Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
« » _____ 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: Метод та засіб забезпечення інформаційної безпеки в системах інтернет-банкінгу

Виконавець: студентка ІІ курсу, групи КБм-21

Анна КУСКОВА

(підпис) (Ім’я, ПРІЗВИЩЕ)

	Ім’я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Микола БРАЇЛОВСЬКИЙ	
Нормоконтроль	Сергій ДАКОВ	

Київ 2025

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
« » _____2024 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Кускова Анна Андріївна (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Метод та засіб забезпечення інформаційної безпеки в системах інтернет- банкінгу

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 4 від 24.10.2024 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процеси забезпечення інформаційної безпеки в системах інтернет-банкінгу.
Предмет досліджень	Методи та засоби захисту інформації в системах інтернет-банкінгу.
Мета	Розробка методу та засобу забезпечення інформаційної безпеки в системах інтернет-банкінгу.

Вихідні дані для проведення роботи Методи забезпечення безпеки сесій в інтернет-банкінгу

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна створення нового методу забезпечення інформаційної безпеки, що поєднує сучасні засоби, поведінковий аналіз та методи штучного інтелекту для виявлення загроз у реальному часі.

Практична цінність використання у банківських системах для підвищення рівня їхньої захищеності.

4. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	25.10.2024 – 29.12.2024
Аналіз літературних джерел	30.12.2024 – 12.02.2025
Аналітичний огляд сучасних загроз інформаційної безпеки в інтернет-банкінгу та аналіз наявних методів захисту.	13.02.2025 – 26.02.2025
Розробка концепції методу MiDIS та засобу CIBA-SHIELD як інноваційних рішень для підвищення захисту користувацьких сесій і авторизацій.	27.02.2024 – 1.04.2024
Проєктування архітектури і алгоритмів функціонування обох рішень з урахуванням контекстної поведінки користувачів.	1.04.2024 – 15.04.2024
Формування висновків і рекомендацій, а також підготовка матеріалів до захисту кваліфікаціної роботи.	15.04.2024 – 25.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	26.04.2024 – 15.05.2025
Подача пакету документів на розгляд ЕК	15.05.2025-19.05.2025

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (Ім’я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Анна КУСКОВА
(підпис) (Ім’я, ПРІЗВИЩЕ)

Дата видачі завдання: 25.10.2024 р.

Термін подання кваліфікаційної роботи до ЕК 19.05.2025 р.

РЕФЕРАТ

Пояснювальна записка містить 97 сторінок, включає 14 рисунки, 6 таблиць, 36 джерел за переліком посилань.

Об’єктом дослідження є процеси забезпечення інформаційної безпеки в системах інтернет-банкінгу.

Метою роботи є розробка інноваційного методу та засобу забезпечення інформаційної безпеки, що здатні адаптуватися до змінної поведінки користувачів та новітніх кіберзагроз.

У дослідженні застосовано методи аналізу кіберзагроз, поведінкового моделювання, криптографічних перетворень, аналізу активності користувачів, архітектурного проєктування програмних засобів та тестування інформаційних систем.

У результаті дослідження вдосконалено:

метод MiDIS (мікросегментованої динамічної ізоляції сесій), що дозволяє розділяти дії в онлайн-банкінгу на ізольовані сегменти з окремими політиками доступу, забезпечуючи гнучке управління ризиками в реальному часі;

засіб CIBA-SHIELD, який розширює стандарт OpenID Connect CIBA, додаючи рівень поведінкової автентифікації на серверній стороні без участі користувача, що підвищує безпеку бекенд-авторизацій.

Запропоновані розробки дозволяють суттєво знизити ризики компрометації облікових даних, реалізувати контроль доступу без втрати сесії, підвищити зручність і захищеність клієнтів банку. Економічний ефект полягає у зменшенні втрат від шахрайства, а соціальний — у підвищенні довіри до інтернет-банкінгу.

Результати роботи можуть бути використані банківськими установами, розробниками систем електронних платежів та постачальниками платформ цифрової автентифікації. Перспективними є дослідження адаптивного ризик-менеджменту в банківських сесіях, інтеграції MiDIS з SIEM-системами та розширення CIBA-SHIELD для багатоагентних сценаріїв.

Ключові слова: інформаційна безпека, інтернет-банкінг, автентифікація, поведінковий аналіз, контроль доступу, CIBA, мікросегментація, авторизація, машинне навчання, штучний інтелект, токен, сесія, протоколи безпеки, серверна логіка, ізоляція.

ЗМІСТ

ВСТУП

Розвиток цифрових технологій та активне впровадження інтернет-банкінгу створюють нові можливості для користувачів, але водночас породжують значні загрози інформаційній безпеці. Кіберзлочинність, шахрайство, несанкціонований доступ до конфіденційних даних стали актуальними викликами для банківських установ і користувачів фінансових послуг. Тому дослідження методів і засобів забезпечення інформаційної безпеки в системах інтернет-банкінгу є надзвичайно важливим завданням.

Інформаційна безпека інтернет-банкінгу є однією з ключових проблем сучасного фінансового сектору. За даними міжнародних досліджень, кібератаки на банківські системи з кожним роком зростають, що свідчить про необхідність вдосконалення методів захисту. У зв’язку з цим розробка ефективних методів і засобів забезпечення інформаційної безпеки має важливе теоретичне та практичне значення.

Наукові дослідження в цій сфері проводяться такими вченими, як У. Діффі, М. Геллман, Б. Шнайдер, які розробили криптографічні методи захисту інформації. У вітчизняній науковій літературі значний внесок у розвиток інформаційної безпеки зробили В. Г. Кореневський, О. В. Синявський та інші. Проте питання комплексного підходу до забезпечення інформаційної безпеки інтернет-банкінгу, що враховує новітні методи автентифікації, шифрування та виявлення аномалій, потребує подальшого дослідження.

Метою роботи є розробка методу та засобу забезпечення інформаційної безпеки в системах інтернет-банкінгу. Для досягнення цієї мети необхідно вирішити такі завдання:

- провести аналіз сучасних методів забезпечення інформаційної безпеки;
- розробити новий підхід до захисту банківських систем;
- реалізувати новий метод;
- оцінити ефективність розробленого засобу.

Об'єкт дослідження – процеси забезпечення інформаційної безпеки в системах інтернет-банкінгу.

Предмет дослідження – методи та засоби захисту інформації в системах інтернет-банкінгу.

Методи дослідження включають аналіз загроз, математичне моделювання, криптографічні методи захисту, а також тестування розроблених засобів.

Наукова новизна полягає у створенні нового методу забезпечення інформаційної безпеки, що поєднує сучасні засоби, поведінковий аналіз та методи штучного інтелекту для виявлення загроз у реальному часі.

Практичне значення одержаних результатів

Розроблений метод може бути використаний у банківських системах для підвищення рівня їхньої захищеності. Він дозволяє зменшити ризики шахрайства, підвищити стійкість до атак та забезпечити безпечний доступ до фінансових послуг.

Подальше впровадження та тестування розробленого методу можуть стати основою для майбутніх публікацій і презентацій у сфері інформаційної безпеки.

Таким чином, проведене дослідження сприяє підвищенню рівня безпеки інтернет-банкінгу та може бути корисним для фінансових установ, розробників програмного забезпечення та дослідників у сфері кібербезпеки.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНТЕРНЕТ-БАНКІНГУ

1.1. Загрози та вразливості систем інтернет-банкінгу

Системи інтернет-банкінгу відіграють важливу роль у сучасній фінансовій сфері, забезпечуючи швидкий і зручний доступ до банківських послуг. Однак із розвитком цифрових технологій збільшується і кількість загроз, що можуть спричинити серйозні фінансові та репутаційні втрати для банків та їхніх клієнтів. Основні загрози та вразливості інтернет-банкінгу включають наступні аспекти.

Фішинг є одним із найпоширеніших способів шахрайства в інтернет-банкінгу. Зловмисники створюють підроблені веб-сайти, що імітують офіційні сторінки банків, або надсилають електронні листи та повідомлення, які містять шкідливі посилання [1]. Користувачі, нічого не підозрюючи, вводять свої логіни, паролі та іншу конфіденційну інформацію, яка в подальшому використовується для несанкціонованого доступу до рахунків.

Використання вірусів, троянів та інших видів шкідливого програмного забезпечення (ПЗ) є ще однією суттєвою загрозою. Троянські програми можуть перехоплювати натискання клавіш, зчитувати файли та викрадати дані користувачів під час входу до системи інтернет-банкінгу [2]. Зловмисники можуть використовувати кейлогери (програми для запису натискання клавіш), руткіти та інші інструменти для збору конфіденційної інформації.

DDoS-атаки спрямовані на перевантаження серверів банку великою кількістю запитів, що призводить до порушення нормальної роботи системи [3]. Це може зробити сервіси інтернет-банкінгу недоступними для користувачів і завдати фінансових збитків банківським установам.

Методи соціальної інженерії використовуються зловмисниками для маніпуляції користувачами з метою отримання конфіденційних даних або змушення

їх виконати певні дії. Наприклад, шахраї можуть телефонувати під виглядом представників банку та просити підтвердити особисті дані або одноразові паролі [4].

Недосконаліть програмного забезпечення або його застарілі версії можуть містити критичні вразливості, які дозволяють зловмисникам отримати доступ до системи інтернет-банкінгу [5]. Виявлення та використання таких вразливостей може призвести до витоку персональних даних, фінансових втрат та порушення цілісності банківських транзакцій.

Багато банків все ще використовують однофакторну автентифікацію (логін і пароль), що робить систему вразливою до атак [6]. Відсутність багатофакторної автентифікації значно спрощує можливість зловмисників отримати несанкціонований доступ до рахунку користувача.

Підключення до систем інтернет-банкінгу через публічні Wi-Fi мережі або використання незахищених пристроїв підвищує ризик перехоплення даних [7]. Відсутність сучасних засобів шифрування даних може призвести до їх витоку та компрометації облікових записів.

Загрози та вразливості систем інтернет-банкінгу постійно розвиваються, тому необхідно впроваджувати новітні методи захисту, зокрема багатофакторну автентифікацію, поведінковий аналіз та алгоритми штучного інтелекту для виявлення загроз. Впровадження сучасних технологій кібербезпеки сприятиме підвищенню рівня захисту банківських систем та мінімізації ризиків для користувачів.

1.2. Методи автентифікації користувачів

Автентифікація є ключовим етапом забезпечення інформаційної безпеки в системах інтернет-банкінгу. Вона дозволяє перевірити особу користувача та запобігти несанкціонованому доступу до банківських послуг. Основні методи автентифікації можна розділити на три категорії: знання, володіння та біометричні дані [1].

Парольна автентифікація є найпоширенішим методом підтвердження особи в інтернет-банкінгу. Вона ґрунтується на знанні користувачем секретної комбінації символів (пароля або PIN-коду) [2]. Однак цей метод має суттєві недоліки, такі як можливість підбору пароля, використання слабких паролів та схильність до фішингових атак [3]. Одноразові паролі є більш безпечним варіантом, оскільки вони генеруються для кожної окремої сесії або транзакції. OTP можуть надсилатися користувачам через SMS, електронну пошту або мобільні додатки (наприклад, Google Authenticator) [4]. Хоча цей метод зменшує ризик компрометації основного пароля, він також має вразливості, такі як перехоплення SMS або зловживання з боку шкідливого програмного забезпечення [5].

Двофакторна автентифікація передбачає використання двох незалежних методів підтвердження особи. Найчастіше це поєднання традиційного пароля з OTP або біометричними даними [6]. Цей підхід значно ускладнює зловмисникам можливість отримати несанкціонований доступ до банківського рахунку. Апаратні токени є фізичними пристроями, які генерують одноразові паролі або використовують криптографічні механізми для автентифікації. Ці пристрої можуть бути USB-ключами (наприклад, YubiKey) або смарт-картами, що містять захищені сертифікати [7]. Хоча вони забезпечують високий рівень безпеки, їх використання пов’язане з додатковими витратами та ризиками втрати пристрою.

Сканування відбитків пальців широко використовується у мобільному банкінгу та фінансових додатках завдяки зручності та швидкості автентифікації [8]. Цей метод забезпечує високий рівень безпеки, але може бути вразливим до атак, що використовують підроблені відбитки або вразливості сенсорів. Сучасні мобільні пристрої підтримують розпізнавання обличчя та голосу як методи біометричної автентифікації. Алгоритми машинного навчання аналізують унікальні риси обличчя або голосові характеристики користувача [9]. Проте ці методи можуть бути обійдені за допомогою високоякісних фотографій, відеозаписів або синтетичних голосів. Поведінкова автентифікація використовує унікальні патерни поведінки користувача, такі як динаміка натискання клавіш, швидкість введення тексту або спосіб утримання пристрою [10]. Використання штучного інтелекту дозволяє створювати

профілі поведінки та виявляти аномальні дії, що можуть свідчити про компрометацію облікового запису.

Ефективна автентифікація користувачів є основою кібербезпеки у системах інтернет-банкінгу. Використання мультифакторних методів, а також інтеграція біометричних та поведінкових факторів дозволяє значно знизити ризик компрометації облікових записів і підвищити рівень захисту фінансових операцій.

1.3. **Сучасні засоби кібербезпеки у банківській сфері**

Забезпечення кібербезпеки у банківській сфері є критично важливим завданням, оскільки фінансові установи залишаються однією з головних цілей кібератак. Сучасні засоби захисту включають як традиційні методи, так і інноваційні технології, що використовують штучний інтелект і машинне навчання для виявлення загроз і запобігання шахрайським операціям [1].

Шифрування є основним методом забезпечення безпеки банківських даних. Використання протоколів SSL/TLS гарантує захищений зв’язок між клієнтом і банком, а алгоритми симетричного та асиметричного шифрування забезпечують збереження конфіденційності переданих даних [11]. Додатковим рівнем захисту є впровадження апаратних модулів безпеки (HSM), які дозволяють надійно зберігати криптографічні ключі [12].

Системи виявлення та запобігання вторгненням (IDS/IPS) відіграють важливу роль у виявленні аномальної активності та запобіганні несанкціонованому доступу до банківських систем. Вони аналізують мережевий трафік і блокують підозрілі запити, використовуючи як сигнатурний аналіз, так і поведінкові алгоритми [13]. Фаєрволи також залишаються основним інструментом кібербезпеки, контролюючи трафік між зовнішніми та внутрішніми мережами банку, запобігаючи атакам типу DDoS та несанкціонованому доступу [14].

Системи багатофакторної автентифікації (MFA) дозволяють підвищити рівень безпеки доступу до банківських рахунків. Вони включають використання одноразових паролів, біометричних даних та поведінкового аналізу, що робить

процес аутентифікації більш надійним [15]. Крім того, у фінансовому секторі активно впроваджуються технології безпарольної автентифікації, що використовують криптографічні ключі та біометричні фактори замість традиційних паролів [16].

Штучний інтелект та машинне навчання відіграють важливу роль у забезпеченні безпеки банківських операцій. Аналітичні системи аналізують фінансові транзакції в режимі реального часу, виявляючи підозрілі операції та шахрайські дії. Використання поведінкової аналітики дозволяє створювати профілі звичайної активності користувачів і виявляти відхилення, що можуть свідчити про компрометацію облікового запису [17].

Захист мобільного банкінгу є окремим напрямом кібербезпеки. Банки впроваджують захищені мобільні додатки, що використовують вбудовані механізми безпеки, такі як захищені середовища виконання (Secure Enclaves), біометрична автентифікація та захист від реверс-інжинірингу [18]. Також активно розвиваються методи виявлення шкідливого програмного забезпечення, яке може красти банківські дані користувачів.

Фінансові установи також застосовують системи безперервного моніторингу та управління подіями безпеки (SIEM), які агрегують та аналізують журнали подій у реальному часі, дозволяючи швидко реагувати на потенційні загрози [19]. Крім того, банки регулярно проводять тестування на проникнення (penetration testing) та оцінку вразливостей, що допомагає виявляти слабкі місця у системах безпеки.

Отже, сучасні засоби кібербезпеки у банківській сфері поєднують класичні методи захисту з новітніми технологіями штучного інтелекту, що дозволяє значно зменшити ризики кібератак і шахрайських операцій. Впровадження комплексного підходу до безпеки, що включає багаторівневий захист, аналіз поведінки користувачів і автоматизовані системи виявлення загроз, є необхідною умовою для забезпечення надійності банківських систем.

1.4 Використання штучного інтелекту та поведінкового аналізу для підвищення безпеки

Штучний інтелект (ШІ) і поведінковий аналіз відіграють ключову роль у сучасних стратегіях кібербезпеки банківських систем. Вони дозволяють автоматизувати виявлення загроз, аналізувати поведінкові патерни користувачів і забезпечувати адаптивний рівень захисту від кібератак та шахрайських дій [20].

Впровадження ШІ в кібербезпеку банківських систем дозволяє ефективно аналізувати великі обсяги транзакційних даних у реальному часі. Алгоритми машинного навчання навчаються на основі історичних даних та можуть прогнозувати потенційні шахрайські операції ще до їхнього завершення [21]. Крім того, використання нейронних мереж дозволяє покращувати точність виявлення аномалій у банківських транзакціях, що знижує кількість хибнопозитивних спрацьовувань [22].

Одним із найбільш ефективних напрямів застосування ШІ є поведінковий аналіз. Традиційні методи автентифікації базуються на статичних факторах, таких як паролі чи одноразові коди, які можуть бути скомпрометовані. Натомість поведінковий аналіз враховує такі параметри, як стиль набору тексту, швидкість натискання клавіш, траєкторія руху миші, спосіб утримання пристрою та навіть місцезнаходження користувача [23]. Це дозволяє системам банківського захисту автоматично визначати відхилення у поведінці та виявляти потенційні загрози.

ШІ також використовується для запобігання атакам типу "людина посередині" (MITM), фішинговим атакам та витоку конфіденційної інформації. Наприклад, аналітичні платформи можуть аналізувати електронні листи, виявляючи підозрілі повідомлення, що містять фішингові посилання, а також визначати зламані акаунти на основі зміни звичної активності користувача [24].

Захист мобільного банкінгу також значною мірою покладається на ШІ та поведінковий аналіз. Банківські додатки можуть автоматично аналізувати рівень ризику користувача, адаптуючи методи автентифікації в залежності від контексту доступу. Наприклад, якщо користувач входить у систему з нового пристрою або

нетипового місцезнаходження, система може вимагати додаткову перевірку особи, наприклад, за допомогою біометричних даних або багатофакторної автентифікації [25].

Поведінковий аналіз також дозволяє ефективно боротися з ботами та автоматизованими кібератаками. Використовуючи алгоритми машинного навчання, системи безпеки можуть відрізняти реальних користувачів від автоматизованих ботів на основі патернів їхньої активності. Це особливо важливо для запобігання атакам на банківські API, де зловмисники намагаються автоматично отримати доступ до клієнтських даних [26].

Застосування ШІ для підвищення безпеки у банківській сфері також включає автоматизований аналіз журналів подій та інцидентів безпеки. Використовуючи технології обробки природної мови (NLP), такі системи можуть автоматично виявляти загрози в повідомленнях аналітиків, визначати критичні події та пропонувати оптимальні стратегії реагування на кіберзагрози [27].

Таким чином, використання штучного інтелекту та поведінкового аналізу у банківських системах значно підвищує рівень безпеки, зменшуючи ризики шахрайських операцій, несанкціонованого доступу та автоматизованих атак. Інтеграція цих технологій дозволяє фінансовим установам забезпечити проактивний підхід до кіберзахисту, що є ключовим фактором у сучасному цифровому середовищі.

1.5. Огляд сучасних технологій і підходів до захисту даних

Впровадження хмарних технологій у банківській сфері дозволяє значно оптимізувати обробку, зберігання та аналіз великих обсягів даних, водночас забезпечуючи підвищення безпеки та відповідності нормативним вимогам. Одним із ключових рішень є хмарні платформи, що пропонують інтегровані інструменти для захисту даних, включаючи шифрування, моніторинг загроз і управління доступом.

Основними перевагами хмарних рішень є висока масштабованість, можливість обробки даних у режимі реального часу та зниження витрат на локальну

інфраструктуру. Наприклад, використання хмарного середовища дозволяє банківським установам швидко адаптуватися до змінних вимог бізнесу, зокрема під час обробки транзакцій або аналізу великих обсягів історичних даних клієнтів.

Сучасні хмарні рішення також інтегрують технології багаторівневого шифрування для забезпечення конфіденційності даних. Наприклад, шифрування "у спокої" (encryption at rest) та "у русі" (encryption in transit) гарантує захист як збереженої, так і переданої інформації. Ці технології особливо важливі у випадках міжхмарної міграції або гібридних архітектур, які поєднують локальні дата-центри та хмарну інфраструктуру.

Розглянемо існуючі рішення від провідних провайдерів хмарних технологій. Amazon Web Services є одним із лідерів ринку хмарних рішень, пропонуючи банкам широкий спектр інструментів для захисту даних. Одним із ключових продуктів є AWS Key Management Service (KMS), який дозволяє керувати ключами шифрування на рівні додатків та інфраструктури. Крім того, AWS пропонує сервіс GuardDuty для виявлення загроз у реальному часі та CloudTrail для аудиту дій користувачів.

Інноваційною функцією AWS є система IAM (Identity and Access Management), яка забезпечує детальний контроль доступу користувачів до хмарних ресурсів Рис.1.1. Завдяки підтримці багатофакторної автентифікації та налаштуванню політик доступу, банки можуть мінімізувати ризики несанкціонованого доступу до даних [13].

