DOI: 10.34185/1991-7848.itmm.2025.01.105

АДАПТИВНА СИСТЕМА ОЦІНЮВАННЯ РИЗИКІВ ОНЛАЙН ТРАНЗАКЦІЙ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ

Носов В.О.[1], Островська К.Ю.[2]

[1]*Український державний університет науки і технологій, аспірант, Україна*

[2]*Український державний університет науки і технологій, к.т.н., доцент, Україна*

Анотація. *З кожним роком кількість фінансових операцій неспинно зростає, а з нею і відповідні кіберзагрози, зокрема шахрайство, тому виявлення ризикових транзакцій в електронній комерції набуває все більшої актуальності. У дослідженні розглянуто адаптивний підхід до оцінювання ризиків онлайн транзакцій на основі інтелектуального аналізу даних, зокрема машинного навчання. Запропонована система передбачає багаторівневу структуру в яку входять поведінковий аналіз, семантична оцінка транзакцій та інтеграція результатів для формування фінального індикатора ризику. Увагу приділено виявленню відхилень від типових шаблонів, зіставленню історичних даних з поточними діями користувача, а також гнучкому реагуванню на підозрілі активності та аномалії у режимі реального часу. Зазначений підхід дозволить підвищити точність виявлення шахрайських операцій, зменшити кількість хибнопозитивних спрацювань, і забезпечити здатність моделі до адаптації в умовах постійно зростаючих загроз у динамічному середовищі.*

Ключові слова: *оцінка ризиків, транзакція, машинне навчання, поведінковий аналіз, інтелектуальна система.*

Вступ. Збільшення кількості онлайн-операцій у фінансовому секторі супроводжується зростанням кількості злочинних ризиків, пов’язаних із шахрайством. Статистика Європейського центрального банку [1] та Національного банку України [2] свідчить про стрімке зростання кількості та складності шахрайських транзакцій. Класичні підходи виявлення шахрайства, засновані на фіксованих правилах (так звані rule-based), все складніше підтримувати через адаптивність зловмисників, тому виникає потреба в системах, які будуть доповнювати їх роботу.

Метою цієї роботи є розробка інтелектуальної системи виявлення ризикових транзакцій, яка поєднує різні методи аналізу для підвищення точності виявлення та зниження кількості транзакцій, які помилково класифікуються як шахрайські. Основний акцент зроблено на побудові

багаторівневої моделі, здатної працювати в умовах обмеженого часу та великої кількості запитів.

Виклад основного матеріалу

За допомогою інтелектуальних систем виявлення аномалій можна здійснювати комплексний аналіз поведінкових характеристик користувача, історії його транзакцій та контексту кожної нової операції. Для ефективної реалізації такого підходу доцільно поєднувати різні типи моделей: ті, що виявляють відхилення від звичних шаблонів, і ті, що здійснюють класифікацію подій на основі набору визначених ознак.

Поведінковий рівень системи аналізує усталені шаблони дій користувача, серед яких: часові межі активності, геолокація, тип пристрою, а також послідовність транзакцій. Аномальні відхилення, наприклад, такі як несподівана зміна місця проведення операції, або нестандартна сума платежу, оцінюються окремо як потенційно ризикові події.

Наступний рівень – семантичний. Він передбачає оцінку логічного узгодження транзакцій із типовою фінансовою поведінкою. Зокрема, враховується співвідношення між торговельною точкою (визначається як Merchant Category Code), категорією придбаних товарів або послуг і відповідною сумою платежу. Наприклад, оплата дорогих товарів у нетиповий час або в новій локації може сигналізувати про необхідність поглибленої перевірки. Виявлення таких відхилень здійснюється з використанням методів детекції аномалій та ймовірнісної класифікації.

Застосування методів машинного навчання дозволяє моделювати складні залежності між ознаками транзакцій та поведінковими характеристиками користувача. До таких підходів належать як наглядові методи (логістична регресія, дерева рішень), так і ненаглядові – зокрема, методи кластеризації та автокодувальники, які дають змогу виявляти відхилення без наявності міток. Окрему групу становлять ансамблеві моделі, що поєднують кілька алгоритмів задля підвищення загальної точності, стійкості до шуму та здатності адаптуватися до нових шаблонів.

На інтеграційному рівні результати попередніх етапів поєднуються для формування зваженого індикатора ризику. При цьому враховується значущість кожного виявленого фактору відхилення в контексті звичної поведінки конкретного користувача.

