

ПОРІВНЯННЯ МЕТОДІВ АУТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ В БАНКІВСЬКИХ СИСТЕМАХ. ПОЄДНАННЯ АВТОРИЗАЦІЇ НА ОСНОВІ RBA ТА IDENTITY SERVER

Вінницький національний технічний університет

Анотація

У статті досліджено, описано та проаналізовано порівняння методів аутентифікації та авторизації в банківських системах та описано переваги поєднання методів авторизації на основі поєднання RBA та IDENTITY SERVER.

Ключові слова: банківська система, система, клієнт-сервер, аутентифікації, авторизації.

Abstract

The article investigates, describes and analyzes the comparison of authentication and authorization methods in banking systems and describes the advantages of combining authorization methods based on the combination of RBA and IDENTITY SERVER.

Key words: banking system, system, client-server, authentication, authorization.

Мета

Метою даного дослідження є здійснення порівняльного аналізу сучасних методів аутентифікації та авторизації в банківських системах, визначення їх переваг та недоліків, а також обґрунтування ефективності впровадження комбінованого підходу на основі Role-Based Authorization (RBA) та технології Identity Server для підвищення безпеки та зручності доступу до банківських ресурсів.

Вступ

У сучасній банківській сфері, на тлі зростання кількості кіберзагроз і складності цифрових атак, особливої ваги набуває питання забезпечення надійної автентифікації та авторизації користувачів. Вимоги до безпеки фінансових систем постійно підвищуються, що спонукає банки шукати та впроваджувати інноваційні методи управління доступом до ресурсів. Одним із перспективних напрямів є застосування комбінованих підходів, зокрема поєднання авторизації на основі ролей (Role-Based Authorization, RBA) із централізованими рішеннями для керування ідентифікацією користувачів, такими як Identity Server.

Використання комплексних підходів до авторизації є важливим напрямом для забезпечення належного рівня захисту банківських даних, оптимізації процесів адміністрування прав доступу та відповідності регуляторним стандартам. Водночас інтеграція таких методів у фінансових установах вимагає аналізу наявних технологій та оцінки можливостей їх застосування в умовах сучасної банківської інфраструктури. У зв'язку з цим актуальним є дослідження, що присвячене порівнянню методів автентифікації та авторизації, а також можливості їхнього поєднання, зокрема шляхом використання авторизації на основі ролей (RBA) та технології Identity Server.[1]

Перспективи використання технологій розгортання у хмарі у розробці інформаційних систем для підтримки банківських транзакцій

Аналіз підходів до автентифікації та авторизації користувачів у банківських системах має велике значення для забезпечення належного захисту фінансових операцій та конфіденційності даних. В умовах постійного зростання загроз цифрової безпеки фінансові установи змушені використовувати різні методи і технології контролю доступу, що здатні протидіяти сучасним викликам кібербезпеки.

Сьогодні банки інтенсивно цифровізують свої послуги, активно переходячи до мобільних і веб-додатків, що робить питання автентифікації та авторизації ще більш актуальним. Збільшення кількості дистанційних транзакцій та постійне використання клієнтами різноманітних пристроїв потребують

впровадження гнучких, адаптивних і водночас надійних механізмів контролю доступу.

До найважливіших факторів, які впливають на вибір технологій авторизації та автентифікації, належать рівень безпеки, зручність для користувача, швидкість обробки запитів та відповідність жорстким регуляторним вимогам фінансового сектору. Саме тому аналіз сучасних підходів, що дозволяють одночасно досягти балансу між безпекою та комфортом користувачів, є ключовим завданням при розробці банківських цифрових платформ.

Банківські цифрові сервіси використовують різноманітні технології підтвердження особи та управління доступом, що забезпечують захист фінансової інформації клієнтів. Серед найбільш поширених виділяють такі підходи:

1. Автентифікація за одним фактором (Single-factor authentication, SFA) – базується лише на одному засобі ідентифікації користувача, переважно паролі. Цей метод популярний через простоту реалізації, але характеризується високим ризиком витоку даних через фішинг та несанкціонований доступ.
2. Багатофакторна автентифікація (Multi-factor authentication, MFA) – передбачає одночасне використання декількох способів ідентифікації, таких як тимчасові коди (OTP), біометричні ознаки (відбитки пальців, Face ID) або спеціальні фізичні пристрої (токени). Цей спосіб значно підвищує безпеку, проте може бути менш зручним для користувачів через додаткові кроки підтвердження.
3. Рольове управління доступом (Role-Based Access Control, RBAC) – надає права доступу залежно від того, яку роль займає користувач у банківській системі. Така модель широко використовується в корпоративних фінансових середовищах для регулювання доступу до певних операцій та функцій.
4. Контекстно-залежна автентифікація (Context-Aware Authentication) – враховує додаткові характеристики та умови входу користувача, включаючи місце розташування, тип пристрою чи IP-адресу. За виявлення підозрілої активності система може запитувати додаткову перевірку особистості.
5. Автентифікація на основі оцінки ризиків (Risk-Based Authentication, RBA) – підхід, що передбачає динамічний аналіз кожної спроби доступу та зміну рівня перевірки залежно від потенційних ризиків у конкретній ситуації.[2]

У межах даного дослідження запропоновано інтеграцію Identity Server та RBA для вдосконалення механізму контролю доступу в банківських додатках. Identity Server використовується як централізоване рішення для автентифікації, що реалізує стандарти OpenID Connect та OAuth 2.0, тоді як RBA здійснює аналіз ризиків в режимі реального часу та адаптивно регулює необхідність додаткових етапів перевірки для менш ризикових сценаріїв.