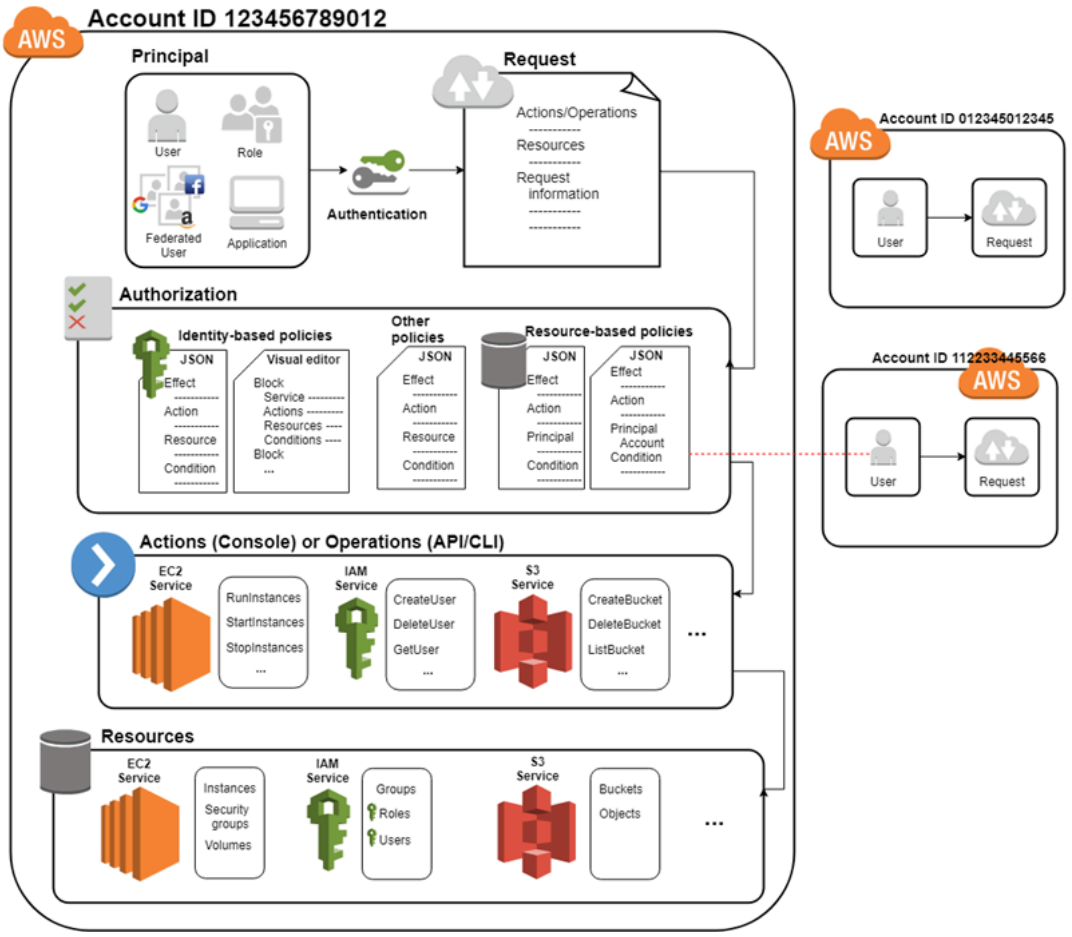

Рисунок 1.1. - Access Management (IAM) компонент хмарної безпеки

Робота IAM починається з ідентифікації користувачів, ролей або програм, які звертаються до ресурсів AWS. Користувачі можуть бути фізичними особами, федеративними користувачами, що підключаються через зовнішні системи автентифікації, або автоматизованими сервісами, які діють від імені ролей IAM. Кожна дія в AWS починається із запиту, який включає інформацію про бажану операцію, ресурс, а також автентифікаційні дані.

Після отримання запиту IAM перевіряє, чи належить ідентифікатор до системи AWS, використовуючи облікові дані, такі як ключі доступу, паролі або токени. Автентифікація підтверджує, що запит надходить від дійсного користувача або ролі. Далі виконується процес авторизації, який визначає, чи дозволено користувачу виконати запитану дію. Це досягається шляхом перевірки політик доступу, які описують дозволи у форматі JSON. Політики можуть бути прив’язані як до ідентифікаторів, так і до самих ресурсів, що дозволяє гнучко контролювати доступ.

Якщо запит авторизований, IAM дозволяє користувачеві виконати запитану дію, таку як запуск екземпляра EC2, створення бакету S3 або редагування групи безпеки. Усі операції реєструються для подальшого аудиту.

Наступним до розгляду є Google Cloud Platform який пропонує рішення, орієнтовані на високий рівень автоматизації та безпеки даних. GCP включає сервіси Cloud KMS для управління ключами шифрування та Security Command Center для моніторингу загроз.

Унікальною особливістю GCP є Confidential Computing, яка забезпечує захист даних навіть під час їхньої обробки. Це досягається завдяки використанню захищених середовищ виконання, які унеможливлюють доступ до даних навіть адміністраторів хмарної платформи [14]. Розглянемо детальніше архітектуру на Рис.1.2.

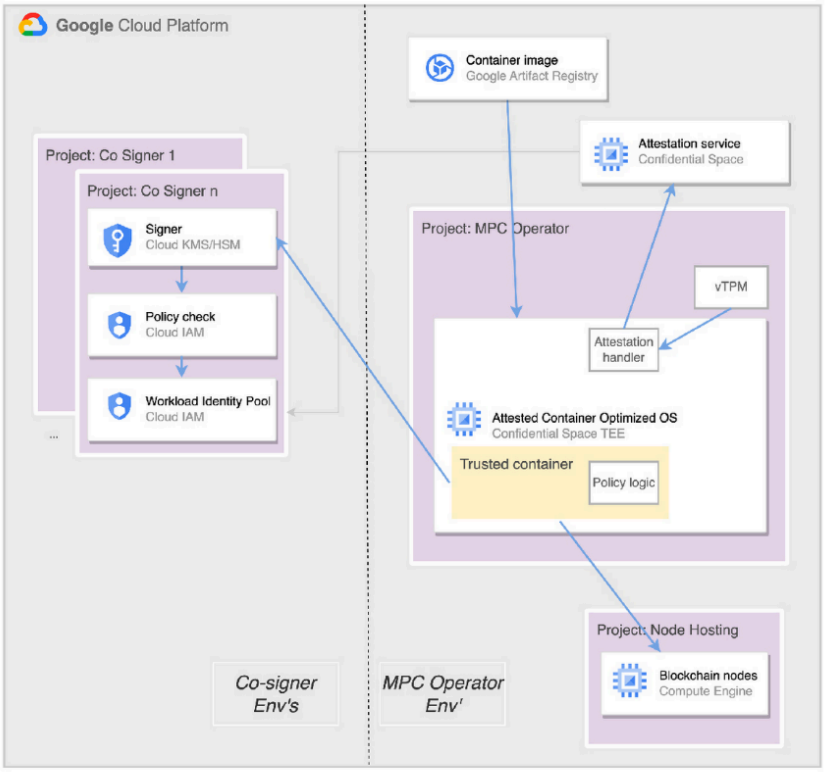

Рисунок 1.2. – Використання сервісів GCP для захищеного виконання операцій із використанням контейнерів

На лівій частині представлений процес підписання даних (Co-Signer). Для кожного підписувача використовується сервіс Cloud KMS/HSM, який забезпечує безпечне управління ключами. Додатковий контроль здійснюється за допомогою Cloud IAM, де перевіряються політики доступу, а також використовується Workload Identity Pool для інтеграції ідентифікаційних даних.

Центральна частина відповідає за обробку в довіреному середовищі (MPC Operator). Тут використовується Attestation Service, що перевіряє контейнерні образи з Google Artifact Registry. Контейнер завантажується в захищене середовище виконання (Trusted Container) на базі Attested Container Optimized OS, яке забезпечує дотримання політик доступу через Policy Logic. Для додаткового захисту інтегрується віртуальний TPM (vTPM) для керування криптографічними операціями.

У правій частині представлений модуль Node Hosting, який розгортає вузли блокчейну на Compute Engine, забезпечуючи їх роботу в ізольованих та захищених середовищах.

І останнім до розгляду є Microsoft Azure пропонує інтегровані рішення для безпеки даних, такі як Azure Security Center, який надає можливості для виявлення загроз і рекомендації щодо їхнього усунення. Azure також забезпечує шифрування даних за допомогою Azure Disk Encryption, що базується на BitLocker та DM-Crypt.

Особливістю Azure є підтримка гібридних рішень, що дозволяє банкам поєднувати локальну інфраструктуру із хмарними сервісами. Це забезпечує високу гнучкість та відповідність нормативним вимогам. Крім того, Azure Active Directory забезпечує централізоване управління автентифікацією та дозволами доступу користувачів [15]. Розглянемо детальніше зображення яке описує Azure AD на рис.2.3.

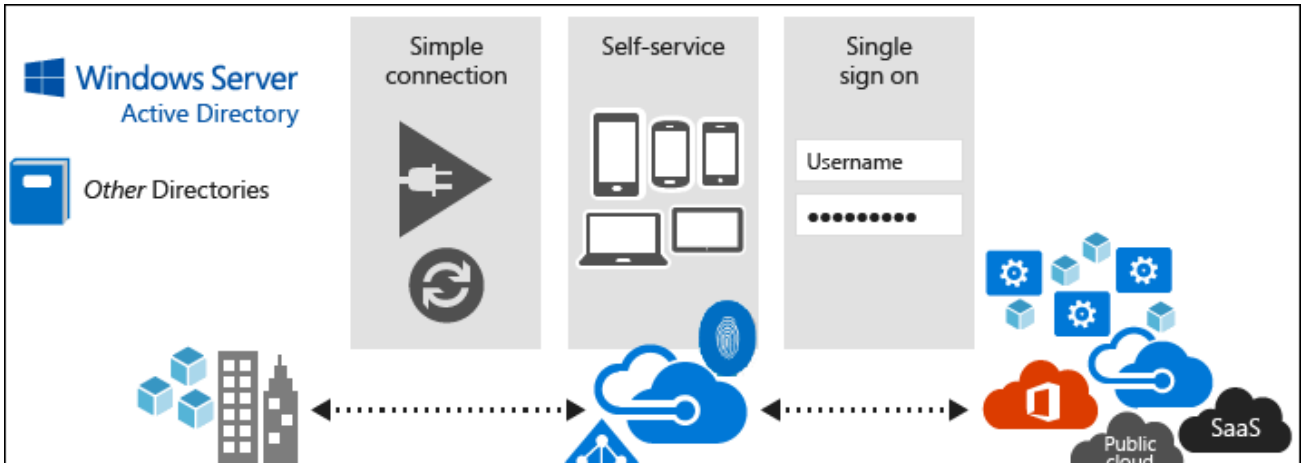

Рисунок 1.3. – Azure AD інтегрує локальні інфраструктури з хмарними сервісами

Azure AD забезпечує просте підключення через синхронізацію локальних каталогів з хмарою, функцію самообслуговування користувачів (зміна паролів, відновлення доступу) та єдиний вхід (Single Sign-On), що дозволяє користувачам отримувати доступ до локальних і хмарних ресурсів за допомогою одного облікового запису.

Це підвищує безпеку, спрощує управління ідентифікаціями та забезпечує безперебійну роботу з публічними хмарами, SaaS-додатками та іншими сервісами. Узагальнюючи попередню інформацію розглянемо таблицю 1.1.

Таблиця 1.1.

Технологія	Переваги	Недоліки
AWS (Amazon Web Services)	Розвинений набір інструментів безпеки, включаючи KMS для шифрування ключів і GuardDuty для моніторингу загроз. IAM забезпечує детальний контроль	Складність у налаштуванні політик безпеки для великих організацій. Висока вартість сервісів при довготривалому використанні.

Технологія	Переваги	Недоліки
	доступу з багатофакторною автентифікацією. Глобальна доступність та масштабованість.	
Microsoft Azure	Підтримка гібридних рішень для інтеграції локальної та хмарної інфраструктури. Azure Security Center для моніторингу загроз та Azure Disk Encryption для безпеки даних. Azure AD забезпечує централізоване управління доступом.	Може бути складним у впровадженні для організацій з великими локальними системами. Залежність від мережевого підключення для інтеграції з локальною інфраструктурою.

Порівняння основних хмарних технологій для банківської системи

Продовження таблиці 1.1

Google Cloud Platform (GCP)	Confidential Computing гарантує захист даних навіть під час обробки. Автоматизація процесів безпеки через Security Command Center.	Обмежена підтримка гібридної інфраструктури порівняно з Azure.

	Інтеграція з потужними інструментами аналітики Google для аналізу даних.	

Хмарні технології, що пропонуються провідними провайдерами, надають банківським установам надійні інструменти для забезпечення безпеки даних. AWS акцентує увагу на управлінні ключами та аудиту доступу, Azure виділяється підтримкою гібридних рішень і централізованим управлінням доступом, тоді як GCP зосереджений на захисті даних під час їхньої обробки. Обираючи відповідне хмарне рішення, банки повинні враховувати свої бізнес-потреби, технічні вимоги та нормативні обмеження, забезпечуючи баланс між безпекою, продуктивністю та гнучкістю.

1.6 Загрози та виклики безпеки великих даних у банківській системи

Великі дані є важливим ресурсом для банківських установ, але разом із можливостями, які вони надають, виникають і суттєві виклики в забезпеченні їхньої безпеки. Банківська сфера, яка працює з великими обсягами конфіденційної інформації, зокрема фінансовими транзакціями, персональними даними клієнтів і операційними записами, постійно піддається ризику кібератак та інших загроз.

Однією з найбільш значущих загроз є несанкціонований доступ до даних, який може статися через слабкі механізми автентифікації, компрометацію облікових записів або використання вразливостей у програмному забезпеченні. Наприклад, витік даних у Capital One у 2019 році, що охопив понад 100 мільйонів клієнтів, призвів до витрат у $150 мільйонів на відновлення та компенсації. Згідно з дослідженням IBM Security, 19% витоків даних у фінансовому секторі у 2023 році були пов’язані з такими порушеннями.

Не менш серйозною загрозою є кібератаки, зокрема DDoS, фішинг або шкідливе програмне забезпечення. DDoS-атаки, спрямовані на виведення з ладу критичних систем банку, становлять близько 20% усіх атак у фінансовій сфері,

згідно з Akamai. Фішингові атаки, які використовуються для крадіжки облікових даних клієнтів, складають 36% усіх кіберзагроз, за даними Verizon. Такі атаки не лише завдають фінансових збитків, але й підривають довіру клієнтів.

Внутрішні зловживання працівників є ще одним викликом безпеки. Згідно зі звітом Insider Threat Report 2023, 34% порушень безпеки у фінансових організаціях пов'язані з діями співробітників. Це може включати навмисне копіювання, зміну або видалення даних. Наприклад, у 2021 році в одному з європейських банків співробітник незаконно викрав понад 10 000 записів про клієнтів для подальшого продажу.

Останнім викликом є загроза цілісності даних, коли збої в системах або дії зловмисників призводять до спотворення транзакційних записів. За оцінками IDC, 21% банків у світі хоча б раз на рік стикалися з втратою або пошкодженням даних. Така ситуація впливає на звітність, операційну діяльність і довіру клієнтів. На діаграмі на рис.1.2. можна побачити порівняння основних загроз безпеки у банківській системі.

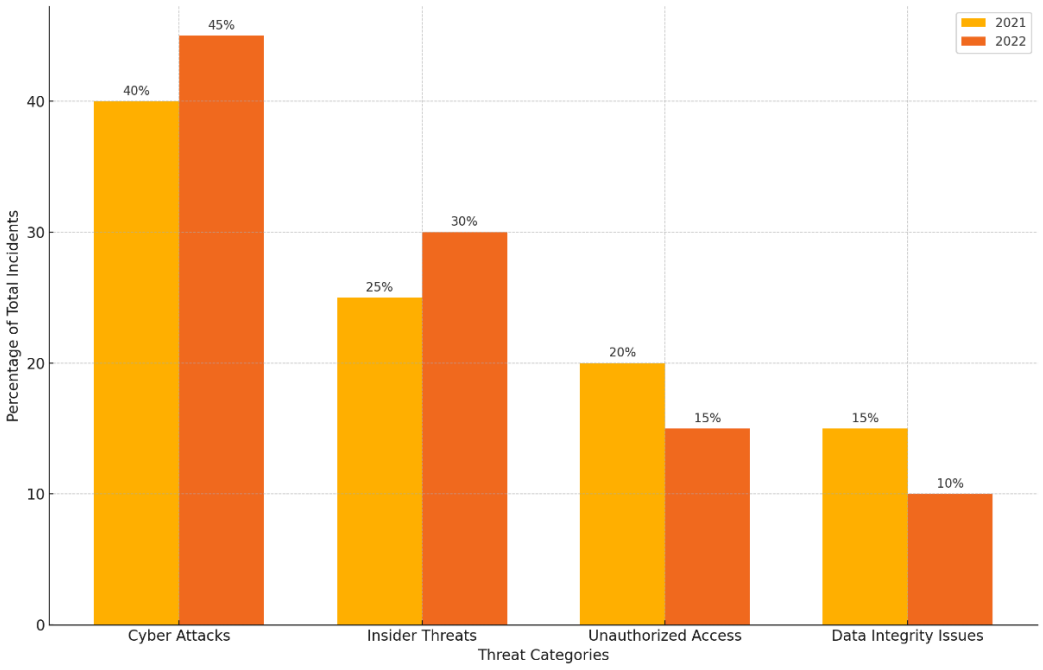

Рисунок 1.4. – Порівняння основних загроз у банківській системі.

Категорії загроз включають кібератаки, внутрішні загрози, несанкціонований доступ та порушення цілісності даних. Графік ілюструє зростання або зменшення кількості інцидентів у кожній категорії, підкреслюючи важливість відповідних заходів безпеки для мінімізації ризиків. Узагальнюючи інформацію основних загроз безпеки розглянемо у таблиці 1.2.

Таблиця 1.2.

Основні загрози безпеки

Загроза	Опис	Приклад наслідків
Несанкціонований доступ	Використання слабких механізмів автентифікації або вразливостей для доступу до конфіденційних даних.	Витік даних про клієнтів, злам систем. Наприклад, витік у Capital One (2019) з понад 100 млн клієнтів.

Продовження таблиці 1.2

Кібератаки	DDoS-атаки, фішингові атаки та використання шкідливого ПЗ для порушення роботи систем або крадіжки даних.	DDoS-атака блокує доступ до банківських сервісів, зупиняючи транзакції. Фішинг призводить до крадіжки облікових даних.
Внутрішні зловживання	Несанкціоновані дії співробітників, включаючи крадіжку,	Викрадення понад 10 000 записів клієнтів для

	зміну чи видалення даних.	продажу (2021, один із європейських банків).
Порушення цілісності даних	Зміна або пошкодження транзакційних даних через збої систем або дії зловмисників.	Збій у Banco do Brasil (2020) призвів до пошкодження даних, фінансових втрат у $20 млн.
Витік даних через хмарні платформи	Ризики, пов’язані з децентралізацією зберігання даних у хмарних сервісах, включаючи перехоплення даних під час передачі.	Компрометація доступу до хмарного сховища може призвести до масштабного витоку даних клієнтів.

Розглядаючи виклики забезпечення безпеки великих даних перш за все, одним із головних викликів є масштаб даних. Обробка великих обсягів інформації потребує значних обчислювальних ресурсів і сучасних систем захисту. Це ускладнює забезпечення безпеки, оскільки звичайні засоби не завжди можуть впоратися з такими обсягами даних у реальному часі.

Ще одним викликом є різноманітність даних. Банки працюють із структурованими, напівструктурованими та неструктурованими даними. Забезпечення безпеки для кожного типу даних потребує окремих підходів, що значно ускладнює розробку уніфікованої системи захисту.

Децентралізація зберігання даних, наприклад, у хмарних системах, створює додаткові ризики. Використання хмарних платформ відкриває доступ до даних через мережу Інтернет, що підвищує ризики зовнішніх атак. Забезпечення безпеки в

хмарному середовищі потребує впровадження шифрування, багаторівневих систем доступу та захисту від перехоплення даних під час передачі.

Використання хмарних технологій у банківській сфері забезпечує нові можливості для ефективного зберігання та обробки великих даних, але водночас створює певні виклики у забезпеченні їхньої безпеки. Одним із головних аспектів є децентралізація даних, коли інформація зберігається у розподілених сховищах, що може розташовуватися у різних країнах. Це ускладнює контроль за даними та створює ризики, пов'язані з юридичними вимогами до захисту інформації в різних юрисдикціях.

Під час передачі даних між користувачами та хмарними сервісами виникає необхідність у надійному захисті, який забезпечується використанням сучасних методів шифрування, таких як TLS або SSL. Крім того, важливу роль відіграє шифрування даних під час їхнього зберігання, що мінімізує ризики витоку інформації у разі компрометації хмарної платформи.

Забезпечення безпеки вимагає впровадження багаторівневого управління доступом, включаючи багатофакторну автентифікацію та розмежування прав доступу користувачів. Хмарні платформи також пропонують інтегровані інструменти моніторингу, які дозволяють виявляти загрози в реальному часі. Важливим є і резервне копіювання даних, яке гарантує можливість відновлення інформації у разі збоїв або атак.

Особливістю хмарних сервісів є спільна відповідальність за безпеку даних. Провайдери відповідають за захист інфраструктури, а клієнти, у свою чергу, за налаштування доступу та управління даними. Це потребує від банків високої кваліфікації персоналу для ефективної роботи з хмарними технологіями. Таким чином, впровадження хмарних технологій у банківській сфері вимагає комплексного підходу до забезпечення безпеки, який включає шифрування, моніторинг і чіткий розподіл відповідальності.

Отже, великі дані в банківській системі стикаються зі значними загрозами та викликами, які впливають на їхню безпеку. Основними загрозами є несанкціонований доступ, кібератаки, внутрішні зловживання та порушення

цілісності даних. Виклики безпеки включають масштабність і різноманітність даних, а також децентралізоване зберігання в хмарних платформах. Для ефективного захисту великих даних банки повинні впроваджувати сучасні технології безпеки, такі як шифрування, багатофакторна автентифікація та інструменти моніторингу загроз у реальному часі.

Висновки до розділу 1

У першому розділі було проведено аналіз основних загроз та вразливостей систем інтернет-банкінгу, розглянуто сучасні методи автентифікації користувачів, а також досліджено інноваційні засоби кібербезпеки, що використовуються у фінансовій сфері. Особливу увагу було приділено використанню штучного інтелекту та поведінкового аналізу для підвищення рівня безпеки банківських систем.

Аналіз існуючих загроз показав, що кіберзлочинці активно використовують фішингові атаки, злом облікових записів, атаки типу "людина посередині" та інші методи, спрямовані на компрометацію банківських даних користувачів. Для боротьби з цими викликами фінансові установи впроваджують багатофакторну автентифікацію, криптографічні механізми захисту та системи моніторингу аномальної активності.

Особливу роль у забезпеченні кібербезпеки відіграють інноваційні методи, зокрема застосування штучного інтелекту та машинного навчання для виявлення шахрайських операцій та несанкціонованого доступу. Алгоритми аналізу поведінки користувачів дозволяють визначати підозрілу активність у реальному часі, а автоматизовані системи кіберзахисту забезпечують оперативне реагування на потенційні загрози.

Таким чином, забезпечення безпеки в системах інтернет-банкінгу потребує комплексного підходу, що включає традиційні методи захисту, сучасні технології аналізу даних та використання штучного інтелекту. Подальші дослідження у цій сфері мають бути спрямовані на розробку нових підходів до автентифікації,

підвищення ефективності поведінкового аналізу та інтеграцію передових рішень у кібербезпеці банківських систем.

РОЗДІЛ 2
БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ З ПОВЕДІНКОВИМ АНАЛІЗОМ

2.1. Принципи багатофакторної автентифікації

Багатофакторна автентифікація (БФА) є одним із найефективніших механізмів захисту користувачів банківських систем від несанкціонованого доступу. Вона базується на використанні декількох рівнів перевірки особи, що значно ускладнює зловмисникам можливість отримання доступу до конфіденційних даних клієнтів.

