УДК 004.056.5
DOI https://doi.org/10.32782/2663-5941/2024.6.2/07

Звєрєв В.П.
Державний торговельно-економічний університет

Бушков В.Г.
Державний торговельно-економічний університет

КРОС-КАНАЛЬНІ АНТИФРОД-СИСТЕМИ ЯК ІНСТРУМЕНТ КОМПЛЕКСНОГО ЗАХИСТУ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ЦИФРОВОЇ ЕКОНОМІКИ

У статті розглянуто проблему забезпечення безпеки електронних комунікацій у цифровій економіці, що пов'язана зі зростанням шахрайських дій у фінансовій сфері. Активне поширення кібершахрайства зумовлює необхідність розробки сучасних антифрод-систем, здатних ефективно запобігати шахрайству в режимі реального часу. Основний акцент зроблено на використанні крос-канальних антифрод-систем, що інтегрують машинне навчання, аналіз великих даних, графові моделі й аналіз часових рядів для досягнення максимальної ефективності.

Аналіз у статті включає сучасні підходи до виявлення шахрайства, серед яких методи кластеризації (k-means, DBSCAN), алгоритми прогнозування (ARIMA, LSTM), а також графові моделі (PageRank) для аналізу структурованих даних. Особливу увагу приділено інтеграції багатоканальних даних, які надходять із мобільних додатків, веб-платформ і фізичних точок продажу. Такий підхід дозволяє створювати єдиний профіль користувача, що забезпечує більш точне виявлення аномалій. Увага також акцентується на оптимізації алгоритмів, зменшенні кількості хибнопозитивних результатів і підвищенні масштабованості систем, що є важливими критеріями їх ефективності.

Запропоновано концепцію крос-канальної антифрод-системи, яка використовує дані з різних джерел, інтегруючи їх у єдиний аналітичний простір. Система реалізує функції аналізу зв'язків між транзакціями, що дозволяє виявляти приховані закономірності, поведінкові аномалії та прогнозувати потенційні ризики. Для цього використовується аналіз часових рядів, що дає змогу враховувати поведінкові патерни й оцінювати зміни в динаміці транзакцій.

Результати дослідження показують, що такі системи значно знижують фінансові втрати від шахрайства, підвищують точність ідентифікації підозрілих операцій і мінімізують кількість помилкових блокувань. Крім того, система демонструє гнучкість і здатність адаптуватися до різних обсягів даних і нових загроз, що виникають у цифровому середовищі.

Дослідження є важливим внеском у вирішення проблеми протидії шахрайству в умовах цифрової економіки. Воно корисне для фінансових установ, розробників програмного забезпечення, спеціалістів із кібербезпеки, а також науковців, які працюють у цій сфері.

Ключові слова: *антифрод-система, крос-канальна безпека, цифрова економіка, машинне навчання, біометрична автентифікація, цифрові загрози.*

Постановка проблеми. У сучасному світі цифрова економіка стала невід'ємною частиною повсякденного життя, забезпечуючи зручність та ефективність здійснення фінансових операцій. Проте, разом із розвитком цифрових технологій, зростає і рівень ризиків, пов'язаних із шахрайством у фінансовій сфері. Глобальні збитки від кібершахрайства досягли рекордних масштабів – лише за період із 2019 до 2022 року вони зросли з 1,2 трлн до 7,1 трлн доларів США [1, с. 34–35]. До 2026 року прогнозується, що ці втрати перевищать 20 трлн доларів, що робить проблему безпеки у фінансовому секторі пріоритетною для багатьох установ [1, с. 36].

Україна також не є винятком. За останні роки кількість шахрайських операцій, зокрема із застосуванням соціальної інженерії, збільшилася на 26% порівняно з попередніми періодами [2, с. 56]. Це підкреслює вразливість фінансових установ до сучасних загроз і вимагає швидкого впровадження ефективних рішень для протидії шахрайству.

