентифікації користувачів

Автентифікація користувача в системі може бути реалізована за допомогою різних підходів, базованих на використанні різних факторів та видів технологій . Вибір конкретного рішення залежить від безпеки системи, зручності використання, технічних можливостей які може надати система та інших факторів [3].

Основними підходами для автентифікації користувача можна назвати:

Однофакторна автентифікація (Single-Factor Authentication)

Це найпростіший та найпоширеніший тип автентифікації, при якому підтвердження особи відбувається за допомогою одного фактора – зазвичай це пароль або PIN-код [3].

Рис. 1.1. Однофакторна автентифікація (Single-Factor Authentication)

Переваги однофакторної автентифікації:

1) Простота впровадження і використання Однофакторна автентифікація легко реалізується. Вона не вимагає додаткового обладнання або складних налаштувань. Це робить її доступною для багатьох користувачів і організацій.

2) Швидкість доступу Оскільки використовується лише один фактор, автентифікація швидка. Вона не створює зайвих затримок під час входу в систему.

3) Низькі витрати Відсутність потреби у додаткових пристроях або складних рішеннях знижує загальні витрати на безпеку.

Недоліки однофакторної автентифікації:

1) Низький рівень безпеки Однофакторна автентифікація легко піддається атакам. Це включає фішинг, підбір пароля та повторне використання паролів, що підвищує ризик несанкціонованого доступу.

2) Вразливість до компрометації Якщо пароль чи інший фактор викрадуть або вгадають, зловмисник отримає повний доступ до системи. Це може призвести до витоку конфіденційної інформації або інших серйозних наслідків.

3) Відсутність додаткового рівня захисту Без другого або третього фактора неможливо підвищити рівень безпеки. Це особливо важливо для систем з підвищеними вимогами до захисту.

Оскільки однофакторна автентифікація має свої недоліки, її все частіше замінюють або доповнюють багатофакторними методами. Ці методи забезпечують вищий рівень захисту. Проте через простоту і зручність однофакторна автентифікація все ще використовується в системах з низьким рівнем ризику. Вона також може бути початковим рівнем контролю доступу [3].

Багатофакторна автентифікація (Multi-Factor Authentication, MFA)

Багатофакторна автентифікація є більш безпечною альтернативою однофакторній. Вона передбачає використання двох або більше незалежних факторів для підтвердження особи користувача:

Що користувач знає – зазвичай це пароль або PIN-код.

Що користувач має – фізичні пристрої, такі як токен, смарт-карта або мобільний телефон, що генерує одноразовий код.

Що користувач є – біометричні дані, як-от відбитки пальців, розпізнавання обличчя або райдужної оболонки ока.

Багатофакторна автентифікація значно підвищує рівень безпеки, оскільки зловмиснику потрібно здобути доступ до кількох факторів одночасно, що ускладнює атаку [3].

Принцип роботи багатофакторної автентифікації полягає в тому що під час входу в систему користувач повинен послідовно або одночасно надати інформацію з кількох факторів. Наприклад, після введення пароля система може вимагати ввести код, який надіслано на мобільний телефон, або підтвердити особу за допомогою біометричного сенсора [3].

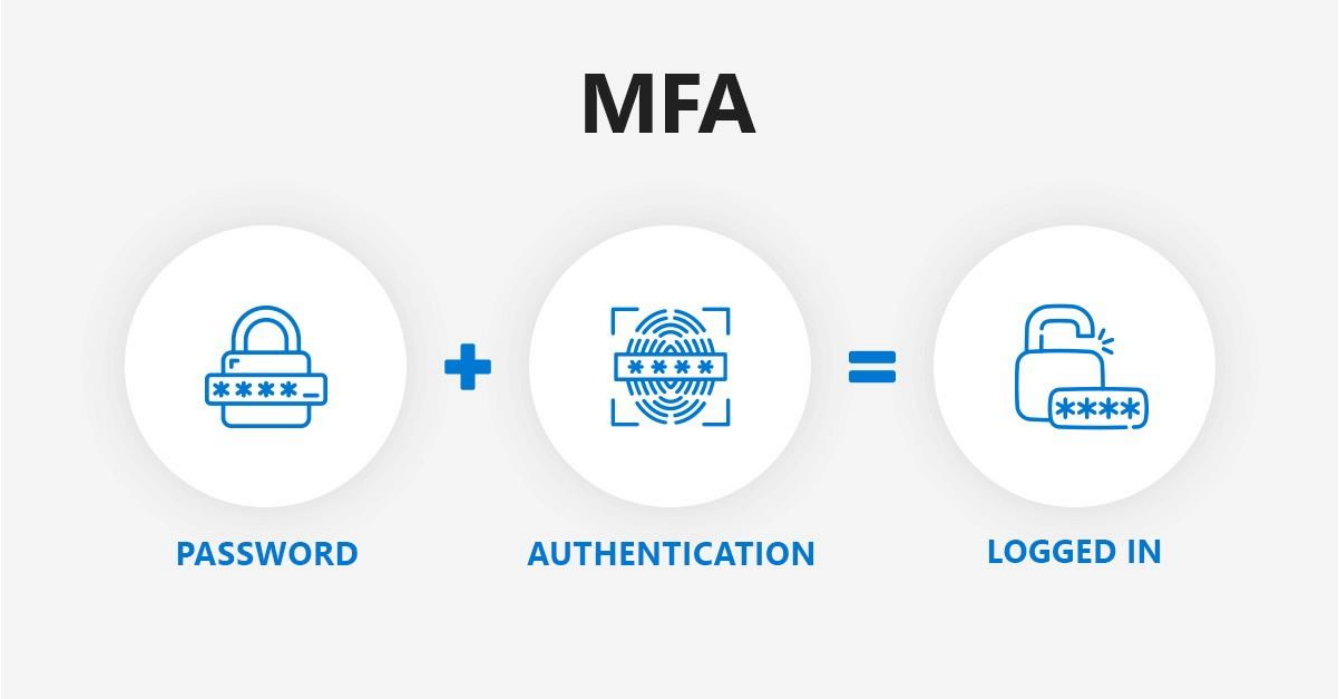

Рис. 1.2. Багатофакторна автентифікація (Multi-Factor Authentication, MFA)

Переваги MFA:

1) Підвищений рівень безпеки – ця комбінація факторів зменшує ймовірність успішної атаки. Це залишається в силі, навіть якщо один із факторів скомпрометовано.
2) Гнучкість і масштабованість – MFA може адаптуватися до різних рівнів безпеки. Вона відповідає вимогам організації та типам користувачів.
3) Захист від широкого спектра загроз – MFA ефективно бореться з фішингом, крадіжкою паролів, атаками "людина посередині" та іншими поширеними кіберзагрозами.

Недоліки MFA:

1) Складність впровадження – потрібні додаткові ресурси для інтеграції та підтримки системи.
2) Зменшення зручності користувача – додаткові кроки автентифікації можуть ускладнити та сповільнити вхід.
3) Залежність від зовнішніх факторів – наприклад, втрата телефону або поломка біометричного сенсора може ускладнити доступ.

Багатофакторна автентифікація захищає критичні інформаційні системи, банківські послуги, державні ресурси та корпоративні мережі. Вона підвищує рівень безпеки та знижує ризики несанкціонованого доступу [3].

Безпарольна автентифікація

Безпарольна автентифікація – це новий підхід, який намагається усунути необхідність введення пароля взагалі [4]. Вона використовує інші методи, такі як:

Електронні ключі – спеціальні пристрої або програмне забезпечення, яке генерує код для автентифікації [4].

Біометрія – використання унікальних фізичних характеристик, таких як відбитки пальців або розпізнавання обличчя.

Одноразові коди (OTP) – коди, які надсилаються користувачу через SMS, електронну пошту або за допомогою мобільних додатків. Ці коди зазвичай мають короткий термін дії і є дієвим способом підтвердження особи [4].

Переваги безпарольної автентифікації:

1) Відсутність проблем із паролями – зникають ризики, пов’язані зі слабкими, вкраденими паролями, їх забуванням або повторним використанням.
2) Підвищена безпека – зменшується ймовірність фішингових атак та інших способів компрометації паролів.
3) Покращений користувацький досвід – процес входу стає швидким і простим, що знижує бар’єри для користувачів.
4) Менше адміністративних витрат – немає потреби керувати складними політиками паролів, їх регулярною зміною або підтримкою служби відновлення паролів.

Недоліки безпарольної автентифікації:

1) Залежність від інших каналів зв’язку – наприклад, затримки або втрати повідомлень можуть виникнути при надсиланні OTP через SMS.
2) Потенційна вразливість апаратних пристроїв – втрата або крадіжка токена чи смартфона ускладнює доступ користувача.
3) Необхідність впровадження нових технологій – для безпарольних методів треба модернізувати системи, що може вимагати додаткових ресурсів.

Безпарольна автентифікація стає популярною у фінансовому секторі, IT-компаніях і сервісах. Вона допомагає підвищити рівень безпеки та покращити користувацький досвід. Часто її поєднують з багатофакторною автентифікацією. Це забезпечує оптимальний баланс між безпекою і зручністю [4].

Біометрична автентифікація:

Біометрична автентифікація є одним із найсучасніших і найефективніших підходів до підтвердження особи користувача в інформаційно-комунікаційних системах. Вона ґрунтується на використанні унікальних фізіологічних або поведінкових характеристик людини, що робить її надзвичайно надійною та складною для підробки. Завдяки своїй точності і зручності, біометрія здобула широку популярність у багатьох сферах – від мобільних пристроїв до державних систем безпеки [5].

Фізіологічні характеристики, які використовуються для біометричної автентифікації, включають відбитки пальців, форму та риси обличчя, структуру сітківки ока, голос, геометрію руки тощо. Поведінкові характеристики базуються на унікальних способах взаємодії користувача з пристроями, наприклад, стилі набору тексту, рухах миші чи навіть почерку.

Однією з ключових переваг біометричної автентифікації є її здатність забезпечувати високу точність і надійність у порівнянні з традиційними методами, такими як паролі або токени. Біометричні дані практично неможливо забути або втратити, що знижує ймовірність помилок під час автентифікації та підвищує рівень безпеки системи загалом [5].

Крім того, біометрична автентифікація забезпечує зручність для користувачів – процес підтвердження особи стає швидким і простим, адже не вимагає введення складних паролів або використання додаткових пристроїв. Наприклад, розпізнавання обличчя або відбитків пальців можна виконати всього за кілька секунд без фізичного контакту.

Варто також зазначити, що сучасні системи біометричної автентифікації часто інтегруються з іншими методами захисту, такими як багатофакторна

автентифікація, що дозволяє поєднати кілька рівнів безпеки для максимального захисту даних.

Проте разом із численними перевагами, біометрія має і певні виклики. Збір, зберігання та обробка біометричних даних викликають питання конфіденційності та безпеки – важливо забезпечити їх захист від несанкціонованого доступу і можливого викрадення. Також технології біометрії можуть стикатися з технічними труднощами, пов’язаними з якістю зчитування або змінами фізичних характеристик користувача (наприклад, через травми або вікові зміни).

У цілому, біометрична автентифікація продовжує швидко розвиватися завдяки прогресу у сфері штучного інтелекту, машинного навчання та сенсорних технологій. Вона є ключовим елементом сучасних систем безпеки, які прагнуть забезпечити одночасно високу надійність і зручність користування для кінцевих користувачів.

Відбитки пальців – Існують дві основні категорії методів порівняння відбитків пальців – це порівняння визначених точок і співставлення цілого малюнку відбитка – шаблона. Метод шаблонної ідентифікації має на увазі порівняння двох зображень, яке дозволяє побачити, наскільки вони схожі. Такий метод, як правило, використовується в системах зчитування відбитків пальців для знаходження дублікатів. Технологією, яка більш широко використовується є розпізнавання на основі порівняння визначених точок [5].