Принципи багатофакторної автентифікації ґрунтуються на застосуванні кількох категорій факторів автентифікації:

Фактор знання – це інформація, яку знає тільки користувач. До цієї категорії належать паролі, PIN-коди, відповіді на секретні запитання.

Фактор володіння – це фізичний об’єкт, який є у розпорядженні користувача. Сюди входять мобільні пристрої, токени, смарт-картки або одноразові паролі (OTP), що надсилаються через SMS або мобільні додатки.

Фактор біометрії – унікальні фізичні характеристики користувача, такі як відбитки пальців, розпізнавання обличчя, сканування сітківки ока або голосова автентифікація.

Фактор поведінки – аналіз звичок користувача, таких як стиль друку на клавіатурі, швидкість введення пароля, траєкторія руху миші, спосіб утримання мобільного пристрою.

Фактор розташування – використання геолокаційних даних для перевірки автентичності користувача. Наприклад, вхід із незвичного місця може вимагати додаткової перевірки.

Ефективність БФА полягає в тому, що навіть якщо один із факторів буде скомпрометований (наприклад, зловмисник дізнається пароль), інші рівні захисту залишаються активними та не дозволяють отримати доступ до облікового запису [7].

Банківські системи активно впроваджують багатофакторну автентифікацію для захисту онлайн-транзакцій, входу в мобільний банкінг та інших фінансових

операцій. Одним із сучасних підходів є адаптивна автентифікація, яка аналізує ризики в режимі реального часу та змінює рівень перевірки залежно від ситуації [8]. Наприклад, якщо користувач входить із нового пристрою, система може вимагати додаткову біометричну автентифікацію.

Отже, багатофакторна автентифікація є ключовим елементом безпеки у банківській сфері, що забезпечує високий рівень захисту від кібератак та шахрайства, одночасно зберігаючи зручність користування для клієнтів.

2.2. Поведінковий аналіз як додатковий рівень захисту

Поведінковий аналіз є ефективним додатковим рівнем автентифікації, який підвищує рівень безпеки банківських систем. Його основна ідея полягає в тому, що кожен користувач має унікальні моделі поведінки при взаємодії з системами, і ці моделі можуть бути використані для ідентифікації та виявлення потенційних загроз .

Основними параметрами, що аналізуються в поведінковому аналізі, є:

Швидкість і ритм друку на клавіатурі – кожен користувач вводить текст із певним ритмом і швидкістю, що може бути унікальним для нього.

Рух миші або сенсорного екрана – система може аналізувати траєкторію руху курсора або жестів на сенсорному екрані.

Спосіб утримання пристрою – використання акселерометрів і гіроскопів у мобільних пристроях дозволяє визначити, як користувач тримає телефон під час введення даних .

Геолокаційні дані – якщо користувач намагається увійти з нетипового місця, система може активувати додаткові рівні перевірки .

Час активності – звичний час входу в систему може бути унікальним для кожного користувача.

Впровадження поведінкового аналізу дозволяє створити профіль користувача, що постійно оновлюється. Якщо система виявляє відхилення від звичних патернів, вона може автоматично заблокувати доступ або вимагати додаткової автентифікації (наприклад, через біометричні дані або підтвердження через інший пристрій).

Однією з ключових переваг поведінкового аналізу є його непомітність для користувача. На відміну від традиційних методів багатофакторної автентифікації, які можуть вимагати додаткових дій (введення коду, сканування відбитку пальця), поведінковий аналіз працює у фоновому режимі та не впливає на користувацький досвід .

Банківські установи активно інтегрують поведінковий аналіз у свої системи безпеки, використовуючи штучний інтелект і машинне навчання для обробки великих обсягів даних у реальному часі. Це дозволяє ефективно виявляти шахрайські дії, такі як викрадення облікового запису або автоматизовані атаки ботів.

Отже, поведінковий аналіз є потужним інструментом кібербезпеки, що дозволяє підвищити рівень захисту банківських систем без шкоди для зручності користувачів. Його інтеграція у багатофакторну автентифікацію дозволяє забезпечити адаптивний підхід до ідентифікації користувачів та ефективне виявлення потенційних загроз.

2.3. Впровадження аналізу місцезнаходження, швидкості введення пароля та пристрою

Впровадження аналізу місцезнаходження, швидкості введення пароля та пристрою є одним із ключових аспектів підвищення рівня безпеки у системах інтернет-банкінгу. Використання цих параметрів дозволяє ідентифікувати аномальну поведінку користувача та запобігати шахрайству на ранніх етапах.

Геолокація є одним із ефективних методів додаткової перевірки користувача. Вона може використовувати:

IP-адресу для визначення регіону, з якого здійснюється вхід у систему.

GPS-координати у мобільних пристроях для точнішого аналізу місцезнаходження.

Wi-Fi та стільникові мережі для отримання географічної прив’язки користувача.

Якщо спроба входу здійснюється з незвичного місця (наприклад, з іншої країни чи міста), система може вимагати додаткової автентифікації або заблокувати сесію до підтвердження особи.

Кожен користувач має унікальну манеру введення тексту, включаючи швидкість набору пароля та паузи між натисканнями клавіш. Впровадження аналізу швидкості введення пароля передбачає:

- Вимірювання середньої швидкості введення та порівняння з історичними даними користувача.
- Аналіз часу між натисканнями клавіш.
- Виявлення нетипових або механічних послідовностей введення, які можуть свідчити про використання ботів чи зловмисників.
- Якщо система фіксує значні відхилення від звичайної швидкості введення пароля, вона може запустити додаткові механізми перевірки, такі як запит на біометричну автентифікацію або одноразовий код підтвердження.

Ідентифікація пристрою, з якого користувач здійснює доступ, є важливим аспектом безпеки. Вона включає:

Аналіз унікальних характеристик пристрою (модель, операційна система, версія браузера, розширення тощо).

Використання цифрових відбитків пристрою (device fingerprinting) для розпізнавання незнайомих пристроїв.

Виявлення змін у конфігурації системи, які можуть вказувати на компрометацію або використання емуляторів.

Якщо користувач входить з нового або підозрілого пристрою, система може вимагати додаткової перевірки, наприклад, через підтвердження в мобільному додатку або SMS-код.

Застосування аналізу місцезнаходження, швидкості введення пароля та пристрою дозволяє суттєво підвищити рівень безпеки інтернет-банкінгу. Впровадження цих механізмів у комплексній системі автентифікації допомагає своєчасно виявляти підозрілі дії, зменшувати ризики шахрайства та забезпечувати більш адаптивний захист користувачів без надмірного ускладнення процесу входу.

2.4. Оцінка ефективності поведінкової автентифікації

Оцінка ефективності поведінкової автентифікації є важливим етапом впровадження цієї технології в банківські системи. Вона дозволяє визначити рівень надійності та точності методу, а також оцінити його вплив на безпеку та зручність користувачів.

Критерії оцінки ефективності

Для аналізу ефективності поведінкової автентифікації використовують такі ключові показники:

Точність ідентифікації (Accuracy) – відсоток коректно ідентифікованих користувачів.

Рівень помилкових спрацьовувань (False Positive Rate, FPR) – частка випадків, коли система помилково блокує легітимного користувача.

Рівень помилкового пропуску (False Negative Rate, FNR) – частка випадків, коли система не розпізнає зловмисника.

Час реагування системи – швидкість аналізу поведінкових параметрів та ухвалення рішення.

Адаптивність – здатність системи коригувати моделі поведінки у відповідь на зміни в звичках користувачів.

Методи тестування та верифікації

Оцінка ефективності поведінкової автентифікації здійснюється шляхом проведення експериментальних досліджень та тестування на реальних даних. Основні методи включають:

Лабораторне тестування – перевірка системи на обмеженій вибірці користувачів у контрольованих умовах.

Польові випробування – аналіз роботи системи в реальних умовах експлуатації банківських платформ.

Аналіз історичних даних – використання раніше зібраних даних для тренування та перевірки моделей машинного навчання.

Вплив на користувацький досвід

Однією з важливих характеристик поведінкової автентифікації є її невидимість для користувача, що покращує загальний досвід взаємодії з банківськими сервісами. Разом із цим необхідно мінімізувати кількість помилкових блокувань та запитів на додаткову верифікацію, щоб не викликати незручностей у клієнтів.

Оцінка ефективності поведінкової автентифікації дозволяє визначити оптимальні параметри роботи системи та підвищити її надійність. Завдяки аналізу ключових показників та впровадженню адаптивних алгоритмів можна досягти високого рівня безпеки без суттєвого впливу на зручність користувачів.

Висновки до розділу 2

У другому розділі було розглянуто основні принципи багатофакторної автентифікації та впровадження поведінкового аналізу як додаткового рівня безпеки в системах інтернет-банкінгу. Проаналізовано ефективність використання таких параметрів, як місцезнаходження, швидкість введення пароля та ідентифікація пристрою для підвищення рівня захисту користувачів.

Здійснено оцінку переваг поведінкової автентифікації, зокрема її високої точності та невидимості для користувача, що сприяє збереженню зручності при взаємодії з банківськими сервісами. Крім того, визначено критерії оцінки ефективності даного підходу та методи тестування його працездатності.

Таким чином, застосування багатофакторної автентифікації у поєднанні з поведінковим аналізом є перспективним напрямом розвитку безпекових механізмів інтернет-банкінгу. Впровадження таких методів дозволяє суттєво знизити ризик несанкціонованого доступу та покращити захист персональних даних користувачів.

РОЗДІЛ 3
ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ОСНОВИ ДОСЛІДЖУВАНОЇ ЗАДАЧІ

3.1 Аналіз предметної області і виявлення наявних проблем та завдань

Системи інтернет-банкінгу є однією з найбільш динамічно розвинутих технологій, що надають клієнтам банків доступ до фінансових операцій у режимі реального часу. Збільшення кількості користувачів та розвиток технологій водночас створюють нові загрози, пов’язані з кібербезпекою. Тому забезпечення надійної автентифікації користувачів та захисту даних є критично важливим завданням у банківській сфері [28, 29].

Системи інтернет-банкінгу працюють на основі централізованих платформ, що забезпечують обробку платежів, перевірку транзакцій та ідентифікацію користувачів. Основні функції таких систем включають автентифікацію та авторизацію користувачів, управління рахунками, здійснення платежів і грошових переказів, надання фінансової аналітики, інтеграцію з іншими банківськими сервісами та мобільними застосунками [30]. Незважаючи на високий рівень розвитку таких систем, існує низка проблем, що потребують вирішення.

Однією з основних проблем є недостатня ефективність традиційних методів автентифікації. Застосування статичних паролів, одноразових кодів та SMS-підтвердження має низку обмежень. Фішингові атаки, витоки баз даних та зловмисне використання персональних даних роблять ці методи вразливими до атак з боку кіберзлочинців [31]. Також спостерігається зростання кількості кібератак, серед яких атаки на основі соціальної інженерії, шкідливе програмне забезпечення та атаки «людина посередині» (MITM), що ускладнюють процес забезпечення безпеки фінансових операцій [32].

Традиційні механізми безпеки мають низьку адаптивність, оскільки вони не враховують поведінкові фактори користувачів. Це унеможливлює ефективне виявлення підозрілих дій у режимі реального часу. Ще однією проблемою є

компроміс між безпекою та зручністю користувачів. Жорсткі заходи безпеки, такі як багаторівнева автентифікація, можуть створювати додаткові труднощі для легітимних користувачів. Знайдення балансу між зручністю та захищеністю є ключовим викликом у розробці сучасних банківських систем [33, 34].

З розвитком технологій штучного інтелекту та машинного навчання з'явилася можливість інтеграції інноваційних підходів до захисту банківських систем. Поведінковий аналіз користувачів дозволяє виявляти нетипові дії в режимі реального часу, використовуючи алгоритми аналізу великих обсягів даних. Аналіз місцезнаходження, швидкості введення даних, пристрою, з якого здійснюється вхід, а також інших характеристик може підвищити рівень безпеки без необхідності постійного підтвердження особи [35].

Враховуючи виявлені проблеми, основними завданнями дослідження є аналіз існуючих методів автентифікації та їх ефективності з метою виявлення основних недоліків та перспектив удосконалення, розробка моделі автентифікації на основі поведінкового аналізу, яка буде враховувати параметри взаємодії користувача із системою, такі як місцезнаходження, швидкість введення даних та використаний пристрій, розробка підходу до інтеграції поведінкової автентифікації у сучасні банківські платформи та оцінка її впливу на безпеку фінансових операцій, а також експериментальна перевірка розробленого підходу та оцінка його ефективності порівняно з традиційними методами захисту. Таким чином, дослідження спрямоване на вдосконалення існуючих методів автентифікації у системах інтернет-банкінгу шляхом застосування сучасних технологій поведінкового аналізу та машинного навчання.

3.2 Порівняльний аналіз переваг та недоліків існуючих рішень

Забезпечення інформаційної безпеки в системах інтернет-банкінгу базується на використанні різних методів автентифікації та засобів кіберзахисту. У цьому підрозділі буде проведено порівняльний аналіз основних існуючих рішень з

урахуванням їхніх переваг і недоліків. Нижче була наведена порівняльна таблиця різних методів автентифікації та засобів кіберзахисту.

Таблиця 3.1

Порівняльна таблиця використанні різних методів автентифікації та засобів кіберзахисту.

Існуюче рішення	Переваги	Недоілки
1. Парольна автентифікація	Простота реалізації та використання. Низькі витрати на впровадження. Широке поширення та сумісність з різними платформами.	Висока ймовірність компрометації через фішинг, атаки перебором та перехоплення. Користувачі часто використовують слабкі паролі або повторюють їх для кількох сервісів. Відсутність додаткового рівня безпеки у випадку крадіжки пароля.
2. Одноразові паролі (OTP) через SMS або додатки	Підвищена безпека у порівнянні з традиційними паролями. Використання тимчасових кодів, що ускладнює компрометацію. Простота інтеграції з існуючими системами.	Можливість атак із підміною SIM-карти (SIM swapping). Залежність від мобільної мережі (у разі використання SMS-OTP). Додаткові незручності для користувачів.

Продовження таблиці 3.1

3. Біометрична автентифікація (відбитки пальців, розпізнавання обличчя, голосова ідентифікація)	Високий рівень безпеки завдяки унікальності біометричних даних. Зручність використання (користувачеві не потрібно запам'ятовувати паролі). Неможливість викрадення або копіювання у традиційному сенсі.	Можливі помилки розпізнавання. Висока вартість впровадження. Ймовірність компрометації біометричних даних у разі злому бази даних.
4. Апаратні токени (USB-токени, смарт-картки)	Висока стійкість до атак фішингу та перехоплення. Можливість використання для багатофакторної автентифікації. Довговічність і надійність.	Висока вартість виробництва та обслуговування. Ризик втрати або крадіжки токена. Необхідність додаткового обладнання.
5.Поведінковий аналіз та штучний інтелект	Автоматичне виявлення підозрілих дій. Мінімальна взаємодія з користувачем. Можливість адаптації та навчання системи на основі поведінкових шаблонів.	Високі вимоги до обчислювальних ресурсів. Ймовірність помилкових позитивних або негативних спрацьовувань. Необхідність збору великого обсягу даних для ефективної роботи.

Різні методи автентифікації мають свої сильні та слабкі сторони. Використання лише одного методу не забезпечує повний захист від сучасних загроз. Найбільш ефективними рішеннями є комплексний підхід, який включає багатофакторну

автентифікацію, поведінковий аналіз та використання штучного інтелекту. Саме поєднання цих технологій дозволяє досягти оптимального рівня безпеки без значного погіршення користувацького досвіду.

З метою оцінки ефективності різних методів автентифікації в інтернет-банкінгу було проведено порівняльний аналіз сучасних рішень, що використовуються провідними фінансовими установами. Основними критеріями оцінки стали рівень безпеки, зручність використання для клієнтів, стійкість до кібератак та можливість впровадження додаткових заходів безпеки.

Нижче представлена таблиця 3.2, у якій наведено порівняння методів автентифікації в різних системах інтернет-банкінгу, а також їхні переваги та недоліки.

Таблиця 3.2

Порівняння методів автентифікації в різних системах інтернет-банкінгу

Банк /Система	Методи автентифікації	Поведінковий аналіз	Двофакторна автентифікація (2FA)	Біометрія	Захист від фішингу	Додаткові заходи безпеки
Privat24 (ПриватБанк)	Пароль + SMS-код / push-повідомлення	Ні	Так	Так (Face ID, Touch ID)	Так (антифішинг-захист)	Динамічні ліміти, перевірка підозрілих транзакцій

Продовження таблиці 3.2

Monobank	Пароль + OTP	Частково (геолокація, пристрій)	Так	Так	Так	Обмеження операцій при зміні пристрою
Revolut	Пароль + push-код	Так	Так	Так	Так	Штучний інтелект для моніторингу шахрайських дій
Wise	Пароль + SMS / push-код	Ні	Так	Так	Так	Додаткове підтвердження великих транзакцій
Raiffeisen Online	Пароль + OTP	Ні	Так	Ні	Так	Адаптивна автентифікація на основі ризиків
			Так	Так	Так	Моніторинг транзакцій в реальному часі

Bank of America	Пароль + SMS-код	Так (обмежено)				

Аналіз свідчить, що традиційні методи автентифікації, такі як паролі та одноразові коди, залишаються найбільш поширеними, проте мають суттєві вразливості. Використання біометричних даних та поведінкового аналізу дозволяє значно підвищити рівень безпеки, зменшуючи ризики, пов’язані з крадіжкою облікових даних та фішинговими атаками. Однак їх впровадження потребує значних ресурсів та відповідного технологічного забезпечення.

Подальший розвиток технологій, зокрема застосування штучного інтелекту для аналізу поведінкових факторів, може суттєво підвищити ефективність автентифікації та забезпечити адаптивний захист банківських систем у реальному часі.

3.3 Формування практичних рекомендацій

Багаторівнева перевірка автентифікації

Поєднання класичних методів (пароль, одноразові коди) з сучасними (біометрія, поведінковий аналіз).

Використання адаптивної автентифікації, яка змінює рівень перевірки в залежності від ризику.

Поведінковий аналіз для підвищення рівня довіри

Врахування особливостей користувацької поведінки (швидкість введення пароля, розклад активності, способи взаємодії з пристроєм).

Виявлення аномальних патернів поведінки, які можуть сигналізувати про компрометацію акаунта.

Географічна та пристрійна аналітика

Аналіз змін місцезнаходження та спроб входу з невідомих пристроїв.

Автоматичне блокування входу з країн або регіонів, які не відповідають типовій активності користувача.

Використання алгоритмів машинного навчання

Моделювання та навчання системи на історичних даних користувача для точнішого визначення ризикових входів.

Впровадження динамічного визначення рівня загрози на основі сукупності факторів.

Розглянуті сценарії впровадження

При розробці комбінованої системи були розглянуті наступні сценарії її використання в реальних умовах:

Мобільний банкінг

Автоматичне оцінювання ризиків під час входу та проведення операцій (наприклад, якщо користувач входить з нового пристрою або незвичної локації, система вимагає додаткову автентифікацію).

Інтеграція з сенсорами смартфона для визначення біометричних та поведінкових характеристик.

Веб-банкінг

Використання багатоетапної автентифікації з поведінковим аналізом перед проведенням фінансових операцій.

Динамічне регулювання рівня перевірки (наприклад, якщо система визначає низький ризик, то OTP може не вимагатися).

Доступ з громадських та незнайомих пристроїв

Запровадження більш жорстких заходів контролю, наприклад, автоматичне відхилення входу або вимога додаткової перевірки.

Використання унікальних апаратних ідентифікаторів пристрою для перевірки легітимності користувача.

Для кращої наочності процесу багатофакторної автентифікації була розроблена блок-схема Рис. 3.1, що демонструє послідовність перевірок користувача під час входу. Вона відображає ключові етапи: введення облікових даних, проходження OTP-перевірки, аналіз поведінкових особливостей, перевірка FingerPrint та оцінку

ризику за допомогою алгоритмів машинного навчання. В залежності від рівня виявленої загрози система або надає доступ, або відхиляє запит на вхід.

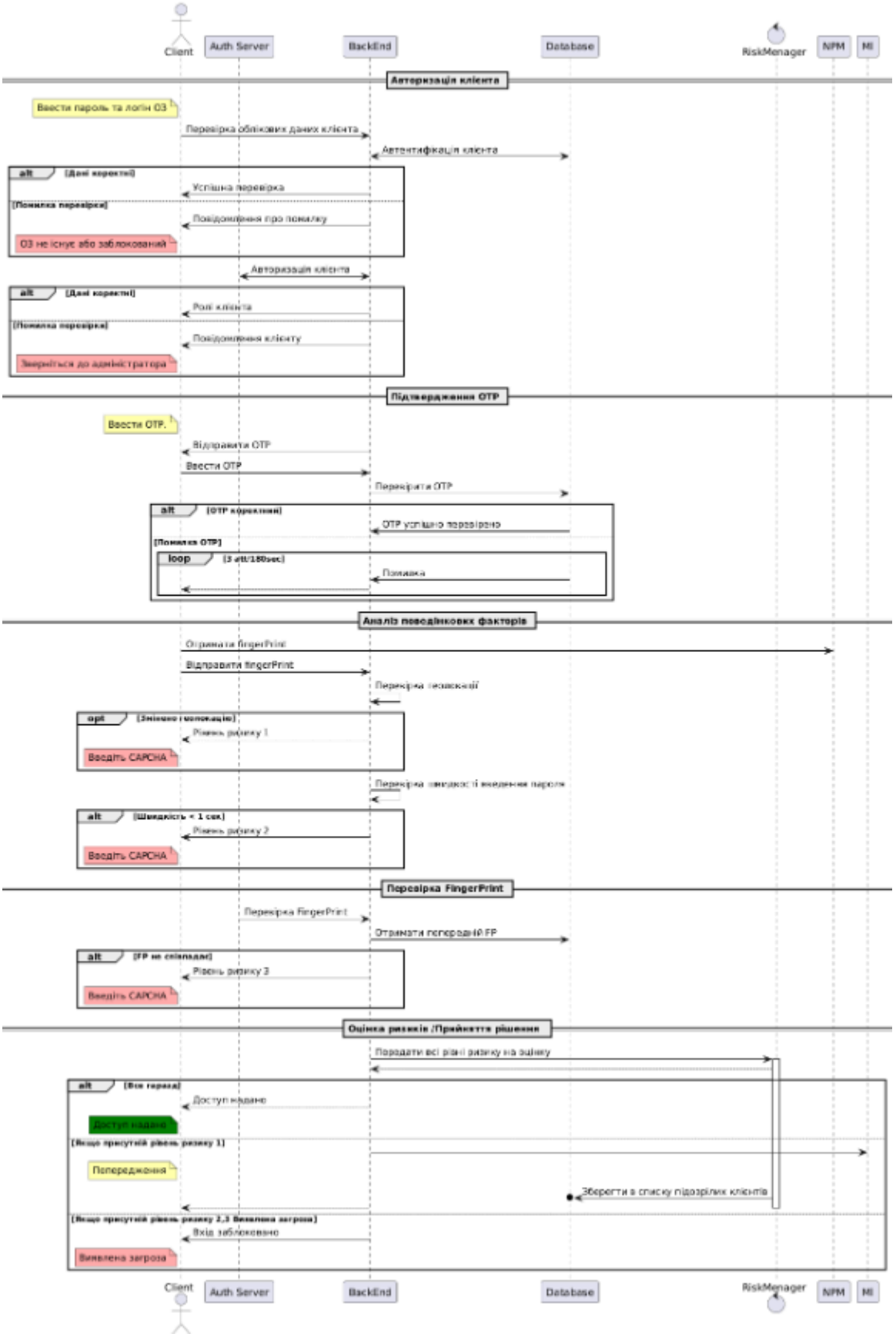

Рисунок 3.1 - Послідовність перевірок користувача

Одним із ключових аспектів захисту інтернет-банкінгу є вибір ефективного методу автентифікації користувачів. Існуючі підходи мають різний рівень надійності, що залежить від їхньої стійкості до атак, зручності використання та можливості інтеграції з додатковими механізмами безпеки.

