Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Пирч Олени Вадимівни

на здобуття ступеня вищої освіти магістра

Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

КРМКБЗІ. 2301149.23.01.08 ПЗ

Виконав студент 2 курсу група КБЗІм-23-1 Олена ПИРЧ
Керівник канд. техн. наук, доцент Віра ТІТОВА
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16 12 2024 р.

Хмельницький 2024

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 2 09 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі		Виконано
Визначення змісту, структури кваліфікаційної роботи		Виконано
Підготовка першого розділу кваліфікаційної роботи		Виконано
Підготовка другого розділу кваліфікаційної роботи		Виконано
Підготовка третього розділу кваліфікаційної роботи		Виконано
Підготовка статті/тези за темою кваліфікаційної роботи		Виконано
Підготовка четвертого розділу кваліфікаційної роботи		Виконано
Підготовка та оформлення ілюстративного матеріалу		Виконано
Оформлення кваліфікаційної роботи		Виконано
Попередній захист кваліфікаційної роботи		Виконано
Захист кваліфікаційної роботи на засіданні ЕК		Виконано

Студент _____ Олена ПИРЧ

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

2 09 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Пирч Олені Вадимівні

1 Тема роботи Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації

Керівник роботи канд.техн.наук, доцент Віра ТІТОВА

Затверджено наказом ректора університету від 26 08 2024 № 60

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи спроєктувати та змоделювати метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих систем аутентифікації, провести дослідження вже існуючої схеми аутентифікації, покращити систему аутентифікації підприємства на основі доступних даних. Провести розрахунок ефективності впроваджених рішень та надати рекомендації для подальшої експлуатації

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ, Огляд існуючих рішень у сфері захисту інформації, Розробка методу підвищення стійкості ЕЦП, Практична реалізація та тестування методу підвищення стійкості ЕЦП, проведення тестування системи та порівняння результатів, Висновки

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації».

Автор роботи: Пирч Олена Вадимівна.

Керівник роботи: к.т.н, доц. Тітова Віра Юріївна

Загальний обсяг роботи: 88 сторінок, 27 рисунків, 1 таблиця, 64 посилань.

Ключові слова: електронний цифровий підпис, комбіновані схеми аутентифікації, контекстуальна аутентифікація, біометрія, штучний інтелект.

Мета даної роботи полягає у розробці методу підвищення стійкості електронного підпису, задля покращення рівня безпеки підприємства або компанії, з використанням комбінованих схем аутентифікації.

В роботі запропоновано метод впровадження комбінованих схем аутентифікації який складається з об'єднанням контекстуальної аутентифікації та біометрії. Даний метод дає можливість ідентифікувати зловмисників та їхні спроби увійти у систему, фільтрувати користувачів, та покращувати систему безпеки за рахунок постійного покращення технології штучного інтелекту, використовуючи новітнє програмне забезпечення.

02.12.2024

ANNOTATION

Theme of the qualification work: "A method for increasing the stability of an electronic digital signature through combined authentication schemes".

Author of the work: Pyrch Olena Vadymivna.

Supervisor: Pd.D Titova Vira Yuriyivna.

Total volume of work: 88 pages, 27 figures, 1 table, 64 references.

Keywords: electronic digital signature, combined authentication schemes, contextual authentication, biometrics, artificial intelligence.

The purpose of this work is to develop a method for increasing the stability of an electronic signature in order to improve the security level of an enterprise or company using combined authentication schemes.

The work proposes a method for implementing combined authentication schemes that combines contextual authentication and biometrics. This method makes it possible to identify intruders and their attempts to log in, filter users, and improve the security system by continuously improving artificial intelligence technology using the latest updates of the software.

02. 12. 2024

ЗМІСТ

ВСТУП

У сучасному цифровому суспільстві електронний цифровий підпис, надалі будемо називати його ЕЦП, є ключовим інструментом для забезпечення захисту інформації та юридичної сили електронних документів, тобто затвердження документів дистанційно, за неможливості бути присутнім особисто під час підписання контрактів. Використання ЕЦП дозволяє підвищити ефективність роботи організацій, оптимізувати документообіг і зменшити витрати, пов'язані з обробкою паперових документів. Під час пандемії у 2020 році ЕЦП набрав ще більшої популярності аніж раніше, проте, розвиток інформаційних технологій супроводжується не лише позитивними змінами, але й зростанням кількості загроз інформаційній безпеці.

Значна частина сучасних атак на системи ЕЦП спрямована на компрометацію аутентифікації. Такі атаки, як нарпиклад фішинг, перехоплення трафіку, атаки методом грубої сили (brute force), експлуатація вразливостей системного забезпечення — можуть спричинити серйозні наслідки, зокрема втрату конфіденційних даних, фінансові збитки компанії або підрив довіри до технологій цифрової ідентифікації загалом. Таким чином, підвищення стійкості аутентифікації є одним із пріоритетних напрямів досліджень у галузі інформаційної безпеки на сьогодні.

Метою даної роботи є розробка методу підвищення стійкості електронного цифрового підпису за рахунок використання комбінованих схем аутентифікації та впровадження методів тренування штучного інтелекту (далі ШІ), для швидшої та більш точної обробки даних.

Для досягнення цієї мети необхідно виконати такі задачі:

- провести детальний аналіз сучасних методів захисту електронного цифрового підпису;

- дослідити існуючі підходи для побудови ефективних комбінованих схем аутентифікації;

- розробити метод підвищення стійкості ЕЦП, який базується на застосуванні декількох факторів аутентифікації;

- оцінити ефективність розробленого методу через моделювання та тестування в умовах типових атак;

- провести порівняння результатів з існуючими підходами для визначення переваг та недоліків методу;

Наукова новизна роботи полягає у розробці й впровадженні методів підвищення стійкості електронного цифрового підпису (ЕЦП) шляхом використання комбінованих схем аутентифікації, які враховують як статичні, так і динамічні параметри користувача. Запропонований підхід базується на інтеграції контекстуальних даних (місце, час, тип пристрою) із сучасними криптографічними алгоритмами, що дозволяє зменшити ризики компрометації ключів ЕЦП і підвищити безпеку транзакцій.

Предметом дослідження є технології аутентифікації та цифрового підпису, зокрема методи їх вдосконалення шляхом використання комбінованих підходів.

Об’єктом дослідження виступають інформаційні системи, які використовують електронний цифровий підпис для забезпечення автентичності, цілісності та конфіденційності даних.

Практична цінність роботи полягає в тому, що результати дослідження можуть бути впроваджені в реальних умовах для підвищення рівня інформаційної безпеки в корпоративних мережах, банківських системах, державних органах і в інших сферах, де використовується ЕЦП. Запропоновані рішення дозволяють зменшити ризики несанкціонованого доступу, що є особливо актуальним в умовах зростання кількості кібератак. Впровадження комбінованих схем аутентифікації також сприятиме зниженню фінансових втрат і репутаційних ризиків для організацій.

1. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Огляд впровадженної системи захисту на підприємстві

На підприємстві запроваджено економне рішення щодо перевірки користувачів, проте воно досить застаріле та не підходить до швидкого обміну інформацією який на сьогодні є у світі. Для того щоб зрозуміти які саме виправлення нам потрібно впроваджувати, варто розглянути те що вже зараз є у системі, і на основі цього зробити висновки.

До повідомлення M (або до підписуваного електронного документа) додається значення ЕЦП, яке може складатися безпосередньо із самого значення підпису, а також із доданого ідентифікатора суб'єкта, що підписав повідомлення, та/або мітки часу [1]

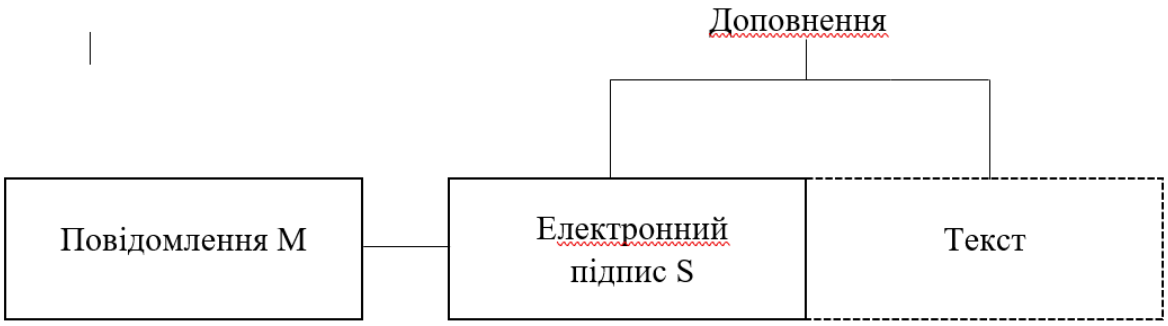


Рисунок 1.1 — Простий приклад підписанного повідомлення ЕПЦ

Схеми ЕП складаються з таких процедур:

- процедури генерації ключів підпису: секретного (закритого) і публічного (відкритого);
- процедури генерації підпису;
- процедури перевірки підпису

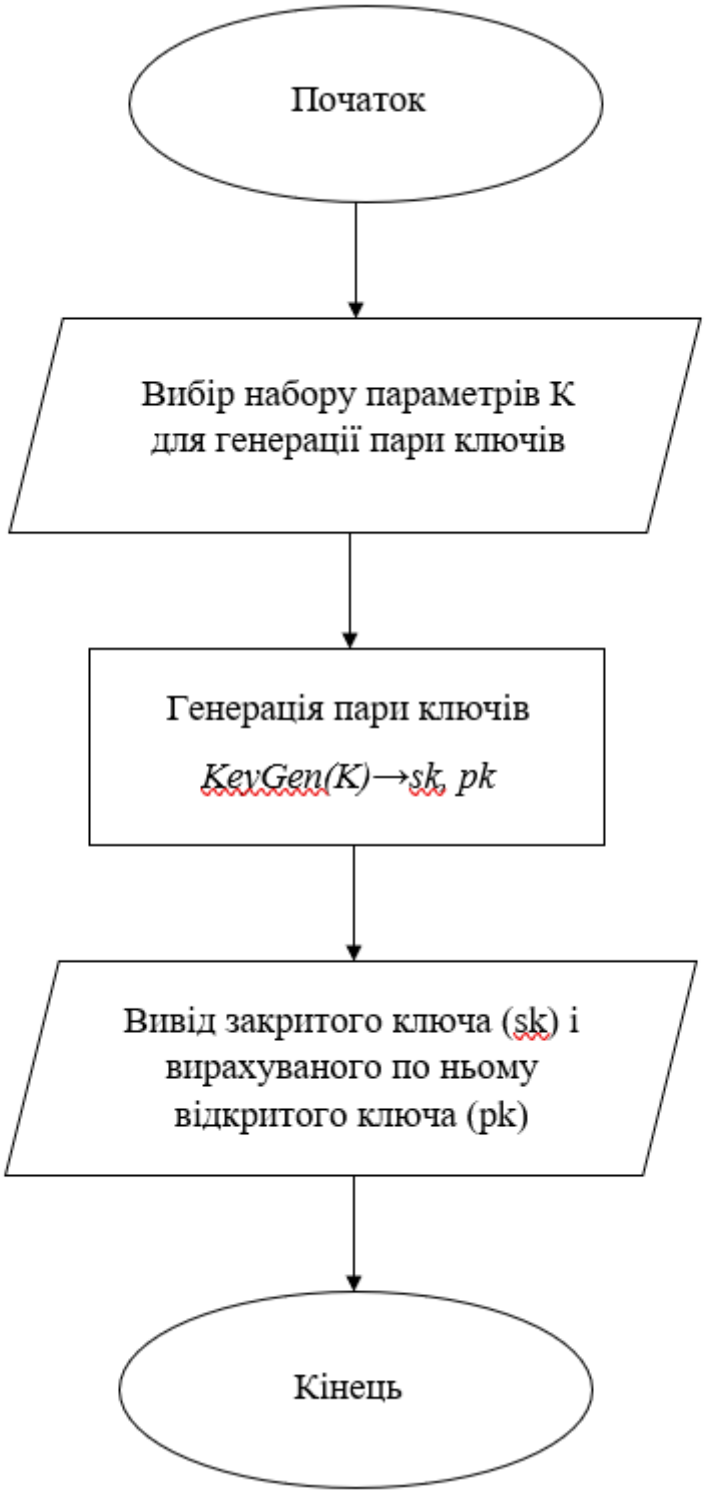


Рисунок 1.2 — Алгоритм генерації пари ключів

На вхід в алгоритм подається деякий набір параметрів системи K (які виробляються заздалегідь і які в загальному випадку краще зберігати в секреті).

Далі за допомогою процедури генерації ключової пари KeyGen виробляються два ключі підписувача: закритий і відкритий ключі.

Відкритий (публічний) ключ pk зберігатиметься в довіднику відкритих ключів користувачів і є загальнодоступними, закритий (секретний) ключ sk зберігається тільки у його власника. Ключова пара може вироблятися як самим користувачем, так і центром сертифікації (засвідчувальним центром, ЗЦ) за запитом користувача. Відкритий і закритий ключі можуть вироблятися одночасно, або відкритий ключ може вироблятися за заздалегідь згенерованим закритим ключем. Зв'язок між ключами визначається деякою математичною залежністю, причому за відомим відкритим ключем обчислювально складно підібрати закритий ключ. [2][3]

Загальний алгоритм генерації електронного цифрового підпису до будь-якого повідомлення або до електронного документа може бути представлений, як Рисунку 1.3 На вхід алгоритму подається електронний документ M, який потім подається на вхід у деяку криптографічно стійку функцію хешування Hash, яка на виході видає хеш H фіксованої довжини. Далі хеш H і закритий ключ sk подаються на вхід у функцію Sign, що створює на виході ЕЦП S до документа M. Як уже зазначалося раніше, відкритий ключ pk зберігається в довіднику відкритих ключів користувачів і є загальнодоступними, закритий (секретний) ключ sk залишається тільки у його власника і тримається в секреті. Процедура KeyGen і подальша передача відкритого ключа pk у довідник відкритих ключів виконується не під час кожного вироблення підпису, а лише під час першої, початкової генерації ключової пари або при зміні закритого ключа.

На вхід перевіряючому подається електронний цифровий підпис S, і підписаний електронний документ M. Документ знову подається на вхід у ту саму функцію хешування Hash, як і під час підписання документа, і на виході отримується значення хешу H. Далі H, підпис S і відкритий ключ pk, узятий, наприклад, із довідника відкритих ключів, відправляються на вхід у функцію

перевірки підпису Verify. Якщо відповідь позитивна, то підпис визнається вірним і з великою часткою ймовірності належить підписанту. Якщо ж відповідь негативна, то в межах допустимого числа помилок алгоритм перевірки можна запустити заново. [4]

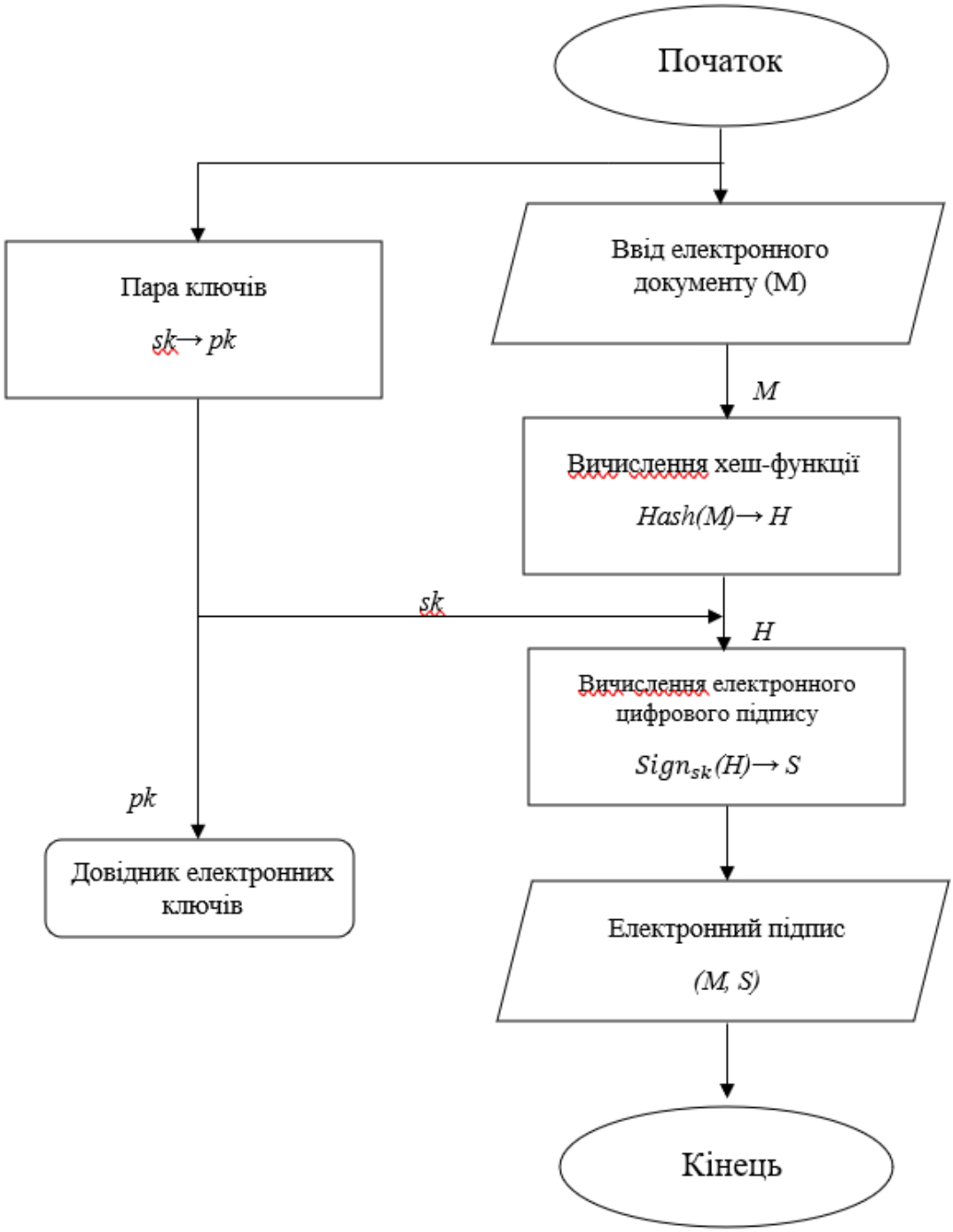


Рисунок 1.3 — Загальний алгоритм генерування електронного цифрового підпису до повідомлення на підприємстві

Розглянувши детально основні процедури електронного цифрового підпису на Рисунку 1.4, а саме методу його використання на підприємстві, можна бачити, що він має певну структуру, яка залежить від бітового тексту, що записується, і секретного ключа підписанта. Цей зв'язок можна перевірити за допомогою відкритого ключа. При цьому знання відкритого ключа не дає можливості згенерувати правильний електронний цифровий підпис. Імовірність помилки або прийняття підробленого повідомлення за легітимне при коректному використанні алгоритмів є вкрай малою. В силу того, що значення підпису безпосередньо залежить від підписаного документа, будь-яка спроба його спотворення призведе до спотворення значення хеша і, відповідно, значення самого підпису. Таким чином, здійснюється завдання забезпечення цілісності інформації. Той факт, що відправлене повідомлення міг підписати лише власник відповідного секретного ключа, може використовуватися, як доказ авторства, тобто завдання здійснення аутентифікації також виконується. [5][6]

Підписаний документ залишається доступним для всіх користувачів, забезпечується завдання доступності, і будь-хто може перевірити факт авторства. Водночас автор не зможе відмовитися від свого підпису, тобто забезпечується завдання невідказуваності. Проте це ще не означає що цей метод неможливо буде зламати. Зловмисники можуть використовувати хеш-функції для атаки на електронний цифровий підпис (ЕЦП), якщо знайдуть уразливості в самій хеш-функції або реалізації системи підпису. Ось кілька способів, як це може відбутися:

- атака на зіткнення;
- атака на підробку;
- атака на другу прообразу;
- атака з використанням довірливих серверів;
- реалізація атаки через слабкі випадкові числа; [7][8]

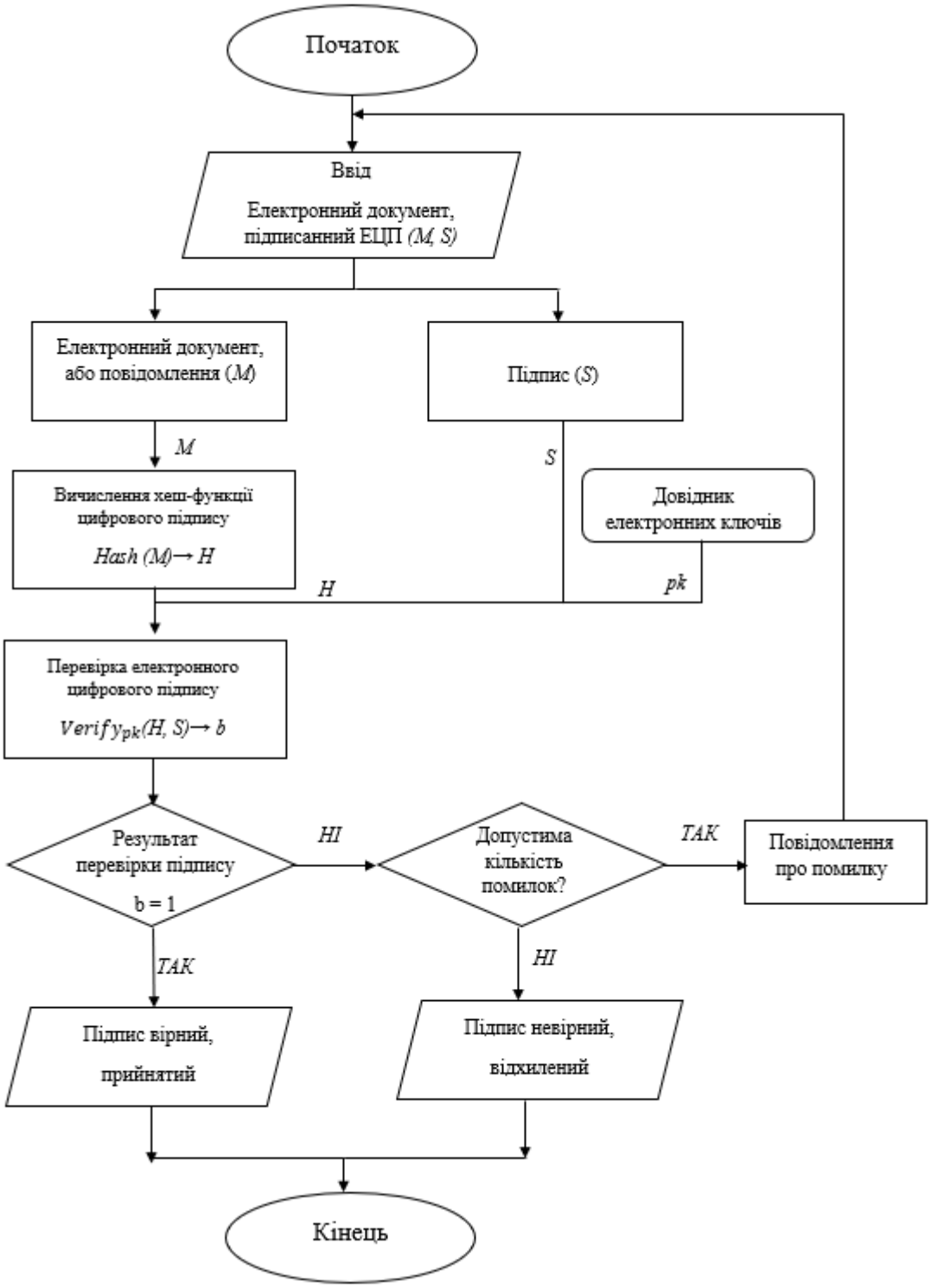


Рисунок 1.4 — Метод підписання документів електронним цифровим підписом на підприємстві

Атака на зіткнення (Collision Attack) — характеризується тим, що хеш-функція, яка призначена для створення унікального хеш-значення для кожного

вхідного повідомлення, може виявитися слабкою, і тоді вже зловмисник може знайти два різні повідомлення (наприклад, M1 і M2), які мають однакове хеш-значення (H(M1) = H(M2)). У цьому випадку атака буде проходити наступним чином: Зловмисник створює невинне повідомлення M1 і його зловмисну версію M2, змушує легітимного користувача підписати M1, потім замінює підписане повідомлення M1 на M2, оскільки хеш-значення ідентичні, і підпис залишається дійсним для обох повідомлень. Якщо алгоритм хешування, наприклад MD5 або SHA-1, використовує слабкі методи, зловмисник може згенерувати підроблене сертифіковане повідомлення, яке видається за аутентичне. [9][10]

Атака на підробку (Preimage Attack) — ця атака спрямована на відновлення повідомлення з відомого хеш-значення, тобто зловмисник отримує значення хешу H(M) і намагається знайти вихідне повідомлення M, яке його створило. Якщо йому вдасться це зробити, він зможе змінити повідомлення та створити його новий підпис. Зловмисник може відновити вихідний текст і змінити його без відома особи.[11]

Атака на другу прообразу (Second Preimage Attack) — ця атака схожа на зіткнення, але зловмисник шукає альтернативне повідомлення M2, яке створює такий самий хеш, як і вже відоме повідомлення M1 (тобто H(M1) = H(M2)). На відміну від колізій, перше повідомлення M1 вже задане. Прикладом може бути ситуація, при якій легітимне повідомлення, що містить певний контракт (M1), знайдене зловмисником, який також знаходить інше повідомлення (M2) з таким самим хешем і підміняє його.[12]

Атака з використанням довірливих серверів — може бути реалізована, якщо система підпису використовує хешування на стороні сервера, але сервер недостатньо захищений. Зловмисник може змінити алгоритм хешування, щоб отримати контроль над хешами, які підписуються. Він підроблює повідомлення та підписує його під іменем легітимного користувача.[13]

Реалізація атаки через слабкі випадкові числа — може бути реалізована, якщо хеш-функції можуть бути небезпечними, і в схемі підпису використовується ненадійний або недостатньо випадковий генератор чисел. Зловмисник може виявити закономірність у хешах або повторно використовувати ці значення для компрометації підпису. [14]

1.2 Програмне забезпечення на підприємстві

На підприємстві також використовується програмне забезпечення Okta, для перевірки аутентифікації користувачів.

Okta — це хмарна платформа, яка призначена для управління ідентифікацією та доступом. Вона використовується для забезпечення безпеки доступу до корпоративних систем, додатків і даних. Ця платформа дозволяє компаніям централізувати керування обліковими записами користувачів, надаючи при цьому простий і безпечний спосіб входу до різноманітних додатків.

Однією з ключових переваг Okta є функція єдиного входу (SSO), яка дозволяє користувачам увійти в систему один раз і отримати доступ до всіх додатків, інтегрованих із платформою. Це значно спрощує процес аутентифікації для користувачів і одночасно знижує навантаження на IT-відділи. Крім того, Okta пропонує багатофакторну аутентифікацію (MFA), яка підвищує рівень безпеки, додаючи ще один рівень перевірки, наприклад, використання SMS, біометрії чи токенів. [15]

Ще одна важлива функція Okta — це управління доступом. Система дозволяє організаціям встановлювати динамічні правила доступу, які враховують контекстні фактори, такі як геолокація чи тип пристрою. Це робить процес аутентифікації більш гнучким і адаптивним до сучасних умов.

Okta підтримує інтеграцію з багатьма популярними сервісами, такими як Slack, Zoom, Salesforce, Google Workspace та Microsoft 365. Адміністраторам потрібно лише кілька хвилин, щоб налаштувати доступ до нових додатків. Така широка сумісність робить Okta універсальним рішенням для компаній різного розміру.

Окремо слід відзначити, що Okta підтримує концепцію Zero Trust, яка базується на постійному контролі доступу незалежно від місцезнаходження користувача чи його пристрою. Це забезпечує додатковий рівень захисту для корпоративних даних.

У реальних умовах використання Okta може значно підвищити ефективність роботи організацій. Наприклад, компанія з декількома сотнями співробітників може централізовано керувати всіма обліковими записами, швидко додавати нових користувачів і видаляти облікові записи звільнених співробітників. Це зменшує ризик витоку даних і покращує безпеку.

Отже, Okta є сучасним і ефективним інструментом, який поєднує зручність для користувачів та високий рівень безпеки. Вона підходить для компаній будь-якого розміру, допомагаючи їм не лише керувати ідентифікацією, а й забезпечувати надійний доступ до важливих ресурсів. [16][17]

Okta — це потужне програмне забезпечення для управління доступом, яке має безліч переваг, але також не позбавлене недоліків. Однією з головних проблем є висока вартість. Це хмарне рішення може бути занадто дорогим для невеликих компаній або стартапів, особливо якщо врахувати витрати на налаштування та підтримку.

Іншою складністю є інтеграція з менш популярними сервісами. Хоча Okta підтримує широкий спектр популярних додатків, її використання для власних внутрішніх систем або менш розповсюдженого ПЗ може виявитися проблематичним. Крім того, як хмарна платформа, Okta повністю залежить від

стабільності Інтернет-з'єднання. Будь-які перебої в мережі можуть призвести до тимчасової недоступності системи.