У наукових дослідження приведено цілий спектр алгоритмів, що застосовуються для вирішення задач виявлення фінансового шахрайства. Найпоширенішими є ансамблеві методи – випадковий ліс (Random Forest) [3] та градієнтний бустинг (Gradient Boosting), які демонструють високу точність класифікації. Такий алгоритм як логістична регресія часто використовується [4] як базова модель завдяки своїй інтерпретованості, тоді як нейронні мережі, зокрема автокодувальники [5], забезпечують виявлення прихованих відхилень у великих масивах даних без потреби в ручному маркуванні. Крім того, опорні вектори (Support Vector Machines), деревоподібні моделі та методи балансування вибірок, серед яких синтетична техніка надмірної вибірки меншості (SMOTE) [6], ефективно застосовуються для обробки даних із нерівномірним розподілом класів. Комбіновані підходи, які інтегрують декілька алгоритмів у межах єдиної системи, забезпечують оптимальний компроміс між точністю та обчислювальною ефективністю.

Ключовим компонентом ефективної системи є механізм адаптації моделі до змінного середовища. Це включає в себе динамічне коригування порогів чутливості залежно від загального фону активності, а також можливість зворотного навчання на підставі нових, підтверджених випадків шахрайства. Такий підхід сприятиме підтриманню актуальності системи та її здатності оперативно реагувати на нові ризики.

Висновки. Запропонований підхід до виявлення ризикових транзакцій у фінансових системах має потенціал стати основою ефективного інструменту моніторингу та оцінювання операцій. Багаторівнева структура, що поєднує поведінковий аналіз, семантичну оцінку та методи машинного навчання, дозволяє враховувати широкий спектр факторів ризику. Очікується, що впровадження такої системи сприятиме підвищенню точності виявлення шахрайських транзакцій та зменшенню хибнопозитивних результатів.

Перспективними напрямами подальших досліджень є підготовка джерел вхідних даних, розробка механізмів навчання та впровадження систем динамічного оновлення моделей у реальному часі.

ЛІТЕРАТУРА

1. European Central Bank. Report on payment fraud, 2024. [Online]. Available: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf.
2. Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами, 2024. [Online]. Available: https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami.
3. L. Guo, R. Song, J. Wu, Z. Xu, F. Zhao, Integrating a machine learning-driven fraud detection system based on a risk management framework, Applied and Computational Engineering 87.1 (2024) P. 80–86. DOI:10.54254/2755-2721/87/20241541.
4. J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H. A. Dwamena, E. O. Owiredu, S. A. Ayeh, J. Eshun, A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions, Decision Analytics Journal 6 (2023) 100163. DOI:10.1016/j.dajour.2023.100163.
5. M. Srokosz, A. Bobyk, B. Ksiezopolski, M. Wydra, Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment, Electronics 12.1 (2023) P. 251. DOI:10.3390/electronics12010251.
6. B. Borketey, Real-Time Fraud Detection Using Machine, Learning Journal of Data Analysis and Information Processing 12 (2024) P. 189-209. DOI:10.4236/jdaip.2024.122011.

ADAPTIVE SYSTEM FOR ONLINE TRANSACTION RISK ASSESSMENT BASED ON INTELLIGENT ANALYSIS

Valerii Nosov, Kateryna Ostrovska

Abstract. *Each year, the volume of financial transactions continues to grow steadily, accompanied by a corresponding rise in cyber threats, particularly fraud. As a result, identifying high-risk transactions in electronic commerce has become increasingly relevant. This study presents an adaptive approach to assessing the risks of online transactions based on intelligent data analysis, including machine learning methods. The proposed system employs a multi-level structure that incorporates behavioral profiling, semantic transaction evaluation, and integration of results to generate a final risk indicator. The approach focuses on identifying deviations from typical user patterns, correlating historical data with current activity, and responding flexibly to suspicious behavior and anomalies in real-time. This methodology aims to improve the accuracy of fraud detection, reduce the number of false positives, and ensure that the model remains adaptive in the face of growing threats in a dynamic environment.*

Keywords: *risk assessment, transaction, machine learning, behavioral analysis, intelligent system.*

REFERENCE

1. European Central Bank. Report on payment fraud, 2024. [Online]. Available: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf.
2. Prychynoiu bil′shosti shakhraiskykh vypadkiv z platizhnymy kartkamy stalo rozgholoshennia danykh yikhnimy korystuvachamy, 2024. [Online]. Available: https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami [in Ukrainian].
3. L. Guo, R. Song, J. Wu, Z. Xu, F. Zhao, Integrating a machine learning-driven fraud detection system based on a risk management framework, Applied and Computational Engineering 87.1 (2024) P. 80–86. DOI:10.54254/2755-2721/87/20241541.
4. J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H. A. Dwamena, E. O. Owiredu, S. A. Ayeh, J. Eshun, A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions, Decision Analytics Journal 6 (2023) 100163. DOI:10.1016/j.dajour.2023.100163.
5. M. Srokosz, A. Bobyk, B. Ksiezopolski, M. Wydra, Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment, Electronics 12.1 (2023) P. 251. DOI:10.3390/electronics12010251.
6. B. Borketey, Real-Time Fraud Detection Using Machine, Learning Journal of Data Analysis and Information Processing 12 (2024) P. 189-209. DOI:10.4236/jdaip.2024.122011.