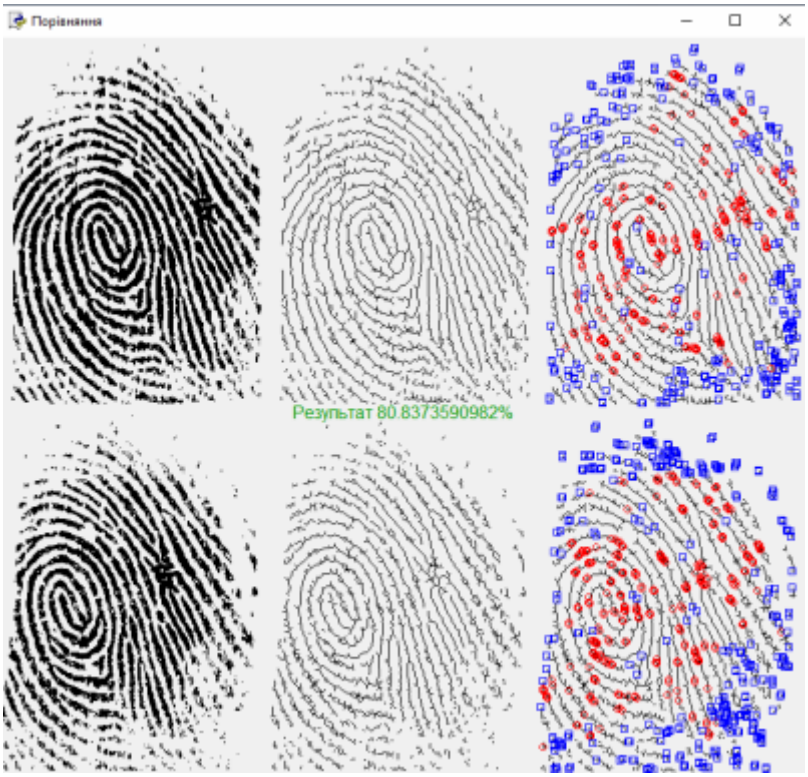

Рис. 1.3. Приклад результату порівняння відбитків

Переваги відбитків пальців:

1) Унікальність та стабільність Візерунки відбитків пальців унікальні для кожної людини. Вони залишаються незмінними протягом життя. Це забезпечує високу точність та надійність автентифікації.

2) Швидкість і простота використання Зчитування відбитків займає лише кілька секунд. Це не потребує складних дій від користувача. Достатньо прикласти палець до сканера для автентифікації.

3) Відносно низька вартість обладнання Сканери відбитків пальців стали доступними і широко впроваджуються у різноманітних пристроях.

4) Широке розповсюдження Цей метод знайомий користувачам і використовується у багатьох сферах. Це підвищує прийнятність та довіру до нього.

Недоліки відбитків пальців:

1) Вразливість до підробок Хоча відбитки пальців є унікальними, їх можна підробити. Це можливо за допомогою штучних відбитків або якісних зліпків, що становить загрозу безпеці.

2) Проблеми зі зчитуванням Стан шкіри, наприклад, пошкодження чи забруднення, може ускладнити зчитування відбитків пальців. Це може призвести до помилок або повторної спроби автентифікації.

3) Обмеженість застосування Відбитки пальців не підходять для людей з пошкодженнями пальців або шкіри. Також це може бути проблемою для професій, де пальці постійно піддаються хімічним речовинам чи механічним навантаженням.

4) Питання конфіденційності Збір і зберігання біометричних даних викликають занепокоєння щодо конфіденційності. Існує ризик несанкціонованого використання або викрадення цих даних [5].

Розпізнавання обличчя – на разі є одним із найбільш інноваційних методів біометричної автентифікації, використовується для автентифікації особи на основі унікальних рис обличчя. Цей метод на разі є одним із найпоширеніших методів автентифікації [6].

Принцип роботи системи розпізнання обличчя базується на спеціальних технологіях та алгоритмах, які мають здатність аналізувати особливості обличчя користувача такі як. *Форма обличчя та його пропорції*, розташування ключових точок таких як (очі, ніс, губи, контур обличчя). *Унікальні біометричні характеристики які базуються на розташуванні ключових точок таких як,* відстань між очима, форма носа та рота, контури щелепи що є незнімними для кожної людини. *Текстура шкіри*, використовуються методи глибинного навчання та аналізу зображень для виявлення детальних текстур шкіри, що також є індивідуальними [6].

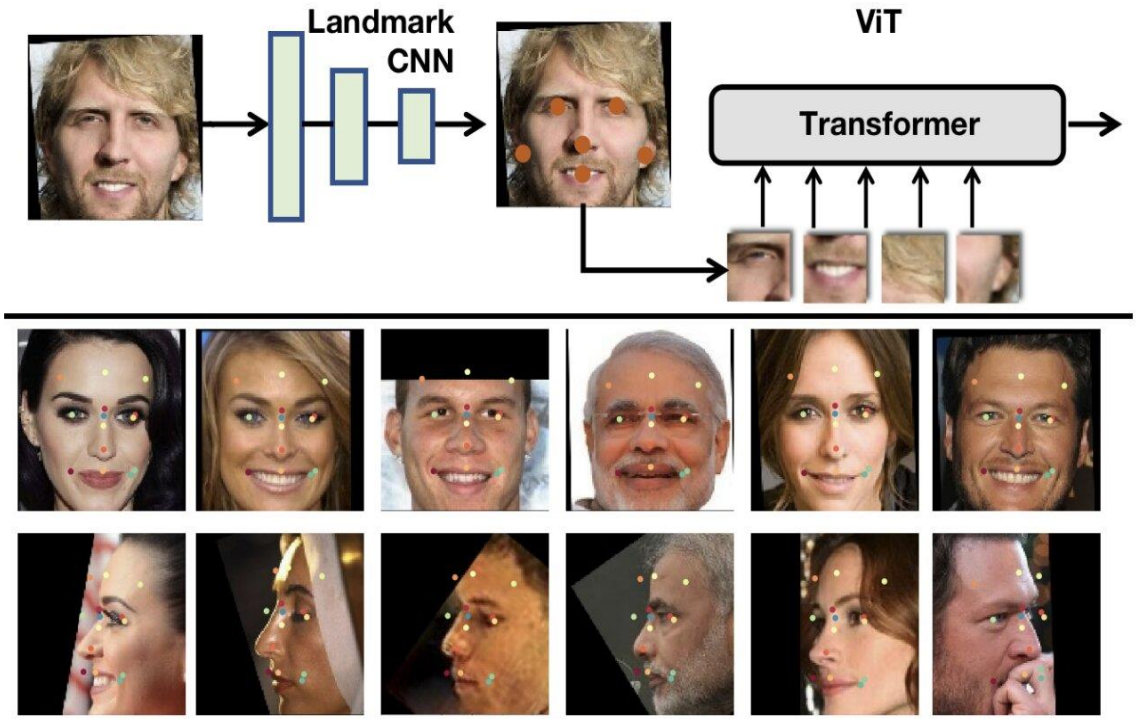

Рис. 1.4. Приклад результату розпізнання обличчя

У більшості випадків ці дані порівнюються з раніше збереженими шаблонами, що забезпечує точність верифікації користувача. Однак, на практиці цей процес може варіюватися залежно від використовуваних технологій та вимог до безпеки [6].

Переваги розпізнавання обличчя:

1) Зручність і швидкість: Розпізнавання обличчя – один з найшвидших і найзручніших методів автентифікації. Користувачеві не потрібно вводити паролі чи додаткові дані. Процес відбувається миттєво і без фізичних контактів, що підвищує зручність використання.

2) Висока точність: Сучасні алгоритми розпізнавання обличчя, засновані на глибинному навчанні, досягають високої точності. Це зменшує ймовірність помилок під час автентифікації.

3) Безконтактність: Система працює через камеру, тому користувач не потребує фізичного контакту з пристроєм. Це робить розпізнавання обличчя дуже зручним у повсякденному використанні, наприклад, для смартфонів або комп'ютерів.

4) Захист від фішингу: Розпізнавання обличчя значно знижує ризик фішингових атак. Зловмисники не можуть отримати доступ до систем за допомогою викрадених паролів або токенів, адже підробити обличчя користувача важко.

Недоліки та ризики:

1) Можливість підробки: Сучасні системи можуть мати високу точність, але є ризик підробки. Зловмисники можуть використовувати фото, відео або 3D-моделі облич для обходу системи. Щоб зменшити цей ризик, багато систем застосовують технології детекції живих облич. Це може бути аналіз рухів або перевірка реального зображення особи.

2) Залежність від якості зображення: Освітлення і якість камери значно впливають на точність розпізнавання. Погане освітлення, низька роздільна здатність чи зміни у зовнішності користувача, наприклад, нова зачіска або окуляри, можуть знизити ефективність системи.

3) Проблеми конфіденційності: Збирання біометричних даних викликає занепокоєння щодо конфіденційності. Зловмисники можуть отримати доступ до чутливих даних про користувача. У деяких країнах існують суворі правила і законодавство для регулювання використання таких технологій.

4) Необхідність додаткових засобів захисту: Для підвищення безпеки, особливо у критичних системах, часто використовують додаткові методи автентифікації. Багатофакторна автентифікація поєднує розпізнавання облич із іншими методами, такими як введення пароля або використання токенів, це зменшує ризики того що зловмисник зможе отримати доступ до засекреченої інформації [6].

Розпізнавання сітчатки ока – є одним з найточніших і найнадійніших методів біометричної автентифікації. Він використовує унікальні фізіологічні характеристики ока для підтвердження особи користувача [7]. Цей метод стає популярним у системах високої безпеки. Наприклад, його застосовують для доступу до державних і корпоративних інформаційних ресурсів. Також його використовують в установах з особливими вимогами до захисту даних [7].

Принцип роботи розпізнання сітчатки ока полягає в тому що він збирає інформацію відносно кровоносних судин розташованих на оці людини вони є

унікальними та їх кількість також відрізняється . Технологія розпізнання аналізує структуру цих судин за допомогою спеціальних інфрачервоних камер, цей процес включає в себе декілька етапів а саме [7]:

Засвічування сітківки ока – інфрачервоне світло освітлює сітківку, що дає чітке зображення судин.

Захоплення зображення – камера з інфрачервоним світлом знімає сітківку, фіксуючи унікальну картину судин.

Аналіз та порівняння – зображення порівнюється з раніше збереженими шаблонами в базі даних для перевірки автентичності користувач [7].

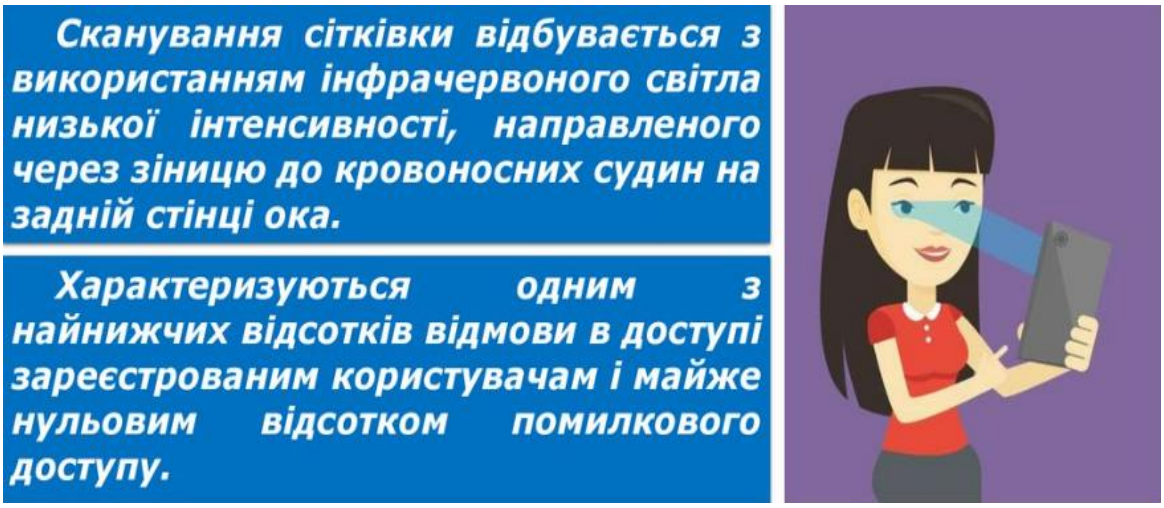

Рис. 1.5. Розпізнавання сітчатки ока

Переваги розпізнавання сітківки ока:

1) Висока точність та надійність: Розпізнавання сітківки ока – один з найточніших методів біометричної автентифікації. Структура кровоносних судин в оці унікальна для кожної людини і не змінюється з часом. Це робить метод майже неможливим для підробки або помилкових спрацьовувань.
2) Стійкість до зовнішніх впливів: На відміну від відбитків пальців чи обличчя, сітківка ока не залежить від умов навколишнього середовища.
3) Освітлення або забруднення не впливають на її точність, так само як і фізіологічні зміни, наприклад, старіння чи хвороби.
4) Неможливість підробки: Технологія розпізнавання сітківки ока важче підробити, ніж інші біометричні методи, такі як відбитки пальців чи розпізнавання обличчя. Це робить її більш безпечною для критичних систем.