Рисунок 1 переконливо демонструє зростання глобальних втрат від шахрайства з 2019 по 2022 роки та прогноз на 2026 рік. На графіку чітко видно експоненціальне збільшення втрат, що потребує проактивних дій з боку всіх гравців на фінансовому ринку.

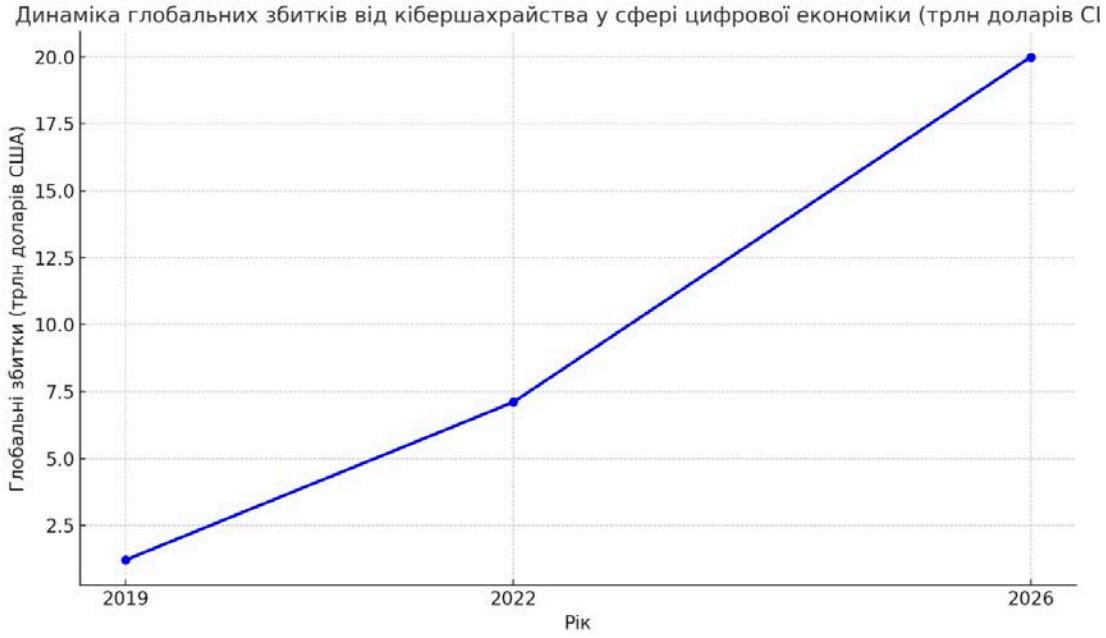

Рис. 1.

Аналіз останніх досліджень і публікацій. Наукова література підтверджує, що використання сучасних технологій, таких як машинне навчання, аналіз великих даних та графові моделі, дозволяє суттєво покращити ефективність антифрод-систем. Наприклад, компанія PayPal інтегрувала алгоритми машинного навчання для аналізу мільйонів транзакцій у реальному часі. Це дало змогу значно скоротити рівень шахрайства та забезпечити проактивний захист платформи [3, с. 78–79]. Mastercard впровадила систему Decision Intelligence, яка використовує штучний інтелект для моніторингу транзакцій, що забезпечило зниження рівня шахрайських операцій на 30% [4, с. 112].

Проте, попри успіхи, більшість існуючих рішень стикається з рядом обмежень. Наприклад, традиційні системи часто не можуть обробляти великий обсяг даних у реальному часі, що є критично важливим для сучасних платформ. Крім того, висока кількість хибнопозитивних результатів створює додаткові перешкоди для користувачів, знижуючи їхню довіру до платформи [5, с. 45–47].

Графові моделі, такі як PageRank, стали важливим інструментом для виявлення зв'язків між транзакціями. Вони дозволяють ідентифікувати складні шахрайські схеми, які залишаються невидимими для традиційних методів. Проте ці моделі вимагають високих обчислювальних ресурсів і ретельної інтеграції з іншими технологіями [6, с. 56].