На діаграмі (Рис. 3.6) нижче представлено порівняння різних методів автентифікації за рівнем їхньої безпеки. Вона відображає ефективність традиційних (парольні системи, одноразові коди) та сучасних (біометрія, поведінковий аналіз) підходів, а також їхню вразливість до різних кіберзагроз.

Це порівняння дає змогу візуально оцінити, які методи забезпечують найвищий рівень захисту та які можуть бути найкращими кандидатами для інтеграції у комплексну систему безпеки інтернет-банкінгу.

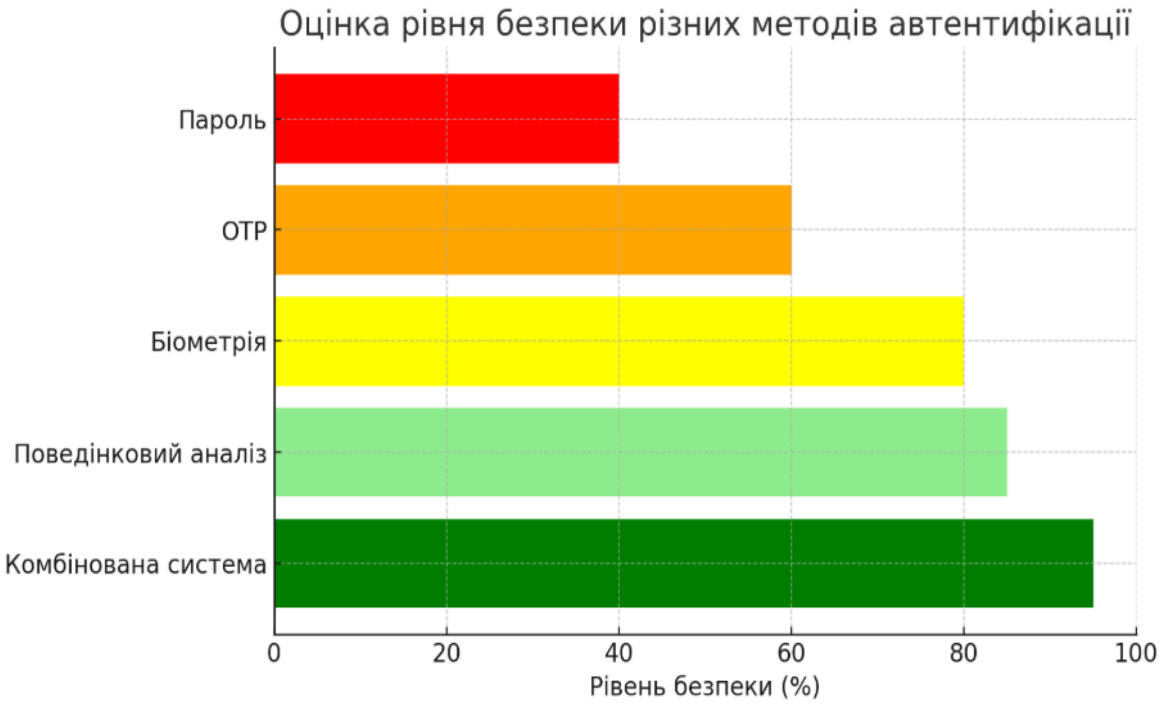

Рисунок 3.2 Рівень безпеки різних методів автентифікації

Оцінка ефективності розробленого підходу здійснювалася шляхом моделювання типових загроз, таких як несанкціонований вхід з нового пристрою або зміна географічного положення користувача. Дослідження показало, що

запропонована система дозволяє суттєво знизити ризики компрометації облікових записів, підвищуючи загальний рівень безпеки інтернет-банкінгу.

Висновки до розділу 3

У третьому розділі роботи було розглянуто теоретичні та практичні основи розробки та впровадження комбінованої системи автентифікації для інтернет-банкінгу. Проведений аналіз предметної області дозволив визначити ключові проблеми сучасних методів захисту, серед яких недостатня стійкість до кібератак, фішингових схем та компрометації паролів.

Порівняльний аналіз існуючих рішень показав, що традиційні методи автентифікації, такі як паролі та одноразові коди, не можуть забезпечити належний рівень безпеки в умовах зростаючої кількості загроз. У зв’язку з цим перспективним напрямком є інтеграція багатофакторної автентифікації з поведінковим аналізом та алгоритмами машинного навчання.

У межах виконання індивідуального завдання було розроблено концепцію системи автентифікації, що поєднує різні рівні перевірки користувача: традиційні методи, поведінкові фактори (геолокація, швидкість введення пароля, особливості використання пристрою) та машинне навчання для оцінки ризиків. Було здійснено моделювання можливих сценаріїв використання цієї системи та оцінено її ефективність.

Результати дослідження підтверджують доцільність використання запропонованого підходу для підвищення рівня інформаційної безпеки банківських систем. Запропонована архітектура автентифікації може бути впроваджена у сучасні банківські системи з метою мінімізації ризиків шахрайства та несанкціонованого доступу. Перспективи подальшого розвитку даного напрямку включають вдосконалення моделей поведінкового аналізу, використання біометричних методів та покращення механізмів виявлення аномалій у діях користувачів.

РОЗДІЛ 4
РОЗРОБКА МЕТОДУ МІКРОСЕГМЕНТОВАНОЇ ДИНАМІЧНОЇ ІЗОЛЯЦІЇ СЕСІЙ В ІНТЕРНЕТ-БАНКІНГУ ЯК ІННОВАЦІЙНОГО ПІДХОДУ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Постановка задачі мікросегментованого захисту сесій

Зважаючи на актуальні виклики в забезпеченні інформаційної безпеки інтернет-банкінгу, запропоновано інноваційний метод мікросегментованої динамічної ізоляції сесій (Microsegmented Dynamic Isolation of Sessions, MiDIS). Цей підхід ґрунтується на розподілі сесії користувача на логічно ізольовані підсесії — мікросегменти, кожен з яких відповідає окремому типу дій або функціональних можливостей користувача в системі (наприклад: перегляд балансу, переказ коштів, зміна налаштувань тощо).

На відміну від традиційних методів контролю доступу, де користувач отримує повний доступ до всіх функцій після автентифікації, MiDIS забезпечує незалежний моніторинг, аналіз ризиків і контроль доступу до кожного сегменту сесії окремо. Це дозволяє ізолювати потенційно небезпечні дії без повного припинення роботи сесії, що знижує ризики, зберігаючи при цьому зручність використання сервісу.

На рис. 4.1 представлено діаграму активності, яка демонструє логіку роботи методу.

(тут можна вставити або посилатися на створену вами UML-діаграму)

Опис етапів:

1. Ініціалізація сесії користувача. Після успішної автентифікації, система ініціює сесію та виконує її логічне розбиття на мікросегменти.

2. Формування мікросегментів. Наприклад:

- Сегмент 1: Перевірка балансу
- Сегмент 2: Переказ коштів
- Сегмент 3: Зміна налаштувань
- Сегмент 4: Завантаження виписок тощо.

2. Моніторинг дій у кожному сегменті. До кожного з мікросегментів застосовується індивідуальний механізм моніторингу, що базується на:
    - поведінковому аналізі;
    - профілю користувача;
    - типових шаблонах активності;
    - біометричних та часових параметрах.

4. Аналіз ризиків і виявлення аномалій. Якщо зафіксовано підозрілу активність у будь-якому сегменті, система автоматично переходить до фази обробки загрози.

5. Локальна реакція на загрозу:
    - Блокування лише проблемного сегменту;
    - Запит повторної автентифікації;
    - Повідомлення служби безпеки.

6. Оцінка результату. У разі підтвердження особи — користувач повертається до виконання дії. У разі невдачі — сегмент блокується, але інші залишаються активними.

7. Завершення сесії. По завершенні роботи користувача відбувається деактивація мікросегментів та збереження журналу дій для подальшого аналізу.

Впровадження методу MiDIS дозволяє:
- зменшити масштаб впливу потенційної атаки;
- абезпечити гнучку модель доступу в реальному часі;
- мінімізувати незручності для користувача;
- інтегрувати засоби ІІ та поведінкової аналітики.

Метод мікросегментованої динамічної ізоляції сесій є ефективним інноваційним інструментом для запобігання загрозам під час активної сесії в інтернет-банкінгу. Його адаптивність, модульність і реакція на ризики відповідають сучасним вимогам до систем ІБ.

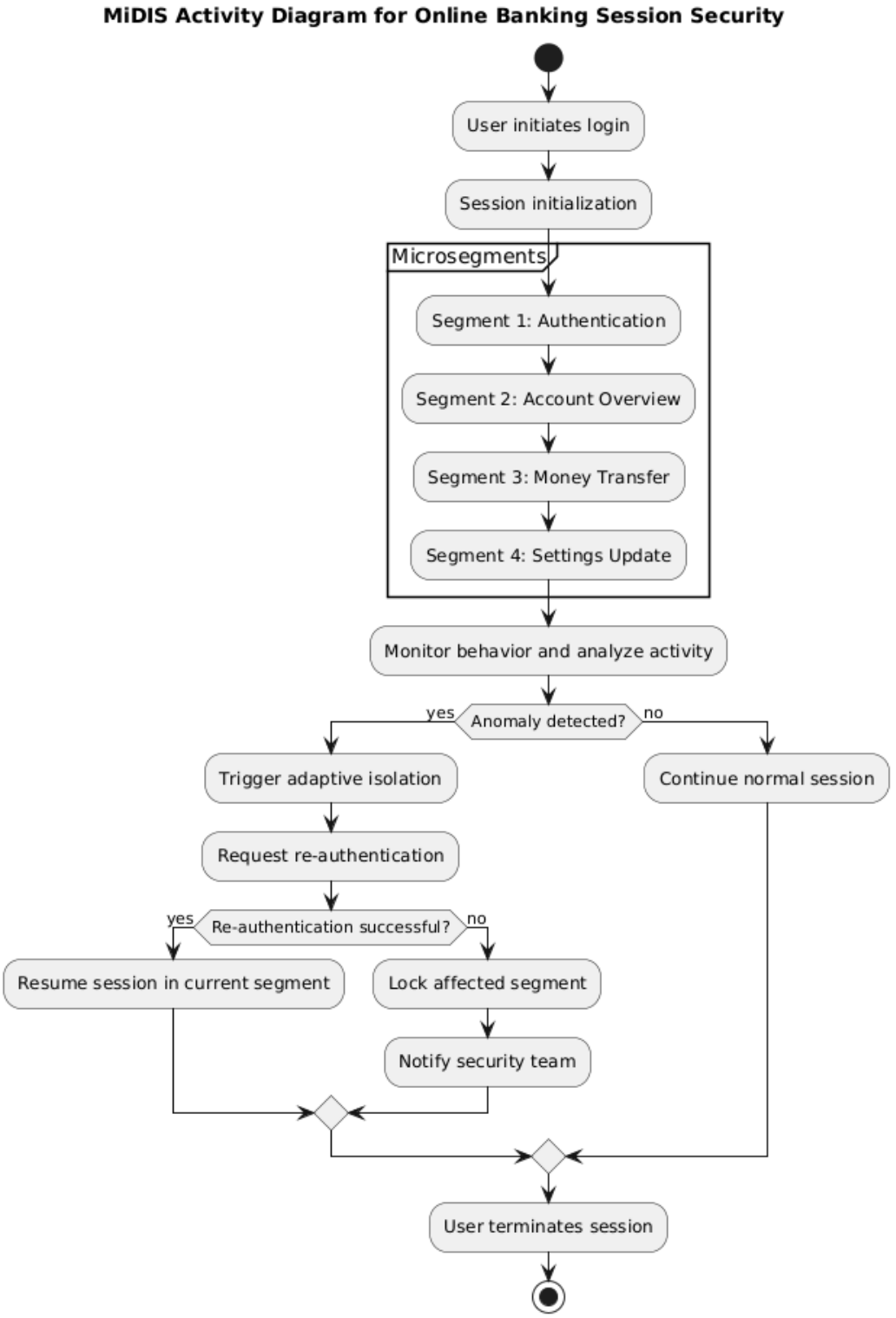

Рисунок 4.1 Загальна логіка функціонування MiDIS

4.2 Переваги запропонованого методу

У сучасних умовах підвищених вимог до кібербезпеки та зручності користувача критично важливою є розробка інноваційних підходів до забезпечення інформаційної безпеки в інтернет-банкінгу. Запропонований метод MiDIS поєднує в собі концепції мікросегментації, динамічного управління доступом та інтелектуального аналізу поведінки, що забезпечує низку унікальних переваг. Розглянемо ключові з них.

Однією з найвагоміших переваг MiDIS є здатність до локалізації загроз у межах окремих сегментів користувацької сесії. На відміну від традиційних систем безпеки, які зупиняють або завершують всю сесію при виявленні підозрілої активності, MiDIS здійснює селективну ізоляцію лише проблемного сегменту. Це дозволяє підтримувати безперервність обслуговування, знижуючи ризик втрати незбережених даних або переривання критичних операцій.

MiDIS використовує засоби штучного інтелекту для аналізу поведінки користувача в реальному часі, що забезпечує динамічну оцінку ризиків. Система формує поведінковий профіль кожного користувача та порівнює поточні дії з еталонною моделлю. У разі виявлення аномалій (наприклад, незвичний час доступу, нове місце входу або нестандартна навігація) система ініціює захисну реакцію. Такий підхід забезпечує високу чутливість до потенційних загроз при мінімальній кількості хибнопозитивних спрацювань.

Завдяки мікросегментації сесій, MiDIS дозволяє налаштовувати індивідуальні політики доступу для кожного сегменту, що підвищує гнучкість у реалізації політик безпеки. Наприклад, можна застосувати суворіші правила для проведення фінансових операцій (із обов’язковою двофакторною автентифікацією) та ліберальніші – для перегляду інформації про баланс чи історію транзакцій. Це забезпечує баланс між безпекою та зручністю, що є важливою вимогою сучасних банківських систем.

Використання MiDIS дозволяє зменшити негативний вплив заходів безпеки на досвід користувача. Оскільки ізоляція здійснюється лише в межах потенційно

небезпечного сегменту, користувач не втрачає доступ до всієї сесії. Після усунення ризику або проходження додаткової перевірки система автоматично відновлює повний доступ, не вимагаючи повторного входу або втручання оператора служби підтримки.

Інтеграція MiDIS у банківське середовище забезпечує багаторівневу захищеність. Навіть у разі часткового компрометування сесії, зловмисник отримає доступ лише до окремого сегменту, який негайно буде ізольовано. Такий підхід суттєво зменшує поверхню атаки та унеможливлює повну компрометацію системи. У поєднанні з поведінковим аналізом, MiDIS формує адаптивне середовище, здатне ефективно протистояти складним і новітнім загрозам.

Таблиця 4.1

Переваги запропонованого методу

Перевага	Пояснення
Локалізація загроз	Атака блокує лише окрему дію, а не всю сесію
AI-аналіз у реальному часі	Система постійно адаптується до поведінки
Гнучкість доступу	Можна застосовувати різні правила до різних сегментів
Менше незручностей для користувача	Автоматичне відновлення, без втрати всієї сесії
Вища загальна безпека	Розширене реагування без «жорсткого» відключення

4.3 Архітектура мікросегментованої динамічної ізоляції сесій (MiDIS)

Архітектура MiDIS (Microsegmented Dynamic Isolation of Sessions) побудована на основі принципу поділу сесії на ізольовані сегменти з автономними політиками безпеки. Це дозволяє більш гнучко керувати рівнем доступу до окремих дій, виявляти загрози на ранніх етапах та забезпечувати автоматичну реакцію без переривання всієї сесії.

На відміну від традиційних підходів, де обробка сесії є монолітною, MiDIS ділить взаємодію користувача з системою на окремі логічні блоки (сегменти), які контролюються незалежно один від одного. Це не лише підвищує стійкість до атак, але й забезпечує безперервність обслуговування при виникненні локальних загроз.

Основні компоненти архітектури MiDIS:

User Client Interface (UCI):

Інтерфейс користувача, через який ініціюються сесії або окремі транзакції. Відповідає за зручність та безпечну взаємодію клієнта з банківською системою.

Session Orchestrator (SO):

Центральний координатор, який створює сесії, динамічно розбиває їх на сегменти відповідно до поточних дій користувача та координує взаємодію між іншими компонентами.

Policy Engine (PE):

Генерує політики безпеки для кожного сесійного сегмента з урахуванням поточного контексту — місцезнаходження користувача, пристрою, часу доби, рівня ризику та історії дій.

Behavioral AI Engine (AI):

Аналізує поведінкові шаблони користувача в режимі реального часу. При виявленні аномалій або потенційної загрози генерує відповідні сигнали до Policy Engine для корекції політики доступу.

Access Control Gateway (ACG):

Фізично або логічно ізольований шлюз, який забезпечує контроль доступу до кожного сесійного сегмента. Застосовує правила, надані Policy Engine, для забезпечення гнучкого, контекстно-залежного захисту.

Segment Sandbox (SS):

Безпечне ізольоване середовище, у якому виконуються окремі дії користувача (наприклад, перегляд балансу, здійснення переказу, зміна налаштувань). У випадку компрометації сегмента, його можна ізолювати без впливу на інші частини сесії.

Audit & Logging Module (LOG):

Веде повну історію подій, рішень щодо безпеки, змін політик та зафіксованих аномалій. Сприяє виявленню довготривалих атак та проведенню пост-фактум аналізу безпеки.

Ця архітектура сприяє досягненню балансу між високим рівнем безпеки та комфортом для кінцевого користувача. Завдяки локалізації ризиків, MiDIS дозволяє забезпечити надійний захист без тотального відключення користувача від сервісу, що є критично важливим у фінансовому секторі.

Нижче наведено схематичне зображення архітектури MiDIS Рис.4.2:

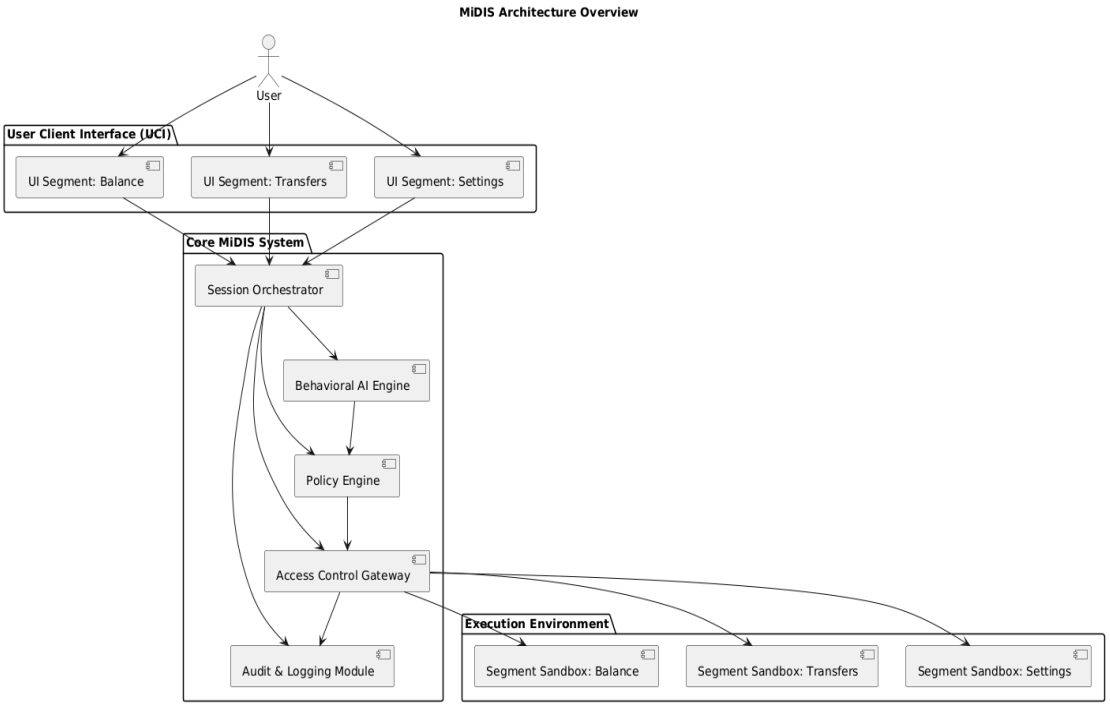

Рис. 4.2 Архітектура MiDIS

Крім того, архітектура MiDIS є масштабованою та гнучкою, що дозволяє інтегрувати її у вже існуючі банківські інформаційні системи без суттєвих змін у їх структурі. Система підтримує адаптацію до змін поведінкових моделей користувачів та еволюції кіберзагроз, що робить її придатною для довготривалого використання в умовах динамічного середовища.

Запропонований підхід відкриває нові перспективи у сфері інформаційної безпеки, оскільки дозволяє реалізувати захист не тільки на рівні доступу до

системи, а й на рівні окремих транзакцій. Таким чином, MiDIS формує нову парадигму безпеки — від реактивної до проактивної, де загрози виявляються та нейтралізуються ще до моменту нанесення шкоди.

Ця архітектура сприяє досягненню балансу між високим рівнем безпеки та комфортом для кінцевого користувача. Завдяки локалізації ризиків, MiDIS дозволяє забезпечити надійний захист без тотального відключення користувача від сервісу, що є критично важливим у фінансовому секторі.

Ключовою особливістю архітектури є її динамічність — система постійно адаптується до поведінки користувача, зберігаючи контекст та історію взаємодій у режимі реального часу. Завдяки цьому можлива оперативна реакція на аномалії, зокрема тимчасове блокування лише небезпечного сегмента або вимога додаткової автентифікації для продовження дії.

Крім того, MiDIS дозволяє інтегруватися з іншими системами моніторингу подій безпеки (SIEM), централізованого управління політиками доступу та ризик-менеджменту. Це забезпечує комплексний підхід до захисту цифрових фінансових сервісів, підвищуючи їхню стійкість до сучасних кібератак, зокрема фішингу, маніпуляцій сесіями та компрометації облікових даних.