5) Безконтактність і простота використання: Процес розпізнавання є безконтактним і простим для користувача. Достатньо просто поглянути на камеру, щоб пройти автентифікацію [7].

Недоліки та ризики:

1) Висока вартість обладнання: Розпізнавання сітківки потребує спеціалізованого обладнання, як-от інфрачервоні камери. Це робить впровадження таких систем дорогим. Тому їх важко використовувати в бюджетних проектах.
2) Проблеми з доступністю та комфортом: Деяким користувачам метод розпізнавання сітківки може бути незручним. Це може статися через проблеми з зором або труднощі з вирівнюванням ока під час автентифікації.
3) Складність інтеграції та обслуговування: Системи розпізнавання сітківки потребують регулярного технічного обслуговування. Важливо налаштовувати та калібрувати обладнання для підтримки точності та ефективності.
4) Проблеми з конфіденційністю: Збір біометричних даних сітківки піднімає питання конфіденційності. Необхідно дотримуватися вимог, як-от GDPR та інших законів, що регулюють використання біометрії [7].

Системи розпізнавання сітківки ока можуть поєднуватися з іншими біометричними технологіями. Це створює комплексні системи автентифікації, як-от багатофакторна автентифікація. Вона об'єднує розпізнавання сітківки з іншими методами, наприклад, відбитками пальців або аналізом поведінки користувача.

З розвитком технологій, як-от штучний інтелект та машинне навчання, точність і швидкість розпізнавання сітківки можуть поліпшитися. Це дозволить зробити цей метод доступним для різних застосувань. Від мобільних пристроїв до систем безпеки в державних установах [7].

Голосова автентифікація – це метод біометричної верифікації, який використовує унікальні характеристики голосу користувача для підтвердження його особистості. Цей підхід набуває популярності завдяки зручності використання, особливо в телефонних службах підтримки, голосових помічниках та інших системах, де можливість підтвердження особи голосом суттєво підвищує безпеку [8].

Принципом роботи голосової автентифікації є аналіз унікальних параметрів голосового сигналу користувача, які важко підробити, система фіксує та аналізує такі характеристики як, тембр і тон голосу, частотні характеристики, швидкість мовлення та ритм, патерни мовлення та акцент.

Після запису зразка голосу користувача, система створює його біометричний шаблон, який використовується для подальшої порівняльної перевірки під час автентифікації [8].

Переваги голосової автентифікації:

1) Зручність для користувачів Голосова автентифікація не потребує додаткового обладнання. Досить мікрофона, який є у більшості сучасних пристроїв. Це робить метод швидким і простим у використанні.
2) Безконтактність Як і інші біометричні методи, голосова автентифікація є безконтактною. Це підвищує гігієнічність та комфорт при використанні.
3) Підвищення рівня безпеки Голосова автентифікація може бути додатковим фактором у багатофакторній системі. Це знижує ризик компрометації паролів або інших засобів автентифікації.
4) Можливість дистанційної перевірки Голосова автентифікація добре підходить для телефонних або онлайн-сервісів. Тут інші методи біометрії можуть бути недоступними [8].

Недоліки голосової автентифікації:

1) Вразливість до шумів та якості зв’язку Шум, погана якість зв’язку або зміни в голосі через хворобу можуть знижувати точність системи.
2) Ризик підробки Зловмисники можуть спробувати обійти систему за допомогою записів голосу, синтезу голосу або інших методів. Для боротьби з цим використовують технології виявлення живого голосу (anti-spoofing).
3) Залежність від фізіологічних змін Зміни в голосі, спричинені хворобами, стресом чи віком, можуть ускладнити автентифікацію.
4) Конфіденційність та етичні питання Збирання і зберігання голосових біометричних даних вимагає дотримання строгих норм конфіденційності та законодавства [8].

З удосконаленням алгоритмів машинного навчання та обробки сигналів, точність голосової автентифікації зростає. Вона стає більш інтегрованою у багатофакторні системи безпеки. Також її використовують у нових сферах, як-от банківські сервіси, мобільні додатки та системи розумного дому [8].

Голосова автентифікація – це зручний метод підтвердження особи. Якщо його правильно впровадити, він може підвищити безпеку та комфорт користувачів [8].

Біометрія є надійною, оскільки біометричні дані важко підробити. Проте є певні ризики, пов’язані з можливістю підробки або маніпуляції з біометричними даними.

Контекстна автентифікація:

Контекстна автентифікація – це сучасний спосіб підтвердження особи користувача. Він враховує додаткові параметри або «контекст» дій для підвищення безпеки. Замість використання лише стандартних факторів, таких як пароль, токен або біометрія, система аналізує умови спроби входу. Це допомагає оцінити рівень ризику [9].

Основними елементами контекстної автентифікації є:

Геолокація – аналіз фізичного місця розташування користувача під час спроби доступу. Якщо трапляється так що вхід відбувається з незвичного або ж підозрілого регіону, система може почати вимагати додаткове підтвердження особи або ж заборонити доступ [9].

Час доступу – аналізує чи вхід здійснюється у звичайний час для користувача (наприклад робочі години) зазвичай час може сигналізувати про потенційну загрозу [9].

Тип і стан пристрою за якого здійснюється вхід до системи – чи цей пристрій раніше використовувався , чи є він оновленим і захищеним. Незнайомі або потенційно небезпечні пристрої можуть бути обмежені в доступі [9].

Мережеві параметри – аналіз IP-адреси користувача , типу мережі (Wi-Fi, мобільна мережа) а також інші характеристики з’єднання для виявлення аномалій які можуть призвести до несанкціонованого доступу [9].

Поведінкові характеристики – оцінка типових дій користувача: швидкість набору тексту, спосіб взаємодії з інтерфейсом, послідовність дій тощо. Відхилення від звичних патернів може свідчити про спробу несанкціонованого доступу [9].

Переваги контекстної автентифікації:

1) Підвищений рівень безпеки Система аналізує різні параметри, щоб краще виявляти загрози.
2) Гнучкість і адаптивність Вона автоматично підлаштовується під поведінку користувача. Додаткові перевірки застосовуються лише за потреби.
3) Покращений користувацький досвід Користувачі не стикаються з труднощами, якщо їхня поведінка звичайна. Це робить автентифікацію простішою та комфортнішою [9].

Недоліки контекстної автентифікації:

1) Складність впровадження Збір та аналіз великої кількості даних потребує складних технічних рішень. Потрібно також створити моделі поведінки користувачів.
2) Питання конфіденційності Збирання контекстної інформації може викликати занепокоєння користувачів. Вони можуть турбуватись про свою приватність та захист персональних даних.
3) Можливі помилки Неправильна інтерпретація контекстних даних може призвести до помилкових відмов у доступі. Це також може викликати надмірні запити на додаткову автентифікацію [9].

Контекстна автентифікація часто використовується у фінансових системах, корпоративних мережах та онлайн-сервісах. Важливо поєднувати високий рівень безпеки із зручністю користувачів. Цей метод забезпечує додатковий рівень захисту. Він доповнює традиційні методи автентифікації [9].

Таблиця 1.2.

Аналіз підходів до автентифікації користувачів

Підхід до автентифікації	**Опис**	**Переваги**	**Недоліки**

Однофакторна автентифікація	Використання одного фактора (найчастіше пароль) для підтвердження особи.	- Простота впровадження і використання - Швидкість доступу - Низькі витрати	- Низький рівень безпеки - Вразливість до компрометації - Відсутність додаткового захисту
Багатофакторна автентифікація (MFA)	Використання двох або більше незалежних факторів (пароль, токен, біометрія).	- Підвищений рівень безпеки - Гнучкість і масштабованість - Захист від широкого спектра загроз	- Складність впровадження - Зменшення зручності користувача - Залежність від зовнішніх факторів
Безпарольна автентифікація	Відмова від паролів на користь одноразових кодів, біометрії, електронних ключів тощо.	- Відсутність проблем із паролями - Підвищена безпека - Покращений користувацький досвід - Менше адміністративних витрат	- Залежність від каналів зв’язку - Ризик втрати апаратних пристроїв - Необхідність модернізації систем
Біометрична автентифікація	Використання фізіологічних чи поведінкових	- Висока точність - Швидкість і простота	- Вразливість до підробок - Проблеми зі

	характеристик (відбитки пальців, обличчя, голос).	використання - Відносно низька вартість обладнання - Широке розповсюдження	зчитуванням - Питання конфіденційності
Розпізнавання обличчя	Аналіз унікальних рис обличчя користувача для верифікації.	- Зручність і швидкість - Висока точність - Безконтактність - Захист від фішингу	- Можливість підробки - Залежність від якості зображення - Проблеми конфіденційності
Розпізнавання сітківки ока	Аналіз унікальної структури кровоносних судин сітківки ока за допомогою інфрачервоних камер.	- Висока точність та надійність - Стійкість до зовнішніх впливів - Неможливість підробки - Безконтактність	- Висока вартість обладнання - Проблеми з комфортом - Складність обслуговування - Проблеми конфіденційності
Голосова автентифікація	Використання унікальних параметрів голосу користувача для підтвердження особи.	- Зручність для користувачів - Безконтактність - Підвищення рівня безпеки - Можливість дистанційної перевірки	- Вразливість до шумів і якості зв’язку - Ризик підробки - Залежність від фізіологічних змін - Проблеми конфіденційності

Контекстна автентифікація	Аналіз додаткових параметрів (геолокація, час, пристрій, поведінка) для підвищення безпеки.	- Підвищений рівень безпеки - Гнучкість і адаптивність - Покращений користувацький досвід	- Складність впровадження - Питання конфіденційності - Можливі помилки і помилкові відмови

Базуючись на рішеннях які при підносить програмне забезпечення ESET та його можливості в захисті інформації від несанкціонованого доступу.

1.4. Аналіз існуючих рішень автентифікації користувачів

Microsoft Azure Active Directory (Azure AD)

Microsoft Azure Active Directory – це хмарна платформа управління ідентифікацією та доступом, яка широко використовується в корпоративних середовищах. Вона забезпечує єдиний вхід користувача (Single Sign-On, SSO), що дозволяє зручно й безпечно отримувати доступ до численних сервісів і додатків. Azure AD підтримує багатофакторну автентифікацію, яка підвищує рівень безпеки шляхом додавання додаткових шарів перевірки користувача. Крім пароля, користувачу може бути запропоновано підтвердити особу через SMS, голосовий дзвінок або мобільний додаток Microsoft Authenticator, що генерує одноразові коди. Особливою функцією Azure AD є умовний доступ, який дозволяє формувати політики безпеки залежно від контексту запиту – наприклад, географічного розташування користувача, типу пристрою чи рівня ризику, виявленого системою. Завдяки цьому підприємства можуть ефективно контролювати доступ до своїх ресурсів, знижуючи можливість несанкціонованого проникнення. Azure AD інтегрується з численними корпоративними сервісами Microsoft, такими як Office 365, Dynamics 365, а також підтримує стандарти OAuth 2.0, OpenID Connect і SAML

для взаємодії зі сторонніми додатками. Однак налаштування цієї системи може бути складним для невеликих організацій, а залежність від хмарних сервісів Microsoft створює додаткову вразливість у разі перебоїв у роботі хмари [10].