Рішення, які використовуються сьогодні, часто обмежені через вузьку спрямованість і недостатню адаптацію до багатоканального середовища. У цьому контексті постає необхідність створення нової системи, здатної інтегрувати дані з різних джерел – мобільних додатків, вебплатформ, фізичних точок продажу – для формування єдиного профілю користувача. Такий підхід дозволяє значно підвищити точність виявлення шахрайських дій, скоротити фінансові втрати та збільшити рівень довіри клієнтів.

Зміни ландшафту загроз стали реальним викликом цифровій безпеці і потребують впровадження дієвих і ефективних заходів. Світові лідери фінансового сектора вже демонструють значні успіхи в упровадженні антифрод-рішень. Зокрема, Mastercard впровадила систему Decision Intelligence, що дозволила знизити втрати від шахрайства на 30% завдяки використанню штучного інтелекту для аналізу транзакцій у реальному часі (Tranzzo, 2023). Компанія JPMorgan Chase використовує інструменти штучного інтелекту для аналізу поведінкових патернів клієнтів, щорічно скорочуючи втрати від шахрайства на понад 50 мільйонів доларів (Fintech Insider, 2023). А відома платформа PayPal застосовує алгоритми машинного навчання, що знизили втрати від шахрайства на понад 60% у деяких сегментах бізнесу (Website Rating, 2023).

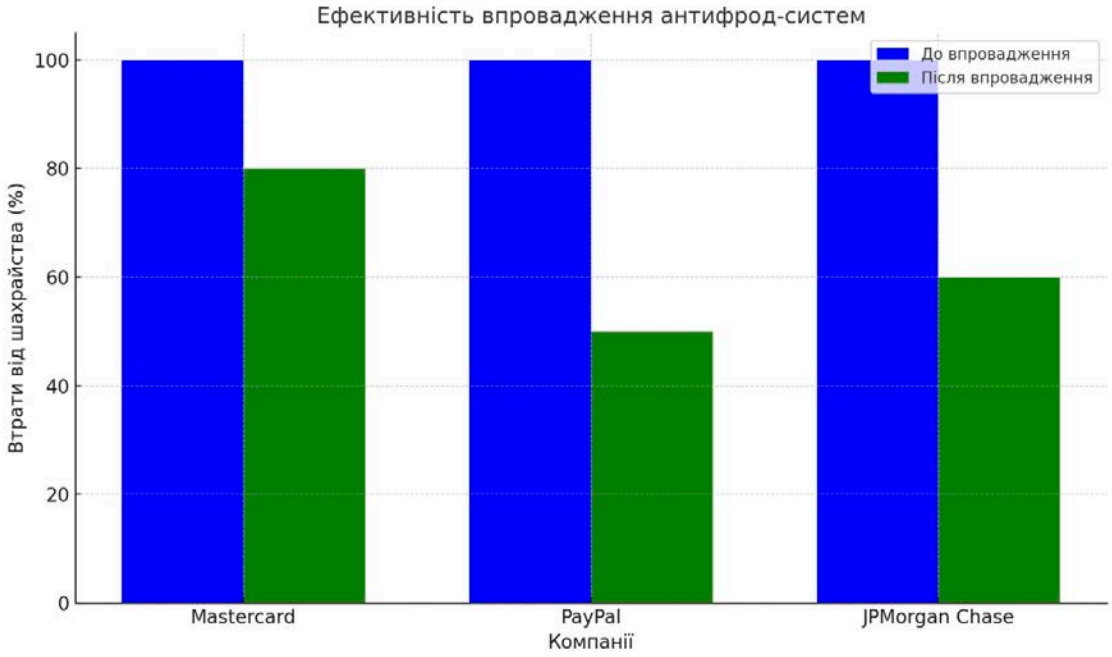

Рис. 2.

Рисунок 2 ілюструє зміни втрат до і після впровадження антифрод-систем у провідних фінансових компаніях.

В основу технології антифрод-рішень покладені наступні принципи:

1. Збір даних: Інтеграція транзакційних даних, поведінкових патернів і геолокації дозволяє створити багатовимірний профіль користувача.