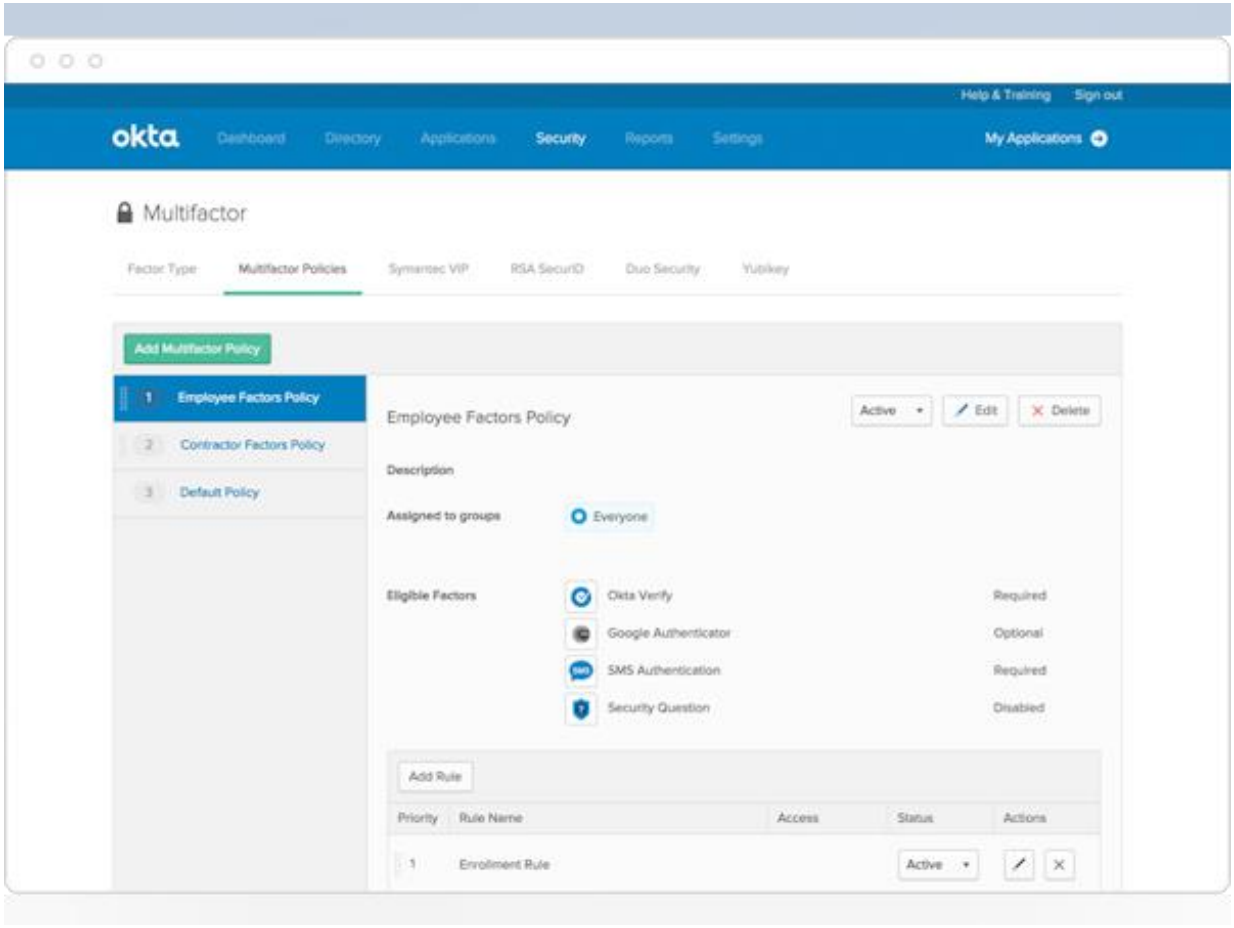


Рисунок 1.5 — Інтерфейс програми

Впровадження Okta часто потребує допомоги досвідчених IT-фахівців, а це може стати проблемою для організацій, у яких відсутній власний IT-відділ. Навіть після впровадження кінцевим користувачам та адміністраторам знадобиться час для адаптації, адже крива навчання є доволі крутою. До того ж, можливості кастомізації Okta для задоволення специфічних потреб компанії можуть бути обмеженими, що іноді вимагає додаткових витрат на оновлення ліцензії.[18][19][20]

Ще одним аспектом є залежність від стороннього постачальника. Організації, які використовують Okta, передають критично важливі процеси

аутентифікації в руки зовнішнього провайдера. У разі технічних проблем чи збоїв з боку провайдера компанія може зіткнутися зі значними труднощами. Підтримка, хоча і доступна, може затримуватися, особливо у випадках критичних проблем.

Okta також не є повністю захищеною від кіберзагроз або технічних несправностей. Хоча її захисні механізми дуже потужні, потенційні ризики збоїв або атак завжди існують. Для організацій, які швидко масштабуються, використання Okta може виявитися складним через необхідність додаткових ресурсів для адаптації системи до зростаючих потреб. [21]

Таким чином, Okta є ефективним інструментом для управління доступом, але її впровадження потребує ретельного аналізу та підготовки. Розуміння цих недоліків допоможе визначити шлях до покращення і впровадження нових рішень для певного покращення безпеки підприємства.

1.3 Матеріально-технічне та технологічне забезпечення яке потрібне для реалізації наших методів

Щоб покращити ці недоліки, ми будемо вводити комбіновані схеми аутентифікації, проте, аби ще більше покращити якість запропонованої системи, ми введемо також машинне тренування, тобто штучний інтелект, надалі ШІ, аби постійно його тренувати та не дати змогу зловмисниками добратися до чутливих даних.

Є досить багато компаній які успішно використовують ШІ для своїх цілей. Наприклад, Linkfluence використовує ШІ для аналізу великих колекцій соціальних даних, щоб надавати інсайти для провідних брендів та агентств. Для реалцізації цього потрібно було розгорнути високопродуктивні виділені сервери, щоб економічно ефективно справлятися з їхніми ресурсоємними робочими навантаженнями.

З цієї причини тут будуть наведені деталі щодо того, як компанії використовують штучний інтелект і які їхні специфічні вимоги до інфраструктури.

Бізнес та IT-керівники вже роблять значні інвестиції в технології, пов'язані зі штучним інтелектом. Штучний інтелект змінює все, і в міру того, як він стає все більш поширеним, організації будуть змушені пристосовуватися до нього на макрорівні, оскільки він змінює цілі галузі, і на мікрорівні, оскільки він впливає на бізнес-стратегію всередині їхніх рядів. Зважаючи на те, що ці зміни відбуваються такими швидкими темпами, варто звернути увагу на деякі ключові аспекти штучного інтелекту, оскільки він стає все більш поширеним, а організації стикаються з новим світом процесів і вимог. [22]

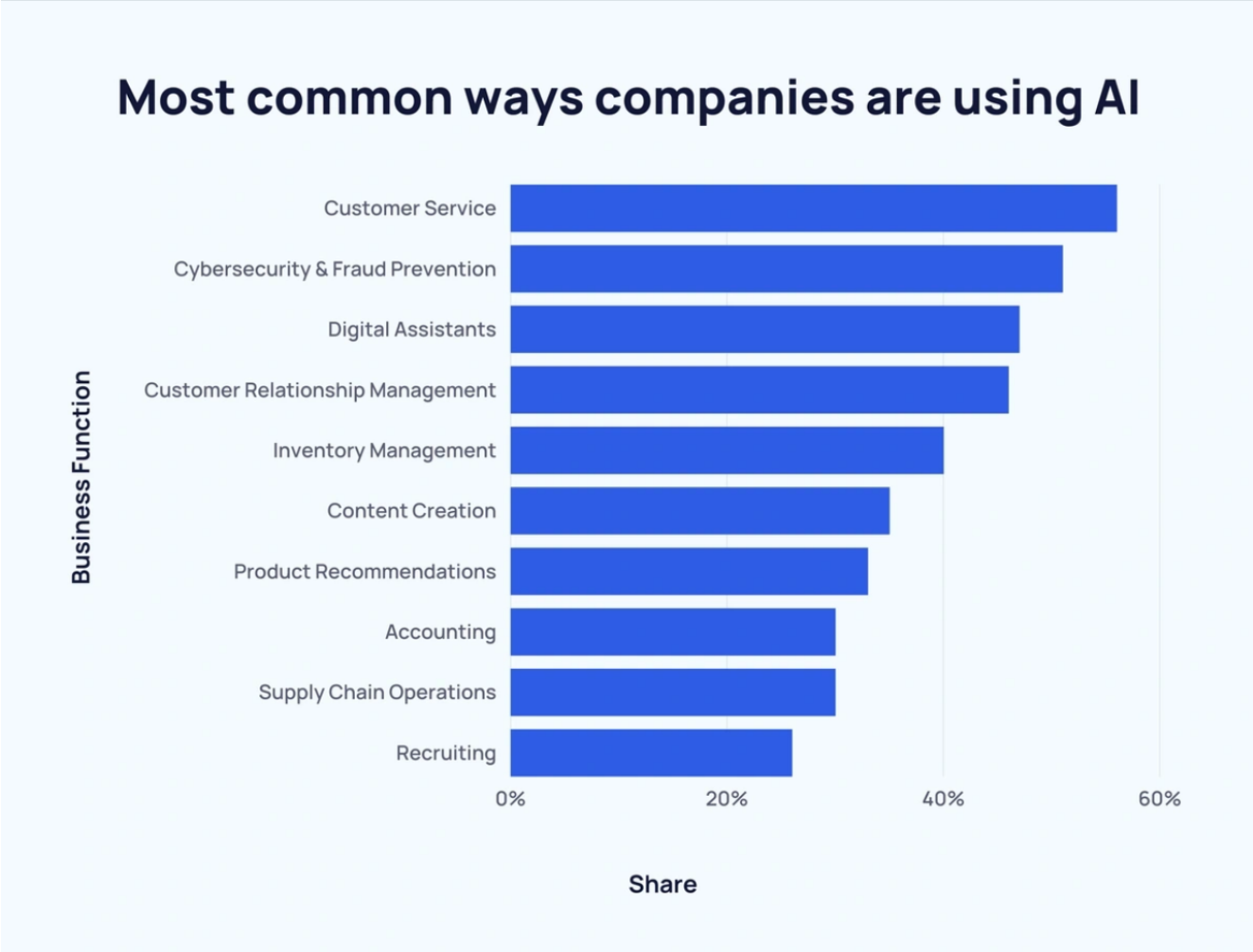


Рисунок 1.6 — Рейтинги використання ШІ у різних сферах

Жак Багін, директор Глобального інституту McKinsey та старший партнер McKinsey, що базується в Брюсселі, і Ніколас ван Зебрук, професор інновацій, IT-стратегії та цифрового бізнесу в Брюссельській школі Solvay, вільний університет Брюсселя, застерігають, що це все ще ранні дні ШІ. За їхніми оцінками, близько 35% компаній або впроваджують, або пілотують ШІ. Тим не менш, вплив на ринки вже відчувається. Проривні та більш ефективні бізнес-моделі в цьому сегменті вже можуть «знижувати галузеву рентабельність». У той же час, ці ранні адепти ШІ вже переходять до другої хвилі ШІ, що, ймовірно, дозволить їм ще деякий час випереджати своїх конкурентів. [23]

З точки зору інфраструктури можна зробити чіткий висновок: у міру того, як ШІ переходить від гіпотетичних експериментів до впровадження на різних підприємствах, він вимагатиме значних обчислювальних ресурсів і витрат на інфраструктуру та її обслуговування. Накладні витрати зростатимуть разом з тим, як технологія буде ставати все складнішою і більш вимогливою до ресурсів, а у світі, що зазнає все більшого впливу ШІ, пошук економічно ефективних середовищ для запуску інтенсивних процесів буде одночасно і вимогою, і конкурентною перевагою. Варто зазначити, що з кожним роком технології на основі штучного інтелекту розвиваються, тому, якщо бізнес та підприємства хочуть бути релевантними у сучасному світі, їм потрібно буде постійно адаптовувати свої системи під штучним інтелект.

Бізнесу доведеться адаптуватися і бути гнучким, особливо в тому, що стосується його інфраструктури. Хмарні технології, зокрема гібридні хмарні рішення для зберігання даних та обробки інформації, є і будуть основою ШІ, оскільки його потреби в значних обсягах даних зростають, і тримати серверні кімнати не кожен бізнес собі може дозволити як з точки зору фінансів, так і з точки зору практичності. Гібридні хмарні рішення забезпечать відповідність технологій потребам бізнесу та робочим навантаженням, які дедалі більше вимагаються для підтримки ШІ, але не тільки це, вони також гарантують, що це буде на належному рівні витрат. [24]

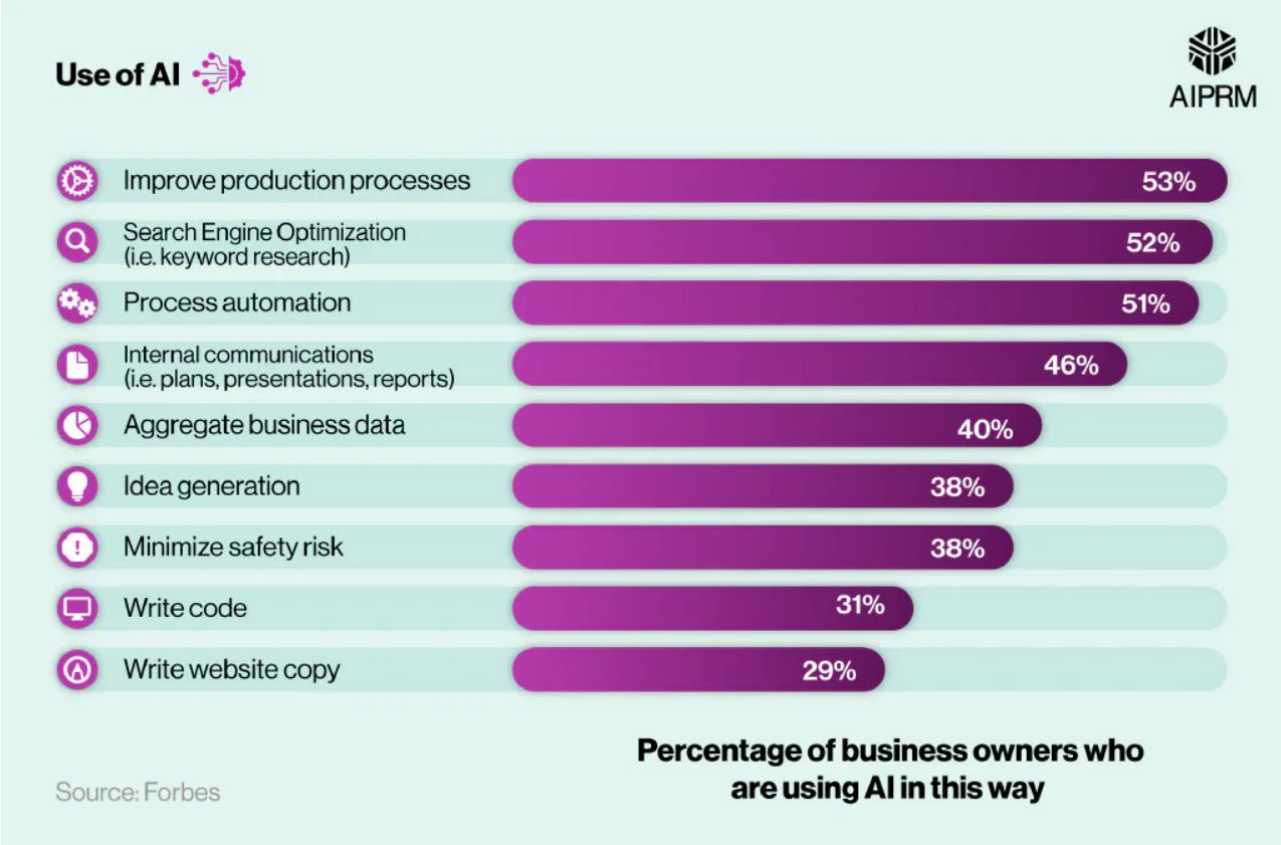


Рисунок 1.7 — Схема використанні ШІ для конкретних задач у бізнесі та на підприємствах

Тому найбільше питання для організацій полягає в наступному: яка інфраструктура дозволяє безперервне використання, розробку і впровадження штучного інтелекту без шкоди для продуктивності, і щоб на це питання відповісти, є п'ять речей, про які слід пам'ятати при оцінці потенційних партнерів, щоб забезпечити вибір найкращої платформи:

- висока обчислювальна потужність — щоб повною мірою скористатися можливостями, які надає ШІ, організаціям потрібні обчислювальні ресурси з достатньою продуктивністю, включаючи центральні та графічні процесори. Середовище на базі CPU може впоратися з основними робочими навантаженнями ШІ, але глибоке навчання передбачає роботу з великими масивами даних і розгортання масштабованих нейромережевих алгоритмів. Для цього обчислень на базі CPU може бути недостатньо. Наприклад, графічні процесори можуть прискорити глибоке навчання в 100 разів порівняно з

традиційними процесорами. Обчислювальна потужність і щільність також зростатимуть, як і попит на високопродуктивні мережі та сховища;

- ємність сховища — дуже важливо, щоб ваша інфраструктура мала можливість масштабувати сховище в міру зростання обсягу даних. Визначення того, який обсяг сховища потрібен організації, залежить від багатьох факторів, зокрема від рівня ШІ, який організація планує використовувати, і від того, чи потрібно їй приймати рішення в режимі реального часу. Наприклад, фінтех-компанії, яка використовує системи штучного інтелекту для прийняття торгових рішень у режимі реального часу, може знадобитися швидка флеш-пам'ять, тоді як для інших компаній найбільш підходящим рішенням буде повільніше, але дуже велике сховище. Підприємствам потрібно враховувати, скільки даних генеруватимуть додатки ШІ. ШІ-програми приймають кращі рішення, коли мають доступ до більшого обсягу даних. Оскільки бази даних з часом зростають, компаніям потрібно контролювати їхню ємність і планувати розширення;

- мережева інфраструктур — мережі це ще один ключовий компонент інфраструктури ШІ. Алгоритми глибокого навчання сильно залежать від зв'язку, і мережі повинні йти в ногу з попитом у міру того, як розширюється сфера застосування ШІ. Ось чому масштабованість має бути головним пріоритетом, а для цього потрібна мережа з високою пропускною здатністю і низькою затримкою. Найкращим вибором для розширення послуг є глобальний провайдер інфраструктури, який може забезпечити узгодженість набору послуг і технологічного стеку в усіх регіонах;

- безпека — ШІ може бути пов'язаний з обробкою конфіденційних даних, таких як записи пацієнтів, фінансова інформація та персональні дані. Порушення цих даних стане катастрофою для будь-якої організації. Крім того, вливання поганих даних може призвести до того, що система штучного інтелекту зробить неправильні висновки, що призведе до помилкових рішень;

Інфраструктура штучного інтелекту повинна бути захищена від початку до кінця за допомогою найсучасніших технологій.

- економічно ефективні рішення — оскільки моделі штучного інтелекту стають все складнішими, вони стають все дорожчими в експлуатації, тому отримання додаткової продуктивності від вашої інфраструктури має вирішальне значення для скорочення витрат. Протягом наступних кількох років можна очікувати подальшого зростання кількості компаній, які використовують ШІ, що призведе до збільшення навантаження на мережу, сервери та інфраструктуру зберігання даних, необхідну для використання цієї технології; [25][26][27]

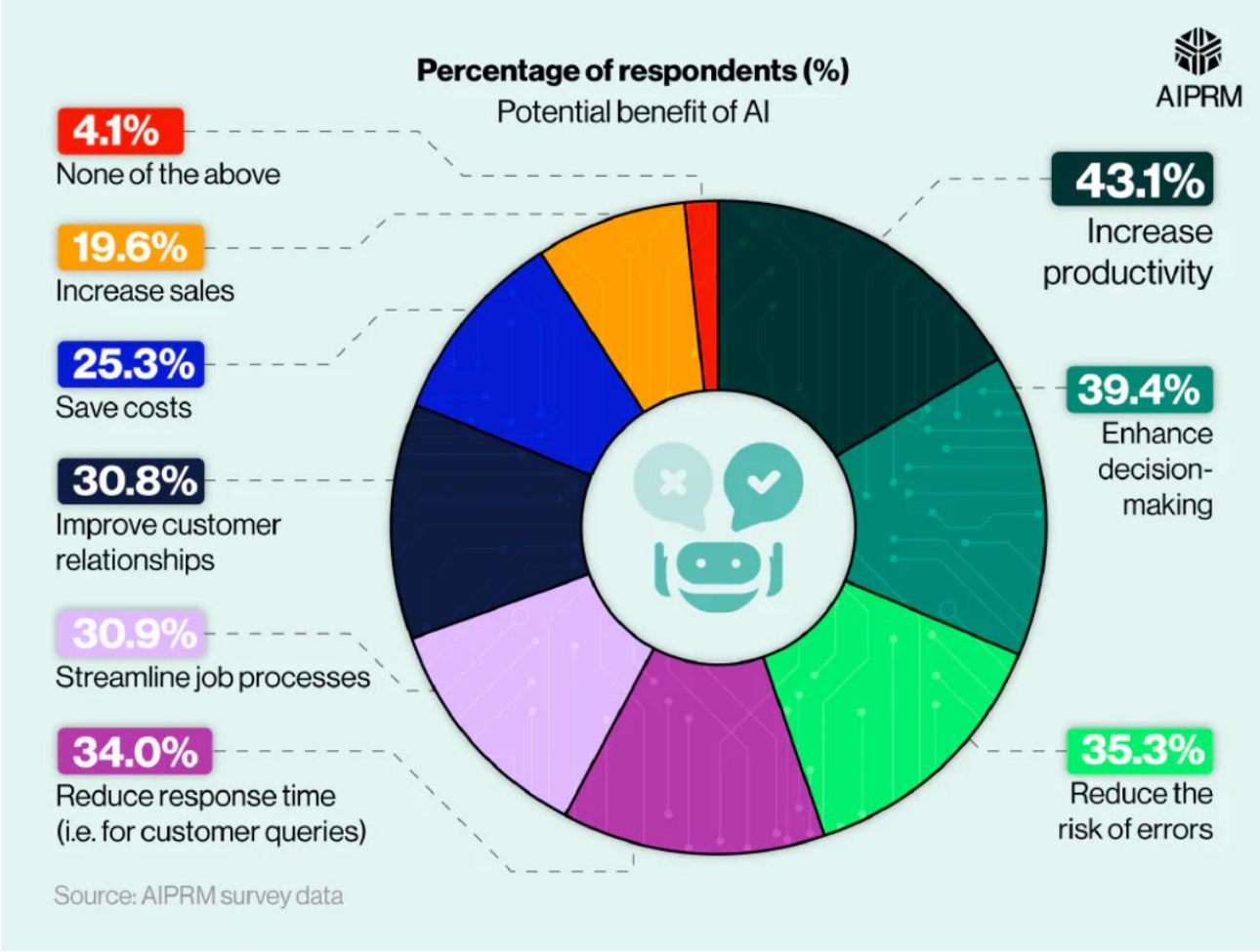


Рисунок 1.8 — Розподілення обов’язків ШІ на підприємствах

Завдяки ретельному вибору та визначенню постачальників, які можуть запропонувати економічно ефективні виділені сервери, є можливість підвищити продуктивність. Це дозволить компаніям продовжувати інвестувати в ШІ без збільшення витрат бюджету. [27]

1.4 Огляд комбінованих схем аутентифікації

Для вирішення вищезазначених проблем в останні роки активно застосовуються комбіновані схеми аутентифікації, які забезпечують високий рівень безпеки шляхом поєднання декількох факторів для підтвердження особи користувача. Комбіновані схеми аутентифікації базуються на принципі, що зламати всі фактори одночасно значно складніше, ніж один.

Основними типами факторів аутентифікації є:

- знання (Something you know) — що користувач знає, наприклад, пароль або відповідь на секретне запитання. Однак цей метод є вразливим до атак, таких як фішинг або атаки методом грубої сили, які можуть просто перебрати усі можливі паролі, або ж взнати пароль за допомогою спеціальних посилань;
- володіння (Something you have) — фізичні пристрої, які користувач має при собі, наприклад, смарт-картка, USB-токен або мобільний телефон з одноразовим паролем, що надсилається через SMS чи додаток певної компанії на робочий, або особистий, гаджет користувача;
- біометрія (Something you are) — фізичні характеристики користувача, такі як відбитки пальців, розпізнавання обличчя або райдужна оболонка ока, щось, що важко підробити; [28]

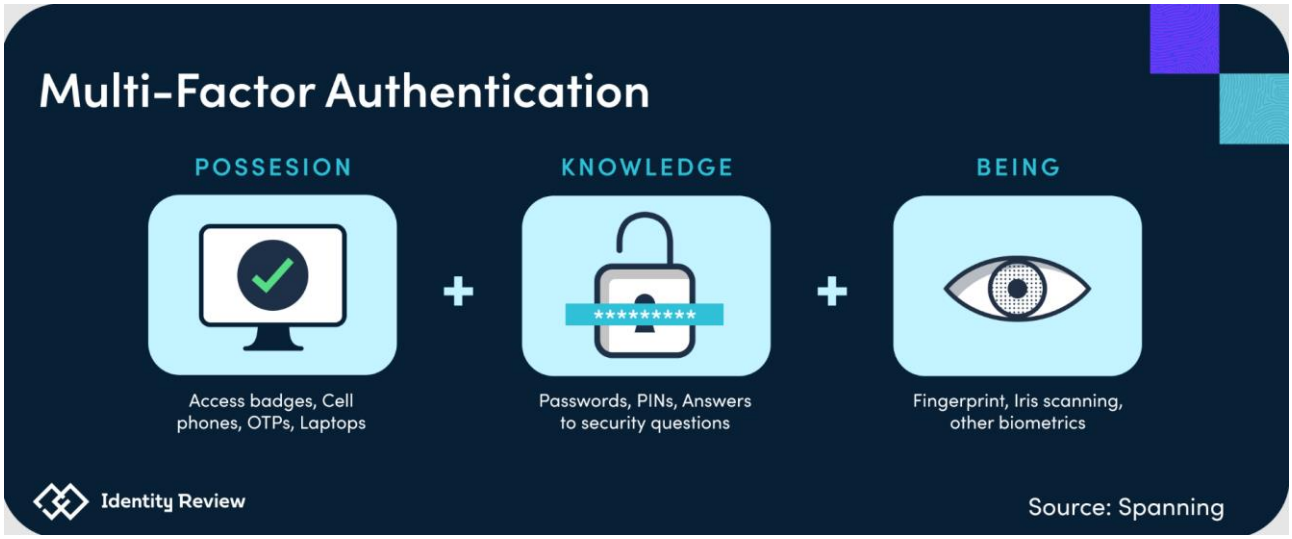


Рисунок 1.9 — Приклад типів аутентифікації

Використання мультифакторної аутентифікації (MFA) дозволяє значно підвищити рівень безпеки, оскільки навіть якщо один із факторів буде скомпрометований, зловмисник не зможе отримати доступ до системи без іншого фактора. Наприклад, у випадку з банківськими додатками застосовується поєднання пароля (щось, що користувач знає) та біометрії або одноразового коду з мобільного додатку (щось, що користувач має). [29]

Однією з найефективніших схем є двухфакторна аутентифікація (2FA), яка поєднує два фактори для доступу до системи. Вона широко використовується в фінансових установах, де кожна транзакція вимагає не лише введення пароля, але й підтвердження за допомогою мобільного пристрою або спеціального токена.

Загрози безпеці систем з електронними підписами зростають із розвитком кіберзагроз та нових методів атак. Для забезпечення стійкості та надійності таких систем важливо враховувати як криптографічні алгоритми, так і методи аутентифікації. Комбіновані схеми аутентифікації є важливим кроком вперед, адже вони забезпечують багаторівневий захист, який значно ускладнює злом системи.

Перехід до комбінованих схем аутентифікації є доцільним для підвищення стійкості електронного цифрового підпису та захисту від сучасних

кіберзагроз. Надалі розробка методів, які поєднують криптографічні підписи з мультифакторною аутентифікацією, стане ключем до створення надійних систем електронного документообігу. [30][31]

2. РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ СТІЙКОСТІ ЕПЦ

2.1 Поняття електронного цифрового підпису (ЕЦП) і його покращення

Електронний цифровий підпис (ЕЦП) є важливим інструментом для забезпечення аутентичності, цілісності та невідкличності електронних документів у цифровому середовищі. Це криптографічна операція, яка застосовується для підписання цифрових повідомлень або документів і використовується для перевірки того, що підписаний документ дійсно створений конкретною особою і не зазнав змін під час передачі.

Визначення ЕЦП з’явилося разом з розвитком Інтернету та електронної комунікації, коли виникла необхідність у забезпеченні безпеки передачі електронних документів. Одним із основних принципів електронного підпису є використання асиметричної криптографії, де застосовуються два ключі: відкритий і приватний. Відкритий ключ використовується для перевірки підпису, а приватний – для його створення. Важливою перевагою цієї системи є те, що приватний ключ ніколи не передається через Інтернет і завжди зберігається в безпечному середовищі.