Okta

Okta є сучасною хмарною платформою для управління ідентифікацією, яка пропонує розширений функціонал для автентифікації та авторизації користувачів. Це рішення дозволяє організаціям надавати єдиний вхід (SSO) до тисяч додатків, що значно спрощує роботу користувачів і водночас підвищує безпеку. Однією з ключових переваг Okta є підтримка багатофакторної автентифікації з різноманітними методами перевірки: SMS-повідомлення, email, push-сповіщення, апаратні ключі безпеки, а також біометричні дані. Особливістю платформи є адаптивна автентифікація, яка дозволяє змінювати вимоги до підтвердження особи в залежності від поведінки користувача та контексту його дій – наприклад, при спробі входу з незвичного пристрою або з підозрілої геолокації. Okta має зручний і інтуїтивний інтерфейс, що робить її популярною серед компаній різного масштабу. Проте, для малих підприємств вартість сервісу може бути досить високою, а адміністраторам потрібен певний час на навчання для ефективного використання всіх функцій платформи [11].

Duo Security (Cisco)

Duo Security – це спеціалізоване рішення для багатофакторної автентифікації, яке наразі є частиною корпорації Cisco. Воно розроблене з урахуванням потреб сучасних організацій у забезпеченні безпеки доступу до мережевих ресурсів. Duo підтримує різноманітні методи перевірки особи користувача: push-повідомлення на мобільний пристрій, одноразові паролі, апаратні ключі безпеки, такі як YubiKey. Особливою функцією цього рішення є можливість перевірки стану пристрою, з якого виконується вхід, – система аналізує, чи оновлено програмне забезпечення, чи включено антивірусний захист, що дозволяє блокувати доступ з потенційно небезпечних пристроїв. Duo легко інтегрується з VPN, хмарними сервісами, операційними системами Windows і Linux, а також іншими корпоративними системами, що робить його гнучким інструментом для різних сценаріїв

використання. Впровадження Duo не потребує суттєвих змін у наявній інфраструктурі, що значно спрощує процес. Однак деякі розширені функції доступні тільки у преміум-планах, а залежність від мобільного пристрою користувача може створювати незручності у певних ситуаціях [12].

Google Identity Platform

Google Identity Platform – це набір сервісів і API, які дозволяють розробникам і компаніям реалізовувати автентифікацію користувачів з використанням сучасних стандартів безпеки. Платформа підтримує вхід через обліковий запис Google, що дає змогу користувачам швидко і безпечно авторизуватися на сайтах і в додатках. Google Identity Platform забезпечує багатофакторну автентифікацію, підтримуючи мобільні додатки, такі як Google Authenticator, а також апаратні ключі безпеки відповідно до стандарту FIDO2/WebAuthn. Завдяки цьому платформа дозволяє створювати системи автентифікації без паролів, які є більш надійними та зручними. Інтеграція з Google API робить її вигідною для розробників, що використовують екосистему Google. Проте користувачі повинні мати обліковий запис Google, а для деяких корпоративних клієнтів можливі обмеження в налаштуваннях і політиках [13].

ESET Secure Authentication (ESA)

ESET Secure Authentication – це спеціалізоване корпоративне рішення для багатофакторної автентифікації, розроблене компанією ESET, відомою своїми рішеннями в сфері кібербезпеки. ESA дозволяє організаціям підвищити рівень захисту доступу до систем шляхом впровадження додаткового фактора автентифікації поряд з традиційним логіном і паролем. Система підтримує кілька методів перевірки користувача. Перший – це одноразові паролі (One-Time Password, OTP), які генеруються за стандартом TOTP і можуть використовуватися як у вигляді кодів у мобільних додатках, так і на апаратних токенах. Другий метод – push-повідомлення, які надсилаються на мобільний додаток ESET Secure Authentication для швидкого підтвердження входу одним натисканням. Також можлива інтеграція з біометричними системами через відповідні платформи, що дозволяє використовувати відбиток пальця чи розпізнавання обличчя [14].

Система легко інтегрується з корпоративною інфраструктурою, зокрема з Microsoft Active Directory, що дозволяє централізовано керувати користувачами і налаштовувати політики доступу. Мобільний додаток ESA підтримує операційні системи iOS та Android, що дає змогу користувачам підтверджувати свій вхід із будь-якого місця. Адміністратори отримують централізовану консоль для моніторингу й управління автентифікацією, що спрощує керування безпекою на підприємстві [14].

Однією з основних переваг ESET Secure Authentication є високий рівень захисту від фішингових атак, спроб повторного відтворення (replay attacks) та інших типів компрометації облікових записів. Впровадження ESA допомагає суттєво знизити ризики несанкціонованого доступу і забезпечити відповідність сучасним вимогам інформаційної безпеки. Рішення добре поєднується з іншими продуктами ESET, наприклад, з системою централізованого управління безпекою ESET PROTECT, що дозволяє створити комплексний захист корпоративної інфраструктури [14].

Серед недоліків варто зазначити, що ESA в основному орієнтований на корпоративний сектор, що може бути складним для впровадження в невеликих організаціях без відповідних ресурсів. Також для адміністраторів потрібне певне навчання для ефективного використання всіх функцій [14].

Таблиця 1.3.

Аналіз існуючих рішень автентифікації користувачів

Параметр	Microsoft Azure AD	Okta	Duo Security (Cisco)	Google Identity Platform	ESET Secure Authentication
Тип рішення	Хмарна платформа управління ідентифікацією	Хмарна платформа управління ідентифікацією	Спеціалізоване MFA-рішення	Хмарна платформа для аутентифікації	Корпоративне рішення MFA
Підтримка багатофакторної	Так, SMS, голосові дзвінки,	Так, SMS, email, push,	Так, push-повідомлення, OTP,	Так, Google Authenticato	Так, OTP (TOTP), push-

автентифікації	мобільні додатки	апаратні ключі, біометрія	апаратні ключі	r, апаратні ключі	повідомлення, біометрія через інтеграцію
Інтеграція з корпоративними системами	Глибока інтеграція з Microsoft, підтримка OAuth, SAML	Велика кількість додатків і API для інтеграції	VPN, ОС Windows, Linux, хмарні сервіси	Google API, веб та мобільні додатки	Інтеграція з Active Directory, VPN, веб-додатки
Умовний доступ / адаптивна автентифікація	Так, за геолокацією, пристроєм, рівнем ризику	Так, адаптивна політика доступу	Обмеження доступу на основі стану пристрою	Частково через політики Google	Немає повноцінного адаптивного доступу
Підтримка мобільних платформ	Так, iOS, Android	Так, iOS, Android	Так, iOS, Android	Так, iOS, Android	Так, iOS, Android
Простота впровадження	Середня, складно для малих компаній	Висока, інтуїтивний інтерфейс	Висока, мінімальні зміни в інфраструктурі	Висока, API для розробників	Середня, потребує навчання адміністраторів
Рівень безпек	Високий, з інтелектуальним аналізом ризиків	Високий, підтримка різних факторів	Високий, перевірка стану пристрою	Високий, підтримка FIDO2/Web Authn	Високий, захист від фішингу, replay-атак
Підтримка біометрі	Обмежена (через мобільні додатки та інтеграції)	Так, через інтеграції та апаратні ключі	Так, через апаратні ключі	Так, через FIDO2	Так, через інтеграцію з біометричними платформами
Ціна та ліцензування	Варіанти для бізнесу, залежить від обсягу	Дорожче для малих компаній	Є безкоштовна та платні версії	Безкоштовно для базових функцій	Орієнтоване на корпоративний сегмент, середня ціна

Основні недоліки	Складність налаштування для невеликих компаній, залежність від Microsoft	Вартість для малих організацій, навчання персоналу	Преміум-функції не завжди доступні, залежність від мобільних пристроїв	Обов’язкова наявність Google-акаунта, обмеження для корпорацій	Орієнтоване на корпоративний сегмент, потреба у навчанні

2 ЗАСОБИ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ, ОДНОРАЗОВИЙ КОД (OTP) ТА БІОМЕТРИЧНИЙ ФАКТОР У ВИГЛЯДІ ВІДБИТКА ПАЛЬЦЯ НА БАЗІ АРХІТЕКТУРИ ESET

2.1. Архітектура рішення ESET

Компанія ESET пропонує рішення, яке поєднує традиційні методи з сучасними технологіями для досягнення максимальної безпеки – одноразові паролі (OTP), а також біометричні фактори, зокрема відбиток пальця. Розглянемо докладно архітектуру такої системи, її компоненти і принципи роботи [15].

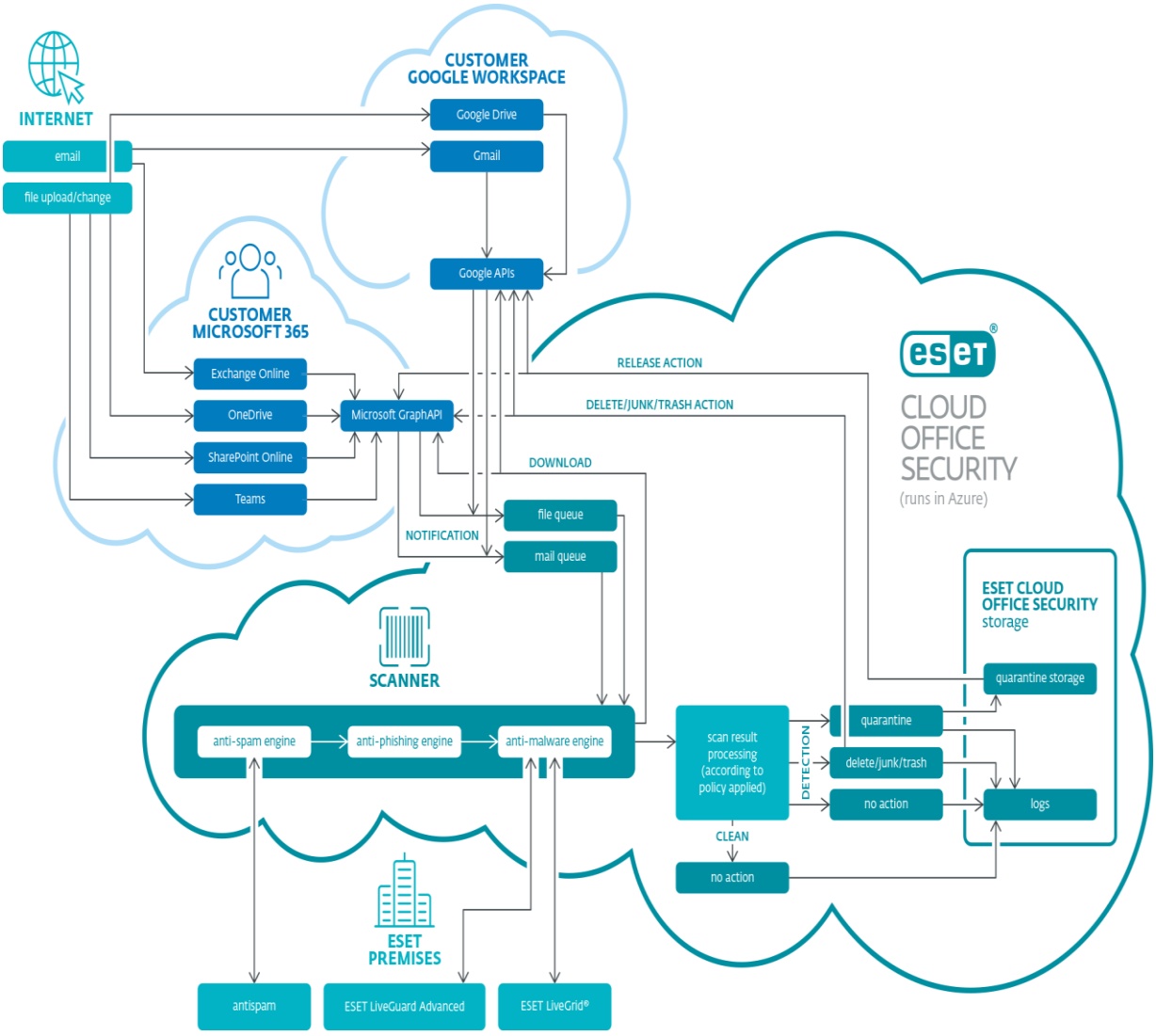

Рис. 2.1. Архітектура рішення ESET

Клієнтський інтерфейс

Клієнтський інтерфейс – це перший контакт користувача із системою автентифікації. В ESET ця частина реалізована комплексно і з урахуванням сучасних вимог безпеки та зручності [15].