Таким чином, архітектура MiDIS поєднує в собі інноваційність, масштабованість і практичну ефективність, що робить її перспективним рішенням у сфері інформаційної безпеки інтернет-банкінгу.

4.4 Алгоритм роботи та модулі системи

Алгоритм роботи системи MiDIS базується на динамічному розбитті користувацької сесії на незалежні сегменти з подальшим застосуванням контекстно-залежних політик доступу та поведінкового аналізу в реальному часі. Такий підхід дозволяє забезпечити локалізований контроль доступу, уникати повного завершення сесії при виявленні загроз, а також адаптувати рівень захисту відповідно до активності користувача.

Процес ініціації сесії є відправною точкою функціонування системи MiDIS і відіграє вирішальну роль у забезпеченні автентичності користувача, а також формуванні контексту для подальшої сегментації дій. Користувач починає взаємодію з системою через клієнтський інтерфейс (User Client Interface, UCI), з якого надходить запит на встановлення сесії. На цьому етапі система фіксує технічні характеристики: тип пристрою, IP-адресу, геолокацію, операційну систему, браузер, мову інтерфейсу, що дає змогу сформувати початковий поведінковий профіль.

Далі відбувається первинна автентифікація користувача. Залежно від політик безпеки банку, вона може включати введення логіну і пароля, двофакторну автентифікацію або біометричну перевірку. Усі отримані дані передаються до модуля Behavioral AI Engine, який проводить миттєвий аналіз контексту на основі історичних шаблонів користувача. Паралельно Policy Engine формує попередній ризиковий профіль, що дозволяє системі оцінити ймовірність несанкціонованого доступу.

У разі виявлення відхилень від типових параметрів — наприклад, новий пристрій, незвична локація або аномальний час входу — система може автоматично підвищити рівень контролю, ініціювавши додаткову автентифікацію або тимчасове обмеження прав. Якщо рівень ризику оцінюється як критичний, ініціація сесії блокується з одночасною реєстрацією інциденту в модулі Audit & Logging.

Після успішного проходження етапів автентифікації та оцінки ризику, Session Orchestrator створює логічну сесію з унікальним ідентифікатором, ініціює її сегментацію та передає контроль Access Control Gateway для подальшого управління доступом на рівні дій. Таким чином, ініціація сесії не лише виконує функцію входу в систему, а й закладає основу динамічної ізоляції майбутніх активностей користувача.

Первинна автентифікація в архітектурі MiDIS виконує ключову функцію перевірки справжності користувача перед наданням доступу до сегментованої сесії. Її мета — підтвердити, що запит на вхід надходить від легітимного суб’єкта, і водночас зібрати контекстуальні дані для подальшого аналізу. На цьому етапі користувач вводить облікові дані, які можуть включати комбінацію імені

користувача, пароля, одноразового коду з мобільного застосунку, а також біометричних параметрів, таких як розпізнавання обличчя або відбитка пальця.

Усі вхідні дані передаються до Behavioral AI Engine, який порівнює поточні параметри входу з історичними шаблонами поведінки конкретного користувача. До таких параметрів належать: часові рамки активності, географічне розташування, швидкість введення пароля, характер кліків миші, послідовність навігації та інші поведінкові характеристики. На підставі цієї інформації система розраховує ризиковий індекс, який передається до Policy Engine для прийняття рішення щодо надання доступу або посилення автентифікаційної процедури.

Якщо виявлено суттєві розбіжності з типовим поведінковим профілем користувача — наприклад, спроба входу з іншої країни, незвичний пристрій або підозріло швидка взаємодія з інтерфейсом — система може застосувати механізми багатоетапної перевірки. Це може включати підтвердження через окремий канал (наприклад, push-повідомлення в мобільному додатку або телефонний дзвінок), перевірку геолокації або повторну біометричну автентифікацію.

Якщо індекс ризику не перевищує допустимий поріг, Session Orchestrator приймає рішення про дозвіл на формування повноцінної сесії. У разі підозри або відмови автентифікація завершується із реєстрацією інциденту в Audit & Logging Module для подальшого аналізу спеціалістами безпеки.

Таким чином, первинна автентифікація в системі MiDIS не є лише одноразовою перевіркою облікових даних, а інтегрованим, динамічним процесом, що поєднує класичні механізми і сучасні інструменти поведінкового аналізу для підвищення загальної стійкості інтернет-банкінгу до атак.

Після успішного проходження первинної автентифікації система MiDIS переходить до етапу аналізу контексту, який відіграє важливу роль у формуванні динамічної моделі довіри до користувача. Контекстний аналіз забезпечує додаткову перевірку легітимності сесії шляхом збору та обробки даних про поточне середовище взаємодії користувача з системою.

Збір контекстуальної інформації включає в себе такі параметри, як тип пристрою (мобільний телефон, комп’ютер, планшет), операційна система, браузер,

IP-адреса, геолокація, мова системи, поведінкові шаблони (наприклад, швидкість навігації між елементами інтерфейсу), а також історичні взаємодії користувача з інтернет-банкінгом. Дані агрегуються в реальному часі і передаються до Behavioral AI Engine, який застосовує алгоритми машинного навчання для виявлення відхилень від звичних сценаріїв поведінки.

Особливістю контекстного аналізу в системі MiDIS є його постійний характер: оцінка ризику не завершується на моменті входу в систему, а продовжується протягом усієї сесії. Це дозволяє виявляти зміни у середовищі або підозрілу активність (наприклад, різка зміна IP-адреси чи перехід на незвичні функції), що може свідчити про компрометацію доступу або атаку з боку зловмисника.

Результати контекстного аналізу інтегруються з інформацією з модуля автентифікації та передаються до Policy Engine, де формується адаптивна політика доступу до функціоналу системи. У разі виявлення потенційної загрози можуть бути застосовані заходи додаткового контролю: сегментування сесії, часткова ізоляція функцій, або динамічне зниження рівня доступу користувача.

Таким чином, контекстний аналіз у MiDIS забезпечує багатовимірну оцінку надійності взаємодії користувача із системою, підвищуючи ефективність захисту без зниження зручності використання сервісу. Це дозволяє досягти стійкості системи до складних загроз, таких як атаки типу man-in-the-browser або внутрішні порушення з боку користувачів.

Після успішного проходження первинної автентифікації система MiDIS переходить до етапу аналізу контексту, який відіграє важливу роль у формуванні динамічної моделі довіри до користувача. Контекстний аналіз забезпечує додаткову перевірку легітимності сесії шляхом збору та обробки даних про поточне середовище взаємодії користувача з системою.

Збір контекстуальної інформації включає в себе такі параметри, як тип пристрою (мобільний телефон, комп’ютер, планшет), операційна система, браузер, IP-адреса, геолокація, мова системи, поведінкові шаблони (наприклад, швидкість навігації між елементами інтерфейсу), а також історичні взаємодії користувача з інтернет-банкінгом. Дані агрегуються в реальному часі і передаються до Behavioral

AI Engine, який застосовує алгоритми машинного навчання для виявлення відхилень від звичних сценаріїв поведінки.

Особливістю контекстного аналізу в системі MiDIS є його постійний характер: оцінка ризику не завершується на моменті входу в систему, а продовжується протягом усієї сесії. Це дозволяє виявляти зміни у середовищі або підозрілу активність (наприклад, різка зміна IP-адреси чи перехід на незвичні функції), що може свідчити про компрометацію доступу або атаку з боку зловмисника.

Результати контекстного аналізу інтегруються з інформацією з модуля автентифікації та передаються до Policy Engine, де формується адаптивна політика доступу до функціоналу системи. У разі виявлення потенційної загрози можуть бути застосовані заходи додаткового контролю: сегментування сесії, часткова ізоляція функцій, або динамічне зниження рівня доступу користувача.

Таким чином, контекстний аналіз у MiDIS забезпечує багатовимірну оцінку надійності взаємодії користувача із системою, підвищуючи ефективність захисту без зниження зручності використання сервісу. Це дозволяє досягти стійкості системи до складних загроз, таких як атаки типу man-in-the-browser або внутрішні порушення з боку користувачів.

Після завершення аналізу контексту система MiDIS здійснює оцінку рівня ризику, яка є ключовим етапом в ухваленні рішень щодо подальшого доступу користувача до функціоналу інтернет-банкінгу. Цей процес базується на багатофакторному підході, який враховує результати попередніх модулів: автентифікації, поведінкового аналізу, а також контексту взаємодії.

Behavioral AI Engine формує агрегований ризик-профіль сесії, застосовуючи моделі машинного навчання, натреновані на історичних даних щодо легітимної та підозрілої поведінки користувачів. Аналізуються такі параметри, як частота дій, послідовність переходів, відповідність типових сценаріїв користувача, час доби, географічна зона, а також потенційна наявність ознак автоматизованого втручання або маніпуляцій з боку сторонніх осіб.

Оцінка ризику виконується в умовах реального часу та має динамічний характер, тобто змінюється протягом сесії залежно від поведінки користувача.

Наприклад, якщо після входу з незвичного пристрою користувач намагається здійснити транзакцію на велику суму, рівень ризику буде підвищено, навіть якщо попередні дії не викликали підозр.

Результатом цього етапу є числовий або категоріальний ризиковий рейтинг, що передається до Policy Engine. Відповідно до нього система приймає рішення про:

- допуск до запитуваної дії без обмежень;
- застосування додаткових заходів перевірки (наприклад, повторна автентифікація або перевірка SMS-кодом);
- часткову ізоляцію сесійного сегмента;
- або повне блокування доступу до конкретної функції.

Завдяки гнучкій оцінці ризику система MiDIS дозволяє мінімізувати кількість помилкових спрацювань та підвищити точність виявлення реальних загроз, не створюючи надмірного навантаження на користувача. Такий адаптивний підхід дозволяє досягти балансу між рівнем безпеки та зручністю користування банківським сервісом.

Після виконання попередніх етапів, включно з автентифікацією, контекстним аналізом та оцінкою рівня ризику, система MiDIS переходить до процесу реєстрації сесії. На цьому етапі ініціюється створення логічної структури сесії в межах інтернет-банкінгу, яка надалі динамічно управляється в межах архітектури мікросегментованої ізоляції.

Session Orchestrator, отримавши підтвердження про прийнятний рівень ризику, реєструє сесію як валідну, присвоює їй унікальний ідентифікатор, а також ініціює створення базових сесійних сегментів — логічно відокремлених одиниць, кожна з яких відповідає за окремий тип операцій: перегляд балансу, внутрішні перекази, зовнішні транзакції, зміна налаштувань, управління картками тощо.

Кожен сегмент створюється у власному ізольованому середовищі — Segment Sandbox — що забезпечує обмеження впливу потенційних аномалій у межах одного сегмента на решту системи. На цьому етапі Policy Engine асоціює з кожним сегментом відповідну політику доступу, сформовану на основі поточного ризик-профілю та історії дій користувача. Ці політики визначають рівень контролю,

необхідний для виконання кожної операції (наприклад, просте підтвердження паролем або додаткове біометричне підтвердження).

Паралельно модуль Audit & Logging фіксує мета-інформацію про реєстрацію сесії: час, пристрій, IP-адресу, операційну систему, ідентифікатор користувача та попередній рівень ризику. Це забезпечує відстежуваність усіх дій у межах сесії та є важливим джерелом даних для подальшого аналізу інцидентів інформаційної безпеки.

Реєстрація сесії є відправною точкою для гнучкого та керованого середовища взаємодії користувача з банківською системою. Завдяки сегментованій структурі система MiDIS забезпечує можливість оперативного реагування на загрози, динамічного перегляду прав доступу, ізоляції окремих дій або операцій без припинення всієї сесії, що є особливо важливим у високоризикованих сценаріях.

Система мікросегментованої динамічної ізоляції сесій (MiDIS) є комплексною інформаційною архітектурою, що забезпечує адаптивний, сегментований підхід до захисту користувацьких сесій в інтернет-банкінгу. Функціональність MiDIS реалізується через взаємодію низки спеціалізованих модулів, кожен із яких виконує окрему роль у процесі виявлення загроз, контролю доступу та забезпечення безперервності обслуговування користувача.

Модуль User Client Interface (UCI) є вхідною точкою взаємодії користувача із системою інтернет-банкінгу, яка працює на основі архітектури MiDIS. Він відіграє ключову роль у ініціації сесії, зборі контекстної інформації та передачі запитів до інших модулів системи. UCI реалізується у вигляді веб- або мобільного інтерфейсу, через який користувач вводить облікові дані, здійснює навігацію, виконує банківські операції та отримує зворотний зв’язок від системи. Однією з головних функцій UCI є збір технічних та поведінкових параметрів, які дозволяють системі сформувати початковий контекст сесії. До таких параметрів належать IP-адреса, тип пристрою, операційна система, браузер, мова інтерфейсу, розмір екрану, часовий пояс, швидкість реакції користувача, ритм введення пароля, положення курсора, та інші непрямі ознаки. Ці дані автоматично передаються до модулів аналізу контексту та

оцінки ризику, що дозволяє з перших секунд сесії виявити аномальну або потенційно небезпечну активність.

UCI також забезпечує динамічний зворотний зв’язок у разі спрацювання захисних механізмів: наприклад, може з’явитися повідомлення про необхідність проходження додаткової автентифікації або про тимчасове обмеження доступу до певної дії. Інтерфейс адаптується до рішень, сформованих модулями Policy Engine та Access Control Gateway, що дозволяє користувачу отримувати лише дозволений функціонал відповідно до поточного ризик-профілю. Завдяки інтеграції з іншими компонентами системи, UCI не просто виконує роль “вікна” доступу до банкінгу, а є активним елементом безпекової архітектури, який підтримує контекстну обізнаність, зменшує ймовірність фішингових атак і сприяє ранньому виявленню вторгнень.

Модуль Session Orchestrator (SO) виконує центральну роль у координації всіх процесів, пов’язаних із веденням, поділом і моніторингом користувацьких сесій у рамках архітектури MiDIS. Його головним завданням є управління життєвим циклом сесії, починаючи від її ініціації, проходження через фази автентифікації, до динамічного сегментування та маршрутизації запитів до відповідних мікросегментів. Після отримання підтвердження про успішну автентифікацію та оцінку ризику, SO ініціює створення логічних сегментів усередині сесії — кожен із яких відповідає за окрему дію або групу дій (наприклад, перегляд балансу, переказ коштів, зміна налаштувань профілю).

Кожен сегмент функціонує ізольовано в межах власного оточення, а доступ до нього контролюється відповідно до політик, сформованих модулем Policy Engine. SO відповідає за маршрутизацію запитів між сегментами та іншими модулями системи, зокрема Access Control Gateway, Behavioral AI Engine та Segment Sandbox. У разі виявлення загроз або змін у поведінковій моделі користувача, Session Orchestrator має змогу адаптивно перестворювати сегменти, припиняти окремі дії або змінювати рівень їх доступності — без завершення всієї сесії.

Крім того, SO забезпечує узгодженість між сесією користувача та загальною безпековою політикою системи, синхронізуючи всі події через журнал Audit & Logging Module. У разі потреби модуль також ініціює процедури повторної

автентифікації для підозрілих сегментів або обмежує сесію до режиму перегляду, поки ризик не буде локалізовано. Таким чином, Session Orchestrator виступає як мозковий центр сесійної безпеки в MiDIS, що забезпечує безперервний контроль, гнучку адаптацію до ризиків і безпечну взаємодію між користувачем та банківською системою.

Policy Engine (PE) є ключовим модулем у системі MiDIS, який відповідає за формування, оновлення та застосування політик доступу для кожного окремого сесійного сегмента. Його головна функція полягає у створенні динамічних правил доступу на основі багатофакторного аналізу, що враховує поточний контекст користувача, результати поведінкової аналітики, рівень ризику сесії та специфіку виконуваної дії.

Після проходження автентифікації та оцінки ризику, Policy Engine генерує набір політик, який визначає, яким чином повинні реагувати модулі Access Control Gateway та Segment Sandbox у випадку, якщо поведінка користувача відхиляється від очікуваної. Ці політики включають правила про допустимість дій, обмеження часу, необхідність повторної автентифікації, а також логіку відновлення доступу в разі незначних аномалій.

PE постійно отримує оновлення від Behavioral AI Engine, що дозволяє йому адаптувати політики в режимі реального часу. Наприклад, якщо користувач зазвичай виконує входи з одного геолокаційного регіону, але потім раптово ініціює транзакцію з іншого, Policy Engine може змінити політику доступу, вимагаючи двофакторну перевірку або ізолюючи сегмент для додаткової перевірки.

Архітектурно Policy Engine функціонує як автономний сервіс, але має тісний зв’язок із Session Orchestrator, який надсилає йому запити щодо визначення політик для нових або змінених сегментів. Рішення, прийняті PE, також зберігаються в Audit & Logging Module, що дозволяє здійснювати ретроспективний аналіз безпекових подій і відстежувати зміну політик у часі.

У сукупності, Policy Engine забезпечує гнучкий, адаптивний підхід до управління доступом, дозволяючи системі залишатися ефективною навіть у

випадках нестандартної або потенційно шкідливої поведінки користувача, не порушуючи при цьому безперервність надання послуг.

Behavioral AI Engine (AI) є центральним аналітичним компонентом системи MiDIS, який забезпечує постійний моніторинг та інтерпретацію поведінки користувача з метою виявлення потенційних загроз ще до того, як вони переростуть у фактичні інциденти. Цей модуль застосовує алгоритми машинного навчання та штучного інтелекту для побудови профілів користувацької активності, виявлення відхилень від звичного шаблону та оцінки ризику кожної сесії чи окремої дії.

AI Engine працює на основі попередньо накопичених даних про поведінку користувача, включаючи частоту дій, час і тривалість входу, геолокацію, тип пристрою, а також шаблони транзакцій. Кожна нова дія в рамках сесії аналізується в реальному часі на відповідність цим профілям. Якщо система фіксує аномальні показники — наприклад, занадто велику суму переказу, нехарактерний маршрут навігації або надто швидке введення даних — це може трактуватися як потенційна загроза.

Результати цього аналізу передаються Policy Engine, який відповідно коригує політики доступу. Наприклад, при фіксації підозрілої активності AI Engine може ініціювати зміну статусу сегмента сесії на обмежений або запустити запит на повторну автентифікацію. У випадку критичних ризиків – наприклад, спроби одночасного входу з двох континентів – система може рекомендувати ізоляцію відповідного сегмента або повне блокування дії.

Окрім поточного аналізу, Behavioral AI Engine також виконує довготривалу аналітику, покращуючи власні моделі прогнозування на основі історичних інцидентів і зворотного зв'язку від системи аудиту. Це дозволяє підвищити точність виявлення загроз з часом і мінімізувати кількість помилкових спрацьовувань, що особливо важливо у фінансових додатках з високими вимогами до зручності користування.

Таким чином, Behavioral AI Engine є основним джерелом адаптивності системи MiDIS, забезпечуючи їй здатність до самонавчання, динамічного реагування та випереджувального виявлення ризиків у середовищі онлайн-банкінгу.

Access Control Gateway (ACG) є ключовим компонентом у архітектурі системи MiDIS, який забезпечує безпосереднє застосування політик безпеки до кожного сесійного сегмента в режимі реального часу. Його головною функцією є прийняття рішень про дозвіл або обмеження доступу до певної дії чи ресурсу на основі інформації, отриманої від модулів Policy Engine та Behavioral AI Engine.

ACG виконує роль динамічного фільтра доступу, що контролює кожен запит користувача перед його виконанням. Після отримання запиту, шлюз звертається до сформованих політик доступу, які враховують поточний контекст сесії, рівень ризику, профіль користувача та історію його поведінки. У разі відповідності всім вимогам, доступ до дії дозволяється. Якщо ж параметри викликають підозру або виходять за межі прийнятного шаблону, ACG може ініціювати одну з кількох реакцій — від запиту повторної автентифікації до повного ізолювання сегмента або скасування дії.

Важливою особливістю ACG є його здатність до роботи з високою швидкістю та мінімальними затримками, що критично для онлайн-банкінгу. Завдяки кешуванню політик і оптимізації маршрутів обробки запитів, ACG забезпечує безпеку без помітного впливу на продуктивність або досвід користувача.

Окрім обмежувальних функцій, ACG також підтримує механізми «м’якого» реагування. Наприклад, при середньому рівні ризику може застосовуватися часткове блокування функціоналу, обмеження суми переказу або перенаправлення на додаткову перевірку, без повної зупинки сесії. Такий підхід дозволяє досягти балансу між безпекою та зручністю, що є ключовим принципом системи MiDIS.

Таким чином, Access Control Gateway виступає в ролі захисного бар’єра на шляху до інформаційних ресурсів, реалізуючи детальний, адаптивний і контекстно-залежний контроль доступу, що є основою ефективного функціонування мікросегментованої безпекової моделі.

Segment Sandbox (SS) є спеціалізованим віртуальним середовищем, призначеним для ізольованого виконання окремих сегментів сесії в межах архітектури MiDIS. Його основна роль полягає у забезпеченні локалізації

потенційних загроз, обмеженні їх поширення та збереженні цілісності інших частин сесії в разі інциденту.

Кожна сесія користувача при ініціації розділяється на окремі логічні сегменти відповідно до дій або типів операцій (наприклад, перегляд балансу, переказ коштів, редагування налаштувань). Кожен з цих сегментів виконується у власному середовищі Segment Sandbox, яке повністю ізольоване від інших сегментів на логічному та ресурсному рівні. Завдяки цьому, навіть якщо в одному з сегментів виявляється аномальна активність або спроба атаки, інші сегменти залишаються захищеними та працездатними.

Segment Sandbox створюється динамічно під час запуску відповідного сегмента і конфігурується згідно з політиками доступу, визначеними Policy Engine. У разі виявлення ризику Behavioral AI Engine може ініціювати рестарт або перезавантаження сегмента без впливу на загальну сесію, що забезпечує безперервність користувацького досвіду.

Технічно, SS реалізується з використанням легковагових контейнеризованих середовищ або віртуальних ізольованих процесів, що дозволяє забезпечити масштабованість та ефективне використання ресурсів. Такий підхід також сприяє гнучкості оновлень без зупинки всієї системи.

Завдяки застосуванню Segment Sandbox, система MiDIS не лише підвищує загальний рівень безпеки, але й забезпечує високу стійкість до атак, дозволяючи реагувати на інциденти точково та без втрат для користувача. Це особливо важливо для сфери інтернет-банкінгу, де стабільність, швидкість та довіра мають вирішальне значення.

Audit & Logging Module (LOG) відіграє ключову роль у забезпеченні прозорості, підзвітності та ретроспективного аналізу дій, що відбуваються в межах системи MiDIS. Цей модуль відповідає за детальне фіксування всієї активності, пов’язаної з користувацькими сесіями, системними подіями, змінами політик доступу, а також аномаліями, виявленими модулями безпеки.

