УДК 336.71

**М. А. Томчук**
**С. А. Риндін**

# ПРИНЦИПИ ЗАХИСТУ ТРАНЗАКЦІЙ У БАНКІВСЬКІЙ СИСТЕМІ

Вінницький національний технічний університет

***Анотація:*** *В статті розглянуто систему і принципи захисту банків від шахрайства у транзакціях.*
***Ключові слова****: банк, антифрод, шахрайство, транзакції.*

## THE PRINCIPLES OF PROTECTING TRANSACTIONS IN THE BANKING SYSTEM

***Abstract:*** *The article deals with the system and principles of bank protection from fraud in transactions.*
***Keywords****: bank, anti-fraud, fraud, transactions.*

Виявлення і протидія шахрайським операціям — одне з головних завдань усіх міжнародних платіжних систем. Безпеку онлайн-платіжних транзакцій відслідковують безліч систем на різних рівнях і етапах проходження платежу.

Антифрод або фрод-моніторинг — система, призначена для оцінки фінансових транзакцій в інтернеті на предмет підозрілості з точки зору шахрайства, пропонуючи рекомендації щодо їх подальшої обробки. Як правило, сервіс антифроду складається з стандартних та унікальних правил, фільтрів та списків, по яким і перевіряється кожна транзакція [1].

Такі системи, завдяки комплексному контролю й обміну даними з іншими банками, викривають сотні злочинних, шахрайських угрупувань, що працюють у різних країнах світу, які скоїли злочини з використанням платіжних карток. Моніторинг і антифрод-контроль здійснюються в автоматичному і ручному режимах.

Не дивлячись на різні алгоритми які реалізовані в кожному продукті, загальні принципи на яких працює анти-фрод система залишаються незмінними. Перш за все це пошук аномалій (нетипових подій, дій користувача) в часто повторюваних операціях з великим масивом даних. Більшість систем за замовчуванням матимуть типовий набір дій, які далі потрібно адаптувати під кожен окремий випадок.

У кожному окремому конкретному випадку набір аналізованих даних для анти-фрод системи буде різним. Вибір насамперед залежить від специфіки роботи самої компанії в якій встановлена система, так для банку це один набір даних, для телеком-оператора інший. В цілому ці дані збираються з безлічі фінансово-значущих систем, наприклад, АБС для банку, бази даних по транзакціях для платіжних систем і тому подібне. Так само будуть варіюватися і критерії відбору, так для для SAP систем будуть значимі операції і дії відображаються в головній книзі, для операторів зв'язку це трафік і дії ведуть до зміни балансу рахунку послуг клієнта [2].

У загальному вигляді архітектура системи дистанційного банківського обслуговування (ДБО) зображена на рисунку 1.

У загальному сенсі будь-яка система антифрода ДБО визначає можливість виконання транзакції, яку ініціював користувач ДБО. При цьому система оцінює ризикованість даної транзакції і в разі підвищеного ризику різними способами намагається додатково перевірити, що транзакція легітимна. Способи можуть бути автоматизованими (з точки зору банку) або ручними. Наприклад, можна відправити користувачеві СМС або push-повідомлення, щоб він підтвердив транзакцію, попросити користувача відповісти на контрольні питання, передзвонити користувачеві. Всі ці дії покликані ще раз за допомогою додаткових факторів визначити чи саме користувач виконує транзакцію [3].

Нарешті, після проходження додаткової багатофакторної аутентифікації система антифрода автоматизовано або аналітик вручну вирішує, чи можливо провести транзакцію.

В результаті систему антифрода можна назвати системою багатофакторної адаптивної аутентифікації. Під адаптивністю розуміється здатність системи вираховувати ризикованість транзакцій (в тому числі і вхід в систему ДБО), на підставі цієї інформації здійснювати додаткову аутентифікацію транзакції і потім приймати рішення про можливість виконання транзакції.

