УДК 004

Бондар О.П, Пасічник О.А., Скрипник Т.К., Петровський С.С.

Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ ШАХРАЙСЬКИХ ТРАНЗАКЦІЙ У ФІНАНСОВИХ ОПЕРАЦІЯХ З ЗАСТОСУВАННЯМ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Розглянуто прикладні аспекти розробки інформаційної системи для виявлення шахрайських транзакцій у фінансових операціях із використанням згорткових нейронних мереж. Запропонована система забезпечує ефективну обробку та аналіз великих обсягів транзакційних даних, виявляючи приховані закономірності, характерні для шахрайської поведінки.

The applied aspects of developing an information system for detecting fraudulent transactions in financial operations using convolutional neural networks are considered. The proposed system provides effective processing and analysis of large volumes of transaction data, revealing hidden patterns characteristic of fraudulent behavior.

Поява шахрайських транзакцій з банківськими картками збгається з розвитком електронних та безготівкових способів оплати. Шахрайські дії полягають у незаконному виведенні коштів з користувачів шляхом підробки даних картки або отримання несанкціонованого доступу до рахунків. Збільшення кількості випадків таких дій підштовхнуло фінансові організації до впровадження механізмів підвищеної безпеки, в даному випадку систем спостереження та виявлення сумнівних транзакцій.

Кредитні картки можуть бути фізично викрадені з гаманця або отримані віртуально з незахищених веб-сайтів, через витік даних або схеми крадіжки особистих даних. Наприклад, у 2019 році хакери зламали бази даних Capital One та оприлюднили інформацію про кредитні картки понад 100 мільйонів людей [1].

Захист фінансової інформації є важливим але, попри захист, який вони пропонується банками, кредитні картки не є захищеними від шахрайства. Навпаки, вони постійно є головною мішенню для злодіїв особистих даних, причому у 2024 році до Федеральної торгової комісії було подано майже 450 000 повідомлень про крадіжку особистих даних з кредитних карток [2].

Роль ШІ у виявленні фінансового шахрайства суттєво змінилася, перейшовши від статичних систем, заснованих на правилах, до динамічних, адаптивних алгоритмів. Структури раннього виявлення в основному залежали від заздалегідь визначених правил та ручного перегляду транзакцій, де сповіщення запускалися фіксованими параметрами, такими як сума транзакцій, частота або

географічне розташування. Хоча ці методи пропонували базовий рівень захисту, їм бракувало можливості адаптуватися до нових та складних шахрайських схем. Як наслідок, такі системи часто видавали високий рівень хибнопозитивних результатів, що призводило до неефективних розслідувань та погіршення обслуговування клієнтів.

Досягнення в машинному навчанні змінили цей процес, дозволивши системам аналізувати величезні набори даних та виявляти поведінкові моделі, що свідчать про шахрайську діяльність. Завдяки впровадженню таких методів, як поведінкова аналітика, глибоке навчання та нейронні мережі, сучасні моделі виявлення шахрайства тепер оцінюють численні точки даних у режимі реального часу. Ці системи на основі ШІ не лише оцінюють особу та наміри користувача, але й постійно адаптуються до нових та мінливих загроз. В результаті фінансові установи можуть досягти швидшого, точнішого та адаптивнішого виявлення шахрайства, значно підвищуючи як безпеку, так і операційну ефективність [3].

Розглянемо метод виявлення шахрайства з кредитними картками за допомогою перетворення зображень [4]

Автори розглядають зростаючу складність даних про транзакції з кредитними картками, що характеризуються високою швидкістю, серйозним дисбалансом класів та зміною моделей шахрайства, та пропонують нову структуру під назвою «Виявлення шахрайства за допомогою перетворення зображень» (FDIC) для покращення ефективності виявлення. У FDIC транзакції обробляються як часові ряди та перетворюються на двовимірні зображення за допомогою таких методів, як кутові поля Грама (GAF), поля переходів Маркова (MTF) та діаграми повторення (RP). Ці зображення потім класифікуються за допомогою згорткової нейронної мережі (CNN), тим самим фіксуючи часові та двосторонні зв'язки між характеристиками транзакцій, які може бути важко фіксувати за допомогою звичайних табличних або послідовних моделей. Для підвищення прозорості та інтерпретованості автори застосовують підхід штучного інтелекту (XAI) на основі теплових карт (через Grad-CAM та «сфокусований» варіант), щоб візуалізувати, які області перетворених зображень впливають на прийняття рішень моделлю.

Хоча запропонований підхід FDIC демонструє інновації у представленні даних про транзакції для виявлення шахрайства, певні обмеження та наслідки заслуговують на розгляд. Автори повідомляють про F1-бал 85,49% та повноту 80,35% для класу шахрайства, що демонструє конкурентоспроможну продуктивність порівняно з попередніми дослідженнями.

Мета: розробка та програмна реалізація методу виявлення шахрайських транзакцій у фінансових операціях із використанням згорткових нейронних мереж.

На етапі попередньої обробки даних ознака Amount масштабована за допомогою RobustScaler. Цей метод базується не на мінімальних та максимальних значеннях, а на медіані та інтерквартильному розмаху, що робить його стійким до

наявності викидів у даних – поширеного явища у фінансових транзакціях, де окремі операції можуть мати надзвичайно великі суми. Формула перетворення має вигляд:

$$x' = \frac{x - \text{median}(x)}{\text{IQR}(x)} \quad (1)$$

У результаті більшість значень суми зосереджуються поблизу нуля, тоді як екстремальні транзакції не мають надмірного впливу на навчання моделі. Такий підхід забезпечує стабільнішу збіжність нейронної мережі та підвищує її стійкість до нетипових значень у даних.