2. Аналіз аномалій: Автоенкодери, ізоляційні ліси та методи опорних векторів (Random Forest і Gradient Boosting) ефективно ідентифікують підозрілу активність.

3. Реакція в реальному часі: Миттєве блокування підозрілих операцій мінімізує втрати, зменшуючи кількість хибнопозитивних результатів і покращуючи користувацький досвід.

Для досягнення високої точності виявлення шахрайства можуть використовуватися такі методи:

1. Збір та обробка даних: Інтеграція транзакцій, поведінкових патернів, геолокації, часових позначок. Дані проходять попередню обробку, яка включає очищення, нормалізацію, виявлення аномалій та створення нових характеристик (фічей), що покращують ефективність моделей.

2. Кластеризація: Для моделювання типових профілів користувачів застосовуються методи, такі як k-means і DBSCAN, що дозволяють групувати схожі поведінкові патерни.

3. Аналіз аномалій: Використання автоенкодерів, ізоляційних лісів і методів опорних векторів (Random Forest і Gradient Boosting) допомагає ідентифікувати підозрілі дії.

4. Часові ряди: Для врахування історичних даних і прогнозування майбутніх загроз застосовуються LSTM-мережі та ARIMA.

5. Класифікація: Алгоритми, такі як логістична регресія, , застосовуються для прогнозування ризику шахрайства.

Зазначимо, що графові моделі забезпечують виявлення прихованих зв'язків між транзакціями, допомагаючи виявляти складні схеми шахрайства. Регуляризація моделей та їх адаптація до нових даних здійснюється за допомогою крос-валідації та інших оптимізаційних технік. Проактивний підхід до побудови системи передбачає прогнозування загроз на основі аналізу історичних даних і поведінкових патернів, що дозволяє забезпечити високу ефективність запобігання шахрайству, зменшуючи ймовірність реалізації потенційних загроз (Fintech Insider, 2023). При цьому біометрична автентифікація (розпізнавання обличчя, відбитків пальців, голосу тощо) додає ще один рівень захисту, роблячи шахрайські дії майже неможливими (Tranzzo, 2023).

При запропонованій моделі побудови системи в цілому крос-канальні антифрод-системи демонструють високу масштабованість і модульність. Вони здатні адаптуватися до будь-яких обсягів транзакцій, забезпечуючи стабільність і точність навіть за умов пікових навантажень. Модульність дозволяє інтегрувати нові функції для аналізу,

зокрема машинне навчання, графові моделі чи технології штучного інтелекту. Важливим аспектом побудови таких систем є спрямованість на зменшення хибнопозитивних результатів, що дозволяє уникати помилкових блокувань законних транзакцій. Це в цілому покращує користувацький досвід, підвищує довіру до системи і мінімізує операційні витрати.

Високий рівень автоматизації і здатність до навчання в режимі реального часу роблять ці системи важливим інструментом захисту для фінансових платформ, що постійно стикаються з новими викликами в умовах цифрової економіки.

Таким чином, максимізація інтегрального показника ефективності $\boldsymbol{I}$, який характеризує здатність системи виявляти шахрайські дії, мінімізуючи при цьому кількість хибнопозитивних результатів та операційні витрати, можна представити в загальному вигляді

$$\boldsymbol{I} = f(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z})$$

де:

$\boldsymbol{X}$ – вектор внутрішніх параметрів системи;

$\boldsymbol{Y}$ – вектор зовнішніх параметрів багатоканального середовища;

$\boldsymbol{Z}$ – вектор ресурсів системи (обчислювальні, фінансові тощо);

$f(.)$ – визначений функціонал залежності параметрів моделі, як правило, методом експертних оцінок.

При цьому вектор внутрішніх параметрів системи ($\boldsymbol{X}$) може враховувати наступні компоненти: поведінкові патерни (x_1); геолокаційні дані (x_2); часові мітки (x_3); методи кластеризації, аналізу аномалій та часових рядів (x_4, x_5, x_6); точність моделей класифікації (x_7); швидкість обробки даних (x_8) та інші, в залежності від особливостей системи.