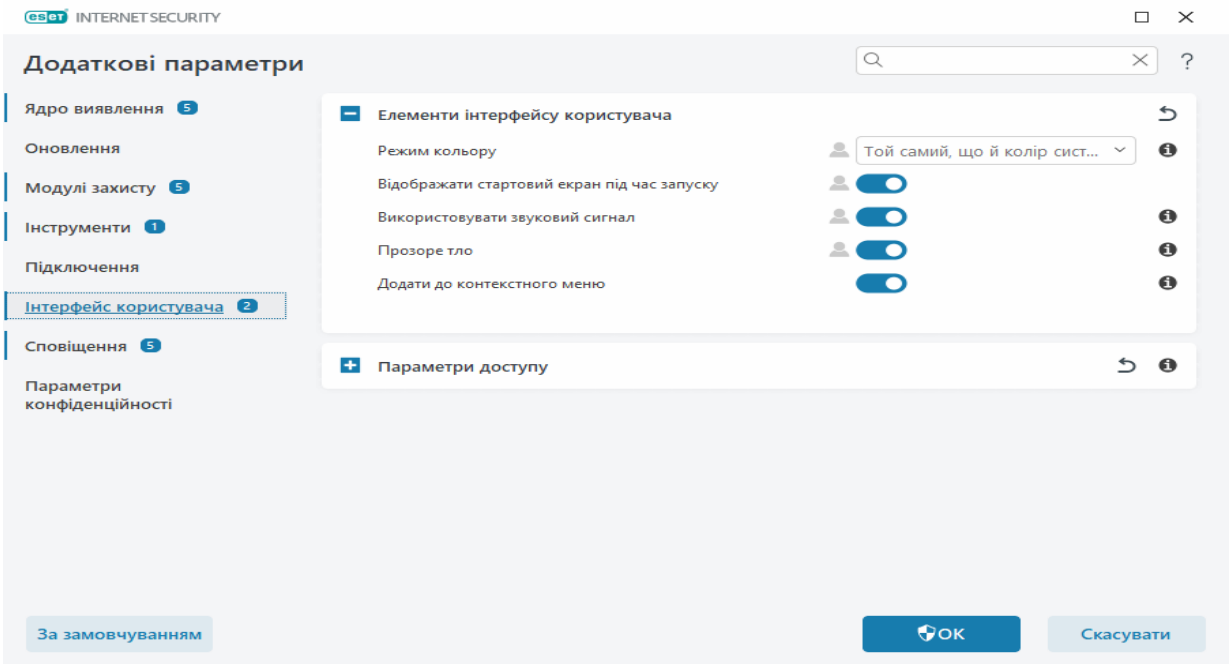

Рис. 2.2. Клієнтський інтерфейс ESET

Види інтерфейсів

Веб-інтерфейс – забезпечує доступ через браузер з будь-якого пристрою, підтримує всі сучасні браузери. Цей інтерфейс використовує протоколи HTTPS з TLS 1.2/1.3 для шифрування трафіку. Захист від XSS і CSRF атак реалізований через Content Security Policy (CSP) та механізми токенів захисту. Важливо, що на рівні UI застосовано механізми введення багатофакторної автентифікації – після введення логіна та пароля з’являється запит на OTP або біометрію [15].

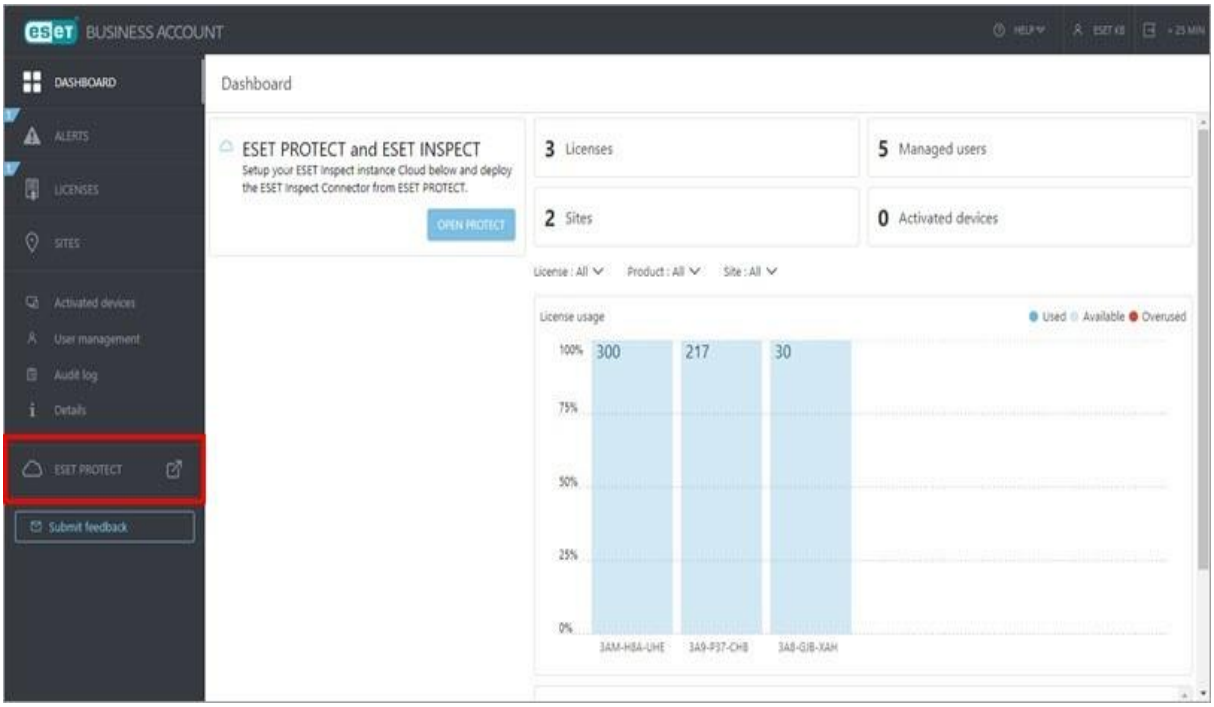

Рис. 2.3. Веб-інтерфейс ESET

Мобільний додаток – ESET Authenticator, що генерує OTP коди локально. Він не залежить від підключення до мережі, оскільки алгоритм TOTP заснований на синхронізації часу. Крім того, мобільний додаток має вбудовані механізми захисту: ключі зберігаються у Secure Enclave або Trusted Execution Environment, а сам додаток може вимагати додаткову аутентифікацію (PIN, біометрія), щоб запобігти несанкціонованому доступу [15].

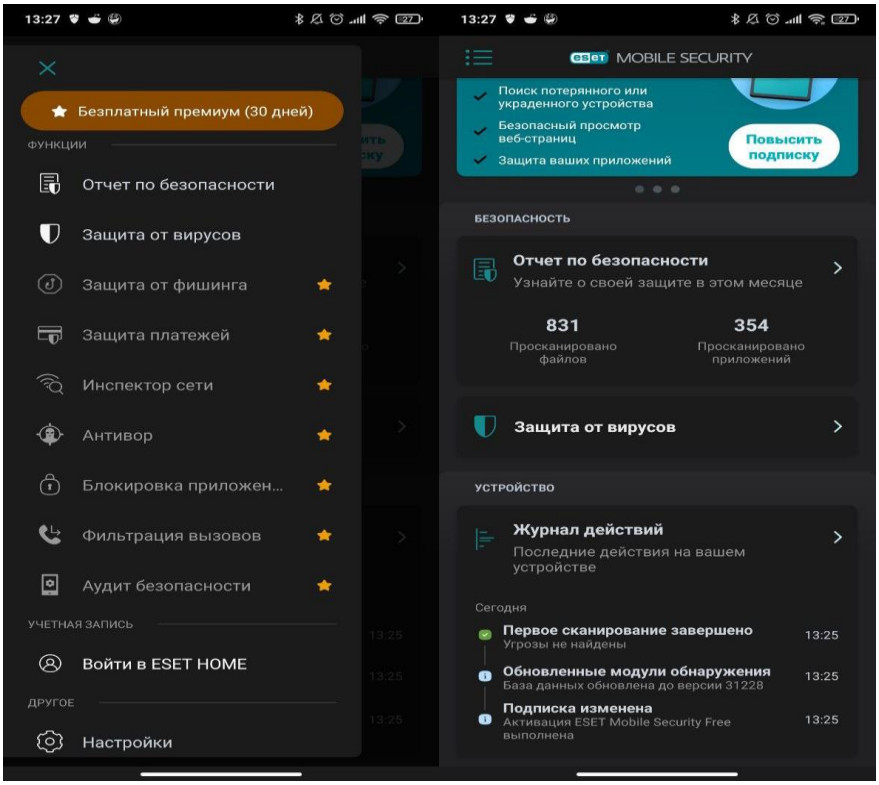

Рис. 2.4. Мобільний інтерфейс ESET

Десктопний клієнт – в корпоративних середовищах іноді використовується для інтеграції з локальними системами, наприклад, з Windows Logon або VPN клієнтами. Він підтримує взаємодію з сервером автентифікації через захищені канали [15].

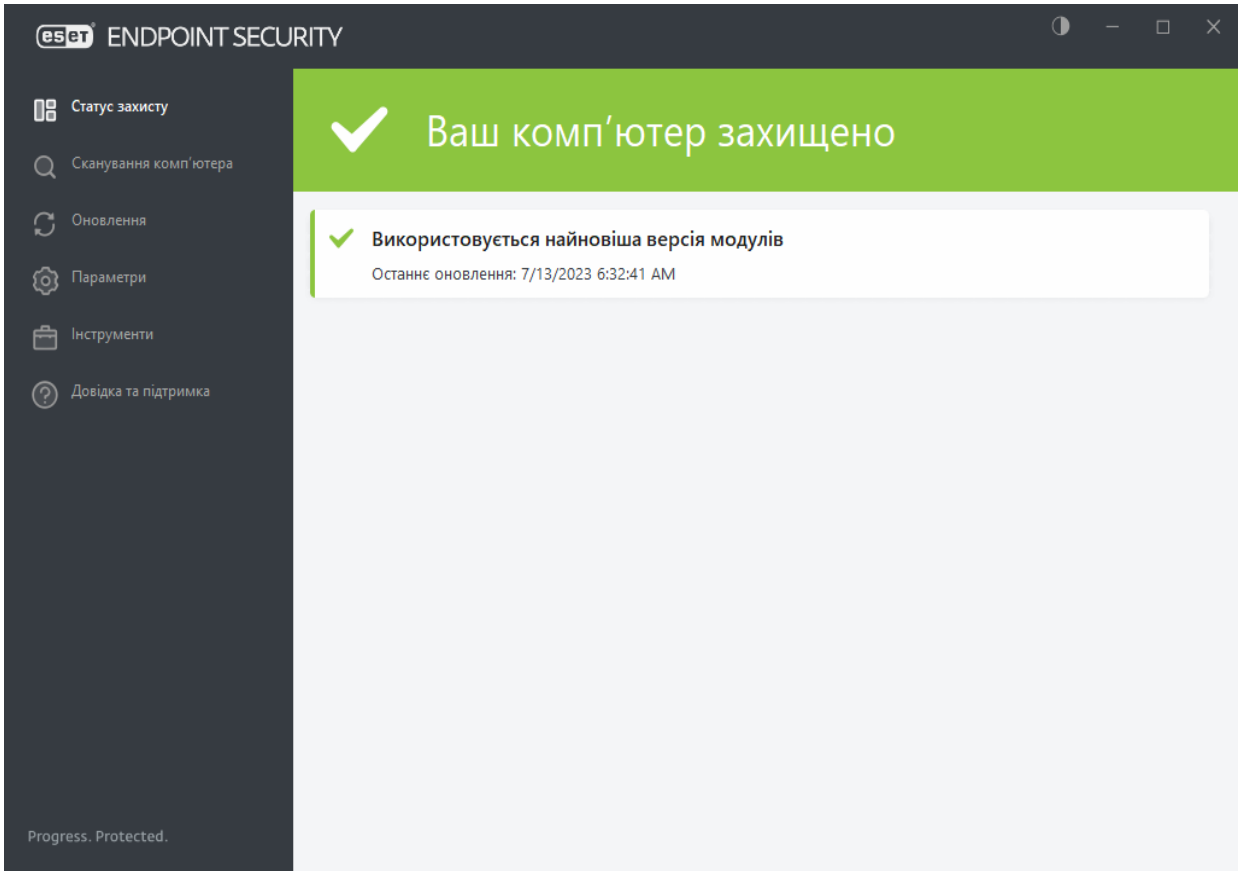

Рис. 2.5. Десктопний клієнт ESET

Безпека клієнтської частини

Особлива увага приділяється захисту секретів. На мобільних пристроях секретні ключі для OTP зберігаються в ізольованих середовищах (наприклад, Apple Secure Enclave) – це гарантує, що навіть при компрометації ОС отримати секретний ключ вкрай складно. При цьому сама передача початкових налаштувань (секретного ключа) відбувається через безпечний канал – наприклад, сканування QR-коду, створеного на сервері [15].