Ознаку Time було нормалізовано до інтервалу [-1,1] за допомогою лінійного перетворення:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (2)$$

Таким чином, найменше значення часу отримує -1, найбільше +1, а всі проміжні значення рівномірно розподіляються між ними.

Після масштабування ознак було виконано балансування вибірки, оскільки у вихідних даних спостерігався суттєвий дисбаланс між кількістю шахрайських та не шахрайських транзакцій. У більшості реальних фінансових наборів даних кількість легітимних операцій значно перевищує кількість шахрайських, що може призвести до переважного навчання моделі на більший клас і, відповідно, погіршення здатності виявляти шахрайство.

Після тренування моделі було проведено оцінювання роботи моделі та отримано основні показники оцінювання роботи моделі (Риснок 1).

```
Epoch 1/5
3110/3110 ━━━━━━━━━━━━━━━━━━━━ 19s 6ms/step - accuracy: 0.9817 - loss: 0.0502 - precision: 0.9831 - re
call: 0.9802 - val_accuracy: 0.9957 - val_loss: 0.0144 - val_precision: 0.9916 - val_recall: 0.9998
Epoch 2/5
3110/3110 ━━━━━━━━━━━━━━━━━━━━ 18s 6ms/step - accuracy: 0.9960 - loss: 0.0145 - precision: 0.9944 - re
call: 0.9975 - val_accuracy: 0.9989 - val_loss: 0.0074 - val_precision: 0.9981 - val_recall: 0.9996
Epoch 3/5
3110/3110 ━━━━━━━━━━━━━━━━━━━━ 18s 6ms/step - accuracy: 0.9974 - loss: 0.0097 - precision: 0.9964 - re
call: 0.9985 - val_accuracy: 0.9979 - val_loss: 0.0077 - val_precision: 0.9958 - val_recall: 0.9999
Epoch 4/5
3110/3110 ━━━━━━━━━━━━━━━━━━━━ 18s 6ms/step - accuracy: 0.9982 - loss: 0.0071 - precision: 0.9974 - re
call: 0.9990 - val_accuracy: 0.9983 - val_loss: 0.0052 - val_precision: 0.9975 - val_recall: 0.9992
Epoch 5/5
3110/3110 ━━━━━━━━━━━━━━━━━━━━ 17s 6ms/step - accuracy: 0.9984 - loss: 0.0061 - precision: 0.9978 - re
call: 0.9991 - val_accuracy: 0.9985 - val_loss: 0.0072 - val_precision: 0.9975 - val_recall: 0.9996
2666/2666 ━━━━━━━━━━━━━━━━━━━━ 4s 1ms/step - accuracy: 0.9981 - loss: 0.0057 - precision: 0.9971 - rec
all: 0.9992

Model Evaluation:
Accuracy: 1.00
Precision: 1.00
Recall: 1.00
F1: 1.00
```

Рисунок 1 – Процес та результати тренування моделі

На основі отриманих результатів навчання розроблена згорткова нейронна мережа (ЗНМ) продемонструвала винятково високу продуктивність у завданні

виявлення шахрайських транзакцій. Протягом п'яти епох навчання точність як навчання, так і валідації постійно зростала, досягнувши приблизно 99,8–99,9% з дуже низьким значенням втрат (близько 0,005–0,007). Значення точності та повноти як на навчальному, так і на валідаційному наборах також були надзвичайно високими (близько 0,998–0,999), що свідчить про те, що модель успішно ідентифікує майже всі шахрайські транзакції, практично не даючи хибнопозитивних результатів.

Під час остаточної тестової оцінки модель досягла 100% точності, прецизійності, повноти та F1-балу, що підтверджує її хороше узагальнення та високу надійність у розрізненні шахрайських та легітимних операцій. Такі результати показують, що кроки попередньої обробки, обрана архітектура ЗНМ та стратегія оптимізації були ефективними. Однак, незважаючи на ці ідеальні показники, важливо зазначити, що така висока продуктивність може також свідчити про незначне перенавчання через синтетичне балансування та відносно просту структуру даних про транзакції. Тому для розгортання в реальних фінансових системах рекомендується додаткова валідація на реальних, невидимих потоках транзакцій, щоб забезпечити стійкість моделі та стабільну продуктивність у динамічних реальних умовах.

Перелік посилань

1. Credit Card Fraud Detection: How To Spot & Avoid Fraud URL: https://www.identityguard.com/news/credit-card-fraud-detection
2. credit card scams to watch out for in 2025 URL: https://lifelock.norton.com/learn/fraud/credit-card-scams
3. Financial Fraud Detection in the AI Era: Best Practices for Compliance and Risk Management – Avahi URL: https://avahi.ai/blog/financial-fraud-detection-in-the-ai-era/
4. Explainable Credit Card Fraud Detection with Image Conversion — d9ffa86ca415aeefcbed3703ed6d602598db.pdf URL: https://pdfs.semanticscholar.org/e437/d9ffa86ca415aeefcbed3703ed6d602598db.pdf