Вектор зовнішніх параметрів багатоканального середовища ($\boldsymbol{Y}$) включає джерела даних, такі як: мобільні додатки (y_1); веб-платформи (y_2); фізичні точки продажу (y_3); транзакційні системи (y_4); біометричні сенсори (y_5); соціальні мережі (y_6); вразливості хакерських атак (y_7); інші канали, що впливають на профіль користувача (y_8).

В підсумку цільова функція має наступний вигляд

$$\boldsymbol{I} = \max\left\{\sum_{t=1}^{T} \alpha_t \cdot \boldsymbol{Q}_t - \beta_t \cdot \boldsymbol{Z}_t - \gamma_t \cdot \boldsymbol{C}_t\right\},$$

де:

$\boldsymbol{Q}_t$ – частка вірно виявлених шахрайських дій (True Positive Rate);

$\boldsymbol{Z}_t$ – частка хибнопозитивних результатів (False Positive Rate);

$\boldsymbol{C}_t$ – витрати на обробку даних за час t ;

$\alpha_t, \beta_t, \gamma_t$ – вагові коефіцієнти, що враховують пріоритетність цілей.

Постановка завдання. Метою статті є аналіз основних методів та алгоритмів, які використовуються для побудови сучасних антифрод-систем у багатоканальних середовищах. Особливу увагу приділено підходам до кластеризації, класифікації, аналізу часових рядів, графових моделей, векторизації даних, регуляризації моделей, оптимізації та прогнозування. Кожна з представлених методик спрямована на вирішення конкретних завдань, пов'язаних із виявленням шахрайства, зменшенням розмірності даних, підвищенням точності прогнозів та оптимізацією роботи моделей машинного навчання.

Виклад основного матеріалу. Найбільш відомими методами, які використовуються при побудові антифрод-систем можна вважати наступні.

1. **Кластеризація** використовується для класифікації користувачів за поведінкою і підходить для сегментації даних.

Метод **K-means** зазвичай передбачає наступний алгоритм:

а) Вибір кількості кластерів k (кожен із яких має власний центроїд).

б) Ініціалізація центрів кластерів $\mu_1, \mu_2, \ldots, \mu_k$.

в) Призначення кожної точки даних до найближчого центру кластера:

$$c_i = \arg\min_j x_i - \mu_j^2$$

г) Оновлення центрів кластерів:

$$\mu_j = \frac{1}{|C_j|} \sum_{x_i \in C_j} x_i$$

д) Повторення кроків в) – г) до збіжності.

Метод **DBSCAN** дозволяє виявляти аномалії (шум) та кластеризувати дані з нерівномірною щільністю (наприклад, для розпізнавання патернів шахрайства). При цьому загальний алгоритм передбачає:

а) Вибір параметрів ϵ (радіус) та minPts (мінімальна кількість точок).

б) Визначення точок як основних, граничних або шумових.

в) Формування кластерів шляхом об'єднання основних точок, які знаходяться в межах ϵ одна від одної.

2. **Класифікація** використовує статистичну обробку результатів для подальшого аналізу з метою прийняття рішення.

Логістична регресія це статистичний метод, який використовується для бінарної класифікації, тобто передбачення двох можливих результатів (наприклад, «шахрайство» або «норма»), в основі якого закладено:

а) Модель:

$$P(y=1x)=\frac{1}{1+e^{-(\beta_0+\beta_1 x_1+\ldots+\beta_p x_p)}}$$

б) Оцінка параметрів за допомогою максимізації правдоподібності, яка виявляє ознаки шахрайства, прогнозування ризиків та ранжування об'єктів за ймовірністю певної дії (шахрай/норма).

Метод **SVM (Support Vector Machine) –** метод машинного навчання, який використовується для задач класифікації, регресії та виявлення аномалій. Послідовність застосування:

а) Вибір ядра (лінійне, поліноміальне, RBF).