Законодавча база, що регулює використання ЕЦП, складається з міжнародних стандартів, таких як ISO/IEC 14888, а також численних нормативних актів, прийнятих на національному рівні. Наприклад, в Україні це регулюється Закон України "Про електронні довірчі послуги". Цей документ визначає основні вимоги щодо створення, перевірки та використання електронних підписів, а також діяльність кваліфікованих постачальників довірчих послуг.[32][33]

Основні характеристики ЕЦП, які забезпечують його ефективність у забезпеченні безпеки, включають:

- аутентичність — підтвердження того, що автор підпису є тим, за кого він себе видає;

- цілісність — підпис підтверджує, що документ не було змінено з моменту підписання;

- невідкличність — гарантія того, що підписант не може відмовитися від підписаного документу, оскільки це свідчить про його добровільну згоду на зміст документа;

Для ефективного підвищення стійкості електронного цифрового підпису (ЕЦП) необхідно враховувати кілька важливих критеріїв, що визначають його надійність. Вибір критеріїв базується на аналізі сучасних загроз безпеці та вимогах до систем захисту даних.[34][35]

Ступінь захищеності від атак на ключі. Приватний ключ є основою для цифрового підпису, тому забезпечення його безпеки є критичним. Використання більш складних криптографічних методів і зберігання ключів у апаратних модулях безпеки (HSM) значно підвищують рівень захисту від атак, що спрямовані на компрометацію цього елементу системи

Захист від перехоплення та підробки підпису. Система має бути здатною забезпечити захист підписаних даних від модифікації або підробки. Для цього використовуються потужні криптографічні алгоритми, такі як алгоритми на основі еліптичних кривих (ECDSA), які дають високий рівень захисту навіть при малих розмірах ключів. [36]

Це дозволяє знижувати ризики атак, таких як повторне використання або відновлення підпису.

Інтеграція з існуючими стандартами та інфраструктурами. Створення нового методу підвищення стійкості ЕЦП повинно передбачати сумісність з уже існуючими стандартами, такими як X.509 для сертифікатів і PKCS#7 для підписів. Це забезпечить можливість інтеграції нових методів у вже діючі інфраструктури електронного документообігу (ECI).

Використання мультифакторної аутентифікації. Додаткові рівні захисту через впровадження мультифакторної аутентифікації (MFA) можуть значно підвищити надійність ЕЦП. Наприклад, поєднання цифрового підпису з

біометричними даними або одноразовими паролями через мобільні додатки забезпечить додаткову перевірку особи, яка підписує документ. [37][38]

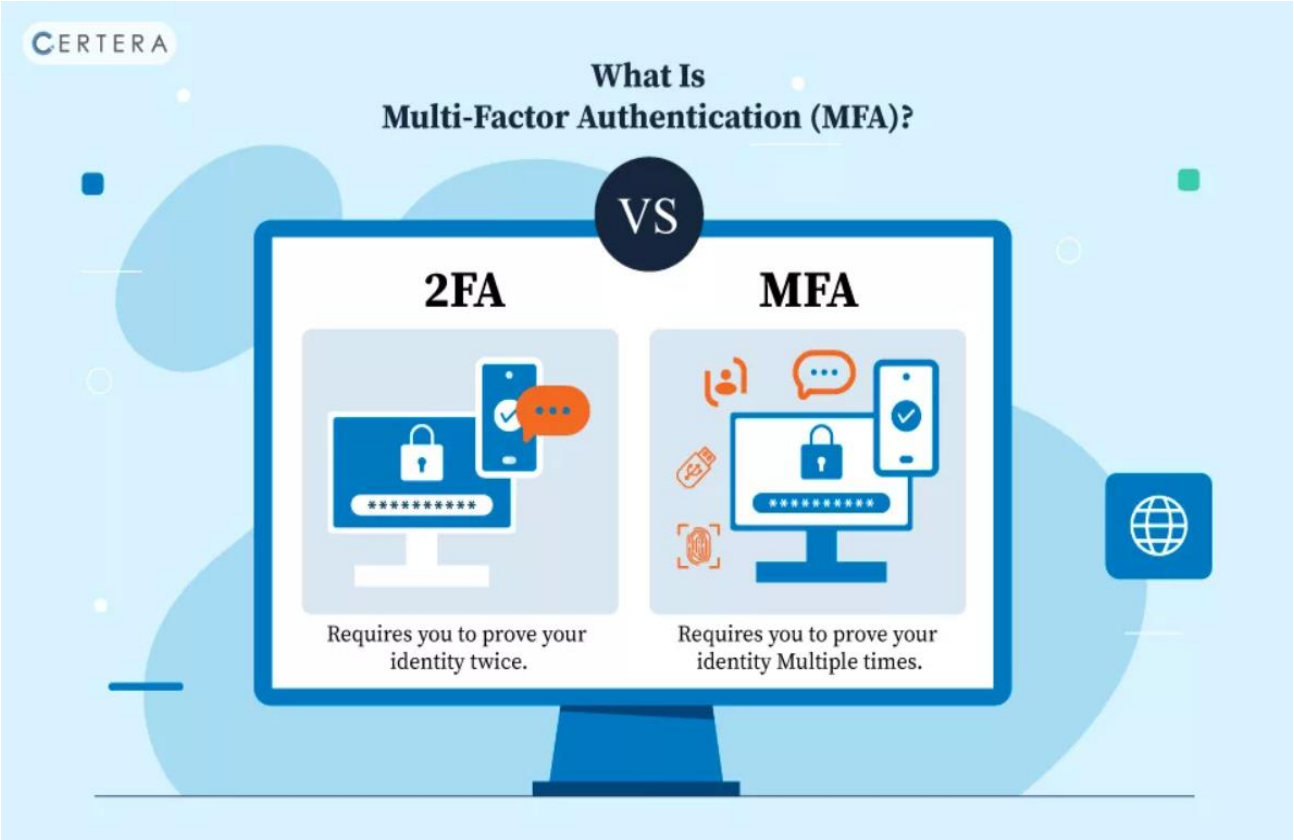


Рисунок 2.1 — Приклад MFA

2.2 Існуючі методи захисту ЕЦП

Основним методом забезпечення безпеки електронного підпису є використання криптографічних алгоритмів, які здійснюють перетворення даних і генерують підпис на основі відкритих і приватних ключів. Найбільш поширеними алгоритмами для створення та перевірки ЕЦП є:

- RSA (Rivest–Shamir–Adleman). Один із перших асиметричних алгоритмів, який широко застосовується для створення підписів і шифрування даних. RSA ґрунтується на складності розкладу великих чисел на прості множники. Це забезпечує високий рівень безпеки, але для забезпечення

достатньої стійкості алгоритм потребує використання великих ключів, що може бути обмеженням для ресурсозатратних середовищ;

- ECDSA (Elliptic Curve Digital Signature Algorithm). Алгоритм, який використовує еліптичні криві замість великих простих чисел. Він забезпечує той самий рівень безпеки, що й RSA, але з меншими розмірами ключів, що робить його більш ефективним для використання в обмежених середовищах, таких як мобільні пристрої чи вбудовані системи;

Одним із важливих аспектів захисту ЕЦП є надійне зберігання приватного ключа. Для цього використовуються різноманітні апаратні засоби, такі як смарт-карти, USB-токени або апаратні модулі безпеки (HSM). Ці пристрої дозволяють зберігати приватні ключі в зашифрованому вигляді і забезпечують додатковий рівень захисту від несанкціонованого доступу. Крім того, для покращення безпеки можна використовувати двофакторну аутентифікацію, коли для доступу до приватного ключа користувач має надавати додаткову інформацію, наприклад, пароль або одноразовий код, надісланий через мобільний додаток.

Також важливо зазначити використання алгоритмів хешування для перевірки цілісності документів. Такі алгоритми, як SHA-256 чи SHA-3, генерують унікальний відбиток документа, що дозволяє перевірити, чи не були внесені зміни до підписаного файлу після його підписання. [39]

2.3 Проблеми стійкості та аутентифікації у системах з ЕЦП

Незважаючи на розвиток криптографічних технологій, існує ряд проблем, що впливають на стійкість систем, що використовують ЕЦП. Однією з головних загроз є людський фактор, а саме ненадійне зберігання приватних ключів або використання простих паролів для доступу до них.

Сучасні методи аутентифікації, які використовують лише один фактор (наприклад, введення пароля або PIN-коду), стали уразливими до атак, таких як наприкад:

- Фішинг;
- атаки методом грубої сили ;
- перехоплення трафіку;
- соціальна інженерія;

Фішинг — це метод обману, при якому зловмисники створюють підроблені веб-сайти, що виглядають як офіційні платформи, для того, щоб отримати конфіденційні дані користувача, зокрема паролі або дані для доступу до цифрових підписів. [40]

Брут форс (атаки методом грубої сили) — це метод за якого зловмисники намагаються перебрати всі можливі варіанти пароля або PIN-коду до того, як знайдуть правильний. Це особливо небезпечно для систем, де паролі є короткими або використовуються застарілі методи хешування. [41]

Перехоплення трафіку — це метод експлуатації незашифрованих каналів для передачі даних, за допомогою яких зловмисники можуть перехопити та отримати доступ до особистих ключів або інших даних, необхідних для створення підпису. [42]

Соціальна інженерія — це метод використання психологічних маніпуляцій для того, щоб переконати користувача надати свої облікові дані або іншу конфіденційну інформацію, або ж дослідження соціальних мереж жертви для того щоб знайти будь яку потрібну інформацію, яку в майбутньому можна використати. [43]

Одним з найбільших викликів є компрометація приватних ключів. У разі зламу цієї інформації зловмисник може створити підроблений підпис від імені власника ключа, що ставить під загрозу безпеку всієї системи. Для мінімізації таких загроз необхідно використовувати багатофакторну аутентифікацію та інші методи додаткового захисту.

2.4 Аналіз та вибір серед існуючих підходів до підвищення стійкості ЕЦП

Сучасні підходи до підвищення стійкості ЕЦП зосереджуються на удосконаленні як криптографічних алгоритмів, так і на використанні новітніх технологій, таких як апаратне забезпечення та комбіновані схеми аутентифікації.

Зміцнення криптографічних алгоритмів — це покращення традиційних криптографічних алгоритми, таких як RSA, що забезпечують високий рівень захисту. Однак варто зазначити, що вони вимагають великих розмірів ключів для досягнення необхідного рівня безпеки. Натомість, алгоритми на основі еліптичних кривих (ECDSA) стали популярними через їхню високу ефективність, що дозволяє використовувати менш об'ємні ключі при збереженні високого рівня безпеки. Це також знижує обчислювальну складність, що робить їх більш підходящими для мобільних пристроїв та обмежених ресурсів

Апаратні модулі безпеки (HSM) — це апаратні засоби для зберігання ключів є важливою складовою стійких систем електронного підпису. Використання апаратних модулів (HSM) дозволяє зберігати приватні ключі в безпечному середовищі, що унеможливлює їх витік при атаках на програмне забезпечення. Система забезпечує захист не тільки від несанкціонованого доступу до ключів, але й від зловмисних спроб їх витягти або скомпрометувати через стороннє програмне забезпечення [44][45]

Комбіновані схеми аутентифікації — тобто інтеграція двофакторної аутентифікації (2FA) разом із криптографічними підписами, що дозволяє значно підвищити рівень захисту. У такій системі для підтвердження дій користувача використовуються два фактори, що є незалежними один від одного (наприклад, пароль і біометричні дані). Це ускладнює роботу зловмисникам, навіть якщо один із факторів буде скомпрометований. Наприклад, застосування

одноразових кодів, що генеруються на мобільних пристроях, або використання біометрії, таких як відбитки пальців або розпізнавання обличчя, додає додатковий рівень захисту до стандартної системи підпису.

Інтеграція з блокчейн-технологіями — адже блокчейн може служити ще однією додатковою технологією для підвищення стійкості ЕЦП, особливо у сфері фінансових і юридичних документів. Використання блокчейн-технології забезпечує постійну перевірку аутентичності документів через розподілену реєстрацію, що унеможливлює зміну даних після підписання. Це значно знижує можливості для шахрайства, зокрема в контексті глобальних фінансових систем та реєстраційних процесів.[46][47]

Запропонований метод підвищення стійкості ЕЦП складається з кількох важливих етапів:

- вибір нових криптографічних алгоритмів;
- інтеграція HSM для зберігання ключів;
- впровадження мультифакторної аутентифікації;

Для забезпечення високої стійкості системи до сучасних атак необхідно використовувати потужніші алгоритми, такі як ECDSA або EdDSA. Ці алгоритми забезпечують високу стійкість навіть при меншому розмірі ключа, що робить їх більш ефективними в умовах обмежених ресурсів. Крім того, вони менш вразливі до атак типу "людина в середині" та "атаки на повторне використання підписів".[48]

Для забезпечення надійного зберігання приватних ключів необхідно використовувати апаратні пристрої (HSM), які виконують криптографічні операції в ізольованому середовищі. Це гарантує, що навіть у разі компрометації комп'ютера, ключі залишатимуться в безпеці. [49]

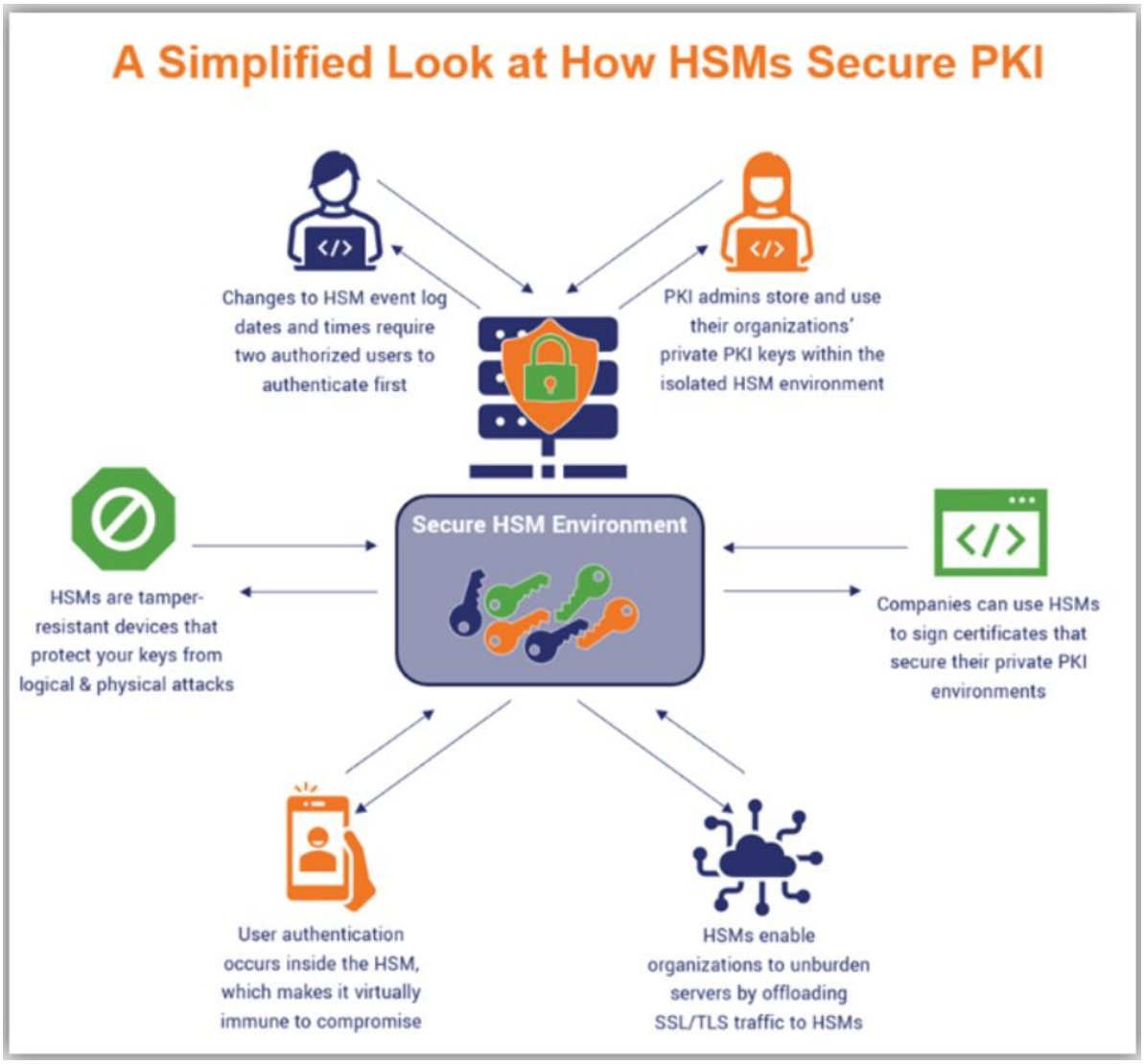


Рисунок 2.2 – Спрощена схема HSM

Для підвищення захисту підписаних документів слід інтегрувати мультифакторну аутентифікацію та використання біометричних даних або OTP-кодів.

Електронні підписи, також відомі як eSignatures, — це метод підписання документів і підтвердження особи підписанта за допомогою цифрових засобів. Результатом є безпечний і юридично визнаний спосіб підписання угод, контрактів або іншої важливої документації без необхідності використання паперу та чорнила. [50]

Однією з ключових переваг електронних підписів є зручність. Вони дають змогу фізичним та юридичним особам оптимізувати свої процеси,

зменшити обсяг паперової роботи та пришвидшити транзакції. У минулому залишилися виснажливі дні друку, сканування, надсилання факсом і поштою контрактів та угод.

Крім того, електронні підписи часто мають вбудовані функції безпеки, такі як шифрування та аудиторський контроль, що робить їх більш надійними та захищеними, ніж паперові документи, підписані вручну.

З юридичної точки зору, електронні підписи визнаються в багатьох країнах завдяки законам і нормативним актам, які підтверджують їх використання. Хоча конкретні правила можуть відрізнятися, електронні підписи стали важливим інструментом для сучасного бізнесу, пропонуючи ефективність, безпеку та гнучкість.[51]

Занурюючись в основи електронного підпису, важливо визначитися з правильною термінологією. Терміни «електронний цифровий підпис» та «цифровий підпис» часто використовують як взаємозамінні, але вони мають чіткі відмінності.

«Електронний цифровий підпис» — це загальний термін для позначення широкого спектру методів електронного підпису, які можуть варіюватися від введення імені до використання сенсорного екрану для фіксації підпису. Цим методам може бракувати передових криптографічних методів, які використовуються в цифрових підписах, що потенційно може призвести до відмінностей у безпеці та аутентифікації. Таким чином, електронні підписи, як правило, використовуються для менш важливих або внутрішніх документів і можуть мати різний ступінь юридичного визнання, залежно від чинного законодавства.

З іншого боку, «цифрові підписи» — це особливий тип електронного підпису, який характеризується використанням технології інфраструктури відкритих ключів (PKI) для забезпечення надійного захисту та аутентифікації. Вони створюють унікальний ідентифікатор для підписанта, забезпечуючи високий рівень довіри та зменшення ризику шахрайства. Цифрові підписи

зазвичай є найкращим вибором для юридично обов'язкових документів, фінансових угод і будь-яких сценаріїв, що вимагають вищого рівня безпеки та загальновизнаної юридичної сили.

Загалом, вибір між електронними та цифровими підписами залежить від вимог до безпеки та юридичної чинності конкретного документа, оскільки цифрові підписи є більш загальновизнаним рішенням для критично важливих або конфіденційних додатків. [52]

Рисунок 2.3 – Різниця між електронним та цифровим підписом

Зазвичай електронний підпис вважається дійсним і юридично обов'язковим, якщо він відповідає певним критеріям. Ці критерії можуть відрізнятися залежно від конкретних законів і нормативних актів у відповідній юрисдикції, але загалом, щоб електронний підпис вважався дійсним, він повинен включати:

- намір підписати — підписувач повинен мати чіткий намір підписати документ в електронному вигляді. Це може бути підтверджено за допомогою

таких дій, як натискання кнопки «Підписати» або згода з умовами надання послуг;

- згоду — усі сторони, що беруть участь у транзакції, повинні бути проінформовані та надати згоду на проведення транзакції в електронному вигляді;

- верифікацію особи — повинен існувати надійний метод перевірки особи підписувача, який гарантує, що електронний підпис є легітимним;

- аудиторські сліди — багато нормативних актів вимагають ведення контрольних журналів або відстеження документів, щоб відстежувати зміни, внесені до підписаного документа;

- відповідність чинному законодавству — електронний підпис повинен відповідати законам і правилам, що регулюють електронні підписи в юрисдикції, в якій він використовується;[53]

Нормативні акти можуть вимагати використання передових технологій електронного підпису, таких як цифровий підпис, у певних випадках, коли потрібен вищий рівень безпеки та аутентифікації. Дуже важливо ознайомитися з конкретними законами та нормативно-правовими актами щодо електронного підпису у регіоні, щоб переконатися, що електронні підписи є юридично дійсними та можуть бути застосовані на практиці. Для особливо важливих або регульованих транзакцій рекомендується проконсультуватися з юрисконсультом і вибрати сертифіковані рішення для електронного підпису, щоб забезпечити дотримання вимог.

Як і слід було очікувати, електронні підписи продовжують розвиватися та адаптуватися до технологічних досягнень і мінливих потреб бізнесу. Ось деякі нові тенденції у сфері електронного підпису, на які слід звернути увагу.

Мобільні електронні підписи поступово набуватимуть популярності. Використання смартфонів і планшетів для електронного підпису зростає. Оскільки популярність зростає від віддалених робочих місць до онлайн-

замовлень, технології електронного підпису дедалі більше задовольняють потреби користувачів, які перебувають у дорозі.

Голосові та біометричні підписи з розвитком технології зустрічатимуться частіше і частіше. Розпізнавання голосу та біометрична аутентифікація (наприклад, розпізнавання відбитків пальців або обличчя) розвинулися настільки, що їх можна використовувати як надійний засіб підтвердження особи користувача. [54]

Інтеграція з блокчейном буде невідворотною. Деякі платформи електронного підпису досліджують технологію блокчейн для підвищення безпеки документів і надання неспростовних доказів підпису та історії документів. Документи на блокчейні вже використовуються для відстеження продажів і прав власності на такі речі, як образотворче мистецтво та інтелектуальна власність.

Дистанційне нотаріальне посвідчення (RON) також стане більш популярним, нажаль з плином часу. Послуги RON дозволяють нотаріусам виконувати свої обов'язки в режимі онлайн і набирають популярності в регіонах, де електронне нотаріальне посвідчення визнано на законодавчому рівні.

Міжнародна експансія загалом, адже багато постачальників послуг електронного підпису розширюють свою діяльність для підтримки міжнародного електронного підпису, включаючи відповідність законодавству різних країн і підтримку різних мов. [55]

Підписи в доповненій реальності (AR), бо навіть зараз деякі платформи експериментують з технологією доповненої реальності, щоб підвищити аутентичність цифрових підписів, роблячи їх більш схожими на рукописні.

Покращені функції відповідності, з невплинним розвитком законодавства постачальники послуг електронного підпису додають функції, щоб забезпечити постійну відповідність зростаючим законодавчим вимогам.

Спільна робота з документами на підприємстві. Функції співпраці в режимі реального часу включаються в платформи електронного підпису, щоб спростити редагування, узгодження та підписання документів між кількома сторонами.

Машинне навчання для оцінки ризиків, адже алгоритми машинного навчання розробляються для оцінки ризиків, пов'язаних з окремими транзакціями з електронним підписом, підвищення безпеки та запобігання шахрайству. [56]

Хмарні та гібридні розгортання, завдяки тому що послуги електронного підпису переміщуються в хмару або пропонують гібридні варіанти розгортання, що забезпечує масштабованість і полегшує доступ для віддалених користувачів.

Ця технологія, безумовно, розвивається, і ми можемо очікувати, що інновації відповідно вплинуть на інструменти електронного підпису. Оскільки технологія електронного підпису продовжує розвиватися, компанії та користувачі можуть очікувати ще більшої гнучкості, безпеки та зручності в процесі електронного підпису. [57]

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ МЕТОДУ ПІДВИЩЕННЯ СТІЙКОСТІ ЕЦП

3.1 Опис середовища реалізації

Для практичної реалізації методу підвищення стійкості електронного цифрового підпису (ЕЦП) був вибраний програмний пакет на основі мови програмування Python із застосуванням криптографічної бібліотеки PyCryptodome. Використання саме цієї бібліотеки забезпечує великий набір криптографічних алгоритмів, включаючи алгоритми для створення ЕЦП, таких як RSA, ECDSA та EdDSA. Це нам дозволяє реалізувати різні варіанти підпису та перевірки підписів у рамках запропонованої системи.

Система має включати такі основні елементи:

- модуль генерації ключів для створення публічного та приватного ключів для кожного користувача;
- модуль підпису для підписання даних із використанням приватного ключа;
- модуль верифікації для перевірки підпису за допомогою публічного ключа;
- модуль для мультифакторної аутентифікації для перевірки особистості користувача за допомогою поєднання кількох методів, таких як OTP або біометрія, для підвищення рівня безпеки;

Для тестування реалізованої системи мною було обрано декілька різних сценаріїв, включаючи як класичні атаки на підпис, таких як, наприклад, модифікація уже підписаних даних користувачами, так і більш складні атаки, що включають спроби компрометації ключів, або ж злам системи і додавання несправжнього ключа, задля його подальшого використання. [58]

Проте нам також потрібно включити у цю систему ШІ, який буде перевіряти дані і завдяки якому буде виконуватися більша частина роботи. Тому, спочатку ми протестуємо усі методи комбінованих схем аутентифікації і

їхню роботу з ШІ, а потім порівняємо результати і виберемо найефективнішу, за декількома параметрами, такі як ефективність захисту інформації, надійність захисту та грошове питання впровадження.

Як же має проходити генерація ключів? Першим кроком буде створення публічного та приватного ключів за допомогою криптографічних алгоритмів ECDSA та RSA для порівняння ефективності та рівня безпеки. Далі нам потрібно організувати зберігання приватних ключів у захищеному середовищі, використовуючи HSM або за допомогою програмних засобів, таких як PyCryptodome, про яку ми вже вказали вище. Далі ми будемо використовувати OpenSSL для генерації сертифікатів та інтеграції із стандартами X.509 аби забезпечити сумісність з існуючими системами.

Алгоритм цифрового підпису еліптичних кривих (ECDSA) — це алгоритм підпису на основі криптографії еліптичних кривих (ECC). ECDSA базується на циклічних групах еліптичних кривих над обмеженими полями та проблемах задачі ECDLP (задача дискретного логарифмування еліптичних кривих). Метод підпису/перевірки ECDSA функціонує наступним чином і базується на множенні точок EC. Ключі та підписи ECDSA мають нижчий рівень безпеки, ніж ключі та підписи RSA при однаковому рівні безпеки. З точки зору безпеки 256-бітний підпис ECDSA можна порівняти з 3072-бітовим підписом RSA. Метод цифрового підпису еліптичної кривої є одним з різновидів електронного підпису (ECDSA). По суті, він використовується як ідентифікаційний документ для біткоїн-трейдерів. В основі процесу створення ключів ECDSA лежить складність методів ECDSA. Теоретично складно зламати код ECDSA, хоча хакери, безсумнівно, намагатимуться це зробити. Веб-сайти прагнуть завантажувати сторінки менш ніж за секунду. Маленькі клавіші, що використовуються в ECDA, допомагають прискорити роботу веб-сайту. Ви повинні використовувати ECDSA, якщо ви працюєте в екосистемі біткоїна. ECDSA виконує ту ж саму задачу, що і будь-який інший цифровий підпис, але швидше. Це дозволяє ECDSA забезпечити такий же рівень безпеки, як і будь-

який інший метод цифрового підпису, але з використанням меншої кількості ключів. ECDSA-сертифікати - тип електронного документа, який використовується для підтвердження особи власника сертифіката - створюються за допомогою ECDSA. Облікові дані містять підпис емітента сертифіката, який є надійною установою, інформацію про ключ, використаний для створення сертифіката, інформацію про власника сертифіката та дані сертифіката. Таким надійним емітентом зазвичай є центр сертифікації, що має підписаний сертифікат, який можна відстежити до центру сертифікації, що його видав, за допомогою ланцюжка довіри. [59]

Цей алгоритм працює на скінченних полях у класичній формі Вейєрштрасса над еліптичними кривими. Тому ці криві представлені параметром домену еліптичної кривої, який визначається різними криптографічними стандартами. Еліптичні криві, які використовуються в криптографії, можна визначити наступним чином:

Точка G — це точка для скалярного множення на кривій, яка множиться на ціле число на точку еліптичної кривої.

G генерує іншу точку n, яка є підмножиною точки еліптичної кривої, що виражає довжину приватного ключа, наприклад, 256 біт.

Процес генерації ключів, генерації підпису та перевірки ECDSA такий самий, як і EdDSA.

Заснований на ECC, EdDSA є варіацією методу підпису Шнорра. Закритий ключ (Prk) в EdDSA - це випадково створене хешоване число в точці шифрування, а відкритий ключ (Puk) є похідним від закритого ключа. Ed25519, точка EdDSA, яка використовує безпечний хеш-метод для створення пари ключів і створення цифрового підпису, була запропонована Бернштейном та ін. у 2011 році (SHA-512). Пара ключів створюється за допомогою криптографічної хеш-функції, яку використовує EdDSA, і ці хеш-функції повинні мати наступні чотири ключові характеристики.

Хеш-функції є односторонніми функціями, тому легко обчислити хеш-значення для заданого повідомлення, але зворотній процес неможливий.

Стійкість до підміни - для заданого повідомлення x і хеш-коду h = H(x) неможливо обчислити повідомлення y, для якого x ≠ y з h = H(y); друга стійкість до підміни - для заданого повідомлення x неможливо обчислити інше повідомлення y з тим самим хеш-значенням.

Сильна стійкість до колізій: неможливо знайти пару повідомлень (x, y) з однаковим хеш-значенням.