Для забезпечення зручності, додаток може автоматично оновлювати час синхронізації, щоб мінімізувати помилки у генерації OTP через зсув часу.

Крім того, UI реалізує механізми захисту від підробки – наприклад, перевірка цілісності додатку, сертифікатів, обмеження роботи на “рутованих” або “джейлбрейкнутих” пристроях [15].

Сервер автентифікаціїS

Сервер – це центральний елемент системи, що відповідає за перевірку достовірності користувача, контроль доступу, ведення логів та захист від атак [15].

Функції сервера

Інтеграція з LDAP/Active Directory: це дозволяє централізовано керувати доступом та групами користувачів. Сервер отримує інформацію про облікові записи, політики паролів, а також проводить перевірку статусу облікового запису (активний, заблокований, термін дії) [15].

Перевірка пароля: коли користувач вводить пароль, сервер порівнює хеш пароля з тим, що зберігається у базі. Паролі зберігаються у захищеному вигляді – як правило, із використанням стійких хеш-функцій, таких як Argon2 або bcrypt, що робить неможливим відновлення пароля з хешу [15].

Перевірка OTP: сервер отримує від клієнта одноразовий код, обчислює правильний OTP на основі збереженого секретного ключа та часу, порівнює коди. Якщо коди співпадають і код не використовувався раніше, доступ дозволяється [15].

Верифікація біометрії: сервер зберігає біометричні шаблони (зашифровані) і проводить порівняння, або, що частіше, передає це завдання на клієнтський пристрій (Edge-процесинг), що знижує ризики викрадення біометричних даних [15].

Аналітика безпеки: ведення журналів вхідних спроб, виявлення аномалій (наприклад, спроби входу з незвичних локацій, масові спроби входу), інтеграція з SIEM-системами для швидкого реагування [15].

Відмовостійкість: сервери налаштовані на кластеризацію та реплікацію даних, що забезпечує безперервну роботу системи навіть при виході з ладу окремих вузлів [15].

Захист від атак: сервер реалізує throttling – обмеження частоти запитів на автентифікацію від одного користувача або IP, а також застосовує CAPTCHA при підозрі на автоматизовані атаки [15].

База даних

База даних є центральним сховищем всіх критично важливих даних: облікові записи користувачів, хеші паролів, секретні ключі OTP, біометричні шаблони.

Організація даних

Дані структуровані у кілька таблиць: користувачі, ключі автентифікації, логи спроб входу, політики доступу [15].

Для біометричних даних зберігаються не повні відбитки пальців, а їхні шаблони, які містять стиснену та криптографічно захищену інформацію про унікальні характеристики [15].

Безпека даних

Дані зберігаються у зашифрованому вигляді – застосовується симетричне шифрування AES-256 з ключами, які зберігаються окремо у захищених модулях (Hardware Security Module – HSM) [15].

Всі доступи до БД суворо контролюються і аудитується. Адміністратори мають лише необхідні права доступу за принципом найменших привілеїв.

Запроваджені політики резервного копіювання та шифрування резервів.

Модуль генерації OTP (TOTP)

Одноразові паролі, що генеруються на основі часу, є найпоширенішим методом другої факторної автентифікації.

Як працює TOTP?

Ключова концепція базується на секретному ключі (shared secret), який генерується під час реєстрації користувача.

Обчислення OTP відбувається за формулою:

OTP = Truncate(HMAC-SHA1(secret_key, time_step))

де time_step – це кількість 30-секундних інтервалів, що пройшли від початку епохи (Unix time) [15].

Тобто в будь-який момент часу клієнт і сервер можуть обчислити однаковий код, не обмінюючись ним напряму, що не забиратиме лишнього часу, та наддасть швидку можливість отримання потрібних даних для обох сторін підвищивши за рахунок цього швидкість роботи системи [15].

Переваги:

1) Висока безпека: через короткий термін дії (30 секунд) код швидко стає недійсним.
2) Відсутність необхідності у мережі: код генерується локально на пристрої.

3) Універсальність: підтримка стандартів RFC 4226 (HOTP) та RFC 6238 (TOTP) дозволяє використовувати різні додатки.

Недоліки і способи їх мінімізації:

1) Зсув часу між сервером і клієнтом може призвести до відхилень. Для мінімізації застосовується «вікно» прийнятних кодів (наприклад, ±1 інтервал).
2) Ключ повинен бути надійно захищеним, щоб уникнути компрометації.

Біометричний модуль (Fingerprint)

Біометрія – це унікальний спосіб підтвердження особи, який важко підробити.

Технології сканування

Оптичні сенсори: роблять фотографію відбитка за допомогою світла. Вони досить прості, але менш стійкі до підробок.

Капацитивні сенсори: вимірюють електричні властивості шкіри. Використовуються у більшості сучасних смартфонів, бо забезпечують кращу якість [15].

Ультразвукові: створюють тривимірне зображення відбитка. Найбільш передові, мають високу стійкість до підробок.

Обробка біометричних даних

Після зняття відбитка система виділяє унікальні точки (мінутії) – місця перетину ліній, відгалуження, кінці.

Створюється математичний шаблон, який не зберігає самі зображення, а лише цифровий «відбиток відбитка».

Порівняння відбувається не по пікселях, а за набором характеристик, що дозволяє бути нечутливим до незначних пошкоджень шкіри [15].

Захист і конфіденційність

Шаблони зберігаються в зашифрованому вигляді, іноді навіть на локальному пристрої (Edge processing), щоб виключити можливість викрадення.

Біометричні дані не передаються через мережу у відкритому вигляді.

У разі невдалого розпізнавання пропонуються альтернативні методи автентифікації [15].

Протокол передачі даних

Для безпечної передачі автентифікаційних даних використовується TLS/SSL – криптографічний протокол, що забезпечує:

Шифрування каналу: всі дані (паролі, OTP, біометричні дані) передаються в зашифрованому вигляді, що унеможливлює їх перехоплення.

Аутентифікацію сервера: користувач впевнюється, що спілкується саме з офіційним сервером ESET, а не із зловмисником.

Цілісність даних: зміни у переданих повідомленнях виявляються [15].

2.2. Функції складових рішення автентифікації ESET

У багатофакторних системах автентифікації, особливо таких, що базуються на платформах ESET, кожен компонент виконує унікальну і критично важливу функцію, спрямовану на підтвердження особи користувача та захист системи від несанкціонованого доступу. Розглянемо детально основні складові цього процесу – логін і пароль, одноразовий код (OTP) та біометричний фактор у вигляді відбитка пальця [15].

Логін і пароль: основа традиційної автентифікації

Роль і призначення:

Логін і пароль є класичним способом ідентифікації користувача в будь-якій інформаційній системі. Логін (імена користувача) виконує функцію унікального ідентифікатора, що однозначно визначає конкретний обліковий запис у базі даних системи. Пароль, у свою чергу, є конфіденційним секретом, відомим лише користувачу, що дозволяє підтвердити його особу [15].

Покрокова робота механізму:

Введення облікових даних: Користувач вводить свій логін і пароль у клієнтському інтерфейсі (веб-додатку, десктопній програмі чи мобільному додатку).

Передача даних на сервер: Введені дані через захищений канал передачі (TLS/SSL) доставляються до сервера автентифікації.

Перевірка пароля: Сервер застосовує алгоритми хешування з додаванням «солі» (унікального випадкового рядка), наприклад bcrypt або Argon2, для перетворення пароля в хеш-значення. Потім отримане хеш-значення порівнюється з записом у базі даних [15].

Прийняття рішення: Якщо логін існує в базі і хеш пароля співпадає з збереженим, користувач проходить перший етап аутентифікації. В іншому випадку система фіксує невдалу спробу [15].

Ведення журналів: Усі спроби входу записуються у лог-файли для подальшого аудиту та аналізу безпеки.

Функції та особливості:

Ідентифікація користувача: Логін дозволяє системі визначити, до якого облікового запису відноситься запит.

Конфіденційність: Пароль гарантує, що лише власник облікового запису може отримати доступ.

Захист від атак: Використання хешування та солі ускладнює атаки перебору паролів і захищає від радужних таблиць.

Обмеження доступу: Система блокує акаунти після п’яти невдалих спроб введення пароля, щоб запобігти автоматизованому підбору [15].

Політика складності: Для підвищення безпеки організації застосовують вимоги до паролів: мінімальна довжина, використання великих і малих літер, цифр та спеціальних символів [15].

Механізми відновлення: У разі втрати пароля система передбачає безпечну процедуру його скидання через підтвердження по електронній пошті або SMS.

Одноразовий код (OTP): динамічний другий фактор автентифікації

Роль і призначення:

Одноразовий пароль (One-Time Password, OTP) є додатковим фактором автентифікації, який забезпечує тимчасовий динамічний код, що використовується лише один раз у межах обмеженого часу. OTP істотно підвищує рівень безпеки, ускладнюючи доступ зловмисникам навіть у випадку компрометації логіна і пароля [15].

Принцип роботи:

1) Генерація секретного ключа: Під час налаштування системи для користувача генерується унікальний секретний ключ, який зберігається на сервері і у клієнтському додатку (наприклад, ESET Authenticator).
2) Алгоритм генерації коду: На базі секретного ключа і поточного часу (зазвичай інтервал 30 секунд) за стандартом RFC 6238 застосовується алгоритм TOTP (Time-based One-Time Password). Клієнтський додаток генерує новий код кожні 30 секунд.
3) Введення коду: При автентифікації користувач вводить поточний код із мобільного додатку.
4) Перевірка на сервері: Сервер обчислює очікуваний код з використанням того ж секретного ключа і порівнює його з введеним.
5) Результат: Якщо коди співпадають і час дії не минув, другий фактор автентифікації вважається успішним [15].

Функції і значення:

1) Динамічність: Кожен код дійсний лише протягом короткого проміжку часу (зазвичай 30 секунд), що виключає його повторне використання.
2) Захист від компрометації: Навіть якщо логін і пароль були викрадені, без OTP отримати доступ неможливо.
3) Відсутність залежності від мережі: Генерація коду відбувається локально у додатку, що зменшує ризик втручання при передачі даних.
4) Простота інтеграції: ESET інтегрує підтримку стандарту TOTP у свої системи, що дозволяє використовувати будь-які сумісні додатки.
5) Гнучкість: Адміністратори можуть встановлювати політики щодо обов’язковості використання OTP для різних категорій користувачів.
6) Безпека: Сервер зберігає секретні ключі у зашифрованому вигляді та застосовує заходи для захисту від несанкціонованого доступу до них [15].

Біометричний фактор у вигляді відбитка пальця: підтвердження особи за фізіологічними характеристиками

Роль і призначення:

Біометрична автентифікація заснована на унікальних фізіологічних або поведінкових характеристиках людини. Використання відбитка пальця – одна з найнадійніших і найпоширеніших форм біометрії, що забезпечує високу точність і зручність ідентифікації [15].

Процес роботи:

1) Зчитування відбитка: Користувач прикладає палець до сканера відбитків, який може бути апаратним пристроєм на ноутбуці, мобільному телефоні або зовнішнім сенсором.
2) Обробка зображення: Система аналізує рельєф папілярних ліній, виокремлює ключові характеристики (мінутії) і формує математичний шаблон.
3) Порівняння з базою: Отриманий шаблон порівнюється із збереженими у базі біометричними даними користувача.
4) Прийняття рішення: Якщо співпадіння відповідає визначеному порогу (наприклад, 95% збіг), автентифікація вважається успішною [15].