Під час кожної сесії модуль LOG збирає структуровані записи про запуск та завершення сесійних сегментів, спроби доступу до окремих ресурсів, результати

автентифікації, оцінки ризику, реакції системи на інциденти та рішення, прийняті Policy Engine і Access Control Gateway. Дані журналювання зберігаються в незмінному форматі з можливістю перевірки їхньої цілісності, що важливо для цифрової криміналістики та аудиту відповідності вимогам безпеки.

Особливістю LOG є підтримка так званого «контекстного логування», що означає не лише фіксацію факту події, а й урахування контексту її виникнення — IP-адреса, геолокація, час, тип пристрою, попередні дії користувача тощо. Це значно полегшує аналіз інцидентів та формування повної картини поведінки користувача.

Крім зберігання даних, модуль забезпечує інтерфейс для аналітичних запитів, що дозволяє системним адміністраторам, аудиторам і системам SIEM (Security Information and Event Management) здійснювати моніторинг у реальному часі та історичний аналіз.

Завдяки Audit & Logging Module система MiDIS здатна не лише виявляти загрози під час виконання сесій, але й вивчати шаблони атак, вдосконалювати політики безпеки на основі зібраних даних, а також забезпечувати доказову базу у разі виникнення інцидентів. Це робить LOG критичним компонентом для побудови довіри, відповідності стандартам (наприклад, PCI DSS) і забезпечення безперервного вдосконалення системи безпеки.

Діаграма, наведена нижче, відображає узагальнений алгоритм функціонування системи MiDIS (Microsegmented Dynamic Isolation of Sessions) в середовищі інтернет-банкінгу. Вона ілюструє логіку обробки користувацьких сесій від моменту ініціації до динамічного керування доступом у реальному часі. Основна увага приділяється етапам первинної автентифікації, поведінковому аналізу, оцінці ризиків, створенню сегментів сесії, накладанню політик доступу та адаптивному реагуванню на загрози.

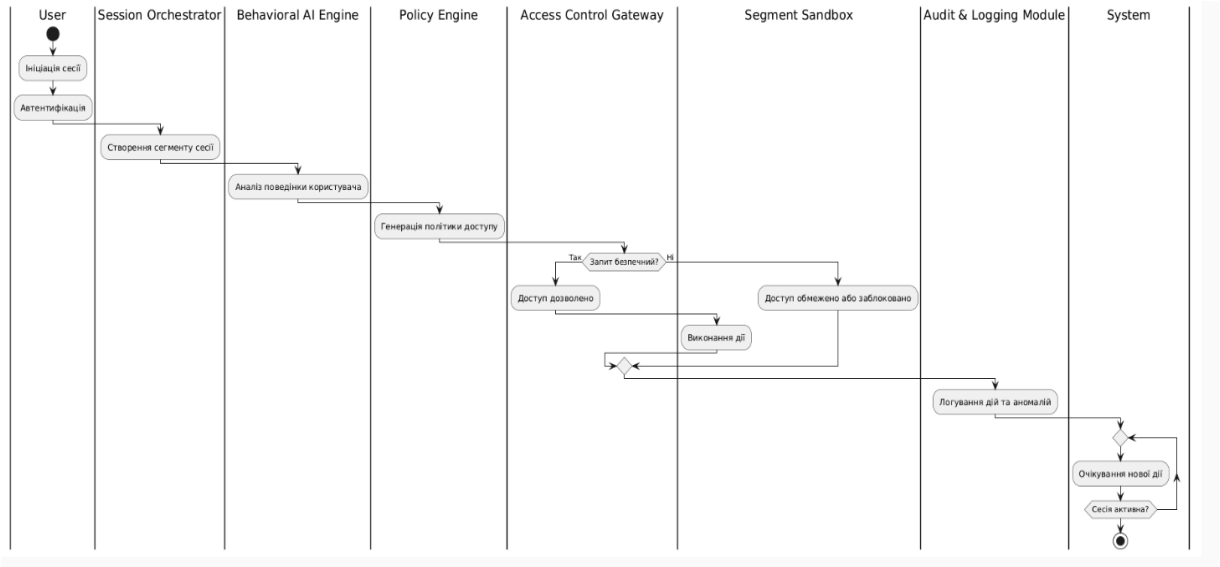

Рисунок 4.3 Алгоритм функціонування системи мікросегментованої динамічної ізоляції сесій (MiDIS) в інтернет-банкінгу

Ця діаграма дозволяє візуалізувати взаємодію ключових модулів системи — зокрема, Behavioral AI Engine, Policy Engine, Access Control Gateway, Session Orchestrator — та демонструє, як реалізується безпека на рівні ізольованих сегментів без втручання в цілісність сесії. Такий підхід забезпечує баланс між надійністю захисту та зручністю користування банківським сервісом.

4.5 Інтеграція з банківськими сервісами

Інтеграція системи мікросегментованої динамічної ізоляції сесій (MiDIS) з банківськими сервісами здійснюється через спеціалізований архітектурний рівень, який забезпечує безпечний обмін даними між модулями системи та інфраструктурою цифрового банкінгу. Основною метою такої взаємодії є забезпечення прозорого контролю доступу, мінімізація ризиків, пов'язаних з несанкціонованими діями, а також збереження стабільності роботи основних банківських функцій.

Архітектура передбачає, що модулі MiDIS діють як проміжний рівень між клієнтським інтерфейсом (User Client Interface) і внутрішніми сервісами банку,

зокрема такими як модуль авторизації, модуль обробки транзакцій, бази даних клієнтів та аналітичні сервіси. Компоненти MiDIS — зокрема, Session Orchestrator, Access Control Gateway та Policy Engine — інтегруються із зовнішніми API банківських систем за допомогою безпечних протоколів (наприклад, HTTPS, OAuth 2.0, Mutual TLS).

Session Orchestrator виконує роль посередника, який приймає запити з клієнтського інтерфейсу, передає їх у відповідні банківські модулі через контролер доступу та аналізує відповідь у контексті активних політик безпеки. У випадку виявлення загроз чи відхилень від типової поведінки користувача, Behavioral AI Engine ініціює відповідні реакції — від обмеження доступу до певного сегмента до повної ізоляції поточної дії без зупинки сесії загалом.

Для забезпечення надійності та безперервності взаємодії архітектура MiDIS підтримує асинхронні запити, кешування метаданих доступу та механізми черг повідомлень, які дозволяють обробляти великі обсяги запитів без перевантаження банківських сервісів. Крім того, всі транзакції, що проходять через MiDIS, логуються в Audit & Logging Module, що дозволяє банку мати централізований журнал безпекових подій та запитів доступу.

Таким чином, архітектурна модель взаємодії MiDIS з банківськими сервісами забезпечує гнучке, масштабоване та безпечне середовище, що може бути впроваджене з мінімальними змінами до наявної IT-інфраструктури банку.

Для наочного представлення принципів взаємодії між системою MiDIS та зовнішніми банківськими сервісами була розроблена архітектурна діаграма. Вона демонструє ключові компоненти системи, їхню роль у забезпеченні інформаційної безпеки, а також потоки даних між клієнтським інтерфейсом, модулями MiDIS і банківською інфраструктурою. Особливу увагу приділено модулю Access Control Gateway (ACG), який виступає центральним елементом при зверненні до критично важливих сервісів, таких як авторизація, транзакції, доступ до рахунків та повідомлення. Діаграма також ілюструє роль поведінкового аналізу та політик доступу у формуванні динамічного, контекстно-орієнтованого захисту сесій.

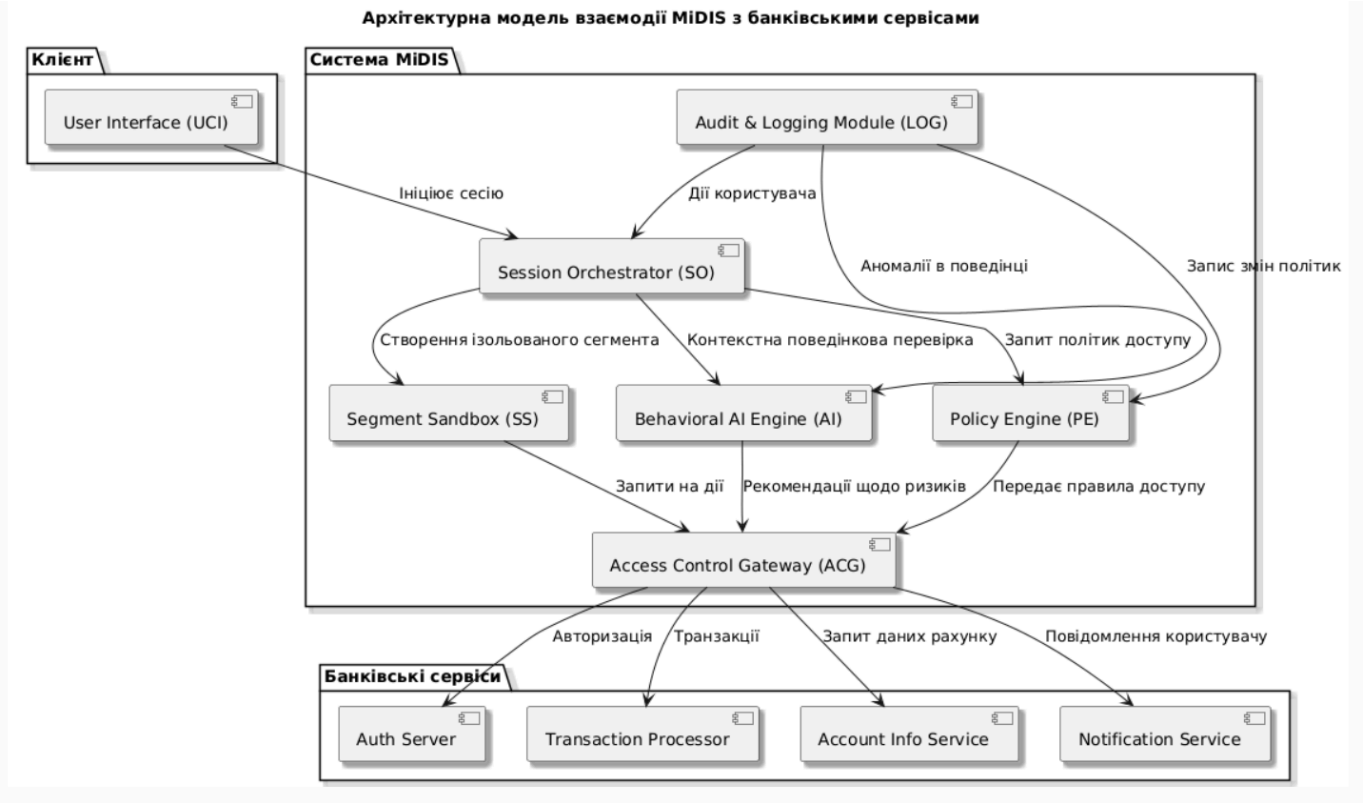

Рисунок 4.4 Архітектурна модель взаємодії MiDIS з банківськими сервісами

Інтеграція системи MiDIS з банківськими сервісами потребує використання стандартних, безпечних та ефективних протоколів взаємодії, які забезпечують надійну передачу даних, автентифікацію сторін та цілісність повідомлень. Основною метою є досягнення сумісності з існуючою банківською інфраструктурою, мінімізація затримок під час обміну інформацією, а також захист від потенційних кіберзагроз.

Надійна передача даних між системою MiDIS і банківськими інформаційними сервісами є критично важливою умовою захисту інформаційних потоків. З огляду на це, ключовим елементом архітектури взаємодії є використання захищених транспортних протоколів, які дозволяють зберігати цілісність і конфіденційність інформації навіть у публічних або потенційно небезпечних мережах.

Основним протоколом транспортування даних є HTTPS (HTTP Secure) — розширення стандартного протоколу HTTP, яке використовує TLS (Transport Layer Security) для шифрування трафіку. У реалізації MiDIS застосовується виключно TLS версії 1.3, яка на сьогодні є найбільш захищеною та рекомендованою до

використання у фінансових установах. Перевагами TLS 1.3 є мінімізація криптографічного накладного трафіку, усунення вразливих алгоритмів (наприклад, RC4, SHA-1), а також покращення швидкодії завдяки скороченому числу раундів узгодження.

Крім HTTPS, для внутрішньої взаємодії між модулями MiDIS та при обміні структурованими даними в режимі реального часу використовується gRPC (Google Remote Procedure Call) у поєднанні з TLS. Цей протокол забезпечує швидку серіалізацію даних (через Protocol Buffers), малий розмір повідомлень і підтримку потокового передавання, що важливо для сесійної динамічної ізоляції. gRPC також дозволяє визначати чіткі контракти взаємодії (API), що спрощує інтеграцію та супровід.

У разі потреби інтеграції з системами, які використовують застарілі технології або не підтримують TLS 1.3, MiDIS підтримує механізми пониження безпеки (downgrade mitigation) з відповідним журналюванням таких подій і автоматичним застосуванням додаткових заходів захисту (наприклад, ізоляція транзакції або попередження адміністратора).

Таким чином, використання сучасних транспортних протоколів дозволяє MiDIS досягти балансу між швидкодією, масштабованістю та максимальним рівнем захисту даних під час обміну між клієнтами, внутрішніми модулями системи та зовнішніми банківськими сервісами.

Інтеграція MiDIS з банківськими сервісами потребує чіткого управління автентифікацією користувачів і системних компонентів, а також визначення прав доступу до захищених ресурсів. У цьому контексті система використовує сучасні відкриті протоколи, що відповідають стандартам інформаційної безпеки в фінансовому секторі.

Ключовим протоколом для автентифікації користувачів виступає OAuth 2.0 — індустріальний стандарт авторизації, який дозволяє делегувати доступ до ресурсів без передачі облікових даних. У межах MiDIS OAuth 2.0 використовується у зв’язці з OpenID Connect (OIDC), що розширює можливості протоколу, дозволяючи проводити ідентифікацію користувача. Після успішної автентифікації сервер

авторизації повертає ID Token у форматі JWT (JSON Web Token), який містить підписані атрибути користувача (принципал, роль, рівень ризику, тощо).

Такий підхід дозволяє реалізувати єдину точку автентифікації (SSO) та централізоване управління сесіями, зокрема підтримку рефреш-токенів, часових обмежень, прив'язки до пристрою та двофакторної автентифікації (2FA). Також OpenID Connect забезпечує автоматичну синхронізацію інформації між MiDIS та іншими внутрішніми системами банку (CRM, AML, аналітика).

Для авторизації між модулями MiDIS та зовнішніми мікросервісами банківської інфраструктури застосовується OAuth 2.0 Client Credentials Grant, що дозволяє сервісам взаємодіяти на основі токенів з попередньо визначеними правами доступу. Усі запити до захищених API супроводжуються токеном, підписаним з використанням асиметричного шифрування (наприклад, RSA або ECDSA), що гарантує недоторканність ідентичності джерела.

У рамках динамічного профілю ризику, протокол авторизації може доповнюватися політиками контекстної авторизації: наприклад, доступ до певного ресурсу дозволяється лише в разі відповідності контексту сесії (геолокації, часу доби, типу операції тощо), що реалізується за допомогою модуля Policy Engine.

Таким чином, інтеграція протоколів OAuth 2.0 та OpenID Connect у систему MiDIS дозволяє створити надійну, масштабовану та гнучку модель автентифікації та авторизації, яка повністю відповідає сучасним вимогам банківської безпеки.

У системі MiDIS для забезпечення уніфікованої взаємодії між модулями системи та банківською інфраструктурою використовуються стандартизовані формати обміну даними, що забезпечують високу сумісність, масштабованість і зручність у подальшому аналізі. Основними форматами є JSON (JavaScript Object Notation) та XML (eXtensible Markup Language), які широко підтримуються в індустрії фінансових технологій.

Формат JSON використовується як основний у внутрішніх RESTful API-запитах між компонентами системи MiDIS, зокрема для передачі:

- інформації про користувача (ID, роль, поведінкові характеристики);
- структур сесій (ідентифікатор, часові мітки, рівень ризику);

- токенів автентифікації (JWT);
- результатів політик доступу.

JSON обрано через його легкість, компактність, просту читаність та сумісність із більшістю сучасних мов програмування. Це дозволяє досягти високої швидкості обробки запитів, що критично важливо для систем реального часу, таких як MiDIS.

У разі взаємодії з легасі-системами або зовнішніми інтеграційними платформами (наприклад, банківськими процесинговими сервісами), MiDIS також підтримує формат XML, який залишається поширеним у сфері міжбанківської взаємодії та стандартів (наприклад, ISO 20022). XML використовується для:

- обміну транзакційними повідомленнями;
- інтеграції з платіжними шлюзами;
- структурованого опису бізнес-правил.

Крім цього, для передачі даних про логування, інциденти безпеки та дії користувачів використовується формат JSON Lines (JSONL) — розширення JSON для потокової обробки великих обсягів подій. Це забезпечує ефективну інтеграцію з системами моніторингу, SIEM (Security Information and Event Management) та аналітики.

Особлива увага приділяється захисту даних під час передачі: усі формати даних інкапсулюються у шифровані канали (наприклад, HTTPS/TLS 1.3), а конфіденційні поля — такі як ідентифікатори користувачів чи токени — додатково шифруються на рівні payload за допомогою алгоритмів AES або RSA.

Таким чином, використання гнучких і безпечних форматів обміну даними дозволяє системі MiDIS легко масштабуватись, адаптуватись до різних середовищ і забезпечувати надійну інтеграцію з широким спектром банківських сервісів.

Для забезпечення гнучкої та масштабованої інтеграції з різними банківськими системами, система MiDIS підтримує концепцію адаптерів (integration adapters), які слугують проміжним рівнем між ядром системи безпеки та зовнішніми інтерфейсами банківських сервісів. Адаптери виконують роль трансляторів протоколів, форматів даних і логіки взаємодії, що дозволяє мінімізувати вплив змін у зовнішніх системах на роботу внутрішньої інфраструктури MiDIS.

Адаптери забезпечують абстрагування бізнес-логіки від деталей реалізації API конкретного банку або сервісу. Кожен адаптер розробляється згідно з інтерфейсом, визначеним у MiDIS API Contract, і може бути налаштований для взаємодії з:

- внутрішніми API банківських систем (core banking, CRM, платіжні шлюзи);
- зовнішніми сервісами перевірки клієнтів (KYC/AML);
- провайдерами платіжних сервісів або мобільного банкінгу;
- системами моніторингу та журналювання подій безпеки (SIEM, SOC).

Кожен адаптер може містити модулі перетворення форматів даних (наприклад, XML ↔ JSON), логіки повторних спроб запиту, буферизації, кешування та конвертації статусів. Завдяки цьому MiDIS здатна адаптуватися до різнорідного технічного середовища банку без потреби в глобальній переробці коду.

Перевагою такої архітектури є модульність: адаптери можуть розгортатися, оновлюватися або замінюватися без впливу на роботу основних компонентів системи. Крім того, реалізація адаптерів на основі загального SDK дає можливість стороннім постачальникам або технічним підрозділам банку самостійно створювати або адаптувати модулі для своїх систем, дотримуючись стандартів безпеки MiDIS.

Таким чином, підтримка адаптерів є ключовим фактором масштабованості та швидкої адаптації системи MiDIS до нових цифрових платформ та фінансових технологій.

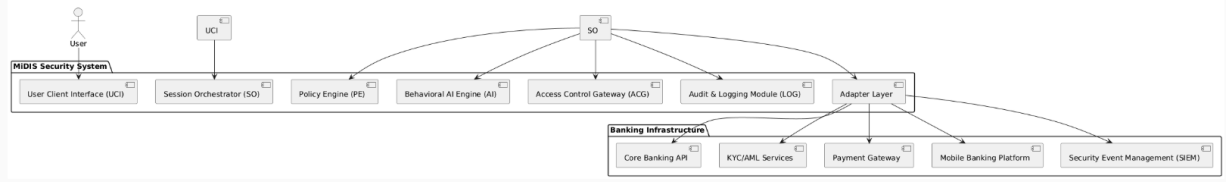

Рисунок 4.5 Логічна взаємодія між модулями системи MiDIS

Представлена блок-схема демонструє логічну взаємодію між модулями системи MiDIS та сервісами банківської інфраструктури. Користувацькі запити обробляються через User Client Interface (UCI), після чого маршрутизуються до Session Orchestrator (SO), який координує взаємодію з іншими модулями безпеки.

Ключову роль відіграє Adapter Layer — універсальний шар інтеграції, що забезпечує безпечне з’єднання з різноманітними банківськими API та зовнішніми сервісами (наприклад, системами перевірки KYC/AML, платіжними шлюзами, мобільними платформами тощо).

Завдяки модульному підходу та гнучкій структурі, система підтримує масштабовану інтеграцію з мінімальними змінами в існуючій інфраструктурі банку. При цьому забезпечується повна підтримка контрольованого доступу, моніторингу активності користувача та централізованого аудиту. Така архітектура дозволяє досягти високого рівня безпеки без шкоди для продуктивності чи зручності використання системи.

Висновки до розділу 4

У цьому розділі було розроблено метод мікросегментованої динамічної ізоляції сесій (MiDIS), який пропонує новий підхід до забезпечення інформаційної безпеки в системах інтернет-банкінгу. Метод базується на ідеї поділу користувацької сесії на ізольовані сегменти з індивідуальними політиками безпеки, що дозволяє локалізувати ризики, оперативно реагувати на аномалії та уникати припинення всієї сесії в разі загроз.

Була представлена архітектура системи MiDIS, яка включає такі ключові компоненти, як Session Orchestrator, Policy Engine, Behavioral AI Engine, Access Control Gateway та Segment Sandbox. Детально розглянуто функціональність кожного модуля, їхню взаємодію та внесок у забезпечення адаптивного, контекстно-залежного захисту.

Також описано алгоритм роботи системи: від ініціації сесії й автентифікації до динамічного формування політик, оцінки ризику та застосування відповідних обмежень до кожного сесійного сегмента. Акцентовано увагу на використанні поведінкового аналізу у реальному часі як основи для прийняття рішень.

Запропонований метод дозволяє досягти балансу між високим рівнем безпеки та зручністю користувача, мінімізуючи кількість помилкових відключень і

забезпечуючи гнучке керування ризиками. Метод MiDIS має високий потенціал для впровадження в інтернет-банкінгові системи наступного покоління.

РОЗДІЛ 5
РОЗРОБКА ЗАСОБУ CIBA-SHIELD ЯК ЕЛЕМЕНТА ПОВЕДІНКОВОЇ БЕЗПЕКИ В ІНТЕРНЕТ-БАНКІНГУ

5.1 Загальна концепція та призначення засобу

У сучасному цифровому середовищі інтернет-банкінг став критично важливим каналом надання фінансових послуг, який потребує найвищого рівня захисту. Одним з найбільш вразливих етапів взаємодії користувача із банківською системою є процес авторизації — підтвердження дозволу на виконання певних дій, зокрема транзакцій. Традиційні механізми авторизації, які базуються переважно на взаємодії клієнтського пристрою з сервером у режимі реального часу, часто не враховують змінний контекст користувача, рівень ризику та особливості поведінки, що створює можливості для скомпрометування або обману системи.