	Properties	RSA	ECDSA	EdDSA
1	Security bits			
	80	1024	160	160
	112	2048	224	224
	128	3072	256	256
	192	7880	384	384
	256	15360	512	512
2	Performance	Slow due to long key size	Fast	Fastest
3	Popularity	Widely used	Not much used	New and widely used

Рисунок 3.1 — Порівняння різних методів за категоріями «Захисні біти», «Продуктивність», «Популярність»

Протестувавши декілька методів ми оберемо EdDSA, адже він по всім параметрам, які наведені на рисунку, випереджає решту методів.

Саме для підпису даних у нас буде інший алгоритм. Для підписання даних використовувалась бібліотека PyCryptodome, що дозволяє працювати з

алгоритмами EdDSA. Дані підписуються користувачем, і при цьому перевіряється кожен крок який користувач робить, щоб гарантувати, що лише власник приватного ключа може створити підпис і ним затвердити документ.

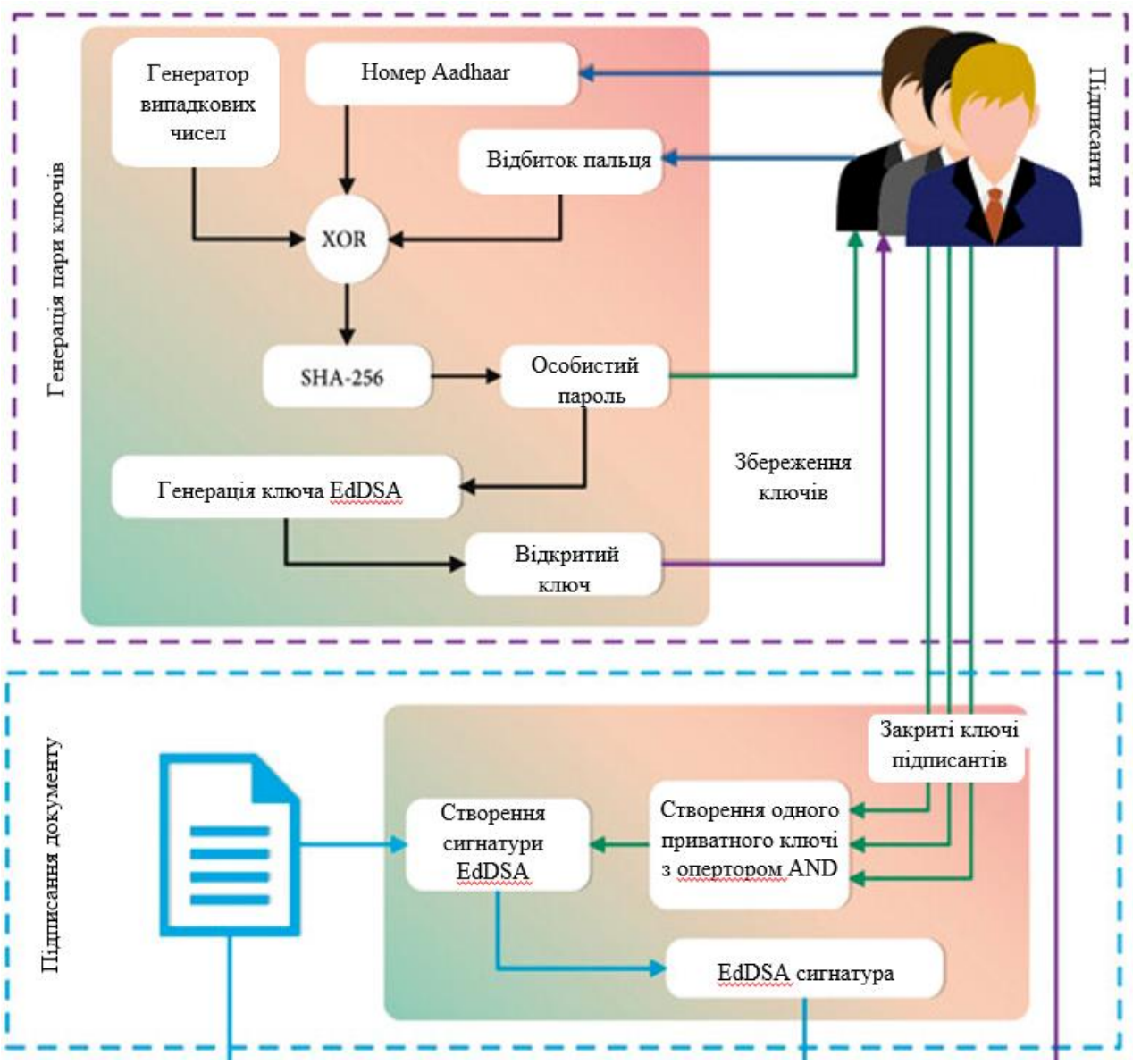


Рисунок 3.2 — Процес створення ключів та підписання документу

Верифікація підпису пройде наступний чином: після підписання документ може бути переданий іншій стороні для перевірки, тоді система використовує публічний ключ для верифікації підпису, а для верифікації

реалізовано додаткові перевірки на цілісність даних, що дозволяє зловити модифікацію даних після підписання.

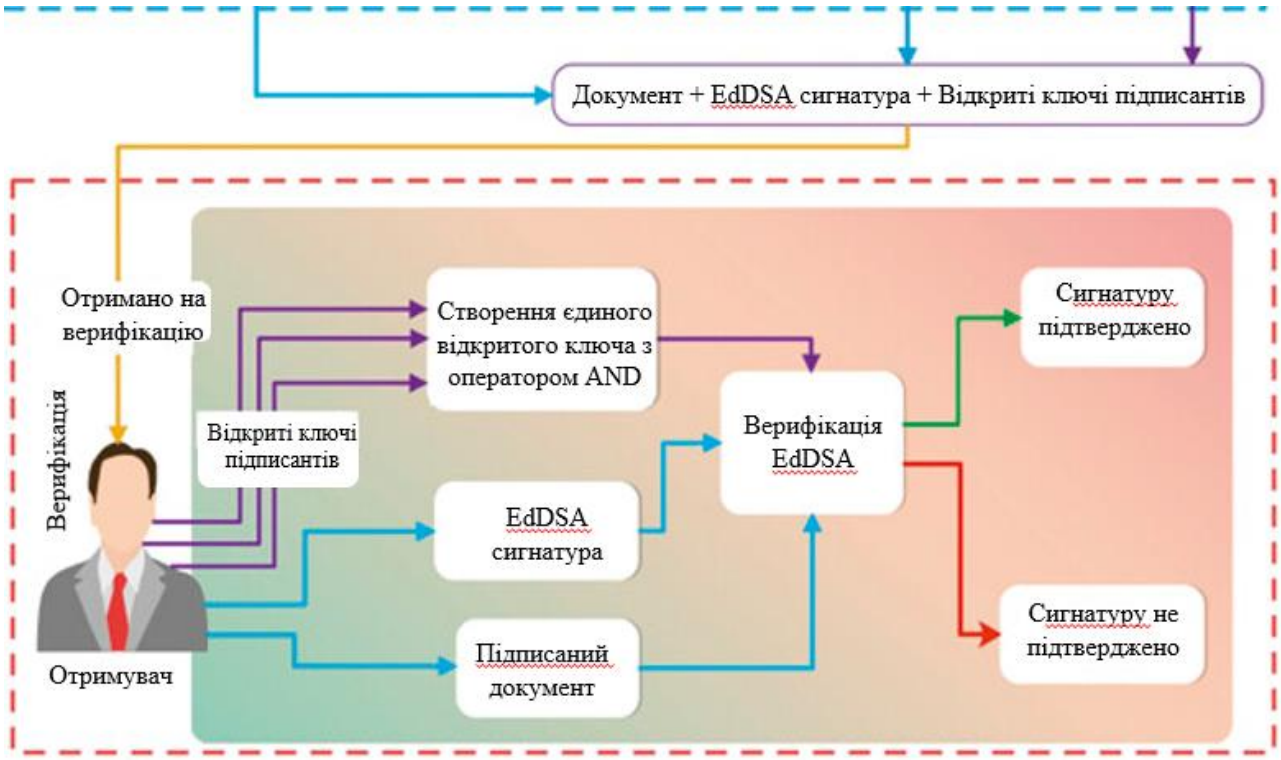


Рисунок 3.3 — Процес перевірки ключів за даним методом

Для тестування мультифакторної аутентифікації був реалізований додатковий модуль для генерування одноразових паролів (OTP) за допомогою Google Authenticator або за допомогою технології TOTP (Time-Based One-Time Password). Підписання даних вимагало не тільки введення пароля, але й верифікації за допомогою OTP-коду, що значно підвищує рівень захисту від фішингових атак. [60]

Для тестування системи було проведено кілька сценаріїв, щоб оцінити її стійкість до різних видів атак. Спочатку була проведена атака на цілісність даних. Метою цього тесту було перевірити, чи система здатна виявити модифікацію підписаних даних серед інших документів. Під час цього тесту підписаний документ був змінений, і система повинна була зафіксувати порушення цілісності. У результаті ті зміни документу які були проведені,

після верифікації підпису за допомогою публічного ключа, було помічено системою, відмічено неможливою, що підтвердило високу ефективність методу захисту.

Наступною була атака на ключі. В цьому тесті було проведено кілька спроб компрометації приватного ключа. Однією з таких спроб була спроба викрадення приватного ключа через фізичний доступ до сервера, де він зберігався. В результаті цієї атаки було досліджено, що використання HSM для зберігання ключів забезпечило високий рівень захисту, оскільки пристрій HSM не виводить ключі за межі захищеного середовища, навіть якщо сервер був зламаний.

Після неї атакою, яка цікавить нас найбільше, була атака на мультифакторну аутентифікацію. Для цього тесту був реалізований сценарій, коли зловмисник намагався отримати доступ до системи, використовуючи лише пароль, без знання одноразового паролю (OTP). У результаті зловмисник не зміг отримати доступ до системи без OTP, що доводить ефективність мультифакторної аутентифікації в захисті від фішингу.

Результати тестування показали високу ефективність запропонованої системи для підвищення стійкості ЕЦП. Всі основні типи атак були успішно відбиті:

- модифікація підписаних даних була швидко виявлена;
- система виявила спроби компрометації ключів завдяки використанню HSM;
- мультифакторна аутентифікація виявилася ефективною проти атак на паролі;

Ці результати підтверджують, що запропонований метод підвищення стійкості ЕЦП може бути застосований для забезпечення високого рівня безпеки в різних сферах, зокрема в банківських системах, державних органах та корпоративних мережах.

Комбіновані схеми аутентифікації використовують більше одного методу для підтвердження особи користувача. Це забезпечує підвищену безпеку, оскільки зловмиснику буде складніше обійти всі рівні захисту одночасно. Ось деякі з найбільш поширених комбінованих схем аутентифікації:

- мультифакторна аутентифікація (MFA);
- двокрокова аутентифікація + PIN/Пароль;
- аутентифікація за допомогою смарт-карти + Біометрія;
- контекстуальна аутентифікація + разовий пароль;
- аутентифікація за допомогою токена + SMS/Email;

Мультифакторна аутентифікація використовує два або більше незалежних факторів для підтвердження особи:

- щось, що знає користувач (пароль, PIN);
- щось, що має користувач (смартфон, токен, одноразовий пароль);
- щось, що є у користувача (біометрія, відбиток пальця, розпізнавання обличчя);

Нариклад, для входу в систему користувач може ввести пароль (щось, що він знає) та потім ввести одноразовий код з додатку на телефоні (щось, що він має). NIST (Національний інститут стандартів і технологій) визначає мультифакторну аутентифікацію як один із найбільш ефективних методів для захисту доступу до критичних системандарт FIDO2 для аутентифікації вимагає використання мультифакторного підходу, зокрема через WebAuthn.

Двокрокова аутентифікація і PIN/Пароль — це комбінація біометрії (наприклад, відбиток пальця або розпізнавання обличчя) з традиційним методом аутентифікації, таким як PIN або пароль. Така схема забезпечує високий рівень безпеки, оскільки біометричні дані складно підробити, а PIN або пароль додають додатковий рівень захисту. [61]

Наприклад, користувач може увійти в систему через відбиток пальця (біометрія) і ввести додатковий PIN-код для підвищення рівня безпеки. Високий рівень ефективності такої схеми показує використання Windows Hello,

яка поєднує біометричну аутентифікацію з додатковим PIN-кодом для доступу до операційної системи. Компанія Apple також використовує цю модель комбінації для аутентифікації в мобільних пристроях.

Аутентифікація за допомогою смарт-карти і Біометрія — у цій комбінації використовується смарт-карта (що містить у собі криптографічні ключі або сертифікати) та біометричні дані користувача. Це дозволяє поєднати фізичний носій (смарт-карту) з унікальними біометричними характеристиками користувача для більшого захисту.

Наприклад, використання смарт-карти для входу до корпоративної мережі разом з відбитком пальця або розпізнаванням обличчя для додаткової перевірки. GEMalto та Thales пропонують такі рішення для корпоративного доступу, де комбінуються смарт-карти з біометрією для критичних інфраструктур. EU Digital Identity у плейського Союзу передбачає використання таких комбінованих схем для доступу до державних послуг .

Контекстуальна аутентифікація і разовий пароль — визначає рівень ризику вхідної сесії на основі різних факторів, таких як географічне розташування, пристрій, з якого здійснюється доступ, та інші контекстні дані. Якщо ризик високий, система додатково запитує одноразовий пароль (OTP) для підтвердження особи. [62]

Наприклад, якщо користувач увійшов з незвичного пристрою або з іншого місця, і система запросила OTP для додаткової перевірки. Компанії, що спеціалізуються на інтелектуальному управлінні доступом, такі як Okta або Ping Identity, активно використовують контекстуальну аутентифікацію в поєднанні з OTP для підвищення безпеки при логіні. Google використовує подібні методи для сесій та запиту додаткової аутентифікації через OTP або push-сповіщення .

Аутентифікація за допомогою токена і SMS/Email — це одна з найбільш поширених схем у фінансових установах. Користувач отримує одноразовий код

на свій мобільний телефон або електронну пошту після введення токена (апаратного або програмного).

Наприклад, для здійснення транзакції користувач отримує одноразовий код на свій телефон, після введення якого транзакція підтверджується. Багато банків і фінансових установ використовують такі системи для підтвердження платежів та доступу до облікових записів. Це дозволяє підвищити безпеку і знизити ймовірність шахрайства .

Ці комбіновані схеми аутентифікації значно знижують ймовірність атак на систему завдяки поєднанню різних методів перевірки користувача. Вибір конкретної схеми залежить від вимог до безпеки, а також від специфіки використовуваних ресурсів. Зважаючи на те що ми будемо працювати на максимальний захист і максимальну ефективність, ми зробимо новий метод, за допомогою контекстуальної аутентифікації та біометрії.

3.2 Впровадження нової комбінованої схеми аутентифікації

Комбінація контекстуальної аутентифікації та біометрії є надзвичайно потужною схемою для підвищення безпеки. Це дозволяє одночасно використовувати контекстуальну інформацію про користувача та його фізичні характеристики для підтвердження особи. Далі буде проаналізовано як ці два методи взаємодіють між собою.

Контекстуальна аутентифікація аналізує різноманітні фактори, що дозволяють оцінити ризик конкретної сесії, таких як:

- географічне місце з якого користувач здійснює вхід (нове або незвичне місце може підвищити ризик). Система може виявити спроби входу з нетипового для користувача місця, використовуючи GPS, IP-адресу або дані з мережі Wi-Fi. Якщо вхід здійснено з іншої країни або незвичного регіону, система може запросити додаткові методи аутентифікації;

- тип пристрою і аналіз використання нового або незнайомого пристрою, що може бути сигналом до того, що аутентифікація має бути перевірена додатково. Контекст також може включати ідентифікацію пристрою, з якого користувач здійснює вхід вперше, використання нового пристрою може підвищити ризик;

- час входу і спроби входу в незвичний час може бути ознакою несанкціонованого доступу. Якщо вхід здійснюється в незвичний час, наприклад, пізно вночі або рано вранці, система може вважати це підозрілим і запитати додаткову перевірку;

- мережеві умови, тобто наявність VPN, проксі-серверів або нестабільних мереж також може підвищувати ризик. Використання VPN, проксі-серверів або нестабільних мереж може сигналізувати про потенційну загрозу, оскільки це може бути ознакою спроби приховати реальне місцезнаходження, що є типовою поведінкою зловмисників, а отже це ставить під загрозу систему;

Виявлення таких аномалій дозволяє адаптувати рівень безпеки відповідно до поточної ситуації, запитуючи додаткові фактори аутентифікації, якщо вони є необхідними.

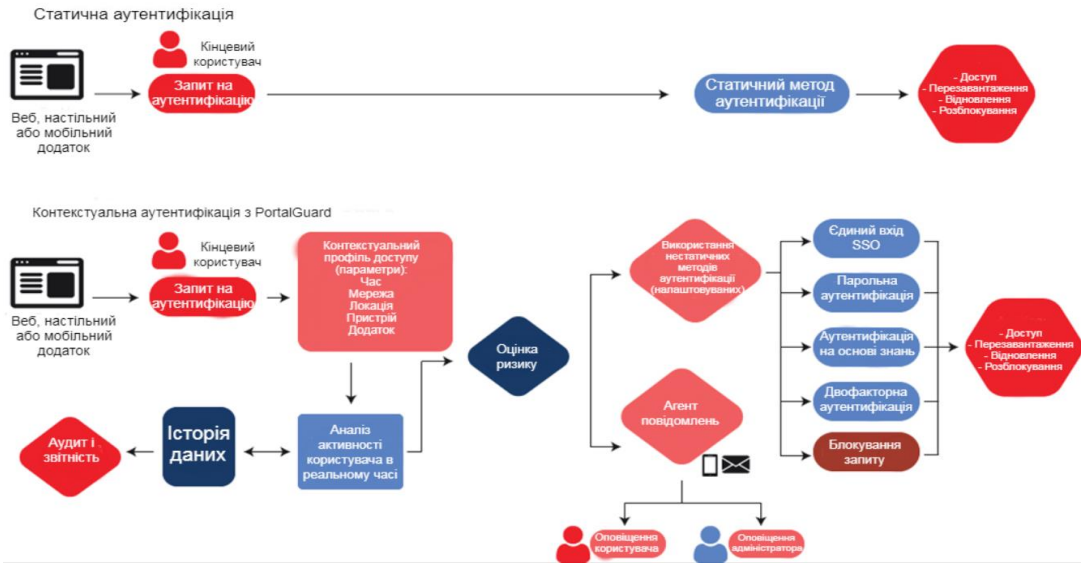


Рисунок 3.4 — Схеми контекстуальної аутентифікації і статичної

Впровадження контекстної аутентифікації у систему може принести безліч переваг. Ось деякі з них:

- підвищена безпека забезпечує більш надійний захист від несанкціонованого доступу;

- зручність для користувачів, оскільки вона може аутентифікувати користувачів на основі їхньої поведінки, вона часто вимагає менше даних від користувача, що робить процес більш плавним;

- зниження ризиків, бо истема може виявити незвичну поведінку і вжити відповідних заходів, тим самим знижуючи ризик витоку даних;

- адаптивність, через те що система здатна адаптуватися до нової поведінки та шаблонів користувачів, що робить її більш гнучкою, ніж традиційні методи;

Критерій	Контекстуальна аутентифікація	Статична аутентифікація
Механізм аутентифікації	Використовує динамічні фактори (геолокація, пристрій, час доступу).	Базується на постійних даних (пароль, PIN-код).
Гнучкість	Дуже гнучка, адаптується до змін у поведінці користувача.	Низька гнучкість, потребує оновлення паролів вручну.
Безпека	Забезпечує вищий рівень безпеки завдяки аналізу декількох контекстів.	Менш захищена через залежність від одного фактора.
Захист від атак	Ефективна проти атак на основі викрадених паролів або пристроїв.	Уразлива до фішингу, брутфорс-атак і перехоплення даних.
Зручність для користувачів	Вимагає мінімальної взаємодії, часто працює у фоновому режимі.	Користувачі повинні пам'ятати та вводити паролі.
Приклади використання	Банківські сервіси, корпоративні мережі, мобільні додатки.	Онлайн-сервіси, прості веб-сайти.
Вартість впровадження	Висока, оскільки потребує складних алгоритмів і обчислень.	Низька, легко впроваджується у базових системах.
Швидкість аутентифікації	Залежить від аналізу даних, але може бути швидкою при оптимізації.	Швидка, залежить лише від введення пароля.
Виявлення аномалій	Швидко виявляє аномальні дії завдяки аналізу поведінки.	Не виявляє аномалій, поки не станеться інцидент.

Рисунок 3.5 — Порівняння контекстуальної аутентифікації і статичної

Біометрія забезпечує додатковий рівень захисту завдяки унікальним фізичним характеристикам користувача. Серед основних біометричних методів:

- відбитки пальців;
- розпізнавання обличчя;
- розпізнавання райдужної оболонки ока;
- розпізнавання голосу;

Відомо, що деякі відбитки пальців важко відсканувати або розпізнати через стан шкіри, пошкодження, шрами або малу площу відбитка. Низька якість, старі, обрізані, пошкоджені зображення відбитків пальців є ще однією проблемою. Методи машинного навчання, такі як штучні нейронні мережі (ANN), глибокі нейронні мережі (DNN), машина опорних векторів (SVM) і генетичні алгоритми (GA), відіграють важливу роль у пошуку нестандартних рішень для проблем ідентифікації за відбитками пальців. Згідно з дослідницьким звітом, глибоке навчання, особливо згорткові нейронні мережі (CNN), досягло великого успіху в галузі комп'ютерного зору та розпізнавання образів, оскільки воно не вимагає спеціального виділення ознак. Глибоке навчання автоматично вивчає особливості та структури на достатній кількості навчальних даних. Ці переваги CNN роблять його ідеальним для різних завдань в системах автоматичного розпізнавання відбитків пальців/ідентифікації: сегментація, класифікація, виділення особливостей (дрібних точок і сингулярних точок), оцінка орієнтації хребта тощо.

Помилкове прийняття та помилкова відмова — давня проблема, пов'язана з різними відтінками шкіри та різними рисами обличчя. Глибоке навчання та машинне навчання зараз дуже популярні серед виробників для аналізу обличчя, що робить ідентифікацію простішою та точнішою. DL і ML довели, що вони можуть вирішувати складні проблеми безпеки; допомагають поліпшити коефіцієнт помилкового прийняття в різних демографічних групах. Після додаткового навчання ми побачили дуже успішні результати в різних атрибутах

обличчя. Ці біологічні ознаки обличчя представляють характеристики обличчя (відтінок шкіри, волосся на обличчі і т.д.) людини.

В одному випадку дослідницька група використала машинне навчання, щоб навчити систему розрізняти райдужну оболонку очей живих і померлих людей, створивши алгоритм і використавши для навчання базу даних очей живих і померлих людей. Вони досягли 99% точності з єдиним застереженням: людина повинна померти щонайменше 16 годин тому.

Системи розпізнавання мови на основі штучного інтелекту аналізують та інтерпретують людську мову, щоб ідентифікувати індивідуальні голосові патерни та інтонації. Ці системи використовують передові нейронні мережі для розрізнення нюансів у мовленні, підтримуючи різноманітні додатки - від голосових асистентів до інструментів доступності для людей з порушеннями мовлення. Здатність точно обробляти розмовну мову, адаптуючись до різних акцентів і шумів, покращує взаємодію з користувачем і підвищує безпеку, розширюючи застосування штучного інтелекту в розпізнаванні поведінки.

Біометрія є дуже потужним інструментом для аутентифікації, оскільки ці дані складно підробити або передати іншій особі. Вона додає фізичну ідентифікацію до процесу аутентифікації. Біометричні дані є надійним методом ідентифікації, оскільки вони важко підробляються або викрадаються в порівнянні з паролями або PIN-кодами. Це також дозволяє значно підвищити зручність, оскільки користувач може легко пройти аутентифікацію, не запам’ятовуючи складні паролі.

Рисунок 3.5 — Найбільш поширені типи біометричною аутентифікації

Коли ці два методи комбінуються, система може досягти високого рівня безпеки, що робить її надзвичайно ефективною у випадках, коли один із методів може бути обійдений. Система працюватиме тоді наступним чином: спочатку система перевіряє, чи є входу підвищений ризик на основі контекстуальних даних (новий пристрій, місце чи час). Якщо контекстний аналіз вказує на підвищений ризик, система запитує біометричну аутентифікацію, наприклад, відбиток пальця або розпізнавання обличчя. Далі, якщо жоден з контекстних факторів не викликає підозри, біометрія може використовуватись для нормальних входів. Однак, якщо контекст вказує на високий ризик, система вимагає біометричну перевірку для підтвердження особи.

Це створює більш складну і надійну перевірку користувача, ніж кожен метод окремо. В результаті зловмиснику буде набагато складніше підробити обидва фактори аутентифікації одночасно.

Наприклад, Google і Apple активно впроваджують таку комбіновану аутентифікацію в своїх системах:

- Google використовує Google Account для підтвердження входу, де спочатку перевіряються контекстуальні фактори, і, якщо це необхідно, вимагається додаткове підтвердження через біометрію (наприклад, за допомогою Google Authenticator або біометричних даних на телефоні);

- Apple використовує схожі механізми для свого Face ID, поєднуючи розпізнавання обличчя з контекстом (наприклад, місцем або пристроєм), щоб визначити, чи потрібно запитати додаткові методи підтвердження для входу;

Застосування ШІ для навчання біометричних алгоритмів не є новим. Галузь почала використовувати ШІ на початку 2000-х років, коли дослідники почали розробляти алгоритми розпізнавання облич, які включали методи ML, такі як машини опорних векторів (SVM), що дозволило комп'ютерам навчатися і розпізнавати обличчя з дедалі більшою точністю. Десятиліття потому галузь почала використовувати нейронні мережі, засновані на глибокому навчанні, для вилучення інформаційно багатих ознак з облич. Цей перехід до ресурсномістких, але точних алгоритмів був головним чином зумовлений наявністю великих наборів навчальних даних і обчислювальних пристроїв, таких як графічні процесори (GPU). Після успіху з розпізнаванням облич дослідники почали вивчати використання ШІ для розпізнавання відбитків пальців - набагато більш вузької сфери.

Оптимальна продуктивність біометричного алгоритму залежить від використання спеціалізованих знань про предметну область для створення надійних функцій, зменшення упередженості за допомогою відповідних стратегій навчання, а також забезпечення життєздатності для розгортання. Тому, аналізуючи технологію будь-якого постачальника, важливо враховувати технічні аспекти, такі як швидкість зіставлення і точність розпізнавання, які були визначені в міжнародних тестах/оцінках, розмір біометричних шаблонів, які можуть вплинути на апаратне забезпечення і загальну вартість володіння, а

також важливий, але часто недооцінюваний правовий аспект, тобто збір біометричних даних для навчання нейронних мереж.

Крім того, вкрай важливо забезпечити, щоб біометричні системи розроблялися і впроваджувалися етично і прозоро, з належними гарантіями захисту персональних даних, враховуючи постійні побоювання щодо потенційного зловживання біометричними технологіями і даними на основі штучного інтелекту, а також наслідки збору, зберігання і аналізу великих обсягів конфіденційної особистої інформації для приватності і безпеки.

Здатність нейронної мережі навчатися і точно зіставляти обличчя, відбитки пальців, райдужну оболонку ока та інші біометричні дані стає можливою завдяки навчанню з використанням великої кількості різноманітних і репрезентативних даних для навчання. Походження цих даних було предметом пильної уваги, а часом і суперечок. Наприклад, для розпізнавання облич в інтернеті є безліч вільно доступних джерел зображень облич - наприклад, соціальні мережі та інші канали. Як наслідок, деякі компанії вилучають ці зображення облич без жодного занепокоєння щодо законності використання зображень і, звичайно, без офіційної згоди власників.

У відповідь на таку практику деякі країни починають створювати і впроваджувати нове законодавство для захисту біометричних даних і прав громадян, а також для забезпечення керівних принципів справедливого і законного використання цих даних. Тим не менш, факт залишається фактом: кожна компанія повинна розробити власну етичну політику, яка визначає, як вона вирішує відповідально використовувати зображення та отримувати біометричні дані для навчання чесно і законно.

Існує три основні фактори, які впливають на швидкість і точність біометричних технологій.

По-перше, отримання біометричних даних на основі згоди для навчання коштує дорого, а обмін цими даними між промисловістю та науковими колами є мінімальним. Відсутність доступу до таких даних призводить до створення

ненадійних і малоефективних алгоритмів, які можуть бути сильно упередженими до певної статі, раси чи етнічної приналежності.

По-друге, розробка високопродуктивного алгоритму, який буде використовуватися, наприклад, в автоматичній системі біометричної ідентифікації (ABIS) і здатний зіставляти потенційно мільярди людей з однаково високою швидкістю і точністю розпізнавання, вимагає наявності команди дослідників і розробників, які володіють знаннями в області біометрії і глибоким досвідом проектування, розробки та впровадження такої системи. Такий досвід можна здобути лише через участь у створенні проектів національного масштабу.

Нарешті, розробка найкращих біометричних алгоритмів вимагає постійних інвестицій у дослідження, тестування та вдосконалення. Існує кілька незалежних міжнародно визнаних біометричних тестових лабораторій та інститутів, таких як NIST (Національний інститут стандартів і технологій), BixeLab, iBeta та інші, де постачальники можуть тестувати свої технології, щоб забезпечити якість і зрозуміти свою позицію на ринку.