б) Розв'язання задачі оптимізації:

$$\min_{\mathbf{w},b}\frac{1}{2}\quad \mathbf{w}\ ^2+C\sum_{i=1}^{n}\xi_i$$

з умовами:

$$y_i\left(\mathbf{w}\cdot\mathbf{x}_i+b\right)\geq 1-\xi_i,\xi_i\geq 0$$

Широко застосовується у фінансовій сфері для виявлення шахрайства, аналізу платоспроможності, прогнозування ризиків, а також для розпізнавання обличчя, тексту тощо.

3. **Аналіз часових рядів** передбачає роботу з даними, які впорядковані за часом, з метою виявлення закономірностей, трендів і сезонності. У задачах боротьби з шахрайством часові ряди допомагають: аналізувати патерни поведінки користувачів (наприклад, регулярність транзакцій, геолокація, часові відмітки), виявляти аномалії у поведінці, які можуть свідчити про шахрайські дії та прогнозувати ризики майбутніх шахрайських операцій на основі історичних даних. При цьому основними інструментами є:

Модель **ARIMA** (Autoregressive Integrated Moving Average), основна ідея якої полягає у визначені автокореляції (**AR**) між поточним значенням ряду та попередніми, інтеграції (**I**) шляхом обчислення різниць між послідовними значеннями та обчисленні середнього змінного (**MA**) для впливу помилок прогнозу попередніх періодів. Включає в себе

а) Вибір параметрів p,d,q для моделі ARIMA (p, d, q).

б) Оцінка параметрів моделі:

$$y_t=c+\phi_1 y_{t-1}+\ldots+\phi_p y_{t-p}+\theta_1\epsilon_{t-1}+\ldots+\theta_q\epsilon_{t-q}+\epsilon_t$$

Модель **LSTM (Long Short-Term Memory)** це тип рекурентної нейронної мережі (RNN), яка здатна обробляти довгі часові залежності, основною перевагою якої є можливість працювати як із лінійними, так і з нелінійними даними. Передбачає

а) Побудову нейронної мережі з LSTM-шарами.

б) Навчання мережі на часових рядах для прогнозування.

4. **Графові моделі** використовуються для аналізу об'єктів і їх взаємозв'язків у вигляді графів (вузли – об'єкти, ребра – зв'язки). Суттєвими перевагами таких моделей слід вважати: відображення складних структур, які неможливо чітко описати за допомогою традиційних табличних моделей; виявлення прихованих залежностей, які можуть вказувати на шахрайську активність (наприклад, схеми відмивання коштів); гнучкість для даних із неоднорідною структурою (нерівномірні зв'язки, різна щільність даних); прогнозування в частині майбутніх зв'язків, наприклад, між транзакціями або учасниками фінансових операцій, а також широкий спектр алгоритмів, таких як PageRank, Random Walks, чи кластеризація графів для виявлення аномалій та аналізу ризиків.

5. Багатовимірна **векторизація даних** як процес представлення даних у вигляді векторів у багатовимірному просторі для аналізу, класифікації чи візуалізації. Основними методами є:

а) PCA (Principal Component Analysis) для зменшення розмірності.

б) Векторизація текстових даних за допомогою методу TF-IDF (Term Frequency-Inverse Document Frequency), який оцінює значущість слова в документі відносно його частоти в усій колекції документів (прямий та інверсний) або Word2Vec – нейронної мережі, яка перетворює слова в багатовимірні вектори, де схожі слова знаходяться ближче одне до одного у векторному просторі.

У контексті боротьби з шахрайством ці методи дозволяють аналізувати як числові, так і текстові дані, забезпечуючи багатовимірний підхід до виявлення ризиків.