Комбінація цих технологій може забезпечити більш комфортний процес автентифікації, скорочуючи витрати часу користувачів, а також покращити стійкість до шахрайських дій. Для ілюстрації ключових характеристик описаних методів нижче наведено порівняльну таблицю.[3][4]

Таблиця 1. - Порівняння методів авторизації

Метод	Рівень безпеки	Зручність для користувача	Масштабованість	Вплив на продуктивність системи
Однофакторна автентифікація (SFA)	Низький – залежність від пароля, високий ризик злому	Висока – проста у використанні, але слабкий захист	Низька – не забезпечує централізованого управління	Мінімальний – не потребує значних ресурсів
Багатофакторна автентифікація (MFA)	Середній – підвищений захист за рахунок додаткових факторів	Низька – потребує додаткових дій при кожному вході	Середня – вимагає налаштування додаткових сервісів	Середній – додаткові перевірки можуть уповільнювати роботу
Рольова модель доступу (RBAC)	Середній – контроль на рівні ролей, без оцінки ризиків	Середня – не змінює процес автентифікації, але вимагає	Висока – легко інтегрується у великі системи	Низький – вплив мінімальний, але контроль доступу фіксований

		адміністрування		
Контекстна автентифікація (Context-Aware Authentication)	Високий – врахування контекстних факторів для підвищення безпеки	Середня – вимагає доступу до контекстних даних користувача	Середня – потребує значних ресурсів для аналізу контексту	Середній – потребує аналізу контекстних факторів
Risk-Based Authentication (RBA)	Високий – динамічний аналіз ризиків перед автентифікацією	Висока – підвищена безпека без додаткових дій, якщо ризик низький	Висока – автоматична адаптація рівня автентифікації	Високий – використовує складні алгоритми оцінки ризиків
Identity Server (без RBA)	Високий – централізоване управління доступом, але без адаптивного аналізу ризиків	Середня – потребує ручного налаштування політик доступу, але зменшує навантаження на користувача	Висока – підтримує розподілену автентифікацію та керування доступом	Середній – обробка запитів через центральний сервер може створювати затримки при високих навантаженнях
Identity Server + RBA (запропонований метод)	Дуже високий – забезпечує централізовану автентифікацію та адаптивний контроль ризиків, але вразливий до хибних позитивних результатів	Висока – автоматична перевірка ризиків, однак можливі затримки при зміні поведінки користувача	Висока – централізоване управління та можливість динамічного регулювання рівня безпеки	Оптимізований – поєднання кешування токенів та адаптивної автентифікації мінімізує затримки

Висновки

У підсумку проведеного аналізу можна визначити, що впровадження комбінованих методів автентифікації та авторизації є важливим і перспективним напрямом у розвитку сучасних банківських систем. Застосування інтегрованих рішень, таких як Identity Server разом із адаптивною авторизацією на основі аналізу ризиків (RBA), забезпечує необхідний рівень безпеки фінансових операцій і суттєво знижує ймовірність шахрайських дій. Крім того, такі рішення дозволяють оптимізувати процедуру доступу користувачів, покращуючи зручність та прискорюючи процеси автентифікації для клієнтів.

Важливим аспектом є також висока масштабованість і централізованість управління доступом, яку забезпечує використання Identity Server у поєднанні з RBA. Це дозволяє банківським установам ефективніше реагувати на зростаючі навантаження, зберігаючи високий рівень продуктивності системи та відповідність сучасним регуляторним стандартам. Водночас, впровадження таких рішень потребує ретельного налаштування політик доступу та контролю ризиків, що вимагає додаткових ресурсів на етапі планування й інтеграції.

Таким чином, поєднання RBA та Identity Server відкриває значні можливості для підвищення ефективності й безпеки банківських цифрових платформ. Банки, що впроваджують подібні інновації, отримують конкурентні переваги завдяки покращенню захисту інформації клієнтів та оптимізації процесів доступу, що позитивно впливає на користувацький досвід і сприяє зміцненню позицій на фінансовому ринку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Усік П.С., Буравченко К.О. "Безпека банківських систем". [Електронний ресурс]. Режим доступу: <https://dspace.kntu.kr.ua/server/api/core/bitstreams/29a2e041-c31e-44d9-b074-a26dfddfa97d/content>
2. Authorization basics. [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-gb/entra/identity-platform/authorization-basics>

3. Identity Server 4 The big Picture.. [Електронний ресурс]. – Режим доступу: https://docs.duendesoftware.com/identityserver/v7/overview/big_picture/
4. Identity Server 4 Terminology [Електронний ресурс]. – Режим доступу: <https://docs.duendesoftware.com/identityserver/v7/overview/terminology/>

Курніцький Дмитро Петрович – аспірант кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця, dmytro.kurnitskiy@gmail.com

Kurnitsky Dmytro P. – student of 11ST-17b, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia, dmytro.kurnitskiy@gmail.com