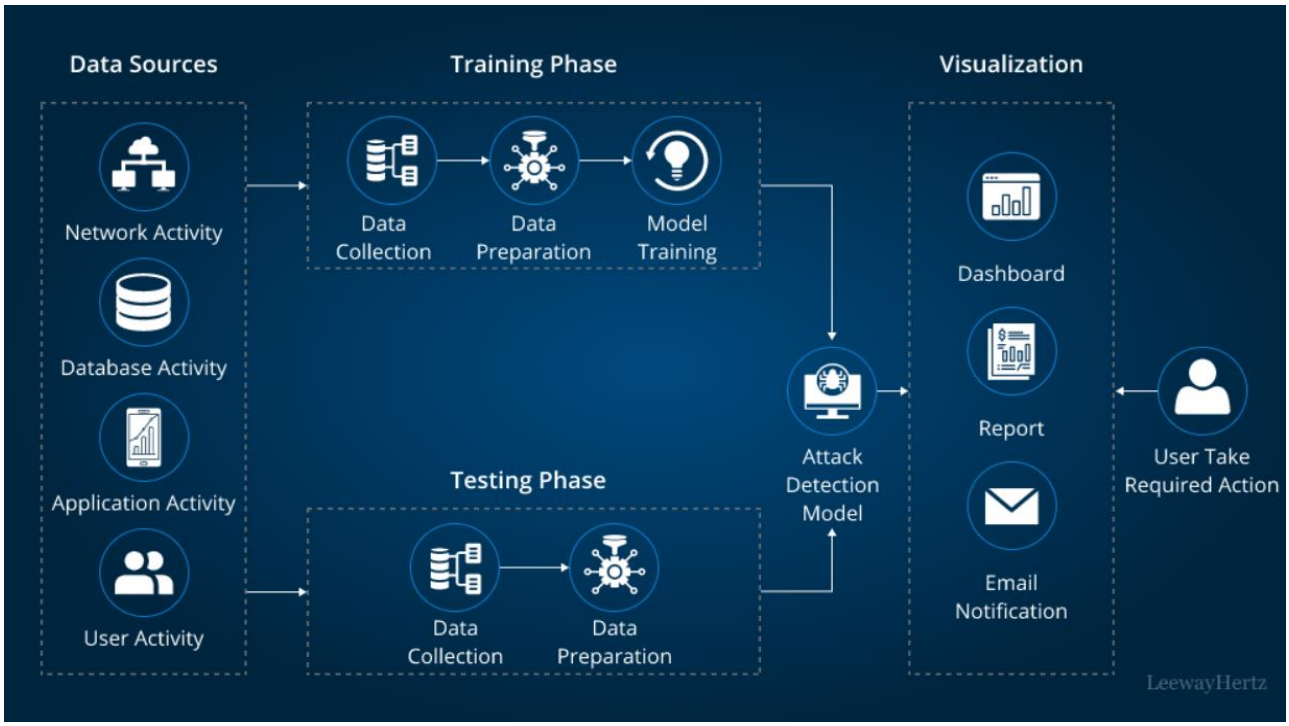


Рисунок 3.6 — Схема тренування ШІ якої ми будемо притримуватися

Переваги такої комбінації:

- покращена безпека — два різні шари аутентифікації значно ускладнюють доступ до системи зловмисникам;

- зручність для користувача — якщо ризик входу низький, користувач може увійти з мінімальними зусиллями, але при високому ризику буде використовувати додаткові методи для підтвердження;

- адаптивність — система може динамічно змінювати рівень безпеки залежно від ситуації;

Але недоліками такої комбінації є:

- потреба більш складного обладнання — для біометрії потрібно використовувати спеціалізовані пристрої, такі як сканери відбитків пальців або камери для розпізнавання обличчя;

- проблеми конфіденційності — збір біометричних даних може викликати занепокоєння щодо конфіденційності користувачів, особливо якщо ці дані зберігаються на віддалених серверах;

Загалом, комбінація контекстуальної аутентифікації з біометрією є дуже ефективною для захисту від несанкціонованого доступу в складних або високоризикованих умовах, таких як фінансові системи, корпоративні мережі чи урядові сервіси.

Коли контекстуальна аутентифікація поєднується з біометрією, користувач отримує додатковий рівень захисту. Якщо система виявляє підвищений ризик (наприклад, вхід із нового пристрою або з іншого місця), вона може вимагати біометричну перевірку для забезпечення ідентичності користувача. Приміром, Google використовує технологію Google Authenticator або вбудовані функції для додаткової перевірки, коли користувач намагається увійти в свій обліковий запис з незвичного місця або пристрою. Після перевірки контексту система запитує біометричну перевірку через смартфон чи планшет. Apple з Face ID активно використовує схожий підхід, коли користувач

має пройти біометричну аутентифікацію після того, як система визначить, що вхід здійснюється з незвичного місця або пристрою.

Цей метод здається ідеальним для впровадження, але перш ніж ми остаточно його впровадимо, нам потрібно також вказати і недоліки даної системи. Перш за все під прицілом будуть біометричні дані, через те що вони є дуже чутливими і вимагають суворого захисту. Їх зберігання та обробка повинні відповідати високим стандартам безпеки, щоб уникнути витоків даних. Необхідно забезпечити шифрування та захист біометричних даних на всіх етапах їх обробки. Регламент ЄС щодо захисту даних (GDPR) вимагає особливої уваги до обробки біометричних даних, оскільки їх розголошення може призвести до серйозних наслідків для конфіденційності користувачів.

Далі потрібно наголосити на витрати на впровадження та підтримку. Використання біометрії вимагає спеціалізованого обладнання, що може бути дорогим для впровадження, особливо в великомасштабних організаціях. Крім того, необхідна регулярна підтримка таких систем, що також може додати витрат. Попри поширені помилкові уявлення, витрати, пов'язані зі штучним інтелектом і кібербезпекою, часто перебільшують. Багато хто вважає, що впровадження рішень з кібербезпеки на основі штучного інтелекту вимагає значних фінансових інвестицій і під силу лише великим корпораціям. Однак технологічний прогрес зробив ці рішення більш доступними і прийнятними для бізнесу будь-якого розміру. Крім того, штучний інтелект може підвищити ефективність і знизити довгострокові витрати, автоматизуючи виявлення загроз і реагування на них, мінімізуючи потребу в активному втручанні людини. Розуміючи справжні витрати і переваги, організації можуть приймати обґрунтовані рішення і використовувати ШІ для посилення своєї кібербезпеки без зайвих витрат.

Хоча початкові витрати на ШІ та рішення з кібербезпеки можуть здатися страшними, ціна недостатнього захисту набагато вища. Є наступна статистика щодо кіберзлочинності:

- середня вартість витоку даних у 2021 році становила $4,24 млн, згідно зі звітом IBM «Вартість витоку даних» (Cost of a Data Breach Report);

- за прогнозами, до 2025 року кіберзлочинність коштуватиме світу $10,5 трлн щорічно, порівняно з $3 трлн у 2015 році (Cybersecurity Ventures);

- 60% малих підприємств, які зазнали кібератаки, припиняють свою діяльність протягом шести місяців (Національний альянс кібербезпеки);

У висновку ми можемо сказати що комбіновані методи контекстуальної аутентифікації та біометрії представляють собою перспективний підхід до підвищення безпеки доступу до інформаційних систем. Цей метод забезпечує високу надійність та зручність для користувачів, що є важливим фактором у сучасному цифровому середовищі. Однак для забезпечення максимальної безпеки важливо враховувати можливі ризики, пов'язані з конфіденційністю даних та витратами на впровадження таких систем.

Практична реалізація комбінованої схеми контекстуальної аутентифікації з біометрією може бути складною, але цілком досяжною. Для цього потрібно розробити систему, яка поєднує кілька методів для перевірки користувача.

Спочатку необхідно реалізувати механізм збору і аналізу контекстної інформації про користувача, щоб система могла оцінити ризик доступу. Визначення місця користувача за допомогою:

- IP-адреси — можна використовувати API для визначення географічного розташування за IP-адресою;

- GPS-дані (для мобільних пристроїв) — можна отримати місцезнаходження через GPS-модуль на телефоні;

- Wi-Fi чи Bluetooth — визначення через місцеві мережі або точки доступу;

Збирати інформацію про пристрій, з якого відбувається вхід може бути організовано через:

- UA-рядок (User-Agent) — відомості про пристрій можна отримати за допомогою HTTP-запитів (браузер, операційна система, версія);

- Ідентифікатор пристрою (на мобільних телефонах) через UUID (унікальний ідентифікатор);

Оцінка часового вікна, коли здійснюється вхід і аналіз цього за допомогою ШІ. Це дозволяє відстежувати нетипові години для доступу. Можна просто порівняти поточний час з найбільш звичними для користувача.

Якщо підключення здійснюється через VPN, проксі-сервери чи інші методи маскування, це має викликати підвищену підозру. ШІ буде це враховувати через перевірку IP-адреси на використання таких сервісів.

Для біометрії потрібно обрати метод, який найкраще відповідає вашим вимогам за рівнем безпеки та зручності.

Розпізнавання обличчя за допомогою камер телефонів або комп'ютерів (як у випадку з Face ID на iPhone чи Windows Hello на ПК). Відбитки пальців, за умови якщо пристрій підтримує цей метод (мобільні телефони чи планшети з вбудованими сенсорами). Розпізнавання райдужної оболонки ока, який є найвищим рівнем безпеки, але потребує спеціального обладнання (наприклад, телефонів з Iris Scanner). Голосова аутентифікація може бути додатковим рівнем перевірки через біометричний голосовий аналізатор, що використовує унікальні характеристики голосу користувача.

Найскладніша частина — інтеграція двох механізмів. Ось як це можна зробити. Перш за все, система повинна проаналізувати контекстуальні фактори (місце, пристрій, час тощо). Наприклад, якщо користувач входить з нового пристрою або в незвичний час, система підвищує рівень безпеки.

Якщо дані вказують на підвищений ризик (наприклад, вхід з нової географічної локації або через VPN), система переходить до другого етапу аутентифікації — біометрії.

Після оцінки контексту, система ініціює перевірку біометричних даних. Біометрія через мобільні пристрої може бути реалізована через спрощену перевірка, наприклад, через відбиток пальця або Face ID. Якщо користувач

успішно пройшов біометричну перевірку, доступ до програм та функцій надається.

У разі підвищеного ризику система може запросити додаткову перевірку. Може бути використано одноразовий пароль (OTP), який буде надіслано на електронну пошту або через SMS. Система може також запитати підтвердження через додаткові біометричні методи, якщо один вже використано (наприклад, після Face ID може бути запитано відбиток пальця).

Для визначення географічного місця можна використати API, наприклад такі як IP-геолокація або GPS-модуль. IP-геолокація може бути реалізована через такі сервіси, як IPinfo.io або GeoIP2, у цій же самі системі також можна використати і GPS-модуль для мобільних пристроїв. Якщо операційна система мобільного пристрою використовує Android — потрібно запровадити API (LocationManager), у випадку якщо операційна система мобільного пристрою використовує iOS — нам краще підійде API (CLLocationManager).

Для того щоб біометрія адекватно працювала на мобільних додатках ми скористаємося BiometricPrompt API для Android, що надає для біометричної аутентифікації, а якщо система підтримує iOS, то тоді ми використаємо LocalAuthentication.framework для Face ID і Touch ID.

Для серверних додатків у офісних приміщеннях можна інтегрувати реалізацію серверних рішень для розпізнавання обличчя або голосу. Краще за все підійдуть такі сервіси як Microsoft Azure Cognitive Services для Face API або Google Cloud Vision для аналізу зображень.

Однією з ключових послуг у цій категорії є комп'ютерний зір. Цей сервіс може аналізувати та розуміти зміст зображень. Він може ідентифікувати об'єкти, розпізнавати обличчя і навіть читати друкований або рукописний текст. Це робить його потужним інструментом для різноманітних застосувань, від автоматизації генерації метаданих для великої бібліотеки зображень до створення системи OCR (оптичного розпізнавання символів).

Далі є Face API. Цей сервіс може виявляти, розпізнавати та аналізувати людські обличчя на зображеннях. Він може ідентифікувати окремих людей, визначати емоції і навіть оцінювати вік і стать. Це можна використовувати в різних сценаріях, від персоналізації користувацького досвіду на основі виразу обличчя до впровадження біометричної аутентифікації, що нас і цікавить.

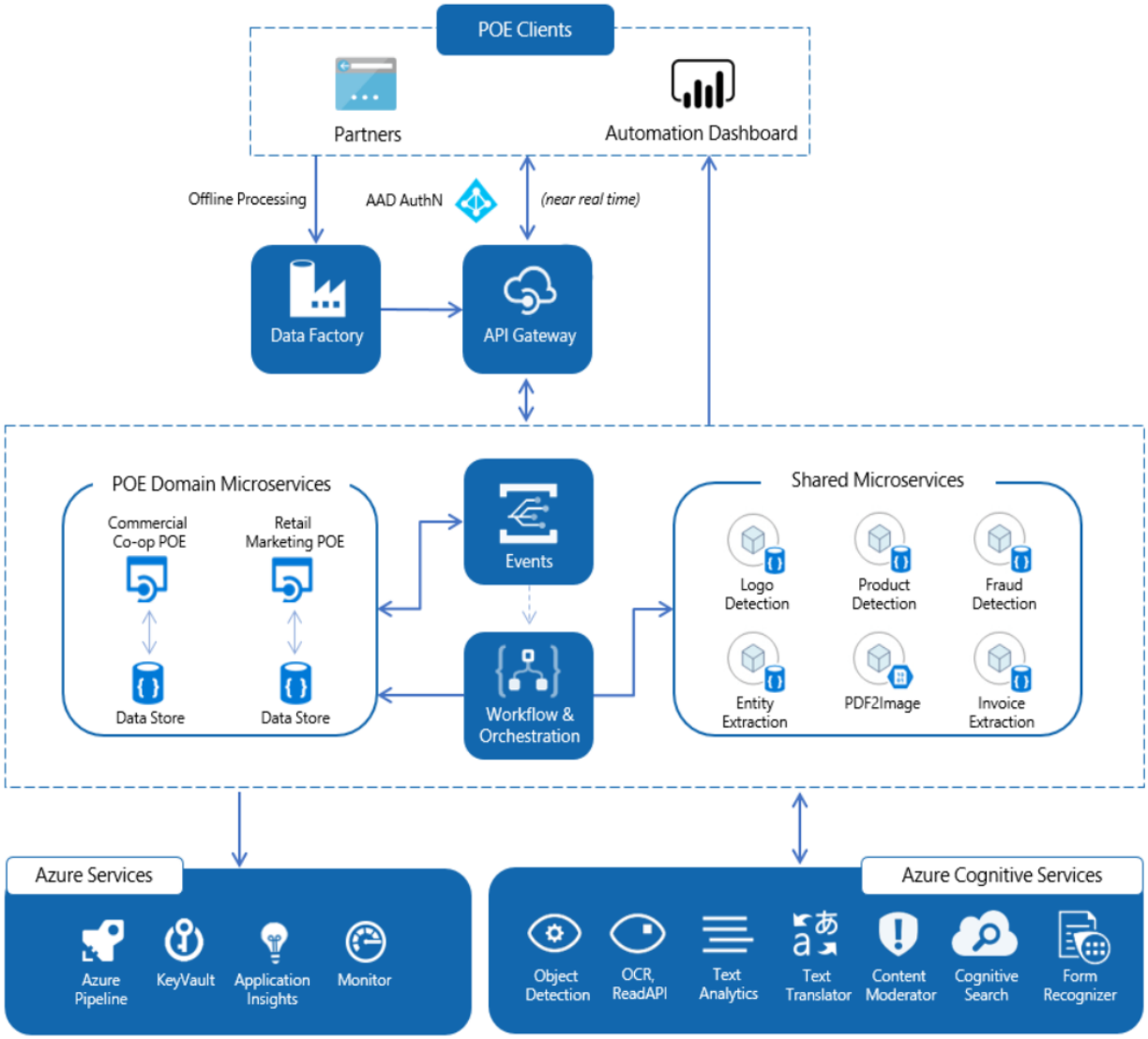


Рисунок 3.7 — Схема роботи Microsoft Azure Cognitive Services

Цей сервіс може витягувати інформацію з відео, включаючи ключові слова, написи та обличчя, і навіть може транскрибувати мову в текст. Це робить його потужним інструментом для творців відеоконтенту, оскільки він дозволяє

їм автоматично генерувати метадані для своїх відео, полегшуючи їх пошук і категоризацію.

Служба Speech to Text — це потужний інструмент, який може перетворювати усну мову на письмовий текст. Його можна використовувати в різних програмах - від служб транскрипції, які перетворюють мову на текстові документи, до функцій голосових команд, що дозволяють користувачам керувати програмами за допомогою голосу.

Окрім розуміння навколишнього світу, програмам також потрібно приймати рішення на основі цього розуміння. Microsoft Azure Cognitive Services надають послуги, які допомагають програмам приймати обґрунтовані рішення, підвищуючи їхню корисність та ефективність.

Azure Content Moderator — це служба автоматизованої модерації, яка може перевіряти та модерувати вміст відповідно до ваших вказівок. Вона може виявляти потенційно образливий або неприйнятний вміст у текстах, зображеннях і відеоданих, допомагаючи підтримувати безпечне та позитивне середовище для ваших користувачів.

З іншого боку, сервіс AI Anomaly Detector призначений для виявлення аномалій у часових рядах даних. Він може ідентифікувати незвичайні шаблони або рідкісні події у ваших даних, які можуть призвести до значних проблем або можливостей. Це можна використовувати в різних сценаріях, наприклад, для виявлення шахрайства у фінансових транзакціях, виявлення системних проблем у даних моніторингу в режимі реального часу або виявлення тенденцій продажів у бізнес-даних. [63]

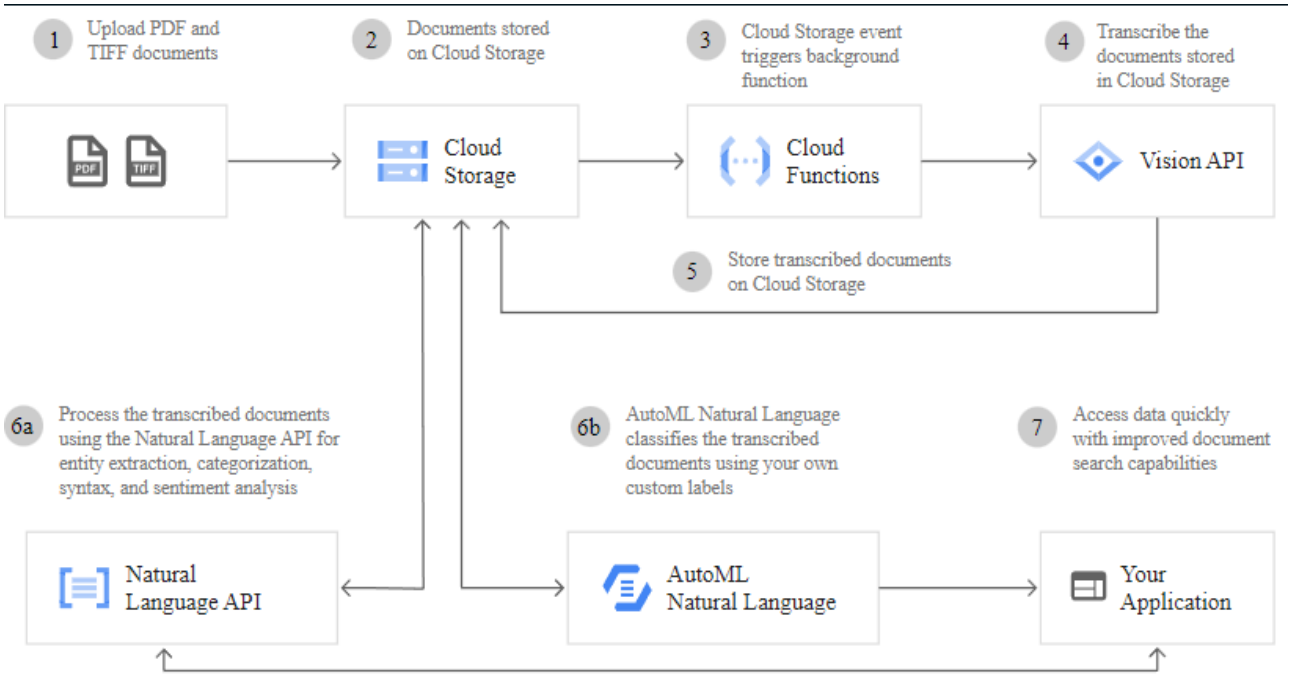


Рисунок 3.8 — Схема роботи Google Cloud Vision

Google Cloud Vision - це передова технологія, яка зробила революцію в галузі комп'ютерного зору в сферах ШІ та ML. Цей потужний API дозволяє розробникам інтегрувати функції розпізнавання зображень у свої додатки, надаючи їм безліч функціональних можливостей. Однією з ключових особливостей Google Cloud Vision є здатність розпізнавати етикетки. Використовуючи потужні моделі машинного навчання, він може точно ідентифікувати та класифікувати об'єкти на зображенні. Ця функція особливо корисна в таких сферах, як електронна комерція, де автоматична категоризація продуктів має вирішальне значення. Виявлення тексту - ще одна важлива функція, яку пропонує Google Cloud Vision. Вона дозволяє розробникам витягувати текст із зображень і розпізнавати різні мови. Ця функціональність відкриває можливості в різних сферах, таких як аналіз документів, переклад і навіть перетворення тексту в мову. Google Cloud Vision також відмінно справляється з розпізнаванням та аналізом облич. Розробники можуть використовувати цю функцію для виявлення облич на зображеннях, аналізу атрибутів обличчя, таких як емоції, і навіть розпізнавання відомих людей. Ця

функція має величезний потенціал у таких сферах, як безпека, аналітика соціальних мереж і навіть у створенні персоналізованого користувацького досвіду. Серед інших важливих функцій Google Cloud Vision — розпізнавання орієнтирів, що дозволяє ідентифікувати популярні об'єкти на зображеннях, та розпізнавання логотипів, що дозволяє компаніям захищати свій бренд, відстежуючи використання своїх логотипів на різних платформах. Отже, Google Cloud Vision — це революційна технологія в галузі комп'ютерного зору. Завдяки різноманітним функціям і можливостям він дає розробникам змогу створювати інноваційні додатки, які використовують силу візуальних даних.

Google Cloud Vision здійснив революцію в галузі комп'ютерного зору в ШІ та ML завдяки своїм потужним можливостям і простоті використання. Ця технологія має широкий спектр застосувань у різних галузях, відкриваючи нові можливості та ідеї. Одне з ключових застосувань Google Cloud Vision - розпізнавання зображень. Завдяки вдосконаленим алгоритмам машинного навчання платформа може аналізувати та ідентифікувати об'єкти, орієнтири та обличчя на зображенні. Ця можливість має ключове значення в різних галузях, таких як електронна комерція, де візуальний пошук був вдосконалений для покращення користувацького досвіду. Платформи електронної комерції тепер можуть дозволити користувачам шукати продукти, просто завантаживши зображення. Ще одне застосування Google Cloud Vision — оптичне розпізнавання символів (OCR). Ця технологія дозволяє витягувати текст із зображень, що робить її ідеальною для галузей, які мають справу з великими обсягами друкованого або рукописного тексту. Від оцифрування документів до автоматичного розпізнавання номерних знаків, OCR стало невід'ємною частиною сучасних систем. Крім того, Google Cloud Vision пропонує розширений аналіз настроїв. Аналізуючи вираз обличчя та розуміючи емоції, передані на зображеннях, компанії можуть отримати цінну інформацію про поведінку та задоволеність клієнтів. Це особливо корисно в роздрібній торгівлі,

рекламі та маркетингових дослідженнях, дозволяючи компаніям відповідно адаптувати свої стратегії та контент. [64]

Інтеграція Google Cloud Vision з технологіями AI (штучний інтелект) і ML (машинне навчання) зробила революцію в галузі комп'ютерного зору. Завдяки поєднанню цих передових технологій Google Cloud Vision став потужним інструментом для аналізу та розпізнавання зображень. Алгоритми ШІ та ML дозволяють Google Cloud Vision точно класифікувати зображення і виявляти на них різні об'єкти, обличчя та орієнтири. Система може навіть ідентифікувати емоції, що відображаються на людських обличчях, що робить її безцінним інструментом для аналізу настроїв і маркетингових досліджень. Крім того, інтеграція з технологіями штучного інтелекту та машинного навчання підвищує точність і швидкість аналізу зображень, що робить її придатною для різних застосувань. Наприклад, інтеграція Google Cloud Vision з алгоритмами машинного навчання дозволяє автоматично тегувати та класифікувати зображення, спрощуючи управління контентом та його організацію для бізнесу. Можливість інтеграції зі штучним і машинним інтелектом також сприяє здатності Google Cloud Vision розпізнавати текст на зображеннях. Ця функція дозволяє автоматично витягувати дані із зображень, що дає змогу ефективно оцифровувати документи, аналізувати бізнес-дані та перекладати тексти. Інтеграція Google Cloud Vision з технологіями штучного інтелекту та машинного навчання трансформувала сферу комп'ютерного зору. Ця потужна комбінація підвищує точність аналізу зображень, автоматизує завдання обробки і відкриває широкий спектр застосувань у таких галузях, як електронна комерція, охорона здоров'я та безпека.

Далі постає проблема обробки даних, якими ми будемо тренувати ШІ.

Всі біометричні дані повинні бути зашифровані за допомогою стандартів шифрування, таких як AES-256 для зберігання і передачі даних, а також дані повинні відповідати вимогам законодавства, зокрема GDPR для зберігання та обробки біометричних даних. Але перш ніж мі впровадимо ці зміни у реальну

систему, нам потрібно провести тестування і визначити, чи не будуть ці зміни гірші на практиці.

Для цього ми створимо середовище для тестування, на базі технологічного забезпечення підприємства, із стандартними налаштуваннями системи. Ми будемо використовувати операційну систему Windows 10, як більш стабільну версію, і проведемо десять спроб атак на різні етапи, щоб впевнитися, що зміни будуть корисні.

4. ПРОВЕДЕННЯ ТЕСТУВАННЯ СИСТЕМИ ТА ПОРІВНЯННЯ РЕЗУЛЬТАТІВ

4.1 Проведення тестувань

Наше тестування проходитиме наступним чином: перш за все ми порівняємо два додатки, а потім проведемо тестування, де користувач намагається увійти до системи. Потім система збирає контекстні дані: місце розташування, тип пристрою, час входу і якщо ці дані не викликають підозр, система дозволяє доступ. Проте, у разі підвищеного ризик (наприклад, новий пристрій, нова геолокація, незвичний час входу у мережу), система запитує біометричну аутентифікацію. Якщо користувач проходить перевірку біометрії успішно — доступ надається, в іншому випадку — доступ блокується або відбувається додатковий запит (OTP).

Таблиця 1 — Порівняння Google Cloud Vision API і Azure Content Moderator

Критерій	Google Cloud Vision API	Azure Content Moderator
1	2	3
Основне призначення	Аналіз зображень для витягу інформації, розпізнавання об'єктів та тексту	Модерація контенту для виявлення неприйнятного тексту, зображень та відео
Переваги	Висока точність розпізнавання об’єктів і тексту. Широкий набір функцій для аналізу зображень.	Потужний інструмент для фільтрації неприйнятного контенту. Інтеграція з іншими сервісами Azure.
Недоліки	Відсутність гнучкого налаштування. Менша увага до тексту і картинок.	OCR підтримується лише через окремі сервіси (не вбудовано). Менший набір функцій для обробки зображень.
Основні функції	Розпізнавання об'єктів, тексту, лого, сортування зображень. Аналіз змісту на небажані елементи.	Виявлення неприйнятного тексту, зображень. Фільтрація тексту на основі регулярних оновлень.

Кінець таблиці 1

1	2	3
Підтримувані формати	Зображення: JPG, PNG, BMP, GIF	Зображення: JPG, PNG. Текст: Plain text, HTML
Розпізнавання тексту (OCR)	Високоточне розпізнавання друкованого тексту (включаючи українську)	OCR підтримується окремими сервісами (наприклад, Read API в Azure Cognitive Services)
Виявлення небажаного контенту	Моделі для виявлення контенту для дорослих, насильства	Розширені механізми для текстової та візуальної модерації
Гнучкість налаштувань	Мінімальні можливості для кастомізації	Можливість налаштування словників і фільтрів для модерації
Інтеграція	Тісна інтеграція з екосистемою Google Cloud	Глибока інтеграція з іншими сервісами Microsoft Azure
Вартість	Платна, з безкоштовним лімітом (до 1000 запитів OCR на місяць)	Платна, безкоштовно до 10,000 текстових запитів щомісяця
Переваги у вартості	Зручна для невеликих проєктів через безкоштовні ліміти	Безкоштовний початковий обсяг запитів дає змогу протестувати сервіс перед масштабуванням
Недоліки у вартості	Може бути дорогою для масштабних проєктів	Вартість швидко зростає при обробці великих обсягів даних
Підтримка мов	Підтримує більше 50 мов, включаючи українську	Підтримує українську для тексту, але не всі функції адаптовані для інших мов
Область використання	Автоматизація візуальних завдань, аналіз документів, безпека контенту	Модерація соціальних мереж, фільтрація текстів і мультимедіа
Додаткові особливості	Розпізнавання рукописного тексту, логотипів, орієнтації	Інструменти для навчання модераторів, можливість автоматизації модерації
Панель керування	Простий інтерфейс для управління запитами	Інтуїтивна панель Azure Portal з кастомними звітами

Надалі ми продовжимо з перевірки існуючої системи, аби мати на руках конкретні результати ефективності уже впроваджених рішень.