6. **Регуляризація моделей**

Використання L1 (Lasso) або L2 (Ridge) регуляризації для зменшення переобучення:

для L1 $$\min_{\beta}\left(\sum_{i=1}^{n}\left(y_i-\beta_0-\sum_{j=1}^{p}\beta_j x_{ij}\right)^2+\lambda\sum_{j=1}^{p}\left|\beta_j\right|\right)$$

та

для L2 $$\min_{\beta}\left(\sum_{i=1}^{n}\left(y_i-\beta_0-\sum_{j=1}^{p}\beta_j x_{ij}\right)^2+\lambda\sum_{j=1}^{p}\beta_j{}^2\right)$$

При цьому L1-регуляризація видаляє несуттєві ознаки (спрощує модель), а L2-регуляризація

контролює величину коефіцієнтів, запобігаючи переобученню. Гіперпараметр λ визначає силу штрафу (збалансовує точність і складність моделі).

7. **Оптимізація за допомогою градієнтного спуску –** оптимізаційний алгоритм, який використовується для мінімізації функції втрат $L(\beta)$ шляхом ітеративного оновлення параметрів моделі β у напрямку її зменшення. Формула оновлення параметрів має вигляд:

$$\beta := \beta - \eta \nabla L(\beta)$$

де η – швидкість навчання, $L(\beta)$ – функція втрат, $\nabla L(\beta)$ – градієнт функції втрат (вектор частинних похідних).

Може застосовуватися для оптимізації антифрод-моделей через використання градієнтного спуску для мінімізації функцій втрат у моделях класифікації (логістична регресія, нейронні мережі) чи аналізу часових рядів (LSTM), для підлаштування параметрів регуляризації з метою знаходження оптимального β, які враховують штрафи L1 або L2 регуляризації, а також використання адаптивних методів для складних даних і нелінійних задач боротьби з шахрайством за рахунок адаптивних варіантів градієнтного спуску (Adam, Nadam), які автоматично налаштовують швидкість навчання.

Вважається основним методом для налаштування параметрів у сучасних моделях. У дослідженнях боротьби з шахрайством він дозволяє створювати більш точні моделі для ідентифікації ризиків та підозрілих транзакцій, ефективно мінімізуючи функції втрат і запобігаючи переобученню.

8. **Прогнозування** – це ключовий етап у боротьбі з шахрайством, який дозволяє моделювати залежності між змінними та передбачати ризики. Використовуються Байєсівські мережі та ансамблеві методи, які на даний час є потужними інструментами для створення точних моделей прогнозування.

Байєсівські мережі – це графові моделі, які представляють залежності між змінними у вигляді орієнтованого ациклічного графу (вузли – змінні, ребра – залежності). Вони базуються на теоремі Байєса для обчислення ймовірностей. Передбачають виконання наступних етапів:

а) Побудова графу, за якою визначається структура мережі, яка показує причинно-наслідкові зв'язки між змінними. Наприклад, у фінансових транзакціях змінні можуть включати: суму операції, частоту транзакцій, геолокацію тощо.

б) Обчислення на основі теореми Байєса апостеріорних ймовірностей певної події (наприклад, шахрайства) з урахуванням наявних даних. Суттєвою превагою такого метода є можливість інтуїтивного моделювання залежностей та можливість працювати з неповними даними.

Ансамблеві методи поєднують кілька моделей (учнів) для покращення точності прогнозів. Вони дозволяють зменшити ризик переобучення та підвищити узагальнюваність.

а) Random Forest полягає в побудові ансамблю незалежних дерев рішень, кожне з яких прогнозує результат. При цьому кінцевий прогноз є середнім (у разі регресії) або голосуванням (у разі класифікації) між прогнозами всіх дерев:

$$\text{Прогноз} = \frac{1}{N} \sum_{i=1}^{N} \text{Прогноз}_i$$

б) Gradient Boosting застосовує послідовне побудування слабких моделей (учнів), кожна з яких покращує результати попередньої.

Формула оновлення моделі::

$$F_m(x) = F_{m-1}(x) + \eta h_m(x)$$

де $h_m(x)$ – новий слабкий учень, η – швидкість навчання.

Ці кроки забезпечують комплексний підхід до побудови антифрод-системи, яка може ефективно виявляти шахрайські дії в багатоканальних середовищах.