У відповідь на зростаючі виклики, пов’язані з фішингом, атаками посередника (MITM), компрометацією мобільних пристроїв та ін'єкціями в клієнтський інтерфейс, актуалізується потреба у переході до більш безпечної та ізольованої форми авторизації. Особливу цінність становлять протоколи, які реалізують концепцію бекенд-авторизації, тобто таких механізмів, де підтвердження відбувається без прямої залежності від активної взаємодії з клієнтським пристроєм, що знижує ризик зовнішнього втручання.

Інноваційним підходом до вирішення цієї проблеми є використання протоколу CIBA (Client Initiated Backchannel Authentication), який дозволяє відокремити процес авторизації від основного сеансу доступу, забезпечуючи при цьому додаткову гнучкість та захищеність. Однак навіть CIBA має низку обмежень у контексті банківських систем. Це створює підґрунтя для розробки нового засобу — CIBA-SHIELD, здатного реалізувати розширену адаптивну бекенд-авторизацію із врахуванням контексту, ризиків і політик доступу, що динамічно змінюються.

Потреба в такому рішенні є надзвичайно актуальною у зв’язку з постійною еволюцією кіберзагроз і високою вартістю компрометації банківських сесій. CIBA-SHIELD дозволяє банківським установам посилити авторизаційні механізми без погіршення зручності для кінцевих користувачів, забезпечуючи новий рівень інформаційної безпеки в цифровому банкінгу.

Протокол CIBA (Client Initiated Backchannel Authentication) є частиною специфікацій OpenID Connect, розроблених для забезпечення асинхронної автентифікації та авторизації, особливо у випадках, коли клієнтський пристрій не має можливості безпосередньої взаємодії з користувачем у режимі реального часу. CIBA дозволяє ініціювати автентифікацію через бекенд-канал (backchannel), що забезпечує вищий рівень безпеки за рахунок зменшення залежності від вразливих клієнтських інтерфейсів.

У класичному сценарії CIBA клієнт (наприклад, банківська система) надсилає запит до авторизаційного сервера, який потім ініціює взаємодію з автентифікатором (наприклад, мобільним додатком користувача) для підтвердження особи або дії. Успішне підтвердження з боку користувача призводить до видачі токену доступу клієнтові. Такий підхід добре працює в системах, де потрібна безпечна взаємодія з різними типами пристроїв (термінали, банкомати, IoT-пристрої) або у випадках делегованої авторизації.

Проте, попри свої переваги, базовий CIBA має низку обмежень, які знижують його ефективність у специфічному контексті інтернет-банкінгу:

Відсутність гнучкої адаптації до ризиків — протокол не передбачає динамічної оцінки рівня загрози під час авторизації.

Статична політика доступу — рішення базується на попередньо визначених правилах і не змінюється в реальному часі відповідно до поведінки користувача.

Відсутність контекстної обробки — CIBA не обробляє параметри сеансу, місце розташування, часові обмеження, тип операції тощо, що знижує гнучкість реагування.

Мінімальний контроль із боку фінансового сервісу — автентифікація відбувається поза основним банківським контекстом, що ускладнює аудит та трасування.

Обмеженість механізмів відновлення сесії — у разі збою немає вбудованих засобів повторної ініціації без втрати статусу операції.

Ці обмеження є критичними для середовища, де швидкість, точність і контроль є визначальними чинниками безпеки. Саме тому на їх основі було сформульовано вимоги до нового засобу — CIBA-SHIELD, який розширює можливості CIBA, додаючи динамічну аналітику, сегментування, політики доступу в реальному часі та глибшу інтеграцію з банківськими сервісами.

CIBA-SHIELD реалізує принцип бекенд-авторизації з багатоконтекстною перевіркою, поєднуючи класичний підхід протоколу CIBA з розширеними механізмами оцінки ризиків у реальному часі. Його основна мета — підвищити надійність серверної авторизації шляхом урахування широкого спектру контекстуальних параметрів під час прийняття рішень щодо надання доступу або підтвердження транзакції.

На відміну від стандартної реалізації CIBA, де авторизація базується переважно на ідентифікаторі користувача та підтвердженні з мобільного пристрою, CIBA-SHIELD інтегрує багаторівневу перевірку з урахуванням:

геолокаційних даних користувача (наприклад, IP, GPS, мережевий сегмент),

часового профілю (збіг із типовими часовими вікнами активності),

типу операції (різні рівні перевірки для перегляду балансу, переказу коштів чи зміни реквізитів),

поведінкового шаблону (відхилення від звичної динаміки дій),

сесійних параметрів, включно з пристроєм, ОС, браузером тощо,

профілю ризику на основі попередніх інцидентів, налаштувань користувача або політик установи.

Після отримання запиту від клієнта, CIBA-SHIELD формує контекстний профіль сесії, який оцінюється спеціалізованим Risk Evaluation Engine. У разі, якщо сукупна оцінка контексту знаходиться в межах безпечного порогу, запит

направляється до мобільного додатку користувача або іншого підтверджувального каналу. У протилежному випадку система:

або повністю блокує запит,

або ініціює додатковий рівень перевірки (наприклад, голосову біометрію, OTP, відеопідтвердження).

Таким чином, бекенд-авторизація CIBA-SHIELD не є сліпим підтвердженням, а контекстно зваженим, динамічним процесом, який знижує імовірність соціальної інженерії, перехоплення авторизації або зловмисної активації сесій на сторонніх пристроях.

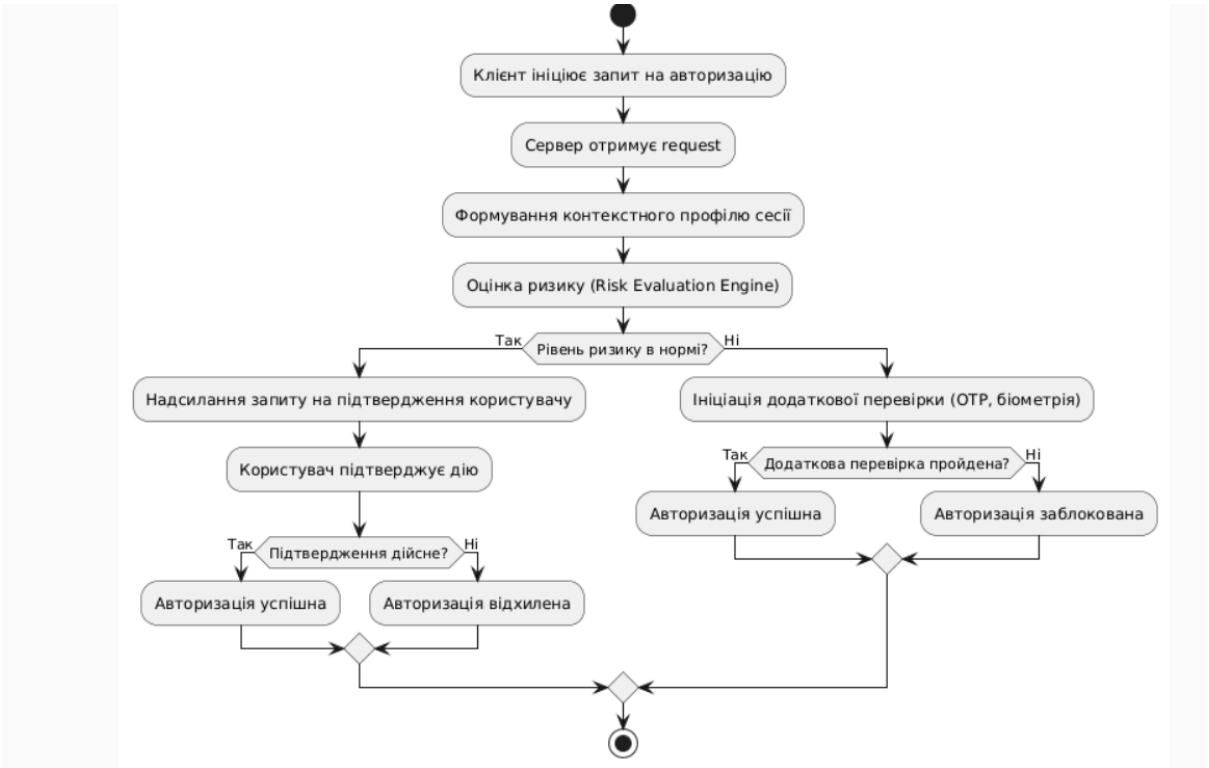

Рисунок 5.1 Принцип дії бекенд-авторизації з багатоконтекстною перевіркою в системі CIBA-SHIELD

Для більш наочного розуміння логіки роботи засобу CIBA-SHIELD доцільно розглянути діаграму активності (Рис. 5.1), що ілюструє ключові етапи взаємодії між клієнтом, сервером авторизації та механізмом оцінки ризиків. Ця діаграма демонструє, як система адаптується до контексту кожного запиту, застосовуючи багаторівневу верифікацію залежно від рівня ризику та поведінкових характеристик

користувача. Такий підхід дозволяє забезпечити гнучкий, але водночас надійний механізм авторизації, що особливо актуально для фінансових систем з високими вимогами до інформаційної безпеки.

5.2 Архітектура засобу CIBA-SHIELD

Засіб CIBA-SHIELD побудований на основі концепції розподіленої серверної авторизації, яка доповнює стандартний протокол CIBA (Client Initiated Backchannel Authentication) розширеним механізмом багатоконтекстної перевірки. Його архітектура орієнтована на обробку запитів автентифікації, які надходять до банківського сервера з боку мобільних чи веб-клієнтів, без участі користувача у прямій сесії (тобто у фоновому режимі), з приєднанням додаткових контекстних даних, необхідних для прийняття обґрунтованого рішення щодо доступу.

Ключовими елементами загальної моделі є:

Frontend Authorization Request Handler – приймає початковий запит на авторизацію з клієнтського боку та ініціює процес перевірки.

Contextual Risk Evaluator – модуль, що аналізує поведінкові, географічні, пристроєві та часові параметри для формування контексту запиту.

Adaptive Policy Engine – механізм генерації динамічних політик доступу на основі результатів оцінки ризику.

Backchannel Auth Server (CIBA Core) – реалізує протокол CIBA для взаємодії з зовнішніми Identity Providers (IdP), наприклад, BankID або Mobile ID.

Security Decision Layer – ухвалює остаточне рішення про надання або відмову в авторизації.

Audit & Trace Logger – відповідає за фіксацію всіх подій та взаємодій у безпечному журналі для подальшого аудиту.

Компоненти системи взаємодіють за асинхронною схемою, що забезпечує як ефективну обробку запитів у реальному часі, так і масштабованість рішення. Структура системи дозволяє легко адаптувати її до потреб конкретного банку або регіональних вимог з безпеки.

Архітектура CIBA-SHIELD включає низку спеціалізованих компонентів, кожен з яких виконує окрему роль у забезпеченні безпечної, багатоконтекстної серверної авторизації. Взаємодія між модулями побудована таким чином, щоб забезпечити мінімальні затримки, високий рівень точності верифікації та збереження прозорості з боку клієнтського додатку.

Frontend Authorization Request Handler (FARH) йей компонент приймає початкові запити на авторизацію, що надходять з клієнтських пристроїв (мобільних або веб-клієнтів). Його завдання – виділити ключові ідентифікатори запиту, сформувати тимчасовий токен сесії та передати запит на подальшу обробку. Він також відповідає за первинну фільтрацію запитів за базовими критеріями безпеки (наприклад, правильність структури або форматів параметрів).

Contextual Risk Evaluator (CRE) виконує збір та аналіз контекстних даних, таких як геолокація, тип пристрою, часовий профіль активності, частота транзакцій тощо. На основі цих параметрів система формує профіль ризику для кожного запиту. CRE є критичним компонентом у виявленні аномалій та захисті від соціальної інженерії чи викрадення сесій.

Adaptive Policy Engine (APE) формує політику авторизації у режимі реального часу. На відміну від традиційних жорстко заданих правил, APE динамічно адаптується до результатів оцінки ризику та поточного рівня довіри до запиту. Це дозволяє балансувати між рівнем безпеки та зручністю користувача, не вимагаючи завжди максимальної багатофакторної автентифікації.

Backchannel Authentication Core (BAC) реалізує протокол CIBA. Саме цей модуль встановлює зв’язок з постачальником ідентичності (IdP), надсилає запит на підтвердження авторизації користувачу через мобільний додаток чи інший канал, та очікує відповіді. BAC працює асинхронно, що дозволяє продовжити інші перевірки без затримки відповіді користувача.

Security Decision Layer (SDL) приймає остаточне рішення щодо авторизації запиту на основі інформації від CRE, APE та BAC. SDL може відхилити запит, перевести його у режим додаткової перевірки, або надати доступ. Це ядро логіки

системи, яке забезпечує відповідність загальній політиці інформаційної безпеки установи.

Audit & Trace Logger (ATL) фіксує всі ключові події та дії, включаючи запити, відповіді, рішення про авторизацію, зміну політик і ризикові індикатори. ATL необхідний як для внутрішнього аудиту, так і для зовнішніх перевірок (зокрема, у відповідності до вимог GDPR, PCI DSS тощо).

Механізм обробки запитів на авторизацію в системі CIBA-SHIELD є важливою частиною архітектури, яка забезпечує безпечний і ефективний процес верифікації користувачів без необхідності для них вводити дані авторизації на кожному етапі транзакції. Механізм базується на інтеграції з протоколом CIBA (Client Initiated Backchannel Authentication), що дозволяє виконувати авторизацію через канали зворотного зв'язку без необхідності взаємодії користувача з інтерфейсом авторизації.

Коли користувач ініціює дію, що потребує авторизації (наприклад, здійснення фінансової транзакції), клієнтська система (мобільний додаток або веб-клієнт) відправляє запит на авторизацію до Frontend Authorization Request Handler (FARH). У цьому запиті передаються дані, що описують контекст транзакції, тип операції та ідентифікаційні дані користувача.

Після отримання запиту FARH передає його до Contextual Risk Evaluator (CRE), який здійснює оцінку контексту запиту. Оцінка включає перевірку параметрів, таких як геолокація, IP-адреса, час доби, тип пристрою користувача, його попередня активність та інші фактори, які можуть вплинути на рівень ризику транзакції. Якщо CRE визначає, що ризик надзвичайно високий, запит може бути направлений на подальшу перевірку або додаткову авторизацію.

Adaptive Policy Engine (APE) є компонентом, що формує адаптивну політику авторизації. На основі результатів оцінки ризику від CRE та інших поточних даних, APE визначає найбільш підходящий механізм авторизації для кожного запиту. Це може бути стандартна одноразова авторизація або додаткові фактори підтвердження, такі як відправлення SMS-коду або використання біометричних даних.4. Виконання бекенд-авторизації

Якщо APE визначає, що для запиту потрібно виконати бекенд-авторизацію, запит передається до Backchannel Authentication Core (BAC). Цей компонент ініціює запит до постачальника ідентичності (Identity Provider, IdP), через який здійснюється підтвердження авторизації за допомогою каналу зворотного зв'язку. Користувач отримує сповіщення через мобільний додаток або інші засоби, і підтверджує свою дію.

Після того як користувач підтверджує або відхиляє авторизацію, відповідь надходить до Security Decision Layer (SDL). Це ядро логіки системи, яке приймає остаточне рішення щодо авторизації запиту на основі інформації від CRE, APE і BAC. SDL може прийняти рішення про надання доступу, додаткову перевірку або відхилення запиту. У випадку відхилення запиту система може відправити сповіщення користувачеві про відмову в авторизації.

Всі дії, пов'язані з обробкою запиту на авторизацію, фіксуються в Audit & Trace Logger (ATL). Цей компонент записує усі зміни станів запиту, рішення про авторизацію, а також будь-які аномалії або відхилення. Запис про дії може бути використаний для подальшого аудиту, аналізу подій безпеки та забезпечення відповідності вимогам безпеки та регуляцій.

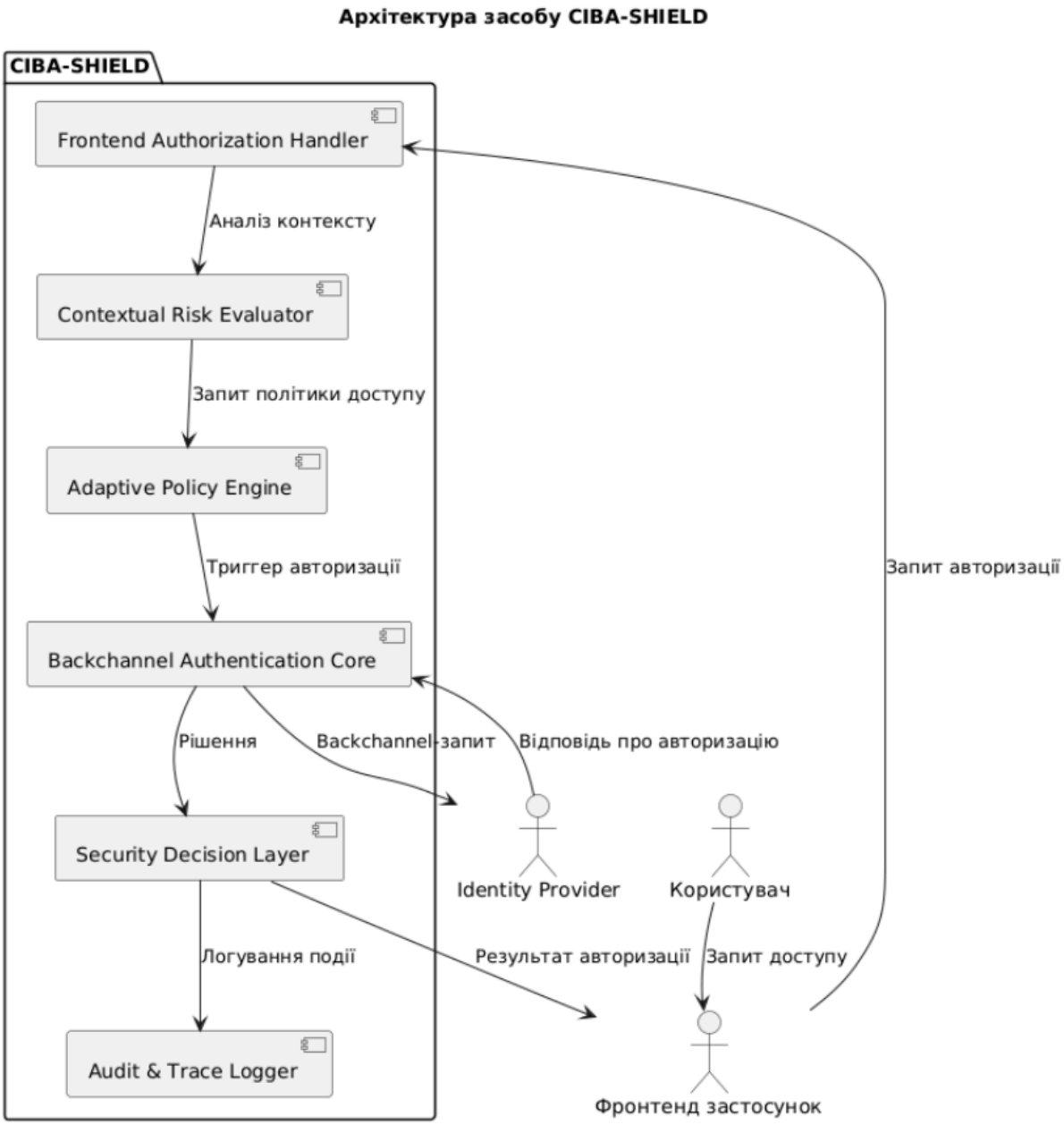

Рисунок 5.2 Архітектурна схема засобу CIBA-SHIELD для серверної авторизації в інтернет-банкінгу

Для візуалізації взаємозв’язків між компонентами та ролями в системі CIBA-SHIELD доцільно представити архітектурну схему, яка демонструє логіку обробки запитів на авторизацію через бекенд-канал з урахуванням багатоконтекстного аналізу. На ній відображено основні функціональні модулі засобу, включно з адаптивною системою політик, аналізом ризиків, ядром обробки авторизації, а також взаємодією з зовнішніми учасниками, такими як користувач, фронтенд-застосунок та провай

5.3 Алгоритм роботи та логіка реагування

Процес ініціації запиту на авторизацію у системі CIBA-SHIELD починається з боку клієнтської програми, яка виступає ініціатором взаємодії між користувачем та сервером авторизації. Особливістю цієї моделі є те, що авторизація виконується без прямої участі браузера чи фронтенд-клієнта, тобто користувач не взаємодіє з банківським вебінтерфейсом у момент входу. Замість цього ініціатор (наприклад, бекенд мобільного застосунку) надсилає авторизаційний запит безпосередньо до сервера авторизації через стандартизований endpoint протоколу CIBA.

Ключовим елементом на цьому етапі є формування унікального ідентифікатора запиту auth_req_id, який дозволяє ідентифікувати конкретну сесію авторизації, відстежувати її стан у часі та пов'язати запит із конкретним користувачем. Запит містить необхідні атрибути — ідентифікатор клієнта, запитувані області доступу (scope), інформацію про кінцевого користувача (login_hint) та інші параметри, передбачені специфікацією OpenID Connect.

На цьому етапі запит також передається до модуля CIBA-SHIELD, де здійснюється попередня фіксація запиту та підготовка до багатоконтекстної перевірки. Це дозволяє реалізувати «контроль у точці входу» до подальших етапів авторизації. Таким чином, ще до участі користувача система має змогу відфільтрувати потенційно небезпечні або аномальні запити.

Такий підхід значно знижує ризик несанкціонованого доступу, адже дозволяє виконати оцінку запиту до того, як буде надана можливість підтвердження з боку користувача, а також підвищує ефективність обробки запитів завдяки попередній валідації та реєстрації у внутрішній черзі обробки.

Після формування авторизаційного запиту на стороні клієнта (наприклад, бекенд-застосунку банку), запит передається до сервера авторизації, який інтегровано з модулем CIBA-SHIELD. Цей модуль виступає як проміжний фільтр і логічний шлюз між зовнішніми клієнтами та внутрішніми компонентами інфраструктури авторизації банку.

Запит передається з використанням захищеного каналу зв’язку — переважно через HTTPS із обов’язковою двосторонньою TLS-автентифікацією. Це забезпечує цілісність і автентичність переданої інформації. На цьому етапі відбувається повна десеріалізація даних та формування внутрішнього представлення запиту, яке адаптоване до специфіки обробки CIBA-SHIELD.