Рисунок 4.1 — Діаграма результатів тестування початкової системи аутентифікації

Реалізація комбінованої схеми контекстуальної аутентифікації з біометрією є високоефективною для підвищення безпеки в цифрових системах. Вона дозволяє максимально використовувати як контекстуальну інформацію, так і фізичні характеристики користувача для забезпечення надійного доступу, мінімізуючи ризик несанкціонованого входу. Щоб перевірити це, ми введемо у роботу нову комбіновану схему і проведемо такі ж самі тести, щоб визначити наскільки якісно вона справляється із атаками на дані. Для підвищення рівня безпеки ця система буде аналізувати контекстні фактори, такі як:

- географічне розташування користувача — щоб відслідковувати, звідки здійснюється вхід. Наприклад, якщо співробітник намагається увійти в систему з країни, де компанія не веде бізнес, або з нової локації, система сигналізує про високий рівень ризику;

- тип пристрою — кожен пристрій співробітника реєструється в системі. Якщо доступ здійснюється з нового або незареєстрованого пристрою, система запитує додаткову перевірку через біометрію;

- час входу — якщо співробітник намагається увійти в систему поза робочим часом, це також викликає підвищену увагу і активує біометричну перевірку;

- біометрія — якщо йде не співпадіння з даними які числяться у сховищі системи, то буде запропоновано або ж пройти біометрію ще раз, або, за вичерпанням спроб, звернутися до адміністратора;

Зважаючи на вимоги безпеки та зручності, було вирішено використовувати розпізнавання обличчя для біометричної аутентифікації на мобільних пристроях, а для користувачів із робочими ноутбуками та ПК — відбитки пальців через вбудовані сканери. Це дозволяє зберігати високий рівень безпеки, не створюючи зайвих незручностей для співробітників.

Впровадження комбінованої схеми аутентифікації виявилося важливим кроком у забезпеченні більш надійного доступу до внутрішніх систем компанії.

Початкова перевірка здійснюється тоді, коли співробітник намагається увійти в систему, і у цей же час система автоматично збирає контекстну інформацію. Це включає перевірку місця розташування за допомогою IP-адреси або GPS на мобільному пристрої. Якщо ж вхід здійснюється через VPN або з нового регіону, система оцінює це як високий ризик і переходить до наступного етапу — біометрії. Якщо контекстна перевірка не викликає підозри, система дозволяє користувачу пройти стандартну біометричну перевірку (Face ID на мобільних телефонах або відбиток пальця через вбудовані сканери). У разі виявлення ризику (наприклад, вхід із нової географічної локації, нового пристрою або через незвичний час), система запитує додаткову біометричну перевірку. Наприклад, після успішної перевірки через розпізнавання обличчя на мобільному телефоні, може бути запитано підтвердження через відбиток

пальця або одноразовий пароль (OTP), надісланий через SMS або електронну пошту.

На етапі тестування система піддається стрес-тестуванню для того, щоб перевірити її ефективність в умовах реальних атак. Спочатку ми проведемо тестування на вхід з незнайомої географічної локації.

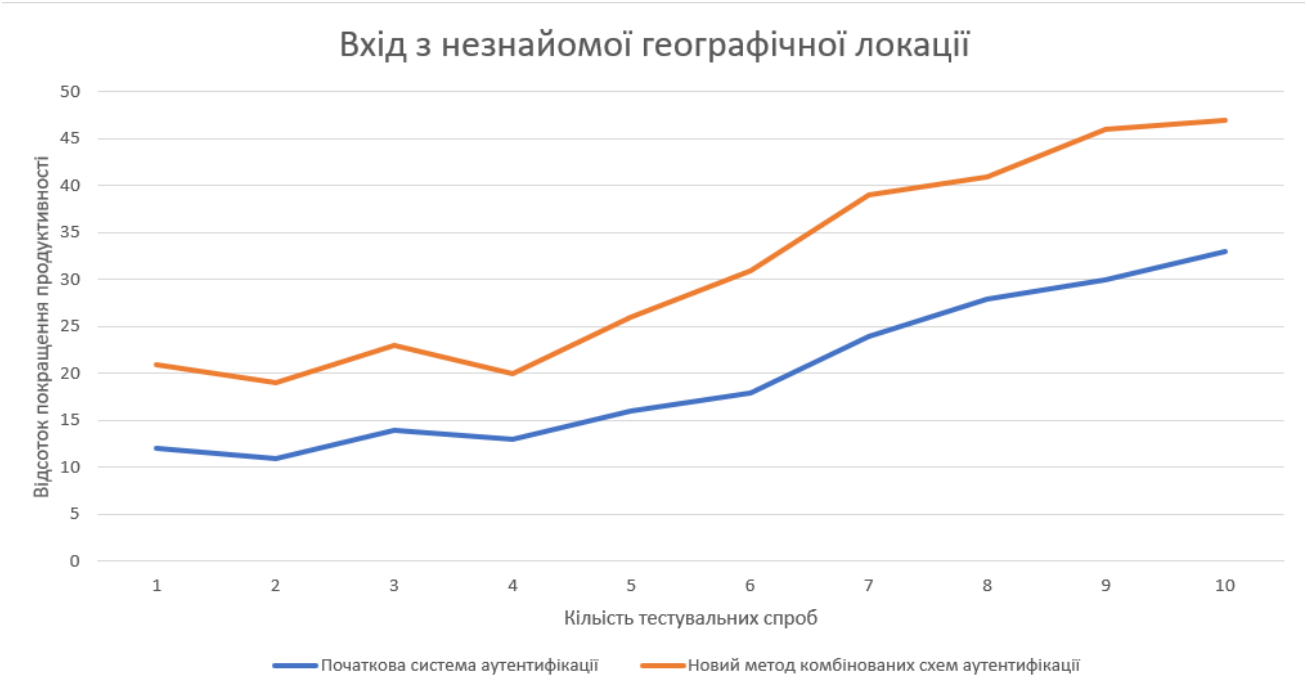


Рисунок 4.2 — Результати тестування входу з нової локації

На діаграмі помітно, що стара система і нова система мають досить велику різницю. Наша нова комбінована схема показала себе стабільною і ефективною, засікаючи вхід з незнайомого місця частіше, аніж це робила стара схема. Ми також бачимо суттєвий стрибок, який, як виявилося під час тестування, вдалося реалізувати за допомогою штучного інтелекту та машинного навчання.

Далі у нас йде тестування на вхід через новий пристрій або після оновлення ОС. На Рисунку 4.3 у нас йде досить різка зміна у поведінці двох систем. Стара система аутентифікації, показувала кращі результати на початку, проте до кінця завершення тестів, було очевидно що нова схема справляється з

роботою також добре. Проблема полягала у спрацюванні механізму false positive, під час якого наша нова система з штучним інтелектом помічала майже усі входи з незнайомих пристроїв як «високий ризик», і декілька разів не могла знайти відповідник відбитку пальців особи з бази даних системи, проте з часом, завдяки постійним спробам, система почала розрізняти їх краще, що допомогло нам справитися із цією проблемою.

Рисунок 4.3 — Результати тестування входу з незнайомих пристроїв

Далі у нас буде тестування на вхід у незвичний час доби, тобто ми візьмемо користувачів, занесемо у базу даних їхній типовий час роботи, коли вони активні у робочій мережі і коли зазвичай вони закінчують працювати, і порівняємо як систему буде реагувати на такі зміни.

Під час тестування входу у незвичні для користувача часи доби було встановлено, що контекстуальна аутентифікація ефективно виявляє підвищені ризики, пов’язані з нетиповою активністю. Якщо вхід здійснювався поза звичайними часовими рамками, система автоматично активувала додаткові

перевірки, щоб підтвердити аутентичність запиту. Це дозволило знизити ймовірність несанкціонованого доступу, водночас забезпечивши гнучкість та адаптивність для легітимних користувачів.

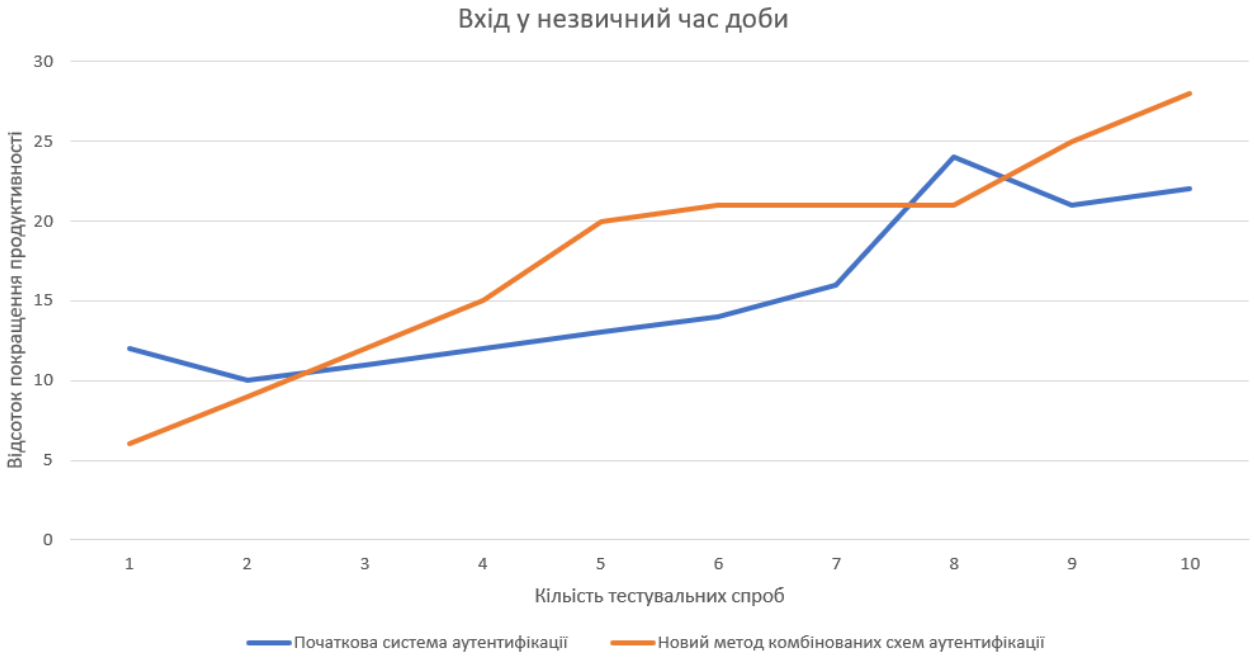


Рисунок 4.4 — Результати тестування входу у незвичні часи доби

Останнім нашим тестом буде вхід з використанням біометрії, у разі якщо всі попередні методи видалися невдалими.

Рисунок 4.6 — Результати тестування входу за допомогою біометричних даних

Під час тестування входу за допомогою біометричних даних було досліджено ефективність цього методу як надійного механізму аутентифікації користувачів. Біометричні дані, такі як відбитки пальців, розпізнавання обличчя та сканування райдужної оболонки ока, продемонстрували високий рівень захисту від несанкціонованого доступу. Цей метод виявився значно стійкішим до традиційних загроз, таких як підбір паролів або використання вкрадених облікових даних. Тестування показало, що аутентифікація за допомогою біометрії забезпечує швидкість та зручність для користувачів, оскільки виключає необхідність запам’ятовування паролів. Однак було виявлено, що точність розпізнавання залежить від умов середовища. Наприклад, низька якість зображення або недостатнє освітлення могли ускладнити процес аутентифікації, особливо при використанні розпізнавання обличчя. Водночас відбитки пальців ідентифікували користувачів стабільно і незалежно від зовнішніх факторів. Система також продемонструвала здатність відхиляти спроби зловмисників використати фальшиві біометричні дані, що підтвердило її надійність у захисті конфіденційності. Проте було виявлено, що біометричні

дані потребують безпечного зберігання, оскільки компрометація цих даних може мати серйозні наслідки, адже їх неможливо змінити, як це можна зробити з паролем.

Загалом результати тестування підкреслили важливість правильного впровадження та налаштування біометричних систем для забезпечення балансу між високим рівнем безпеки та зручністю використання.

4.2 Висновки і подальші рекомендації

Тестування показало, що комбінована система успішно ідентифікує потенційно небезпечні спроби доступу та миттєво реагує на них. Після успішного тестування система аутентифікації вбудовується у всі внутрішні ресурси компанії. Співробітники отримують інструкції щодо використання нової системи, а служба підтримки готується до можливих питань і проблем з переходом.

Незважаючи на те, що біометрична аутентифікація може бути дещо новою для частини працівників, система значно спрощує процедуру входу і одночасно підвищує рівень безпеки. Всі дані, які збираються через контекстуальну аутентифікацію, шифруються і зберігаються відповідно до вимог законодавства (наприклад, GDPR), що гарантує захист особистих даних співробітників.

Через кілька місяців використання комбінованої системи підприємству рекомендується провести оцінку її ефективності. Проте можна навести результати вже, з тих даних які було отримано під час початкового тестування.

Рисунок 4.7 — Підсумки роботи нової комбінованої схеми аутентифікації

За результатами тестувань також виявилося, що рівень кібератак знизився на 10%, а кількість фішингових атак, націлених на отримання доступу до внутрішніх систем, зменшилась на 15%. Оскільки система дозволяє швидко виявляти ризиковані спроби входу, а також автоматично забезпечує додаткові перевірки в таких випадках, загальний рівень безпеки в організації значно зріс. Варто зазначити, що система, саме через впровадження штучного інтелекту, буде рости надалі, і результати будуть лише покращуватися.

Впровадження комбінованої схеми аутентифікації, яка поєднує контекстуальну аутентифікацію з біометрією, дозволяє значно підвищити рівень безпеки, забезпечуючи одночасно зручність для користувачів. Це рішення не лише захищає від атак з використанням скомпрометованих паролів, але й дає змогу ефективно реагувати на потенційні загрози в реальному часі. В кінцевому підсумку, воно дозволяє компанії не тільки зберегти високий рівень безпеки, але й оптимізувати робочі процеси для своїх співробітників.

В якості рекомендацій можна зосередити увагу на ключових точках: подальше вдосконалення біометричних технологій, інтеграція з іншими системами безпеки, регулярний моніторинг і аудит безпеки, навчання співробітників, забезпечення відповідності законодавству, масштабування та адаптація до майбутніх потреб, а також зниження вартості та підвищення доступності технологій.

З огляду на стрімкий розвиток біометрії, варто інвестувати у нові технології, такі як розпізнавання вен пальців, динамічне розпізнавання голосу або розпізнавання райдужної оболонки ока, які забезпечують ще вищий рівень безпеки. Використання новітніх технологій дозволить зменшити ймовірність підробки або обходу системи.

Для забезпечення комплексного захисту організаціям варто розглянути можливість інтеграції комбінованої аутентифікації з іншими засобами безпеки, такими як системи моніторингу аномалій, антивірусні програми, та системи виявлення вторгнень (IDS). Це дозволить швидше виявляти загрози, підвищуючи загальний рівень безпеки.

Після впровадження нової системи необхідно регулярно проводити її аудит, а також моніторинг для виявлення потенційних вразливостей. Технології та методи захисту постійно еволюціонують, тому важливо своєчасно оновлювати програмне забезпечення та процедури для підтримки високого рівня безпеки.

Після впровадження нової системи аутентифікації важливо провести навчання для співробітників щодо нових процесів аутентифікації. Вони повинні бути обізнані про важливість правильного використання біометрії та контекстуальної аутентифікації, а також про можливі загрози, що можуть виникнути через неналежне поводження з системою (наприклад, неналежне зберігання біометричних даних).

Оскільки використання біометрії та персональних даних для аутентифікації супроводжується значними юридичними зобов'язаннями,

важливо забезпечити, щоб система відповідала всім актуальним вимогам захисту персональних даних (наприклад, GDPR в Європейському Союзі). Це включає шифрування біометричних даних, контроль доступу та регулярні перевірки збереження даних.

У разі розширення компанії або зміни умов її роботи, систему аутентифікації слід адаптувати до нових реалій. Масштабування системи безпеки для великих організацій потребує врахування географічних особливостей, множинних точок доступу, а також можливості роботи з мобільними пристроями та віддаленими користувачами.

З часом технології біометрії стають дедалі доступнішими, а також менш затратними для впровадження у бізнес-середовищі. Це дозволяє малим та середнім підприємствам використовувати подібні методи безпеки, забезпечуючи їх захист від кіберзагроз.

Запропонований метод комбінованої аутентифікації, що поєднує контекстуальну аутентифікацію з біометрією, являє собою потужний інструмент для підвищення рівня безпеки в сучасних інформаційних системах. Цей підхід дозволяє враховувати різноманітні фактори ризику та застосовувати кілька рівнів перевірки, що значно знижує ймовірність успішних кібератак. В результаті організації можуть забезпечити високий рівень захисту своїх даних і систем безпеки, при цьому зберігаючи зручність для користувачів.

З огляду на постійно зростаючі кіберзагрози та нові методи атак, комбінована аутентифікація є важливою складовою частиною стратегії забезпечення інформаційної безпеки, яка допомагає організаціям залишатися на передовій у боротьбі з кіберзлочинцями.

ВИСНОВКИ

У даній роботі було розроблено метод підвищення стійкості електронного цифрового підпису (ЕЦП) шляхом комбінування контекстуальної аутентифікації та біометрії, що є важливим кроком у розвитку сучасних методів кібербезпеки. Системи аутентифікації, які поєднують кілька рівнів перевірки, можуть значно підвищити рівень захисту інформації, що є необхідним у умовах постійно зростаючих загроз у цифровому середовищі.

Аналіз сучасних методів аутентифікації показав, що традиційні методи, такі як введення пароля або одноразові паролі (OTP), вже не здатні забезпечити достатній рівень безпеки, особливо в умовах сучасних кіберзагроз, таких як фішинг, використання викрадених паролів, а також складні атаки на багаторівневі системи захисту. Двофакторна аутентифікація (2FA) значно знижує ризики, але, як показало дослідження, цього недостатньо для захисту від більш складних атак. Контекстуальна аутентифікація була визнана ефективним інструментом для виявлення аномальних ситуацій. Вона враховує динамічні фактори, такі як географічне місце розташування користувача, час входу, пристрій, з якого здійснюється вхід, а також історію поведінки користувача. За допомогою цих факторів система може виявити підозрілу активність і вчасно зреагувати, блокуючи або затримуючи доступ до ресурсу. Біометрична аутентифікація, зокрема розпізнавання обличчя та відбитків пальців, надає додаткову ступінь захисту, оскільки біометричні дані значно складніше підробити або викрасти, ніж традиційні паролі. Крім того, використання біометрії дозволяє користувачам уникати необхідності запам'ятовувати складні паролі, що підвищує зручність без шкоди для безпеки.

Комбінована схема аутентифікації, яка об'єднує ці два методи, забезпечує гнучкість і додатковий захист, оскільки навіть якщо один рівень безпеки (наприклад, контекстуальний аналіз) не дасть чітких результатів, система перейде до додаткових перевірок, таких як біометрія. Це дозволяє створити багаторівневий захист, де кожен рівень підвищує стійкість системи до атак.

Практичне застосування комбінованої схеми аутентифікації на прикладі великої фінансової компанії продемонструвало значне покращення в безпеці. Використання цієї системи дозволило знизити кількість успішних кібератак, значно зменшивши кількість спроб несанкціонованого доступу до конфіденційних даних. Це свідчить про високу ефективність комбінованого підходу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Digital 2023: Ukraine [Електронний ресурс]: — Режим доступу: https://datareportal.com/reports/digital-2023-ukraine#:~:text=Ukraine%27s%20internet%20penetration%20rate%20stood,percent)%20between%202022%20and%202023.

2. What are the infrastructure requirements for Artificial Intelligence? [Електронний ресурс] : — Режим доступу: https://blog.leaseweb.com/2019/07/04/infrastructure-requirements-ai/

3. The Promise and Pitfalls of AI [Електронний ресурс] : — Режим доступу: https://www.project-syndicate.org/commentary/artificial-intelligence-digital-divide-widens-inequality-by-jacques-bughin-and-nicolas-van-zeebroeck-2018-09

4. Josefsson S. and Liusvaara I., Edwards-curve digital signature algorithm (eddsa), Internet Research Task Force. (2017) 8032, 257–260. [Електронний ресурс] : — Режим доступу: https://scholar.google.com/scholar_lookup?hl=en&volume=8032&publication_year=2017&pages=257-260&journal=Internet+Research+Task+Force&author=S.+Josefsson&author=I.+Liusvaara&title=Edwards-curve+digital+signature+algorithm+%28eddsa%29

5. Brendel J., Cremers C., Jackson D., and Zhao M., The provable security of ed25519: theory and practice, Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), May 2021, Francisco, CA, USA, IEEE, 1659–1676. [Електронний ресурс] : — Режим доступу: https://scholar.google.com/scholar?hl=en&q=%0ABrendel+J.%2C+%0ACremers+C.%2C+%0AJackson+D.%2C+and+%0AZhao+M.%2C+The+provable+security+of+ed25519%3A+theory+and+practice%2C+Proceedings+of+the+2021+IEEE+Symposium+on+Security+and+Privacy+%28SP%29%2C+May+2021%2C+Francisco%2C+CA%2C+USA%2C+IEEE%2C+1659–1676.

6. What Is Context-Based Authentication? . [Електронний ресурс] : — Режим доступу: https://www.ninjaone.com/it-hub/remote-access/what-is-context-based-authentication/

7. AI and Cybersecurity Costs: Hidden Truth Behind the Soaring Numbers (And How to Outsmart Them) [Електронний ресурс] : — Режим доступу — https://www.linkedin.com/pulse/ai-cybersecurity-costs-hidden-truth-behind-soaring-numbers-lqd2f?trk=organization_guest_main-feed-card_feed-article-content

8. Unleashing the Power of Google Cloud Vision: Revolutionizing Computer Vision in AI & ML [Електронний ресурс]: — Режим доступу: https://www.softobotics.com/blogs/unleashing-the-power-of-google-cloud-vision-revolutionizing-computer-vision-in-ai-ml/

9. Building Intelligent Applications with Azure Cognitive Services [Електронний ресурс]: — Режим доступу: https://agileit.com/news/building-intelligent-applications-with-azure-cognitive-services/

10. Best practices for eSignatures: Legally binding and secure [Електронний ресурс]: — Режим доступу: https://www.acronis.com/en-us/blog/posts/best-practices-for-e-signature/

11. Large provably fast and secure digital signature schemes based on secure hash functions [Електронний ресурс] : — Режим доступу: https://patents.google.com/patent/US5432852A/en

12. Introducing the Digital Signature Activation Protocol for Remote Server Signing [Електронний ресурс] : — Режим доступу: https://www.cryptomathic.com/blog/introducing-the-signature-activation-protocol-for-remote-server-signing

13. A Beginner’s Guide to Digital Signatures for Verifiable Credentials [Електронний ресурс] : — Режим доступу: https://www.dock.io/post/digital-signatures

14. Electronic authentication [Електронний ресурс] — Режим доступу: https://en.wikipedia.org/wiki/Electronic_authentication

15. Multi-factor authentication [Електронний ресурс] : — Режим доступу: https://en.wikipedia.org/wiki/Multi-factor_authentication

16. What are the Key Differences between 2FA and MFA? [Електронний ресурс] : — Режим доступу: https://www.incognia.com/the-authentication-reference/what-are-the-key-differences-between-2fa-and-mfa

17. What is Multi-Factor Authentication (MFA) and How does it Work? [Електронний ресурс] : — Режим доступу: https://www.rsa.com/resources/blog/multi-factor-authentication/what-is-mfa/

18. How to Setup 2FA or Multifactor Authentication for an Application [Електронний ресурс] : — Режим доступу: https://support.okta.com/help/s/article/how-to-setup-2fa-or-multifactor-authentication-for-an-application?language=en_US

19. What Is Two-Factor Authentication (2FA)? How It Works and Example [Електронний ресурс] : — Режим доступу: https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp

20. What is two-factor authentication (2FA)? [Електронний ресурс] : — Режим доступу: https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

21. What is eSignature [Електронний ресурс] : — Режим доступу: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/What+is+eSignature#:~:text=An%20electronic%20signature%20is%20an,to%20which%20the%20signature%20relates.

22. What is an electronic signature? [Електронний ресурс] : — Режим доступу: https://www.signaturit.com/blog/what-is-an-electronic-signature/

23. What is eSignature [Електронний ресурс] : — Режим доступу: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/What+is+eSignature#:~:text=An%20electronic%20signature%20is%20an,to%20which%20the%20signature%20relates.

24. Electronic signature [Електронний ресурс] : — Режим доступу: https://en.wikipedia.org/wiki/Electronic_signature

25. Electronic Signatures Explained [Електронний ресурс] : — Режим доступу: https://blog.admincontrol.com/en/electronic-signatures-explained

26. How to create a signature online: A beginner’s guide [Електронний ресурс] : — Режим доступу: https://www.ilovepdf.com/uk/blog/create-digital-signature-online#:~:text=But%20first%2C%20you%20must%20create,an%20image%20of%20a%20signature.

27. How to create an electronic signature and e-sign your documents for free (6 methods) [Електронний ресурс] : — Режим доступу: https://www.pandadoc.com/blog/how-to-create-an-electronic-signature/

28. Digital Signature [Електронний ресурс] : — Режим доступу: https://osvita.diia.gov.ua/en/courses/digital-signature

29. How to get a digital signature certificate? [Електронний ресурс] : — Режим доступу: https://oneflow.com/blog/digital-signature-certificate/

30. 3 Different Types of Digital Signatures and When to Use Them [Електронний ресурс] : — Режим доступу: https://www.proof.com/blog/3-different-types-of-digital-signatures-and-when-to-use-them

31. The digital signature: explained simply [Електронний ресурс] : — Режим доступу: https://www.skribble.com/en-eu/blog/digital-signature/

32. Digital signature [Електронний ресурс] : — Режим доступу: https://www.techtarget.com/searchsecurity/definition/digital-signature

33. What is a digital signature? [Електронний ресурс] : — Режим доступу: https://www.signiflow.com/what-is-a-digital-signature/

34. What are digital signatures? [Електронний ресурс] : — Режим доступу: https://www.zoho.com/sign/how-it-works/electronic-signature/digital-signature.html

35. How Does AI Training Work to Make Frictionless Facial Liveness Possible? [Електронний ресурс] : — Режим доступу: https://www.idrnd.ai/how-does-ai-training-work/

36. How Artificial Intelligence (AI) Is Used In Biometrics [Електронний ресурс] : — Режим доступу: https://www.aratek.co/news/how-artificial-intelligence-ai-is-used-in-biometrics

37. Leveraging AI to Develop Best-in-Class Biometric Algorithms [Електронний ресурс] : — Режим доступу: https://tech5.ai/leveraging-ai-to-develop-best-in-class-biometric-algorithms/

38. Digital authentication - factors, mechanisms and schemes [Електронний ресурс] : — Режим доступу: https://www.cryptomathic.com/blog/digital-authentication-factors-mechanisms-schemes

39. Biometrics in Banking: Which Biometric System Ensures 100% Security [Електронний ресурс] : — Режим доступу: https://binariks.com/blog/biometric-security-onilne-banking/

40. Phishing Attack - What is it and How Does it Work? [Електронний ресурс] : — Режим доступу: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/

41. What Is A Brute Force Attack? [Електронний ресурс] : — Режим доступу: https://www.fortinet.com/resources/cyberglossary/brute-force-attack

42. Traffic Interception - an overview [Електронний ресурс] : — Режим доступу: https://www.sciencedirect.com/topics/computer-science/traffic-interception#:~:text=Traffic%20interception%20refers%20to%20the,disturbances%20in%20the%20network%20traffic.

43. What is Social Engineering [Електронний ресурс] : — Режим доступу: https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,or%20giving%20away%20sensitive%20information.

44. 8 Best Use Cases of Artificial Intelligence In Fintech with Examples [Електронний ресурс] : — Режим доступу: https://binariks.com/blog/artificial-intelligence-in-fintech/

45. Context-Aware Authentication: Meaning, Tools, Examples [Електронний ресурс] : — Режим доступу: https://www.pomerium.com/blog/context-aware-authentication-meaning-tools-examples#:~:text=Unlike%20traditional%20authentication%20methods%2C%20which,e.g.%2C%20country%2C%20city).

46. What is Contextual Authentication? - senhasegura Glossary [Електронний ресурс] : — Режим доступу: https://senhasegura.com/post/what-is-contextual-authentication

47. Context-Based Authentication: Examples Across Industries [Електронний ресурс] : — Режим доступу: https://www.beyondidentity.com/resource/context-based-authentication-examples-across-industries

48. Take Your Security to the Next Level with Context-Based Authentication [Електронний ресурс] : — Режим доступу: https://www.okta.com/identity-101/context-based-authentication/

49. What is the Elliptic Curve Digital Signature Algorithm (ECDSA)? [Електронний ресурс] : — Режим доступу: https://www.hypr.com/security-encyclopedia/elliptic-curve-digital-signature-algorithm#:~:text=The%20Elliptic%20Curve%20Digital%20Signature%20Algorithm%20(ECDSA)%20is%20a%20Digital,public%20key%20cryptography%20(PKC).