Основні функції:

1) Унікальність: Кожна людина має неповторний відбиток пальця, що унеможливлює підробку.
2) Зручність і швидкість: Процес сканування та порівняння триває секунди, що пришвидшує доступ.
3) Безпека зберігання: Біометричні шаблони зберігаються у зашифрованому вигляді і не можуть бути відновлені у вигляді реального зображення.
4) Захист від фальсифікації: Використання технологій виявлення «живого» пальця (liveness detection) – перевірка температури, реакції на дотик, електропровідності.
5) Інтеграція: ESET використовує стандартні API операційних систем (наприклад, Windows Biometric Framework), що забезпечує надійну роботу з різноманітними пристроями.
6) Комбінування з іншими факторами: Біометрія виступає як третій рівень захисту, доповнюючи пароль та OTP, підвищуючи рівень впевненості в ідентифікації користувача [15].

Загальна роль та синергія складових

Окремо кожен фактор має власну цінність, але їх поєднання створює багатофакторну систему, в якій ризик компрометації знижується експоненційно.

Логін і пароль – це перша лінія захисту, яка вимагає базової перевірки [15].

OTP надає динамічний другий фактор, що ускладнює несанкціонований доступ навіть при викраденні пароля.

Біометричний фактор додає «фізичний» рівень перевірки, що неможливо підробити дистанційно [15].

Ця комбінація забезпечує:

Високий рівень безпеки для захисту важливих корпоративних ресурсів.

Зручність користувача, оскільки процес не вимагає надмірних дій або складних налаштувань.

Гнучкість і масштабованість системи завдяки модульній архітектурі та підтримці сучасних стандартів [15].

Таблиця 2.1.

Функції складових багатофакторної автентифікації

Компонент	**Основні функції**	**Особливості**	**Значення для безпеки**
Логін і пароль	Ідентифікація користувача, перевірка пароля, контроль доступу	Хешування пароля, політика складності, блокування після 5 невдалих спроб	Перша лінія захисту, основа системи
Одноразовий код (OTP)	Генерація динамічного коду, перевірка коду на сервері	Коди дійсні 30 секунд, відсутність залежності від мережі	Другий фактор, ускладнює несанкціонований доступ
Біометричний фактор	Зчитування відбитка,	Зберігання зашифрованих	Третій фактор, унікальна

	формування шаблону, порівняння з базою	шаблонів, виявлення «живого» пальця	фізіологічна перевірка

Рис. 2.6. Архітектура багатофакторної автентифікації

3 РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ ЗАСОБІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

3.1. Розробка варіанту засобу автентифікації користувачів на прикладі багатофакторної системи

Розробка варіанту засобу автентифікації користувачів на прикладі багатофакторної системи є комплексним процесом, що включає кілька етапів, спрямованих на створення надійного, зручного та безпечного механізму підтвердження особи користувача в інформаційно-комунікаційних системах. Цей процес передбачає детальне опрацювання як технічних, так і організаційних аспектів автентифікації [16].

Перший етап – аналіз вимог та умов експлуатації системи. На цьому кроці визначаються цілі впровадження багатофакторної автентифікації, рівень безпеки, який необхідно забезпечити, а також типи користувачів і пристроїв, з яких здійснюватиметься доступ. Важливо з’ясувати, які саме фактори автентифікації будуть прийнятні для користувачів з урахуванням специфіки їх діяльності, а також розглянути можливі обмеження, такі як швидкість доступу, зручність, сумісність із наявною IT-інфраструктурою [16].

Другий етап – вибір і комбінування факторів автентифікації. Зазвичай це поєднання трьох типів: щось, що користувач знає (пароль, PIN-код), щось, що користувач має (смартфон для отримання OTP, апаратний токен) та щось, що є унікальним для користувача (біометричні дані – відбитки пальців, розпізнавання обличчя, сітчатка ока). Важливо, щоб ці фактори були незалежними, що значно ускладнює можливість компрометації облікового запису. Особливо актуальним є додавання біометричних факторів, які надають високий рівень захисту, оскільки їх складно підробити [16].

Третій етап – розробка архітектури системи. Вона включає сервер автентифікації, що обробляє всі запити, бази даних для збереження інформації про користувачів та їх фактори автентифікації, а також механізми інтеграції із зовнішніми сервісами, наприклад, для генерації одноразових кодів (OTP). На цьому етапі особлива увага приділяється питанням безпеки передачі даних, шифруванню та захисту від атак типу «людина посередині», щоб гарантувати конфіденційність і цілісність інформації під час автентифікації [16].

Четвертий етап – реалізація та тестування. Включає розробку програмного забезпечення або налаштування існуючих рішень, інтеграцію з корпоративними інформаційними системами, а також створення зручного інтерфейсу для користувачів. Тестування проводиться з метою перевірки коректності роботи всіх факторів, оцінки часу автентифікації, а також визначення можливих слабких місць, які можуть бути використані зловмисниками [16].

П’ятий етап – впровадження і навчання користувачів. Для успішного застосування багатофакторної автентифікації необхідно провести інформаційну роботу, пояснити переваги та принципи роботи системи, навчити користувачів правильному використанню всіх факторів, а також організувати підтримку у разі виникнення проблем із доступом [16].

Завершальний етап – моніторинг і підтримка. Система багатофакторної автентифікації потребує постійного контролю за її ефективністю, оновлення засобів безпеки відповідно до нових загроз, а також адаптації під змінні умови роботи організації. Регулярний аудит безпеки дозволяє своєчасно виявляти потенційні вразливості та усувати їх, що забезпечує безперервний захист інформаційних ресурсів [16].

Таким чином, розроблений варіант багатофакторної автентифікації дозволяє значно підвищити рівень безпеки інформаційно-комунікаційної системи, знизити ризики несанкціонованого доступу та забезпечити надійний контроль за користувачами, зберігаючи при цьому зручність і швидкість доступу до ресурсів системи. Цей підхід відповідає сучасним стандартам інформаційної безпеки та може бути ефективно впроваджений у різних сферах діяльності [16].

Архітектура багатофакторної системи автентифікації

Основні компоненти:

Клієнтський пристрій: ПК, смартфон або інший гаджет, через який користувач здійснює вхід у систему. Пристрій може підтримувати біометричні методи автентифікації, а також зберігати токени доступу для спрощення подальших входів.

Інтерфейс автентифікації: Програмне забезпечення, яке взаємодіє з користувачем – це може бути веб – сторінка або мобільний додаток. Воно збирає фактори автентифікації (логін, пароль, OTP, біометрію) і передає їх на сервер для перевірки [16].

Сервер автентифікації: Виконує перевірку кожного фактора автентифікації, обробляє логіку прийняття рішення про дозвіл або відмову у доступі, а також управляє видачею токенів доступу.

Система управління обліковими записами (IAM): Відповідає за керування користувачами, їх ролями та правами доступу, а також зберігає історію сесій і дій для подальшого аудиту.

База даних безпеки: Зберігає захищені копії паролів у вигляді хешів з сіллю, відкриті ключі для криптографії, шаблони біометричних даних, які не можуть бути відтворені.

Логи та моніторинг: Фіксує всі події, пов’язані з автентифікацією – успішні та неуспішні спроби входу, зміни у правах доступу, а також інші події, які потрібні для аналізу безпеки і виявлення потенційних загроз [16].

Детальний покроковий процес автентифікації

Ідентифікація: Починається з того, що користувач вводить свій логін або інший унікальний ідентифікатор, який дозволяє системі визначити його особу. Після цього відбувається перевірка першого фактора – пароля. Сервер порівнює введений пароль з хешем, що зберігається у базі даних. Якщо пароль неправильний, доступ відразу блокується, а сама спроба фіксується для подальшого аналізу безпеки [16].

Перевірка першого фактора (пароль): Сервер порівнює введений пароль із збереженим у базі даних хешем пароля. Якщо пароль неправильний, доступ блокується, а спроба фіксується для подальшого аналізу.

Ініціація другого фактора: Якщо пароль вірний, сервер запитує другий фактор автентифікації – це може бути код одноразового пароля (OTP), підтвердження через апаратний токен або біометрична перевірка.

Перевірка другого фактора: Користувач вводить або надає другий фактор. Сервер перевіряє коректність.

Видача токена доступу: Якщо обидва фактори підтверджені, користувачу надається сесія або токен доступу, наприклад JSON Web Token (JWT), що дозволяє йому користуватися системою без повторної автентифікації протягом певного часу.

Журналювання: Всі дії під час процесу автентифікації, включно з введенням логіну, пароля, другого фактора і видачею токена, записуються для подальшого аудиту [17].

Механізми відновлення доступу та потенційні проблеми

Втрата пристрою: Користувач може випадково втратити смартфон з додатком для генерації одноразових паролів (OTP) або апаратний токен. Щоб забезпечити доступ у таких випадках, вводяться резервні коди – одноразові паролі, згенеровані заздалегідь і збережені користувачем у безпечному місці. Альтернативним способом є багатокрокова верифікація через службу підтримки, що передбачає додаткову перевірку особистості користувача, наприклад, шляхом пред’явлення документів або телефонного дзвінка [17].

Помилки біометрії: Можуть призводити до відмови у доступі навіть легітимним користувачам через неточності у зчитуванні відбитків пальців, обличчя чи інших параметрів. Для уникнення таких ситуацій впроваджують резервні методи автентифікації, які дозволяють користувачу підтвердити особу іншим способом, наприклад, за допомогою пароля або додаткового фактора [17].

Атаки соціальної інженерії: Один з основних ризиків, коли зловмисники намагаються обманом отримати доступ до системи через користувачів або адміністраторів. Для мінімізації цих загроз необхідно регулярно проводити

навчання персоналу і користувачів, роз’яснювати методи розпізнавання шахрайських дій і формувати культуру безпеки, щоб уникнути передачі конфіденційної інформації стороннім особам [17].

3.2. Рекомендації щодо використання засобів ідентифікації користувачів в інформаційно-комунікаційній системі

Для забезпечення надійної та безпечної ідентифікації користувачів у інформаційно-комунікаційних системах (ІКС) необхідно дотримуватися комплексного підходу, який включає технічні, організаційні та процедурні заходи. Основна мета – захистити систему від несанкціонованого доступу, забезпечити конфіденційність, цілісність та доступність даних.

Політика доступу та управління ролями

Розмежування ролей: Передбачає, що кожен користувач отримує лише ті права доступу, які необхідні для виконання його функціональних обов’язків. Цей підхід базується на принципі мінімальних привілеїв, що дозволяє зменшити ризик несанкціонованого доступу та помилок через надлишкові права [18].

Визначення груп користувачів: Створення категорій, таких як адміністратори, звичайні користувачі та гості, кожна з яких має свій рівень доступу і вимоги до автентифікації. Адміністратори, наприклад, мають розширені права для управління системою, тоді як гості мають обмежений доступ тільки до певних ресурсів.

Регулярний аудит: Періодичний перегляд наданих доступів з метою видалення непотрібних акаунтів, а також коригування прав у разі зміни посад або функціональних обов’язків користувачів. Це допомагає підтримувати актуальний і безпечний рівень доступу в системі [18].

Вимоги до паролів та управління ними

Складність: Використанням довгих комбінацій, що містять не менше дванадцяти символів, обов’язково включаючи великі і малі літери, цифри та

спеціальні символи. Такий підхід підвищує стійкість паролів до підбору або атак методом перебору, роблячи їх більш захищеними.

Унікальність: Заборона на повторне використання тих самих комбінацій для різних облікових записів або під час наступної зміни. Крім того, важливо впроваджувати механізми перевірки паролів на витоки у загальнодоступних базах даних, щоб своєчасно ідентифікувати потенційно скомпрометовані паролі і вимагати їх заміни [18].

Регулярна зміна: Рекомендується проводити з певною періодичністю, наприклад, кожні три-шість місяців, проте при цьому слід стежити, щоб користувачі не спрощували свої паролі для полегшення запам’ятовування. Важливо збалансувати вимоги до безпеки і зручності, щоб уникнути ослаблення захисту через надмірну частоту змін [18].

Менеджери паролів: Є корисним інструментом, який рекомендується для безпечного збереження і генерації складних паролів. Вони дозволяють користувачам не запам’ятовувати всі комбінації, а використовувати унікальні, надійні паролі для кожного сервісу, що значно підвищує загальний рівень безпеки.