CIBA-SHIELD виконує початкову верифікацію запиту, зокрема перевірку валідності client_id, відповідності параметрів scope, а також наявності обов’язкових полів, передбачених протоколом OpenID Connect. У разі виявлення відхилень запит автоматично відхиляється, а відповідний запис про спробу зберігається у журналі безпеки.

Окрім технічної перевірки, запит реєструється у тимчасовій черзі обробки, яка використовується для організації асинхронного виконання наступних етапів авторизації. Це дозволяє CIBA-SHIELD масштабувати обробку великої кількості паралельних запитів без втрати ефективності та реагування в режимі реального часу.

Після успішної валідації запиту CIBA-SHIELD ініціює запуск багатоконтекстної перевірки та формує унікальний auth_req_id, який надсилається клієнту для подальшого відстеження статусу авторизації.

Багатоконтекстна перевірка в системі CIBA-SHIELD є одним з ключових етапів захисту, що відрізняє запропонований засіб від класичних реалізацій CIBA. Її основна мета — не просто підтвердити автентичність користувача, а оцінити надійність запиту з урахуванням широкого спектра контекстуальних параметрів, притаманних конкретній сесії, пристрою та поведінці користувача.

Після проходження початкової технічної перевірки авторизаційний запит потрапляє до модуля багатоконтекстної оцінки, де відбувається кореляція з такими факторами:

Географічне положення: аналізується відповідність поточного місцезнаходження користувача типовим шаблонам (наприклад, країна, IP-діапазон, GPS).

Пристрій доступу: здійснюється ідентифікація пристрою та перевірка його довіреності (Trusted Device List), а також наявність змін у конфігурації.

Часовий контекст: оцінюється, чи відповідає час авторизації звичайній активності користувача (наприклад, чи не виконується запит у нічний час або у неробочі дні).

Поведінкові шаблони: використовується AI-модуль, який порівнює поточну поведінку із історичною моделлю користувача (наприклад, швидкість взаємодії, типові дії, частота запитів).

Рівень довіри до клієнта: враховується історія попередніх авторизацій, частота відхилень, успішні й підозрілі сесії.

Кожен із зазначених параметрів оцінюється за допомогою системи балів ризику, що виводить інтегральний ризик-фактор авторизації. У разі перевищення допустимого порогу система або блокує запит, або переводить його на додаткову перевірку — наприклад, підтвердження через незалежний канал (SMS, push, e-mail).

Таким чином, багатоконтекстна перевірка у CIBA-SHIELD дозволяє не лише виконати авторизацію, але й зробити це з урахуванням індивідуального профілю користувача, що підвищує як рівень безпеки, так і захист від соціальної інженерії чи автоматизованих атак.

Після завершення багатоконтекстної перевірки авторизаційний запит у системі CIBA-SHIELD передається до модуля прийняття рішень. Цей етап є критичним, оскільки саме тут формується остаточний вердикт щодо доцільності продовження авторизації або її відхилення. Рішення базується на сукупному аналізі ризик-факторів, отриманих із попередніх етапів, та налаштуваннях політик безпеки, заданих адміністратором системи.

У процесі прийняття рішення враховуються такі ключові елементи:

Зведений ризиковий індекс: результат інтегральної оцінки контекстуальних та поведінкових параметрів.

Політика реакції на рівні сервісу: наприклад, фінансові транзакції можуть мати нижчий допустимий ризиковий поріг, ніж перегляд балансу.

Наявність історії підозрілих дій у користувача: навіть при помірному ризику система може обрати більш консервативну стратегію.

Тип запитуваного ресурсу або дії: авторизація для критично важливих операцій потребує додаткових перевірок.

Залежно від результату система CIBA-SHIELD може прийняти одне з трьох базових рішень:

Авторизацію дозволено — запит проходить до наступного етапу обробки, що передбачає видачу access token або повідомлення клієнту про успішну авторизацію.

Авторизацію тимчасово призупинено — користувача просять пройти додаткову перевірку, наприклад, підтвердити особу через альтернативний канал або повторно верифікувати пристрій.

Авторизацію відхилено — запит заблоковано, а на сервер надсилається повідомлення про невдалу авторизацію із зазначенням причини.

Таке рішення фіксується у журналі дій системи, що забезпечує прозорість та подальший аудит. Крім того, у випадку незвичайних або масових аномалій CIBA-SHIELD може автоматично активувати процедуру інцидентного реагування відповідно до заздалегідь визначених правил.

Таким чином, модуль прийняття рішень у CIBA-SHIELD забезпечує баланс між безпекою та зручністю, адаптуючи реакцію системи до конкретного сценарію загроз.

Після того як система CIBA-SHIELD приймає рішення щодо продовження процесу авторизації, ініціюється взаємодія з користувачем через вибраний канал підтвердження. У цьому підрозділі розглядається, як відбувається отримання, перевірка та обробка відповіді користувача, що є ключовим етапом серверної авторизації за моделлю CIBA.

У типовому сценарії сервер надсилає повідомлення або запит на підтвердження на мобільний пристрій, що був зареєстрований у профілі користувача. Повідомлення може надходити через захищений мобільний додаток банку, SMS з кодом, push-сповіщення або месенджер із криптографічним підписом. Усі варіанти доставки інтегруються з CIBA-SHIELD за допомогою адаптерів повідомлень, що гарантують надійність та шифрування.

Користувач, отримавши запит, має підтвердити або відхилити авторизацію, використовуючи один із доступних способів — наприклад, відбиток пальця, Face ID або введення PIN-коду. Відповідь користувача пересилається на бекенд через захищений транспортний канал (наприклад, mTLS або HTTPS з JWT). На цьому етапі CIBA-SHIELD проводить валідацію відповіді, перевіряючи:

Автентичність пристрою, з якого надійшла відповідь.

Часову дійсність запиту (відповідь має надійти у межах визначеного TTL).

Цілісність відповіді (використання цифрових підписів або HMAC).

Відповідність відповідного коду авторизації до поточної сесії запиту.

У разі успішної перевірки відповідь користувача фіксується в системі, і CIBA-SHIELD завершує авторизацію, видаючи відповідь клієнтському додатку (наприклад, OAuth 2.0 Token Response).

Якщо відповідь некоректна, відсутня, або виявлена спроба фальсифікації, система фіксує подію як інцидент, а запит на авторизацію завершується з відповідним повідомленням про помилку. У критичних випадках можлива активація блокувальних механізмів або тимчасова ізоляція акаунта.

Таким чином, обробка відповіді користувача у CIBA-SHIELD не тільки завершує цикл серверної авторизації, а й виступає ключовим етапом, що поєднує безпеку, гнучкість багатоконтекстного аналізу та зручність для користувача.

Після отримання, перевірки та обробки відповіді користувача на запит авторизації, система CIBA-SHIELD переходить до завершального етапу — ухвалення остаточного рішення щодо надання або відмови в доступі до захищених ресурсів. Цей етап має критичне значення з точки зору як безпеки, так і відповідності стандартам відкритої авторизації (OpenID Connect та OAuth 2.0).

У випадку, якщо багатоконтекстна перевірка та відповідь користувача визнані валідними, система CIBA-SHIELD ініціює генерацію токена доступу (Access Token), а за потреби — і оновлювального токена (Refresh Token) та ID Token. Ці токени створюються модулем токенізації з урахуванням таких параметрів:

Scope запиту, що визначає, до яких ресурсів надається доступ.

Рівень довіри до пристрою та сесії, встановлений у результаті поведінкового аналізу.

Політики доступу, сформовані Policy Engine на основі контексту (наприклад, геолокація, час, історія входів).

Термін дії токенів, що визначається згідно з ризик-профілем транзакції.

Сформовані токени мають цифрові підписи відповідно до стандарту JWT (JSON Web Token), шифруються та передаються до клієнтського застосунку через канал зворотного зв’язку, ініційований банківським сервером (CIBA backchannel). Це дозволяє уникнути відкритої передачі облікових даних, мінімізуючи вразливості класичних авторизаційних фреймворків.

У разі, якщо система виявляє аномалії, відсутність підтвердження, або отримує негативну відповідь користувача, CIBA-SHIELD фіксує запит як невдалий. У відповідь видається стандартизоване повідомлення про помилку авторизації (наприклад, access_denied, unauthorized_user, device_untrusted), що унеможливлює продовження процедури доступу. Також активуються відповідні політики безпеки, включаючи повідомлення адміністратору, блокування сесії або додаткову перевірку.

Таким чином, фінальна фаза CIBA-авторизації забезпечує криптографічно захищене завершення транзакції з максимальним урахуванням ризиків, контексту й рішень користувача, реалізуючи стратегію «zero-trust access» у середовищі інтернет-банкінгу.

Ефективний аудит і логування є ключовими елементами засобу CIBA-SHIELD, що забезпечують як контроль безпеки, так і дотримання регуляторних вимог. У контексті серверної авторизації, особливо в інтернет-банкінгу, важливо не лише забезпечити доступ, а й гарантувати, що всі дії задокументовані для подальшого аналізу, верифікації та розслідування потенційних інцидентів.

Система CIBA-SHIELD реалізує централізовану модель логування, що охоплює всі критичні етапи життєвого циклу авторизаційного запиту: від його ініціації до видачі токена або відмови в доступі. До журналів логування вносяться такі категорії подій:

Відомості про ініціатора запиту (ID пристрою, IP-адреса, ідентифікатор користувача);

Час і контекст запиту;

Результати багатоконтекстної перевірки;

Проміжні рішення системи (наприклад, результат поведінкового аналізу);

Відповідь користувача та її результат;

Стан авторизації (успішна/відмова);

Всі виняткові ситуації або помилки обробки.

Записи ведуться у структурованому форматі (наприклад, JSON або XML), що дозволяє їх легко інтегрувати з зовнішніми системами SIEM (Security Information and Event Management) для централізованого моніторингу. Для забезпечення достовірності журналів застосовуються криптографічні засоби захисту: підпис подій, контроль цілісності та захист від несанкціонованого доступу.

Також передбачена можливість асинхронної реплікації логів на захищені вузли для резервного збереження та відновлення у разі компрометації головної системи.

Логування слугує також основою для машинного навчання — на основі накопичених даних система вдосконалює поведінкові моделі, формує адаптивні політики безпеки та виявляє довгострокові аномалії. Таким чином, підсистема аудиту та логування в CIBA-SHIELD виконує не лише пасивну, але й активну роль у захисті інформаційної інфраструктури.

Для кращого розуміння логіки функціонування CIBA-SHIELD у контексті обробки запитів авторизації пропонується блок-схема, що ілюструє ключові етапи взаємодії між компонентами системи. Діаграма демонструє основні кроки: ініціацію запиту, багатоконтекстну перевірку, ухвалення рішення, обробку відповіді користувача та генерацію або відмову у видачі токена. Такий візуальний підхід дозволяє наочно простежити логіку реагування засобу у режимі реального часу.

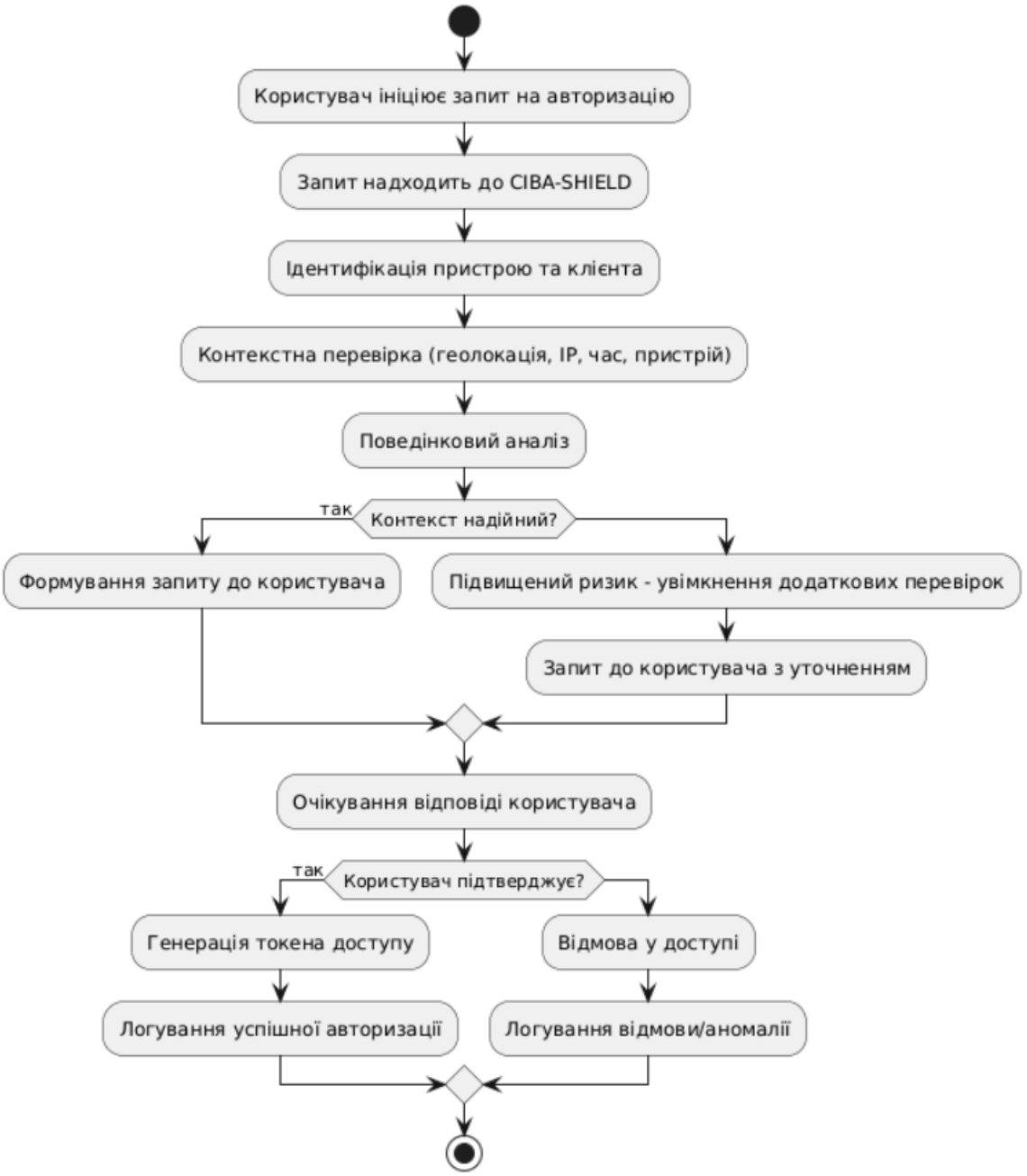

Рисунок 5.3 Алгоритм обробки авторизаційного запиту в системі CIBA-SHIELD

Ця діаграма дозволяє чітко прослідкувати адаптивну природу CIBA-SHIELD, зокрема здатність змінювати поведінку залежно від контексту запиту, що є ключовим елементом сучасних засобів інформаційної безпеки.

Висновки до розділу 5

У цьому розділі було розроблено інноваційний засіб CIBA-SHIELD, що розширює стандартний протокол авторизації CIBA за рахунок інтеграції багатоконтекстної поведінкової перевірки. Запропонована архітектура забезпечує захист від атак на рівні бекенд-авторизації, де класичні засоби контролю доступу є недостатніми.

Було визначено ключові компоненти системи, серед яких: модуль обробки запитів, багатоконтекстний аналізатор, модуль аудиту та генератор токенів доступу. Алгоритм роботи CIBA-SHIELD орієнтований на адаптивне прийняття рішень на основі сукупного аналізу поведінкових, контекстуальних та технічних параметрів запиту.

Особливістю засобу є можливість функціонування без безпосередньої участі користувача, що дозволяє автоматизувати прийняття рішень про авторизацію в умовах високих навантажень, забезпечуючи при цьому збереження високого рівня інформаційної безпеки.

Таким чином, CIBA-SHIELD є ефективним засобом поведінкової безпеки, що дозволяє виявляти аномальні сценарії на етапі бекенд-авторизації та реагувати на них без затримок, що є критично важливим для захисту сучасних банківських сервісів.

ВИСНОВКИ

У кваліфікаційній роботі було досліджено та реалізовано інноваційний підхід до підвищення рівня інформаційної безпеки в системах інтернет-банкінгу, що базується на розробці методу мікросегментованої динамічної ізоляції сесій (MiDIS) та засобу безпечної бекенд-авторизації з багатоконтекстною перевіркою (CIBA-SHIELD).

Аналіз сучасних загроз у сфері фінансових онлайн-сервісів засвідчив зростаючу складність та динаміку атак, зокрема під час активних сесій користувача або при неінтерактивній авторизації. Існуючі механізми безпеки, орієнтовані переважно на фронтенд-автентифікацію або статичні правила контролю доступу, є недостатніми для ефективної протидії новітнім сценаріям атак.

Запропонований метод MiDIS дозволяє поділити активну сесію на незалежні сегменти з окремими політиками безпеки, що уможливлює локалізацію ризиків, автоматичну реакцію на аномалії та збереження користувацького досвіду без повного завершення сесії. Його архітектура реалізує принципи гнучкої адаптивної безпеки з використанням поведінкового аналізу в реальному часі.

Засіб CIBA-SHIELD, у свою чергу, розширює стандарт протоколу CIBA, дозволяючи перевіряти запити авторизації у бекенді з урахуванням множини контекстів: часу, геолокації, профілю пристрою, а також історії поведінки. Це дозволяє підвищити захищеність автоматизованих транзакцій та авторизаційних потоків без залучення користувача, що особливо актуально для мобільного банкінгу та Open Banking API.

Результати роботи підтверджують, що комплексне застосування розроблених методу і засобу дозволяє значно підвищити рівень інформаційної безпеки в інтернет-банкінгу, зберігаючи при цьому високу зручність користування. Реалізовані рішення можуть бути інтегровані у сучасні банківські платформи як доповнення до існуючих систем захисту або як окрема поведінкова лінія безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] VPN Unlimited. "Безпека онлайн-банкінгу". Доступно: https://www.vpnunlimited.com/ua/help/cybersecurity/online-banking-security

[2] NNCIT WUNU. "10 простих порад для безпеки у мережі Інтернет". Доступно: https://nncit.wunu.edu.ua/10-prostih-porad-dlya-bezpeki-u-merezhi-internet

[3] My IT Specialist. "Сучасні кіберзагрози для фінансових установ та методи їх захисту". Доступно: https://my-itspecialist.com/modern-cyber-threats-to-financial-institutions-and-effective-methods-of-their-protection

[4] ITpedia. "Безпечна система Інтернет-банкінгу". Доступно: https://uk.itpedia.nl/2022/08/22/secure-internet-banking-system

[5] UFIN. "Вразливості програмного забезпечення у банківській сфері". Доступно: https://ufin.com.ua/analit_mat/gkr/171.htm

[6] Rating Zone. "Зростання загроз для фінансового сектору". Доступно: https://rating.zone/chem-obernetsia-dlia-ukrayny-rekordnyj-rost-tsen-na-syrevye-tovary

[7] NNCIT WUNU. "Безпека використання мереж Wi-Fi". Доступно: https://nncit.wunu.edu.ua/10-prostih-porad-dlya-bezpeki-u-merezhi-internet

[8] BankInfoSecurity. "Biometric Authentication in Banking". Доступно: https://www.bankinfosecurity.com/biometric-authentication-in-banking-a-12246

[9] IBM Security. "Facial Recognition in Online Banking". Доступно: https://www.ibm.com/security/facial-recognition-in-banking

[10] Cybersecurity Magazine. "Behavioral Authentication Trends". Доступно: https://www.cybersecuritymag.com/behavioral-authentication-trends

[11] IBM Security. "Data Encryption for Banking Security". Доступно: https://www.ibm.com/security/data-encryption-for-banking

[12] HSM World. "Hardware Security Modules in Banking". Доступно: https://www.hsmworld.com/banking-security-modules

[13] Cybersecurity Magazine. "Intrusion Detection Systems for Banks". Доступно: https://www.cybersecuritymag.com/intrusion-detection-for-banking

[14] Check Point. "Next-Generation Firewalls in Financial Security". Доступно: https://www.checkpoint.com/next-generation-firewall-banking

[15] BankInfoSecurity. "Multi-Factor Authentication in Banking". Доступно: https://www.bankinfosecurity.com/mfa-in-banking

[16] Microsoft Security. "Passwordless Authentication for Financial Services". Доступно: https://www.microsoft.com/security/passwordless-authentication-banking

[17] FinTech Futures. "AI and Machine Learning in Fraud Detection". Доступно: https://www.fintechfutures.com/ai-fraud-detection

[18] Mobile Banking Security. "Secure Mobile Banking Applications". Доступно: https://www.mobilebankingsecurity.com/secure-apps

[19] SIEM Today. "Security Information and Event Management for Banks". Доступно: https://www.siemtoday.com/banking-siem

[20] IBM Security. "AI-Powered Cybersecurity in Banking". Доступно: https://www.ibm.com/security/ai-cybersecurity-banking

[21] FinTech Futures. "Machine Learning for Fraud Detection in Banking". Доступно: https://www.fintechfutures.com/ml-fraud-detection

[22] "Neural Networks for Anomaly Detection". Доступно: https://www.cybersecuritymag.com/neural-networks-anomaly-detection

[23] BankInfoSecurity. "Behavioral Biometrics in Online Banking". Доступно: https://www.bankinfosecurity.com/behavioral-biometrics-banking

[24] Microsoft Security. "AI for Phishing Detection and Prevention". Доступно: https://www.microsoft.com/security/ai-phishing-detection

[25] Mobile Banking Security. "AI-Driven Risk-Based Authentication". Доступно: https://www.mobilebankingsecurity.com/ai-risk-authentication

[26] Cyber Defense Magazine. "Using AI to Combat Banking Bots". Доступно: https://www.cyberdefensemagazine.com/ai-banking-bots

[27] SIEM Today. "AI-Powered Security Event Management". Доступно: https://www.siemtoday.com/ai-security-event-management

[28] Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2020.

[29] Bishop, M. Computer Security: Art and Science. Addison-Wesley, 2018.

[30] Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2021.

[31] Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, 2012.

[32] Kaspersky Lab. Global IT Security Risks Survey. Kaspersky, 2022.

[33] Schneier, B. Secrets and Lies: Digital Security in a Networked World. Wiley, 2015.

[34] Bonneau, J., Caesar, M., Borisov, N., & Wang, X. The Tangled Web of Password Reuse. Network and Distributed System Security Symposium (NDSS), 2014.

[35] Bojinov, H., Michalevsky, Y., Nakibly, G., & Boneh, D. Mobile Device Fingerprinting via Motion Sensors. USENIX Security Symposium, 2014.

[36] PlantUML Online Editor [Електронний ресурс]. – Доступно: https://editor.plantuml.com/

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

Тези наукових доповідей

1. Кускова Анна, Микола Браіловський Метод та засіб забезпечення інформаційної безпеки в системах інтернет- банкінгу VIII Міжнародна науково-практична конференції “Проблеми кібербезпеки інформаційно-комунікаційних систем” (PCSICS)