50. Understanding How ECDSA Protects Your Data [Електронний ресурс] : — Режим доступу: https://www.instructables.com/Understanding-how-ECDSA-protects-your-data/

51. AI Biometric Authentication for Enterprise Security [Електронний ресурс] : — Режим доступу: https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security

52. Using Edge Biometrics For Better Office Security System Development [Електронний ресурс] : — Режим доступу: https://mobidev.biz/blog/edge-biometrics-office-workplace-security-system-development

53. Improve AI Facial Recognition Accuracy Using Deep Learning [Електронний ресурс] : — Режим доступу: https://mobidev.biz/blog/improve-ai-facial-recognition-accuracy-with-machine-deep-learning

54. DEVELOPING AN ENTERPRISE VERIFICATION-AS-A-SERVICE SOLUTION [Електронний ресурс] : — Режим доступу: https://mobidev.biz/case-studies/enterprise-verification-as-service

55. How To Integrate Behavioral Biometrics Into AI Assistance for Security [Електронний ресурс] : — Режим доступу: https://hackernoon.com/how-to-integrate-behavioral-biometrics-into-ai-assistance-for-security

56. What is Machine Learning? Definition, Types, Tools & More [Електронний ресурс] : — Режим доступу: https://www.datacamp.com/blog/what-is-machine-learning

57. What is machine learning (ML)? [Електронний ресурс] : — Режим доступу: https://www.ibm.com/topics/machine-learning

58. Comparing ECDSA vs RSA: A Simple Guide [Електронний ресурс] : — Режим доступу: https://www.ssl.com/article/comparing-ecdsa-vs-rsa-a-simple-guide/#:~:text=bit%20ECDSA%20key.-,Performance%20and%20Speed,key%20generation%20and%20signature%20creation.

59. lliptic Curve Digital Signature Algorithm (ECDSA) [Електронний ресурс] : — Режим доступу: https://vaultody.com/blog/131-elliptic-curve-digital-signature-algorithm-ecdsa

60. Time Based One Time Password (TOTP, OTP) [Електронний ресурс] : — Режим доступу: https://www.hypr.com/security-encyclopedia/time-based-time-password-totp-otp#:~:text=A%20Time-Based%20One-Time,QR%20code%20or%20in%20plaintext.

61. Ідентифікація і аутентифікація [Електронний ресурс] : — Режим доступу: https://studfile.net/preview/7788223/page:4/

62. One Time Password (OTP, TOTP) : definition, examples [Електронний ресурс] : — Режим доступу: https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp#:~:text=What%20does%20OTP%20mean%3F,method%20and%20the%20least%20secure.

63. Cloud Vision API [Електронний ресурс] : — Режим доступу: https://cloud.google.com/vision

64. Azure AI Services [Електронний ресурс] : — Режим доступу: https://azure.microsoft.com/en-us/products/ai-services

ДОДАТОК А

Прийнято в журнал «Вісник Хмельницького національного університету. Серія: Технічні науки» Випуск№6 2024 року

УДК 004.023
DOI:

ТІТОВА ВІРА
Хмельницький національний університет
ORCID ID: 0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ ЮРІЙ
Хмельницький національний університет
ORCID ID: 0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ПИРЧ ОЛЕНА
Хмельницький національний університет
e-mail: oleksukolena@gmail.com
ШЕМЧУК УЛЯНА
Хмельницький національний університет
e-mail: shemshyk123@gmail.com
БОЖОК ДМИТРО
Хмельницький національний університет
e-mail: dimasbmw369@gmail.com

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

У даній статті проведено аналіз існуючих методів автентифікації. До таких можна віднести: парольну аутентифікацію, аутентифікацію через сторонній ресурс, аутентифікацію за допомогою графічних паролів, аутентифікацію за допомогою одноразових та динамічних паролів, механізми аутентифікації з використанням сторонніх програмних та апаратних токенів, методи багатофакторної аутентифікації та криптографічні. Порівняння аналізованих методів проведено за трьома основними групами характеристик: зручністю використання, складністю реалізації та безпеки рішення.

У результаті проведеного порівняльного аналізу виявлено найперспективніший підхід – підхід із використанням криптографічних засобів, що забезпечує високий рівень захисту інформації.

Ключові слова: аутентифікація користувачів, методи аутентифікації, криптографічна стійкість, електронний цифровий підпис.

VIRA TITOVA, YURII KLOTS, OLENA PYRCH, ULIANA SHEMCHUK, DMYTRO BOZHOK
Khmelnitskyi National University

ANALYSIS OF MODERN USER AUTHENTICATION METHODS

There are a number of problems in modern asymmetric cryptosystems. They are mostly related to issues of cryptographic stability and acceptable key lengths. The capabilities of computing resources increase every year, which allows legitimate users to receive, process and transmit information faster, but cryptanalysts also remain in the plus - the probability of breaking existing schemes increases, and the time spent by this process decreases. Because of this, there is a constant need to increase the size of the keys, which negatively affects performance.

Due to the above, it can be seen that the so-called combined systems will be an interesting and more than relevant development. Such systems provide double protection: in addition to the standard encryption key, which is widely used in modern cryptosystems, a double protection scheme is provided.

This article analyzes existing authentication methods. These include: password authentication, authentication through a third-party resource, authentication using graphic passwords, authentication using one-time and dynamic passwords, authentication mechanisms using third-party software and hardware tokens, multi-factor authentication, and cryptographic methods. The comparison of the analyzed methods is based on three main groups of characteristics: ease of use, complexity of implementation and security of solutions.

As a result of the comparative analysis, the most promising approach was determined - an approach using cryptographic means, which provides a high level of information protection.

Keywords: user authentication, authentication methods, cryptographic stability, electronic digital signature.

Постановка проблеми

У сучасному інформаційно-розвиненому суспільстві з кожним роком все більша увага як з боку держави, так і з боку приватних компаній починає приділятися цілісності інформації, що передається, аутентифікації користувачів та іншим аспектам інформаційної безпеки. Забезпечити автентичність, доступність і цілісність інформації, що передається, дозволяє електронний цифровий підпис (ЕЦП). В даний час існує велика кількість алгоритмів та протоколів ЕЦП. Найважливішим аспектом застосування підпису є його криптостійкість, яка грунтується на складності обчислення будь-якої односторонньої математичної функції. Поява ефективних методів вирішення того чи іншого завдання спричинить зниження стійкості всього криптоалгоритму.

У 2016 році Національний інститут стандартів та технологій США (NIST) оголосив конкурс на створення нових стандартів шифрування, ЕЦП та обміну ключами. Вирішенням цього питання можуть стати, так звані, комбіновані схеми. Такі схеми припускають подвійний захист: створення алгоритмів і протоколів, заснованих одночасно на кількох складно обчислюваних завданнях.

Формулювання цілей статті

У сучасних асиметричних криптосистемах існує низка проблем. Здебільшого вони пов'язані з питаннями криптографічної стійкості та прийнятною довжиною ключів. Можливості обчислювальних ресурсів з кожним роком збільшуються, що дозволяє легітимним користувачам отримувати, обробляти та передавати інформацію швидше, але й криптоаналітики залишаються у плюсі – ймовірність злому існуючих схем збільшується, а час, витрачений на цей процес, зменшується. Через це виникає постійна потреба у збільшенні розмірності ключів, що негативно позначається на продуктивності.

В силу всього вище викладеного, можна бачити, що цікавою і більш ніж актуальною розробкою будуть так звані комбіновані системи. Такі системи передбачають подвійний захист: крім стандартного ключа шифрування, який повсюдно застосовується в сучасних криптосистемах, передбачається подвійна схема захисту.

Огляд існуючих рішень

Існує велика кількість методів автентифікації. Для порівняльного аналізу виділяється кілька основних груп методів. Варто відзначити, що в кожній із груп можуть бути різні реалізації, що відрізняються одна від одної конкретними характеристиками, а також сильними та слабкими сторонами. У цьому самі показники і тенденції груп, зазвичай, залишаються незмінними.

Найбільш популярним і простим методом, безперечно, можна назвати парольну автентифікацію. Вона використовується в соціальних мережах, платіжних системах, на форумах і на веб-ресурсах, що містять персональні дані. Під паролем мається на увазі спеціальна кодова фраза або набір фраз кожного ресурсу.

Розвитком даного методу є графічні паролі, що базуються на введенні певного нетекстового змісту. Переваги даних методів полягають у спрощенні запам'ятовування таких кодових елементів.

Наступною групою є методи з використанням одноразових та динамічних паролів, наприклад,GrIDsure [1]. Вони вимагають від користувача додаткових дій, але дозволяють посилити захист від атак, що базуються на повторенні паролів.

Також часто використовуваним способом є методи, засновані на аутентифікації за допомогою стороннього ресурсу або децентралізованої аутентифікації, наприклад,OpenID [2] таOAuth [3].

Наступною категорією методів є токени, сюди належать механізми аутентифікації з використанням сторонніх програмних та апаратних токенів.

Методи багатофакторної аутентифікації складають окрему категорію, сюди відносяться, наприклад, механізми з підтвердженням коду через SMS-повідомлення.

Криптографічні методи аутентифікації виділені в окрему категорію, що включає способи від використання сертифікатів до підходів стеганографічних [4].

До останньої категорії віднесено методи біометричної аутентифікації [5] на веб-ресурсі, наприклад, з використанням голосового підтвердження або на основі характеристик введення користувача.

Порівняння проводиться за трьома основними групами характеристик: зручністю використання, складністю реалізації та безпеки рішення.

У таблицях 1-3 цифрою 1 позначено найгірший показник, 2 - середній, 3 – найкращий.

До першої групи належать складність запам'ятовування кодового значення, необхідність наявності допоміжного пристрою, виконання додаткових дій, складність освоєння методу, середній час аутентифікації, частота помилок та складність відновлення аутентифікатора у разі втрати (Таблиця 1).

До другої групи належать характеристики доступності методу, вартості рішення, вимоги до серверної та клієнтської архітектури, а також пропрієтарність методів (Таблиця 2).

До третьої групи відносять стійкість методів до атак перебором, цільового та нецільового спостереження, атак за допомогою непрямого злому, фішингових атак та фізичної крадіжки (Таблиця 3).

Таблиця 1

Порівняння методів автентифікації за зручністю користування

Зручність використання							
	Запамя-товування	**Доп. пристрій**	**Викон. дій**	**Легкість**	**Час**	**Помилки**	**Відновлення**
Пароль	1	3	2	3	3	2	3
Сторонній ресурс	2	3	3	3	3	3	2
Графічні	1	1	2	3	3	2	3
Динамічні	1	3	2	2	3	2	2
Токени	3	1	1	1	2	3	1
Багатофакторна	1	1	1	3	2	2	1
Криптографія	3	1	1	1	1	2	1
Біометрія	3	3	2	3	2	2	1

Таблиця 2

Порівняння методів аутентифікації за простотою реалізації

Реалізація					
	Доступність	**Вартість**	**Серверна середовище**	**Клієнтське середовище**	**Пропрієтарність**
Пароль	3	3	3	3	3
Сторонній ресурс	3	3	1	3	3
Графічні	1	3	1	3	3
Динамічні	2	3	2	2	3
Токени	1	1	1	2	1
Багатофакторна	2	2	2	2	2
Криптографія	1	1	1	2	1
Біометрія	1	1	1	1	1

Таблиця 3

Порівняння методів автентифікації з безпеки даних, що передаються

	Безпека				
	Перебір	**Спостереження**	**Непрямий злом**	**Фішинг**	**Крадіжка**
Пароль	1	1	1	1	3
Сторонній ресурс	2	2	3	3	3
Графічні	1	1	2	2	3
Динамічні	2	3	2	2	3
Токени	3	3	3	3	2
Багатофакторна	1	1	3	3	2
Криптографія	3	3	3	3	3
Біометрія	3	3	1	1	3

Зі сказаного вище можна бачити, що автентифікація з використанням простих паролів найбільш легка в реалізації, але не дуже безпечна, і вимагає постійного запам'ятовування паролів.

Методи використання аутентифікації через сторонні ресурси дуже зручні для користувачів, але вимагають певних налаштувань сервера, а їх безпека заснована на захищеності провайдера даної послуги.

Графічні та динамічні паролі дозволяють трохи збільшити захищеність від різних видів загроз, однак це ускладнює використання та збільшує вимоги до клієнтських та серверних реалізацій.

Методи захисту з використанням токенів є порівняно безпечними, але потребують спеціалізованих налаштувань, а також найчастіше є пропрієтарними та платними.

Двофакторна аутентифікація з використанням мобільних пристроїв дещо знижує зручність використання, але різко підвищує захищеність від деяких видів атак, однак, це призводить до необхідності ускладнення серверної архітектури та вимагає від користувача додаткових дій.

Криптографія та біометрія є найбільш захищеними підходами, але зручність використання та складність реалізації гірша, ніж у інших методів.

З порівняльного аналізу можна побачити, що немає ідеального методу аутентифікації. Кожне поліпшення характеристик безпеки методу тягне за собою погіршення характеристик зручності використання, або призводить до ускладнення клієнтської та серверної архітектур. У результаті, для кожного ресурсу потрібно використовувати метод найбільш підходящий до конкретної ситуації та вимог власників ресурсу, враховуючи ризики, загрози та цінність інформації, що захищається.

Лідером зручності використання є методи аутентифікації через третю сторону, куди відносяться також і децентралізовані підходи. Дані методи, наприклад, OAuth та OpenID широко використовуються в Інтернет і дозволяють легко проводити аутентифікацію на будь-яких ресурсах з використанням всього одного пароля, однак вони природно мають не такий високий рівень безпеки, хоча і більш надійні, ніж традиційні підходи.

Найбільш простим для реалізації є паролі, однак така властивість обумовлена зменшенням захищеності та зручності використання кінцевими користувачами.

Однак якщо говорити про захист критично важливих веб-інфраструктур, то з точки зору безпеки обґрунтованим є використання криптографічних або біометричних методів автентифікації. Але нині біометричні методи є недостатньо розвиненими на веб-ресурсах.

Подальший розвиток кожного методу має природні обмеження, і тенденції їхнього подальшого вдосконалення лежать у сфері комбінованих систем. Цікавим для розгляду є підходи, що використовують криптографічні прийоми для вирішення задач аутентифікації, оскільки можуть розширювати можливості інших методів.

Висновки

В дані статті проведено аналіз існуючих методів аутентифікації у мережі Інтернет. Виявлено найбільш перспективний підхід – підхід із використанням криптографії, що забезпечує високий рівень захисту для критично важливої інформації. Показано, що здійснювати процедуру автентифікації на веб можна за допомогою електронного підпису.

Проаналізовано існуючі наразі схеми електронної підпис. Синтезовано основні складні завдання з теорії чисел, що лежать у їх основі. Наведено оцінку їх криптостійкості.

Виявлено основні проблеми сучасних криптосистем. Обґрунтовано високу затребуваність та актуальність розробки нових комбінованих схем ЕЦП.

Література

1. Grid Authentication [Електронний ресурс] – Режим доступу: https://safenet.gemalto.com/multi□factor-authentication/authenticators/grid-authentication.

2. Open ID foundation [Електронний ресурс] – Режим доступе: http://openid.net.

3. OAuth 2.0 [Електронний ресурс] – Режим доступе: https://oauth.net/2.

4. Mozhaiev, O., Gnusov, Y., Manzhai, O., Strukov, V., Nosov, V., Radchenko, V. i Yenhalychev, S. (2023) «Стеганографічний метод захисту акустичної інформації у системах критичного застосування», СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ, (3 (25), с. 52–63. doi: 10.30837/ITSSI.2023.25.052.

5. Ляшенко, Г.Є & Астраханцев, А.А. (2017). Дослідження ефективності методів біометричної автентифікації. Системи обробки інформації. 2(148). 111-114. 10.30748/soi.2017.148.20.

References

1. Grid Authentication [Elektronnyi resurs] – Rezhym dostupu: https://safenet.gemalto.com/multi factor-authentication/authenticators/grid-authentication.

2. Open ID foundation [Elektronnyi resurs] – Rezhym dostupe: http://openid.net.

3. OAuth 2.0 [Elektronnyi resurs] – Rezhym dostupe: https://oauth.net/2.

4. Mozhaiev, O., Gnusov, Y., Manzhai, O., Strukov, V., Nosov, V., Radchenko, V. i Yenhalychev, S. (2023) «Stehanohrafichnyi metod zakhystu akustychnoi informatsii u systemakh krytychnoho zastosuvannia», SUChASNYI STAN NAUKOVYKh DOSLIDZhEN TA TEKhNOLOHII V PROMYSLOVOSTI, (3 (25), s. 52–63. doi: 10.30837/ITSSI.2023.25.052.

5. Liashenko, H.Ie & Astrakhantsev, A.A. (2017). Doslidzhennia efektyvnosti metodiv biometrychnoi avtentyfikatsii. Systemy obrobky informatsii. 2(148). 111-114. 10.30748/soi.2017.148.20.

Презентація кваліфікаційної роботи

«Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації»

Студентки групи КБЗІм-23-1
Пирч Олени Вадимівни

Науковий керівник
Тітова Віра Юріївна

Аналіз об’єкта захисту

Впровадження комбінованої схеми аутентифікації з використанням ШІ стало значним кроком у підвищенні рівня безпеки для банківської системи. Це дозволило:

- Покращити захист від сучасних кіберзагроз.
- Зробити систему більш гнучкою та адаптивною до потреб клієнтів.
- Зберегти баланс між безпекою та зручністю користування.

Такий підхід можна адаптувати й до інших галузей — корпоративних мереж, інтернет-магазинів чи державних систем, забезпечуючи високий рівень довіри та захисту.

Методи шифрування даних

	Properties	RSA	ECDSA	EdDSA
1	Security bits			
	80	1024	160	160
	112	2048	224	224
	128	3072	256	256
	192	7880	384	384
	256	15360	512	512
2	Performance	Slow due to long key size	Fast	Fastest
3	Popularity	Widely used	Not much used	New and widely used

Рисунок 1 — Порівняння різних методів за категоріями «Захисні біти», «Продуктивність», «Популярність»

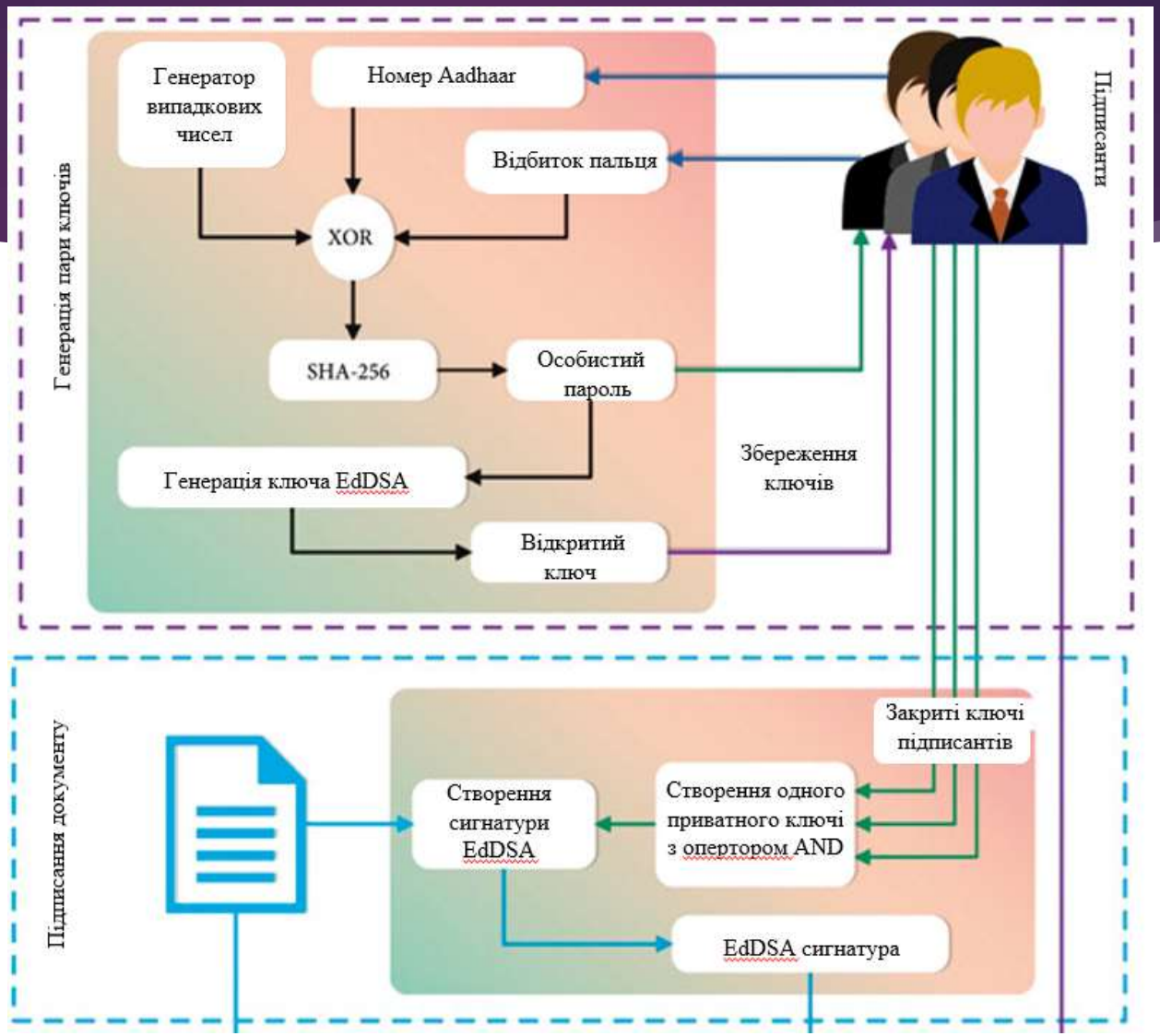


Рисунок 2 — Опис дії ЕПЦ-методу впровадженного на підприємстві

Рисунок 3 — Опис дії ЕПЦ-методу впровадженного на підприємстві (2 частина)

Вибір комбінованих схем автентифікації

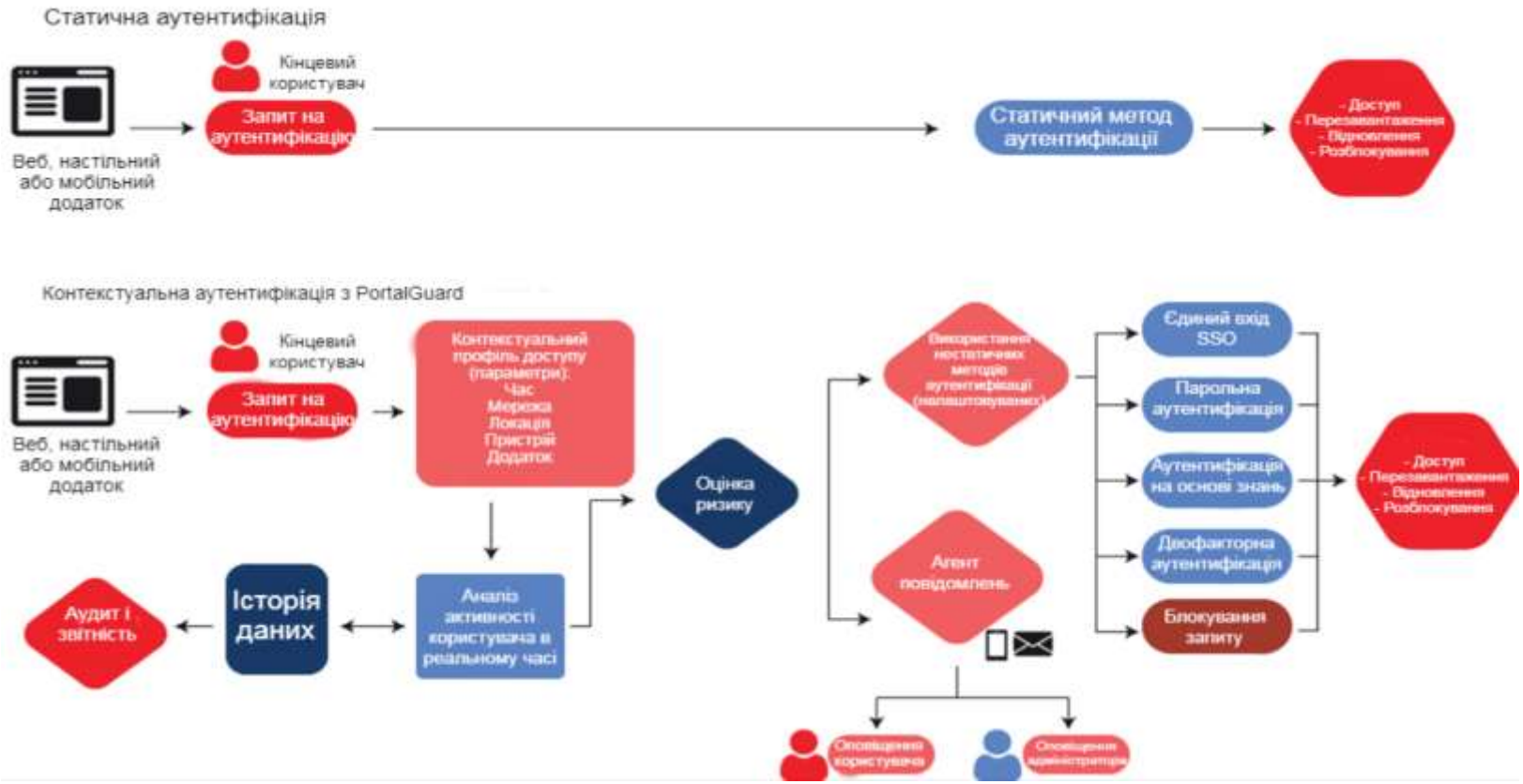


Рисунок 4 — Порівняння контекстуальної аутентифікації зі статичною

Таблиця порівняння

Критерій	Контекстуальна аутентифікація	Статична аутентифікація
Механізм аутентифікації	Використовує динамічні фактори (геолокація, пристрій, час доступу).	Базується на постійних даних (пароль, PIN-код).
Гнучкість	Дуже гнучка, адаптується до змін у поведінці користувача.	Низька гнучкість, потребує оновлення паролів вручну.
Безпека	Забезпечує вищий рівень безпеки завдяки аналізу декількох контекстів.	Менш захищена через залежність від одного фактора.
Захист від атак	Ефективна проти атак на основі викрадених паролів або пристроїв.	Уразлива до фішингу, брутфорс-атак і перехоплення даних.
Зручність для користувачів	Вимагає мінімальної взаємодії, часто працює у фоновому режимі.	Користувачі повинні пам'ятати та вводити паролі.
Приклади використання	Банківські сервіси, корпоративні мережі, мобільні додатки.	Онлайн-сервіси, прості веб-сайти.
Вартість впровадження	Висока, оскільки потребує складних алгоритмів і обчислень.	Низька, легко впроваджується у базових системах.
Швидкість аутентифікації	Залежить від аналізу даних, але може бути швидкою при оптимізації.	Швидка, залежить лише від введення пароля.
Виявлення аномалій	Швидко виявляє аномальні дії завдяки аналізу поведінки.	Не виявляє аномалій, поки не станеться інцидент.