Навчання користувачів

Тренінги: Включають регулярне проведення навчальних сесій, спрямованих на підвищення обізнаності користувачів щодо безпечного поводження з обліковими даними. Вони допомагають користувачам розуміти основні загрози та методи захисту, що значно знижує ризик компрометації системи через людський фактор [18].

Роз’яснення: Як розпізнавати фішинг та соціальну інженерію, а також на важливості не передавати паролі або одноразові паролі (OTP) третім особам. Це дозволяє користувачам бути пильними і уникати поширених пасток, що використовуються зловмисниками для отримання доступу до облікових записів.

Тестування: Проведення імітаційних атак, наприклад, фішингових кампаній, з метою перевірки готовності користувачів і їх здатності реагувати на потенційні загрози. Такий підхід допомагає виявити слабкі місця в безпековій культурі організації та підвищити рівень захисту через практичний досвід [18].

Адаптивна автентифікація

Контекстна оцінка: Система аналізує додаткові параметри, такі як геолокація користувача, IP-адреса, час доступу та тип пристрою, з якого здійснюється вхід. На основі оцінки ризику система може підвищувати вимоги до автентифікації, наприклад, запитувати додатковий фактор підтвердження особистості, якщо активність здається підозрілою або незвичною [18].

Повідомлення користувачів: При виявленні підозрілих спроб входу їм надсилаються сповіщення через SMS або електронну пошту. Це дозволяє користувачам швидко реагувати на потенційні загрози і вчасно вживати заходів, наприклад, змінити пароль або звернутися до служби підтримки [18].

Використання штучного інтелекту: Допомагає автоматично виявляти аномальну поведінку користувачів, аналізуючи великі обсяги даних і шукаючи шаблони, які можуть свідчити про несанкціонований доступ або спроби атаки. Це підвищує ефективність захисту і дозволяє швидше реагувати на загрози.

Захист каналів зв'язку і збереження даних

Шифрування трафіку: Забезпечується за допомогою протоколів TLS, які гарантують захист даних під час їх передачі між користувачем і сервером. Це означає, що інформація не може бути перехоплена або змінена зловмисниками у процесі передачі, що особливо важливо для конфіденційних даних, таких як паролі, персональна інформація чи фінансові дані [18].

Захищене зберігання: Передбачає використання хешування і соління для паролів. Хешування перетворює пароль у зашифрований код, а сіль додає унікальність, щоб унеможливити відновлення оригінального пароля навіть у разі витоку даних. Біометричні дані зберігаються у вигляді шаблонів, які є математичними представленнями відбитків пальців, обличчя чи інших унікальних ознак користувача і не можуть бути відтворені в оригінальному вигляді, що запобігає їх крадіжці або зловживанню [18].

Обмеження кількості спроб: Блокування облікового запису після кількох невдалих спроб аутентифікації. Це допомагає запобігти атакам типу brute-force, при яких зловмисник намагається підібрати пароль шляхом багаторазового введення

варіантів. Блокування може бути тимчасовим або вимагати додаткового підтвердження особистості користувача.

Регулярне оновлення систем: Своєчасне встановлення патчів та оновлень безпеки, які виправляють виявлені уразливості і покращують захист від нових загроз. Це дозволяє підтримувати систему у актуальному стані, знижує ризик експлуатації відомих вразливостей і забезпечує стабільну роботу безпекових механізмів. Ігнорування оновлень може призвести до успішних атак і компрометації даних [18].

Моніторинг та аудит

Журналювання: Автоматичний процес запису всіх дій користувачів у системі. До таких дій належать вхід та вихід з системи, спроби доступу, а також будь-які зміни в налаштуваннях або роботі з даними. Завдяки журналюванню можна відстежити хронологію подій, виявити несанкціонований доступ або помилки в роботі користувачів. Наприклад, до журналу заносяться успішні та неуспішні спроби аутентифікації, зміна паролів, редагування важливих файлів чи зміни прав доступу [18].

Аналіз: Полягає у регулярному перегляді цих журналів, що дозволяє виявляти аномалії – дії, які виходять за межі нормальної поведінки користувачів або системи. Це можуть бути численні невдалі спроби входу за короткий проміжок часу, доступ із незвичних локацій або IP-адрес, а також несанкціоновані зміни у правах доступу. Для цього часто використовують спеціалізовані системи управління подіями безпеки (SIEM), які автоматизують пошук і класифікацію подій.

Оповіщення: Забезпечують автоматичне повідомлення адміністратора або команди безпеки про підозрілі активності. Це можуть бути електронні листи, SMS, повідомлення у системах моніторингу або push-повідомлення. Сповіщення запускаються, наприклад, при серії невдалих входів, спробі доступу з незвичних місць або при отриманні прав адміністратора без відповідного дозволу [18].

Відновлення: Наявність чіткого плану дій у випадку інцидентів безпеки. План включає ідентифікацію та локалізацію інциденту, усунення наслідків

(наприклад, блокування облікових записів), відновлення нормальної роботи системи, а також аналіз причин інциденту для запобігання повторенню подібних випадків. Такий підхід дозволяє швидко реагувати на загрози і мінімізувати можливі збитки.

ВИСНОВКИ

Розділ 1.

У ході аналізу проблеми автентифікації користувачів в інформаційно-комунікаційній системі було встановлено, що автентифікація є ключовим етапом забезпечення інформаційної безпеки, що гарантує доступ лише уповноваженим користувачам.

Проаналізовані основні ризики і загрози, що пов’язані з ідентифікацією користувачів, включають загрозу компрометації паролів, фішингові атаки, крадіжку облікових даних, а також атаки типу «людина посередині». Ці ризики свідчать про необхідність впровадження більш надійних методів автентифікації.

Розглянуті сучасні підходи до автентифікації показали, що найбільш ефективними є багатофакторні системи, які поєднують кілька факторів: знання, володіння та біометрію. Використання одноразових паролів (OTP) та біометричних факторів суттєво підвищує рівень безпеки систем.

Проаналізовані існуючі рішення автентифікації, серед яких Microsoft Azure AD, Okta, Duo Security, Google Identity Platform та ESET Secure Authentication, демонструють широкий спектр функціональних можливостей та високий рівень захисту. Впровадження таких рішень у інформаційно-комунікаційних системах дозволяє значно знизити ризики несанкціонованого доступу.

Отже, для підвищення захищеності інформаційних систем рекомендується використовувати багатофакторні засоби автентифікації, які поєднують сучасні технології та відповідають специфічним вимогам організації.

Розділ 2.

Вивчення архітектури рішення ESET Secure Authentication показало, що воно побудоване за модульним принципом, що включає сервер автентифікації, клієнтські додатки та інтеграційні плагіни для різних систем. Така архітектура забезпечує гнучкість, масштабованість і можливість інтеграції з різними інформаційно-комунікаційними системами.

Основними функціями складових рішення ESET є генерація одноразових паролів (OTP), підтримка багатофакторної автентифікації, а також використання біометричних факторів, зокрема відбитків пальців, для підвищення рівня безпеки. Завдяки мобільному додатку користувачі можуть швидко і зручно підтверджувати свою особистість, що суттєво знижує ризик компрометації облікових даних.

Використання одноразових кодів OTP у поєднанні з біометрією дозволяє реалізувати надійну багатофакторну автентифікацію, яка відповідає сучасним вимогам інформаційної безпеки. Завдяки архітектурі ESET рішення легко адаптується під потреби різних організацій і забезпечує високий рівень захисту від несанкціонованого доступу.

Отже, впровадження засобів автентифікації на базі архітектури ESET з використанням OTP та біометричних факторів є ефективним і доцільним кроком для підвищення безпеки інформаційно-комунікаційних систем.

Розділ 3.

У процесі розробки варіанту засобу автентифікації користувачів на прикладі багатофакторної системи було встановлено, що впровадження багатофакторної автентифікації суттєво підвищує рівень захисту інформаційно-комунікаційних систем. Поєднання різних факторів — знання (пароль), володіння (мобільний пристрій або токен) та біометрії (відбиток пальця) — дозволяє мінімізувати ризики несанкціонованого доступу навіть у разі компрометації одного з факторів.

Рекомендації щодо використання засобів ідентифікації користувачів передбачають впровадження адаптивних систем автентифікації, які враховують контекст доступу (наприклад, геолокацію, час, тип пристрою). Це дозволяє балансувати між зручністю користувачів і безпекою системи. Крім того, важливо забезпечити навчання користувачів та впровадження політик безпеки, що регламентують використання засобів автентифікації, а також регулярний аудит та оновлення систем для протидії новим загрозам.

Враховуючи сучасні виклики кібербезпеки, рекомендується активно впроваджувати багатофакторні засоби автентифікації з використанням сучасних технологій, таких як одноразові коди (OTP) та біометричні фактори, зокрема

відбитки пальців. Це дозволить ефективно захищати інформаційні ресурси та підвищити довіру користувачів до системи.

ПОСИЛАННЯ

1. Authentication – OWASP Cheat Sheet Series. OWASP.
URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (дата звернення: 20.05.2025).
2. NIST Special Publication 800-63B: Digital Identity Guidelines. National Institute of Standards and Technology.
URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf (дата звернення: 20.05.2025).
3. Authentication methods and features – Microsoft Entra ID. Microsoft Learn.
URL: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods (дата звернення: 20.05.2025).
4. Автентифікація без пароля? Друкарня.
URL: https://drukarnia.com.ua/articles/avtentifikaciya-bez-parolya-Kq2Rg (дата звернення: 20.05.2025).
5. Fingerprint recognition. National Cyber Security Centre (NCSC), UK.
URL: https://www.ncsc.gov.uk/collection/biometrics/fingerprint (дата звернення: 20.05.2025).
6. The Dangers of Facial Recognition Technology. Syracuse University Surface.
URL:
https://surface.syr.edu/cgi/viewcontent.cgi?article=2479&context=honors_capstone
(дата звернення: 20.05.2025).
7. Iris Scans Come to Nursing Homes. Next Stop, Your Phone. Wired.
URL: https://www.wired.com/2017/04/iris-scans-come-nursing-homes-next-stop-phone
(дата звернення: 20.05.2025).
8. Що таке голосова біометрія: як працює і в чому переваги. PSM7.
URL: https://psm7.com/uk/analytics/chto-takoe-golosovaya-biometriya-kak-rabotaet-i-v-chem-preimushhestva.html (дата звернення: 20.05.2025).
9. What is Adaptive Authentication? VPN Unlimited.
URL: https://www.vpnunlimited.com/ua/help/cybersecurity/adaptive-authentication
(дата звернення: 20.05.2025).

10. How effective is multifactor authentication at deterring cyberattacks? Microsoft Research.
URL: https://www.microsoft.com/en-us/research/publication/how-effective-is-multifactor-authentication-at-deterring-cyberattacks (дата звернення: 20.05.2025).
11. Use of Multi-Factor Authentication (MFA) Nearly Doubles Since 2020, New Okta Secure Sign-In Trends Reports Finds. Okta.
URL: https://www.okta.com/press-room/okta-secure-sign-in-trends-report-2022 (дата звернення: 20.05.2025).
12. Multi-Factor Authentication (MFA). Duo Security.
URL: https://duo.com/product/multi-factor-authentication-mfa (дата звернення: 20.05.2025).
13. Adding multi-factor authentication to your web app. Google Cloud Identity Platform Documentation.
URL: https://cloud.google.com/identity-platform/docs/mfa (дата звернення: 20.05.2025).
14. Enhancing Security: Multifactor Authentication. ESET.
URL: https://www.eset.com/int/about/newsroom/press-releases/article/enhancing-security-multifactor-authentication (дата звернення: 20.05.2025).
15. Overview | ESET Secure Authentication On-Prem 3.0. ESET Online Help.
URL: https://help.eset.com/esa/3/en-US/index.html (дата звернення: 20.05.2025).
16. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management
URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата звернення: 20.05.2025)
17. Lessons Learnt from a 2FA roll out within a higher education organisation. arXiv.
URL: https://arxiv.org/abs/2011.02901 (дата звернення: 20.05.2025).
18. Методичні рекомендації щодо впровадження засобів автентифікації користувачів в інформаційно-комунікаційній системі. Державна служба спеціального зв'язку та захисту інформації України.
URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53982 (дата звернення: 20.05.2025).