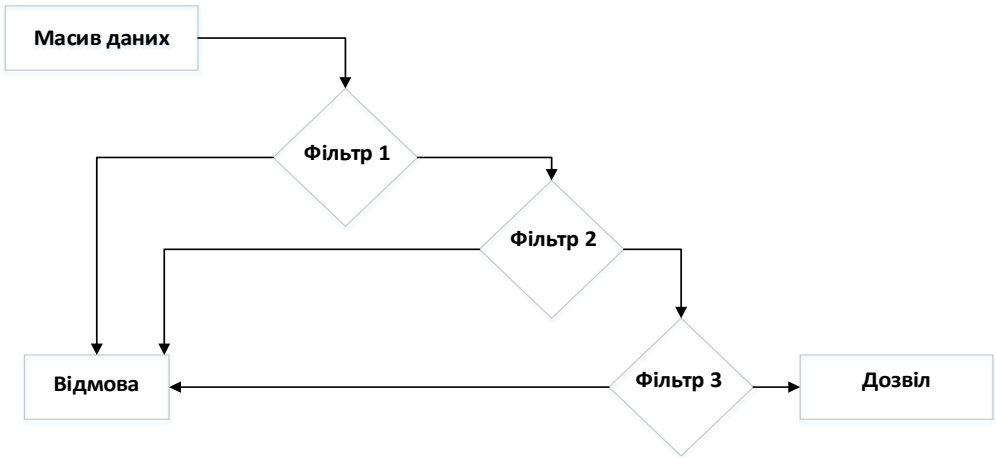


Рисунок 1 – Загальний вигляд роботи ДБО

Типові причини, коли транзакція може бути розціненою антифрод-фільтрами як підозріла [4]:

- Онлайн-оплата здійснюється не у тій країні, де було видано банківську картку платника.
- Картка є у «чорному списку» антифрод-систем.
- Платіжною системою заблоковано прийом карток, виданих у певних країнах. Як правило, це деякі країни Азії, Африки, Латинської Америки тощо, де за даними міжнародних статистичних звітів зафіксовано максимальну кількість ризиків і злочинів із банківськими картками

У антифрод-системі існує чотири відповіді (рекомендованих дії): ALLOW (дозволити дію), DENY (заборонити дію), CHALLENGE (провести додаткову аутентифікацію) і REVIEW (дозволити дію, але при цьому створити кейс в компоненті Case Management для подальшого маркування).

По відповіді CHALLENGE запускається додаткова аутентифікація дії користувача. Після того як користувач її пройде, в залежності від результату система антифрода дозволяє або забороняє дану подію.

По відповіді REVIEW також передбачається додатковий процес, подія дозволяється, але відкладається (створюється кейс) в Case Management для подальшої обробки вручну фрод-аналітиком. Фрод-аналітик може відзначити подію як «точно фрод», «можливо, фрод», «точно легально», «можливо, легально» і «важко класифікувати». Дане рішення потім передається в Adaptive Authentication і враховується системою в моделі для скорингу наступних подій. Іноді процес з відповіді REVIEW налаштовують таким чином, що подія не буде вирішуватися, а інтернет-банк буде чекати, поки фрод-аналітик не винесе свого рішення (по суті, це деяке перекриття функціональності відповіді CHALLENGE, де методом додаткової аутентифікації є рішення фрод-аналітика ).

Таким чином вибір банком ефективної системи фрод-аналізу дуже важливий, адже така система дозволяє звести ризики крадіжки грошових коштів клієнтів, а також репутаційні ризики самого банку до мінімуму.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Антифрод [Електронний ресурс] // Режим доступу: https://uk.wikipedia.org/wiki/Антифрод
2. Анти-фрод системы и как они работают [Електронний ресурс] // Режим доступу: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/339929.php
3. Как защищают банки [Електронний ресурс] // Режим доступу: https://xakep.ru/2017/04/21/antifrod-1
4. Антифрод-перевірка платежів [Електронний ресурс] // Режим доступу: https://tickets.ua/uk/content/antifraud-verification.html

**Томчук Микола Антонович** – канд. техн. наук, доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: tomchuk@vntu.edu.ua.

***Риндін Сергій Анатолійович***, студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: rindin70@gmail.com

**Tomchuk M. A.** Cand. Sc. (Eng.), Assistant Professor of Department of Health and Safety Studies, Vinnitsa National Technical University, Vinnytsia, e-mail: tomchuk@vntu.edu.ua.

***Serhii Ryndin,*** a student, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: rindin70@gmail.com