Рисунок 5 — Таблиця з результатами порівняння

Біометрична автентифікація

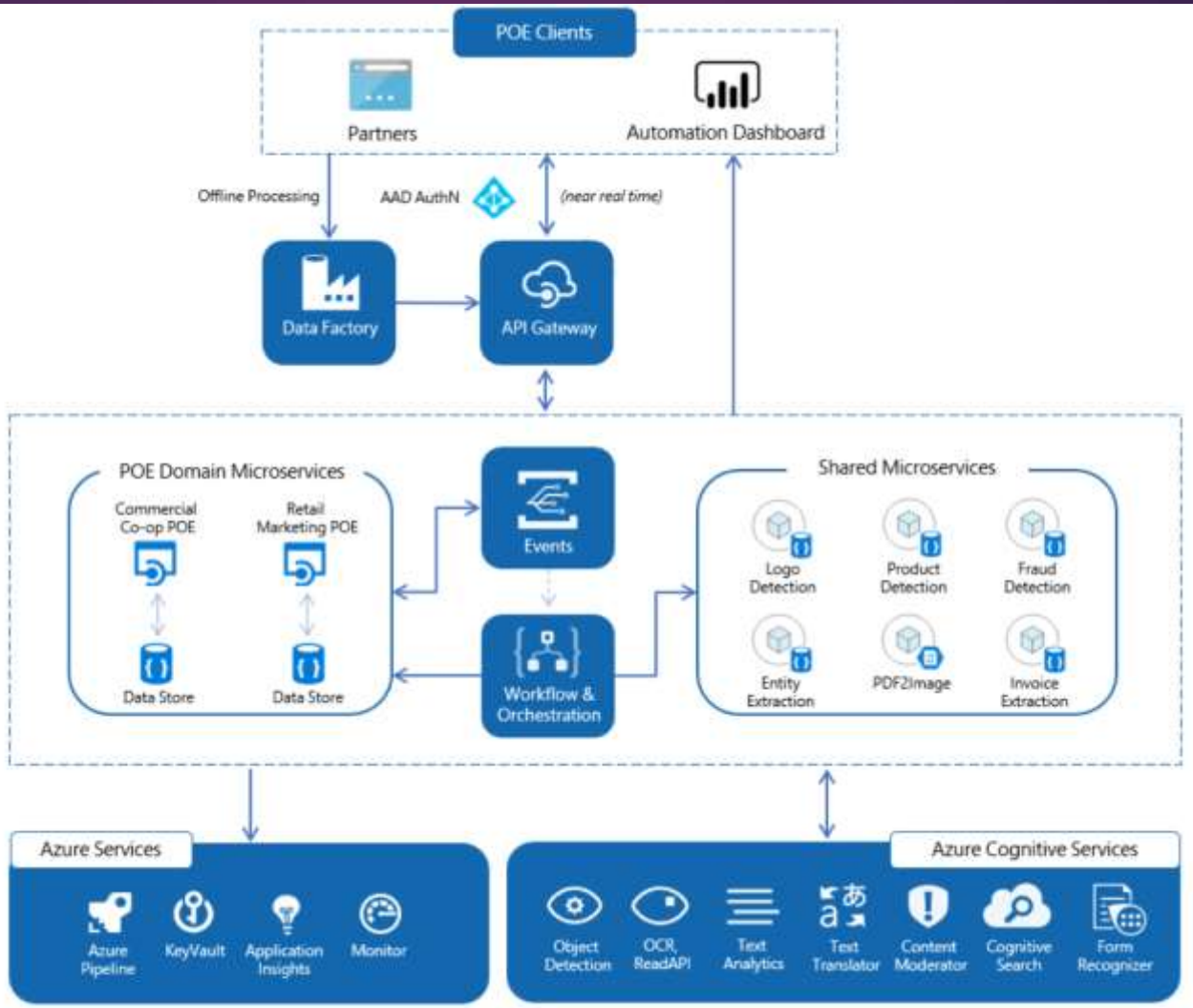


Рисунок 6 — Схема роботи Microsoft Azure Cognitive Services

Біометрична автентифікація

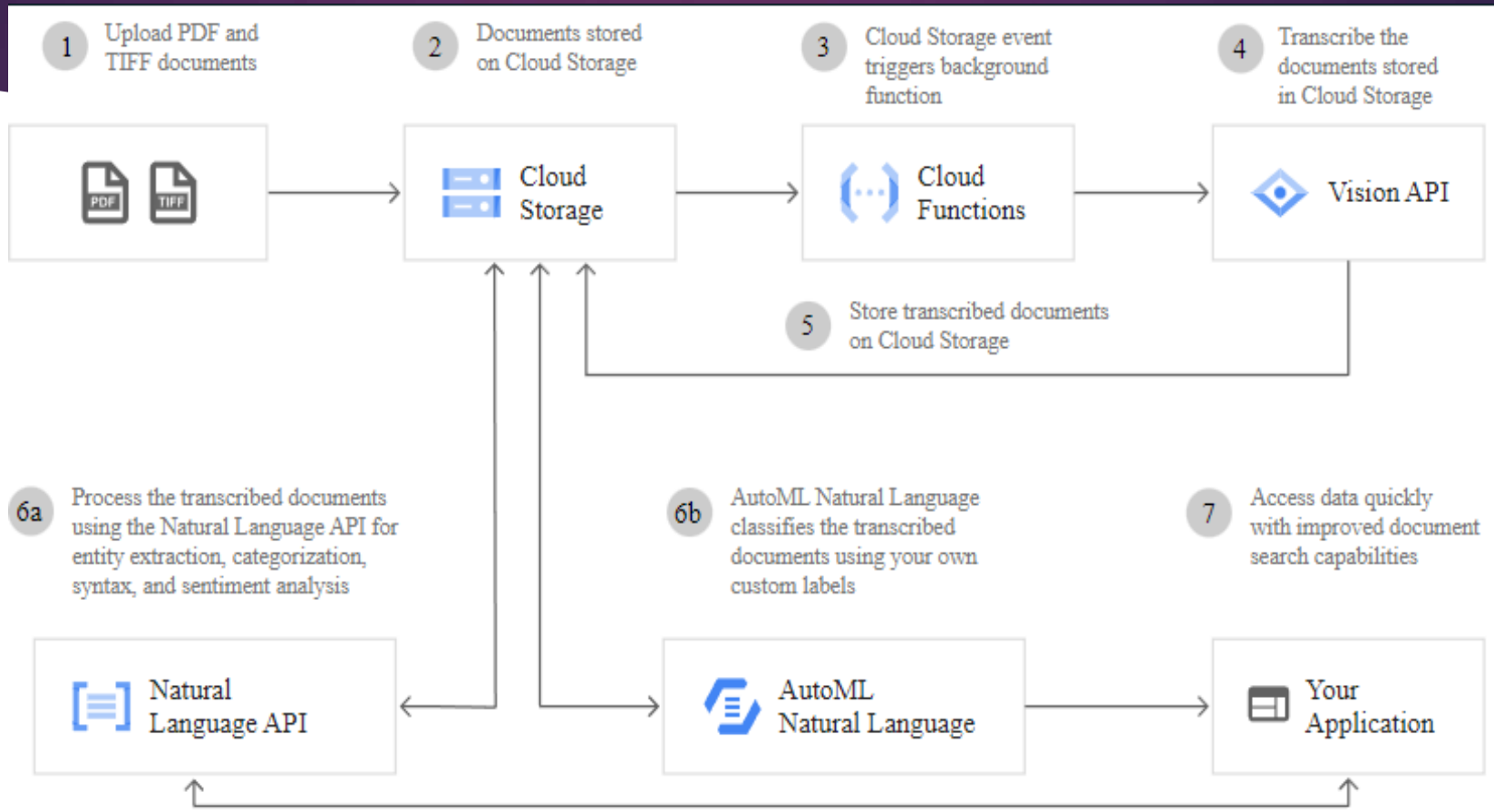


Рисунок 7 — Схема роботи Google Cloud Vision

Результати впровадження комбінованої схеми аутентифікації

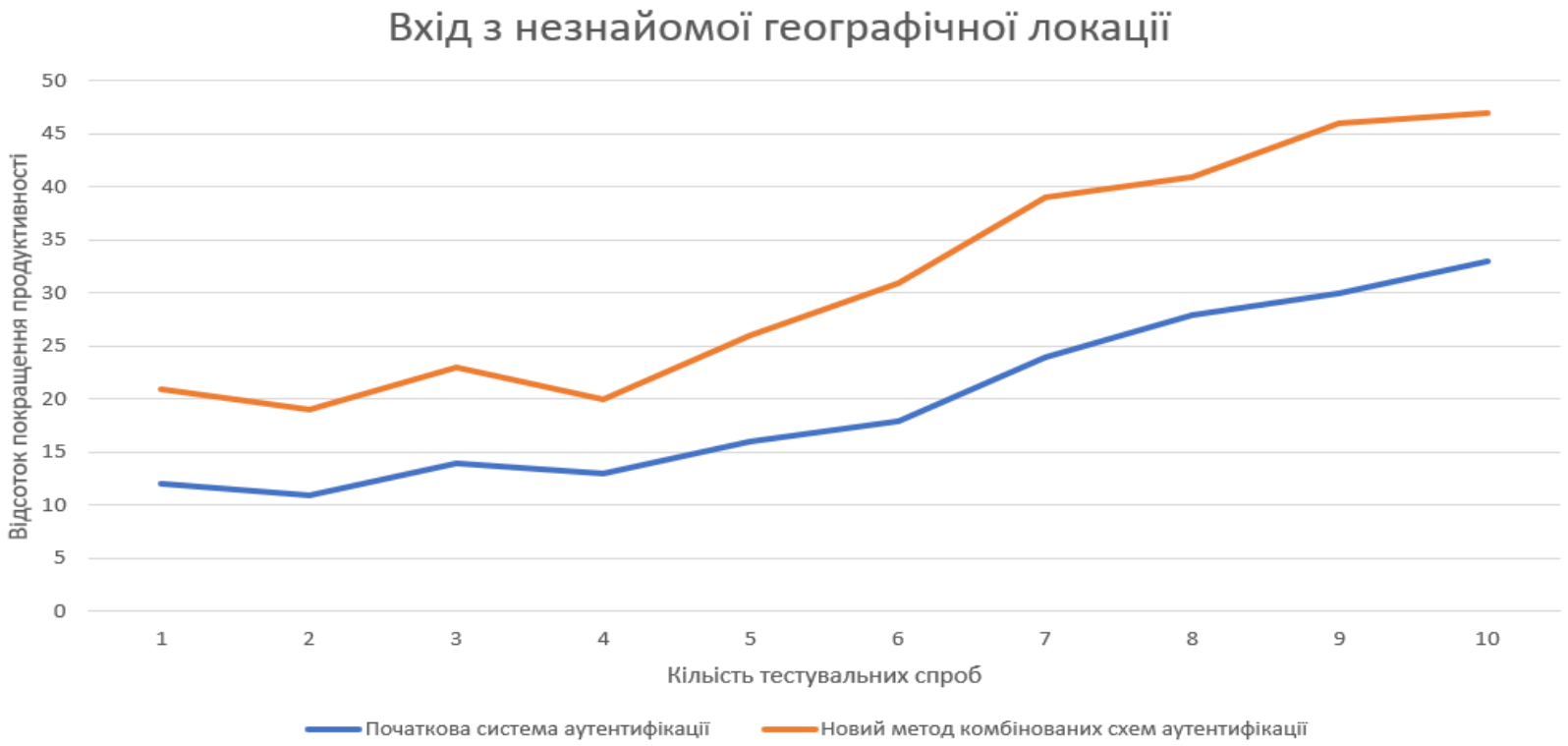


Рисунок 8 — Результати тестування входу з нової локації

Результати впровадження комбінованої схеми аутентифікації

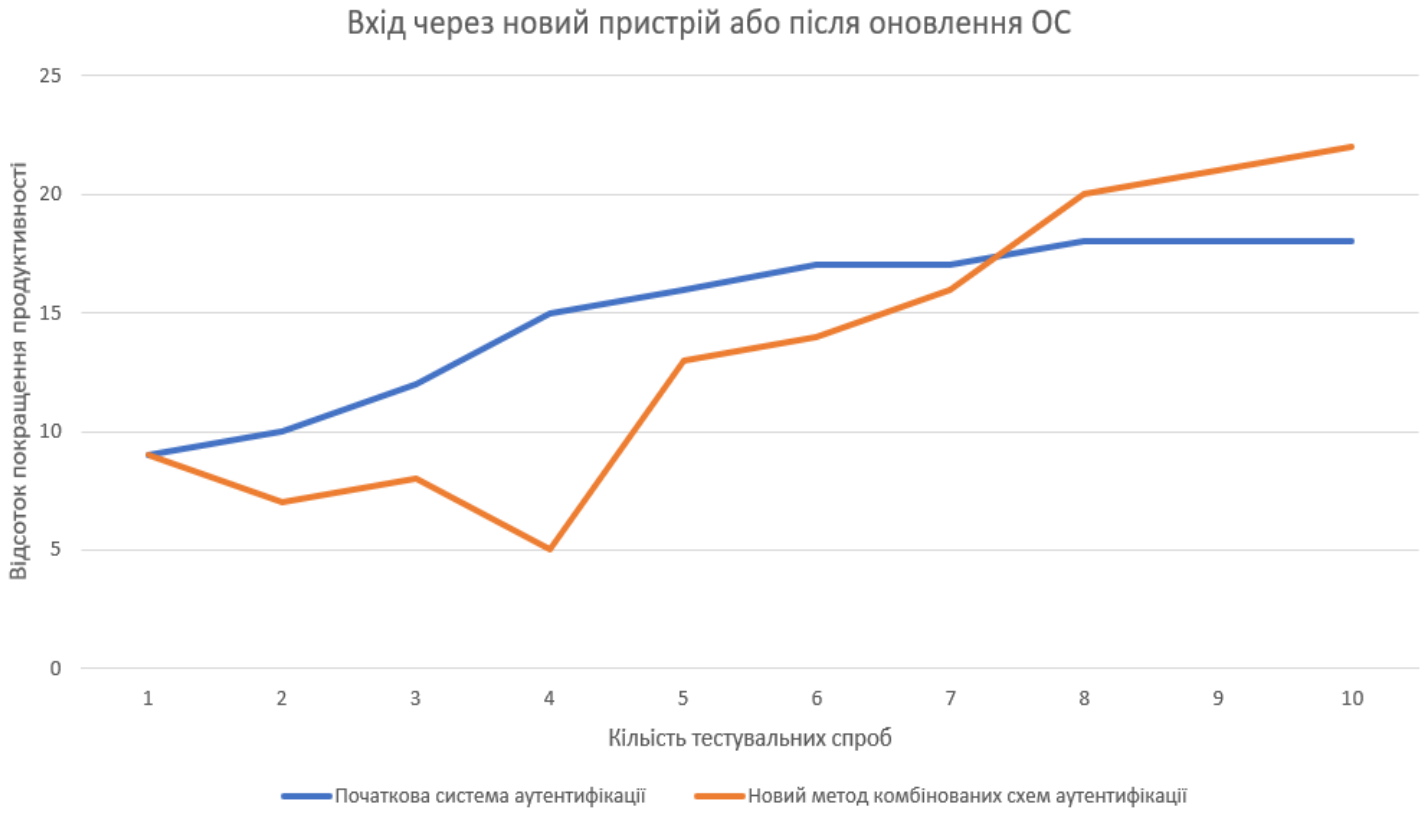


Рисунок 9 — Результати тестування входу з незнайомих пристроїв

Результати впровадження комбінованої схеми аутентифікації

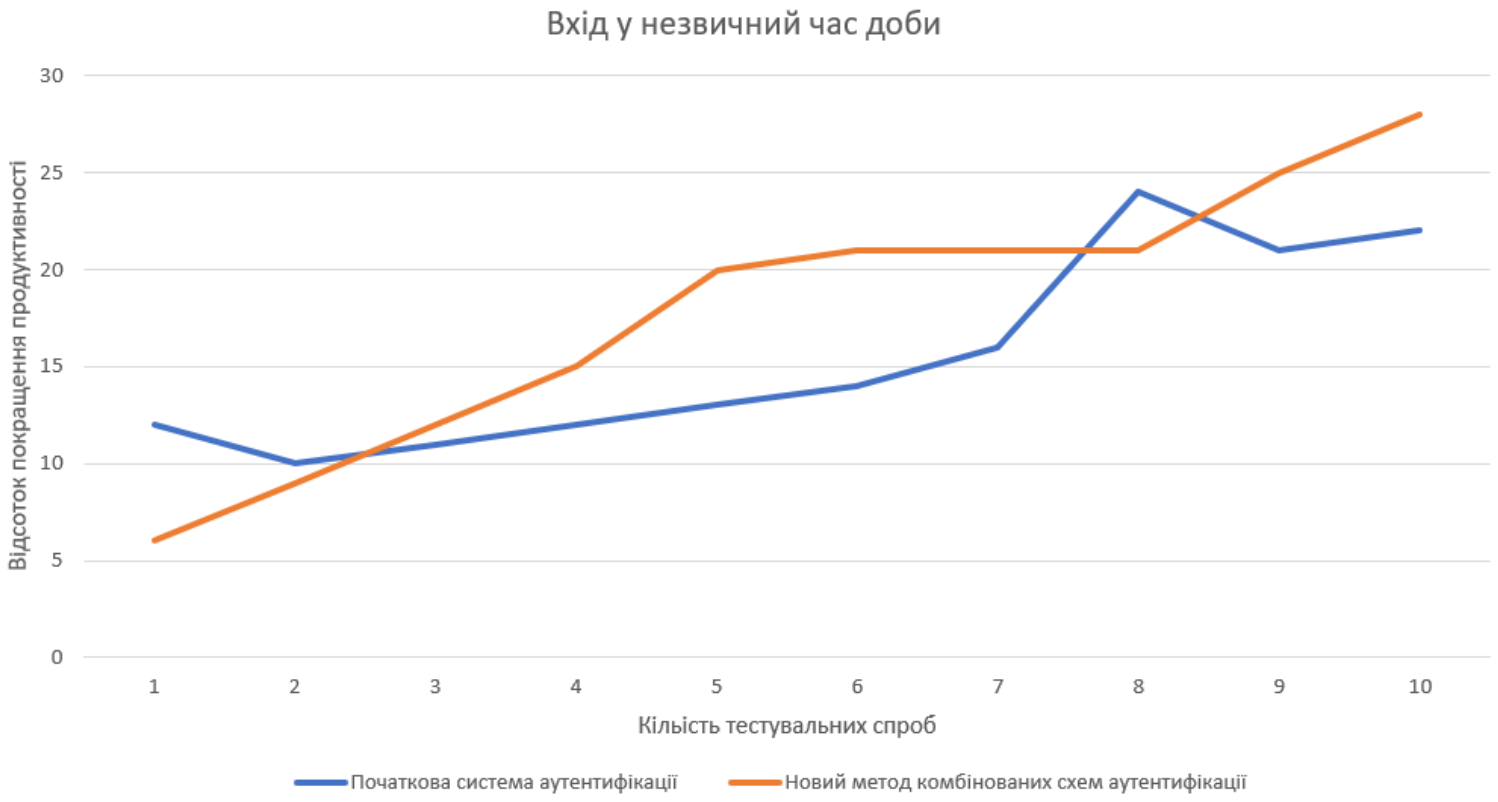


Рисунок 10 — Результати тестування входу у незвичні часи доби

Результати впровадження комбінованої схеми аутентифікації

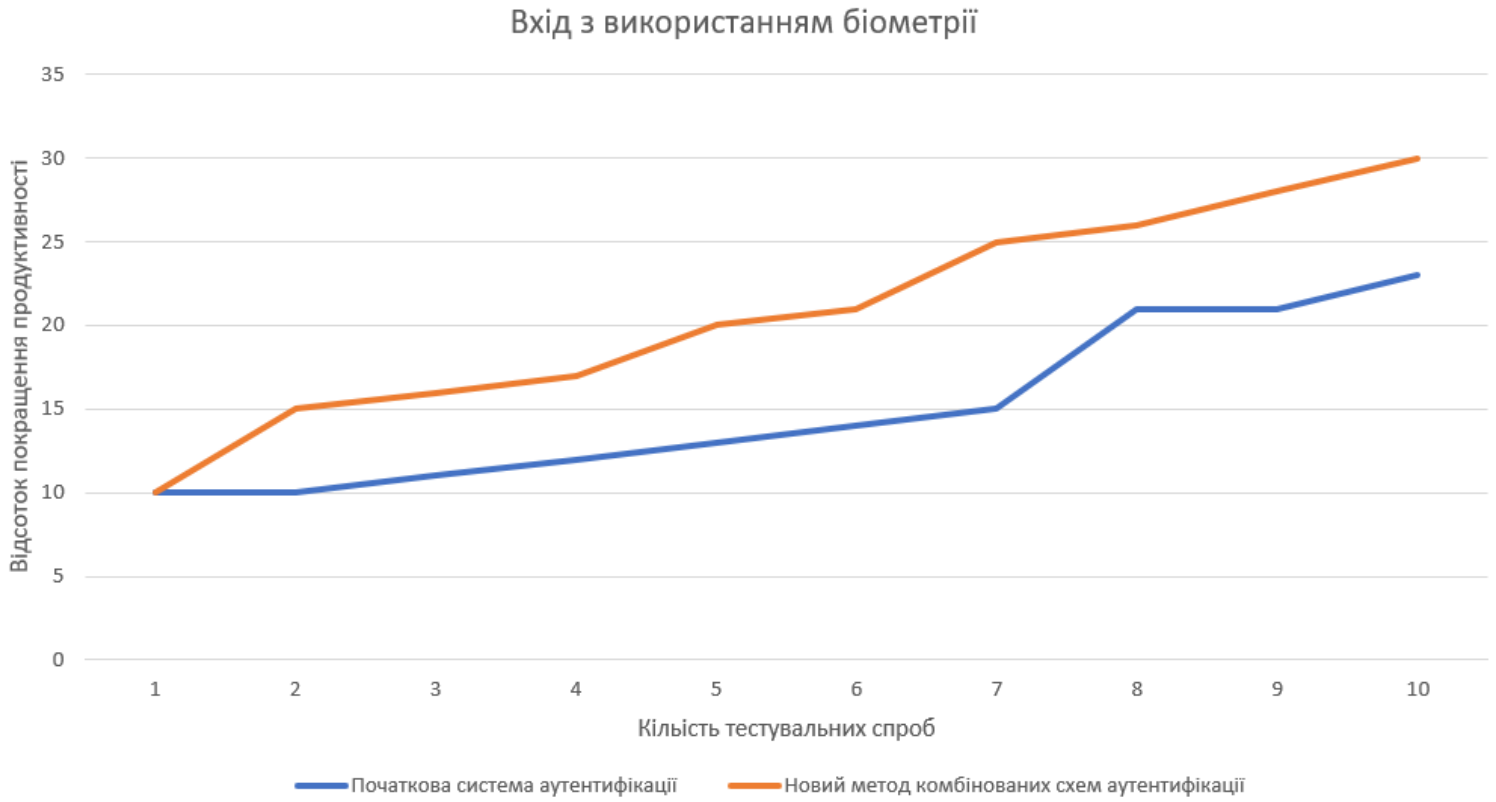
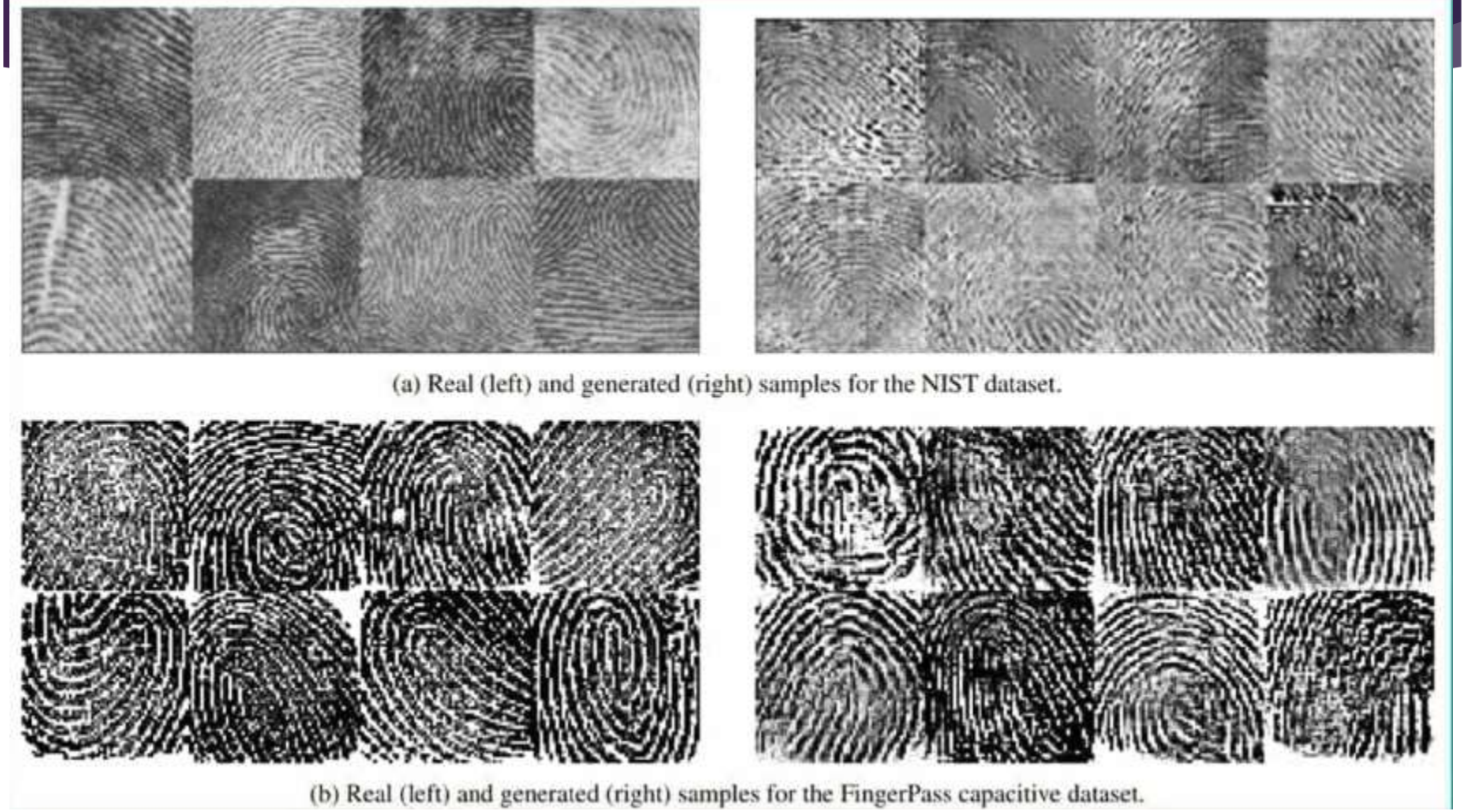


Рисунок 11 — Результати тестування входу за допомогою біометричних даних

Результати впровадження комбінованої схеми аутентифікації

Рисунок 12 — Результати роботи впровадженого методу

Можливі проблеми



(a) Real (left) and generated (right) samples for the NIST dataset.

(b) Real (left) and generated (right) samples for the FingerPass capacitive dataset.

Рисунок 13 — Тестування ШІ на створення відбитків пальців

Висновки

Протягом виконання роботи мною було проаналізовано предметну область, процеси обробки інформації для забезпечення безпеки підприємства, знайдено недоліки існуючої схеми автентифікації, виявлено найбільш небезпечні та найчастіші загрози та вразливості.
На основі проведеного аналізу мною було запропоновано програмне забезпечення та архітектуру кобмінованої схеми автентифікації, та протестовано програмне забезпезпеченя на сумсність
Було перевірено ефективність запропонованих пропозицій шляхом проведення тестування різних методів та порівняння статистики захисту

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Пирч Олени Вадимівни
ПІБ здобувача вищої освіти
Студентки ФІТ, 2 курсу, групи КБЗІм-23-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщена та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення текстових збігів в роботах.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

09.12.2024
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

ID: 158620 Назва: Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації Додано в БД: 2024-12-13 Автора: Пирч Олена Керівники: Тітова В.Ю. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	103534	758	771 (1%)	9 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Олена Пирч

Співавтор:

Назва: Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації

Науковий керівник: Віра Тітова

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:6%

Коефіцієнт подібності 2:2.7%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-13 13:07:48.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата 13.12.2024 експерт

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації

Автор: Пирч Олена Вадимівна

Спеціальність: 125 – Кібербезпека та захист інформації

Освітня програма: Кібербезпека та захист інформації

Науковий керівник: Тітова Віра Юріївна

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 94%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 97,4%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Виявлені модифікації стосуються математичних формул і не є порушенням академічної доброчесності.

Керівник роботи _____ Віра ТІТОВА

Гарант ОП _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

ОПП «магістр»

Магістр Пирч Олена Вадимівна
Тема: Метод підвищення стійкості електронного цифрового підпису за рахунок комбінованих схем аутентифікації

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації

Обсяг дипломної роботи ОПП «магістр»:

кількість листів креслень _____; кількість сторінок записки 91

1. Короткий зміст ДР та прийнятих рішень: В рамках магістерської роботи проведено детальний аналіз сучасних комбінованих схем аутентифікації. Розроблено новий підхід комбінованої схеми аутентифікації, який базується на системі штучного інтелекту. Запропонована методика дозволяє ідентифікувати потенційні загрози шляхом генерування тестових запитів і аналізу реакцій серверів, що значно підвищує ефективність та точність процесів тестування безпеки. Проведено тестування розробленої методики в реальних умовах, результати якого підтверджують її високу ефективність.
2. Висновок про відповідність ДР дипломному завданню Кваліфікаційна робота магістра повністю відповідає поставленим завданням, як у теоретичній, так і в практичній частинах. Отримані результати підтверджують доцільність інтеграції великих мовних моделей у процеси кібербезпеки.
3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У роботі обґрунтовано ефективність впроваджених методів ЕПЦ, проаналізовано існуючі підходи, визначено їх переваги та недоліки. Окреслено можливості комбінованих систем аутентифікації, для виявлення підозрілої активності користувачів. Розроблено новий метод впровадження комбінованих схем, що довів свою ефективність у реальних умовах. Отримані результати доповнені рекомендаціями щодо подальшого вдосконалення методу.
4. Позитивні сторони проекту: Запропонований метод значно підвищує ефективність процесів виявлення підозрілої активності і спроб втручання у систему безпеки підприємства завдяки інтеграції сучасних технологій штучного інтелекту і контекстуальної аутентифікації. Цей метод дозволяє полегшити виявлення загроз і автоматизувати рутинні задачі, скорочуючи час та ресурси, необхідні для аналізу безпеки. Метод також забезпечує адаптивність до змінних умов і масштабованість для великих проєктів, завдяки чому може бути застосований у широкому спектрі організацій. Особливо цінним є зниження впливу людського фактора, що мінімізує ризики помилок під час аналізу.
5. Негативні сторони проекту: Для ефективного впровадження методу потрібні значні обчислювальні ресурси, оскільки великі моделі штучного інтелекту для забезпечення

біометрії мають високу вимогливість до апаратного забезпечення. Крім того, успішна реалізація потребує кваліфікованої команди фахівців із кібербезпеки, здатних інтегрувати цей метод у вже існуючі системи. Також є певні ризики пов'язані з етичними аспектами використання біометричних даних користувачів, зокрема їх можливе зловживання зловмисниками.

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики дипломної роботи.

8. Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що вона заслуговує оцінку «відмінно»

РЕЦЕНЗЕНТ (прізвище, ім`я, по батькові, посада, місце роботи)
Мартинюк Валерій Володимирович, доктор технічних наук, професор

« _____ » _____ 2024 . _____ (підпис)

ХНУ. Зам. 54. тир. 6000. 2007.