Нижче наведено приклад результатів кластеризації даних.

Графік кластеризації k-means демонструє кілька ключових аспектів, які мають безпосереднє відношення до роботи антифрод-систем.

По-перше, він показує сегментацію транзакцій або поведінки користувачів, де точки, згруповані в кластери, представляють групи з подібними характеристиками. У контексті антифрод-систем це може свідчити про типові операції, які відповідають нормальній поведінці користувачів, або незвичайні операції, які виділяються та можуть сигналізувати про шахрайство.

По-друге, на графіку можна виявити аномалії, які представлені точками, що знаходяться далеко від основних кластерів або не відповідають жодній групі. Ці аномалії часто потребують додаткової перевірки, адже можуть вказувати на підозрілу активність.

По-третє, графік дозволяє оцінити розподіл ризиків. У реальній антифрод-системі це означає, що кожен кластер може бути асоційований із певним рівнем ризику, наприклад, низьким для типових транзакцій, середнім для транзакцій

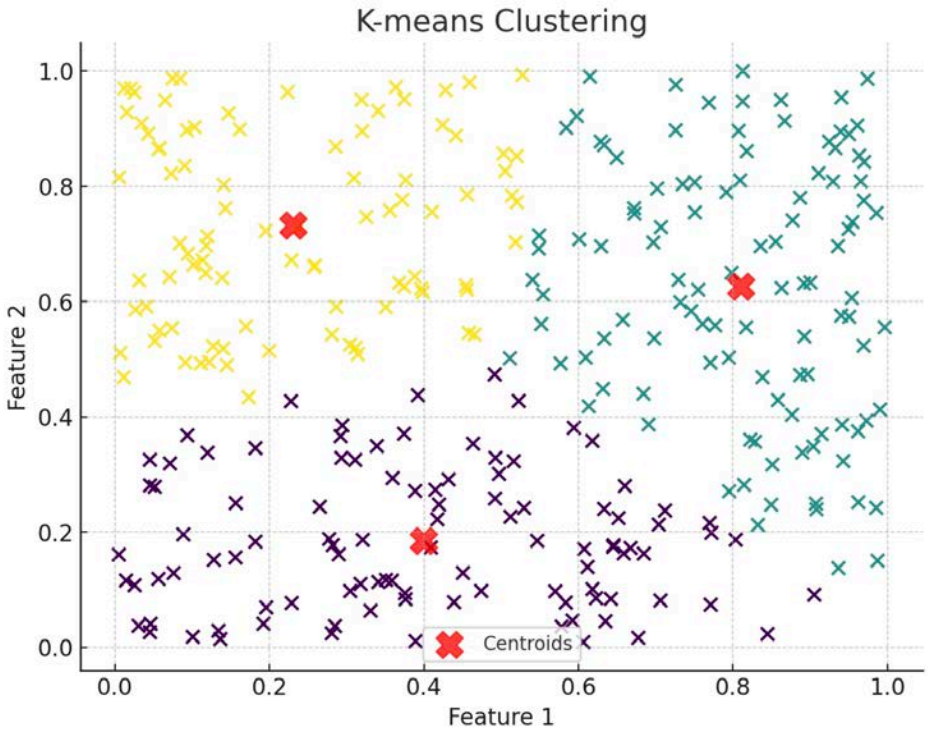

Рис. 3.

з деякими відхиленнями та високим для явних аномалій або нових типів шахрайських схем. Крім того, графік ілюструє, як алгоритм працює з багатоканальними даними. Якщо дані надходять із різних платформ, таких як мобільні додатки, веб-сайти чи банкомати, кластеризація дозволяє інтегрувати ці дані та створювати єдині групи, що є важливим для крос-платформних антифрод-систем. Центроїди кластерів, які відображаються на графіку, також свідчать про ефективність кластеризації. Якщо центроїди розташовані далеко один від одного, це свідчить про чітке розділення кластерів, що є корисним для аналізу різних типів поведінки. У підсумку, графік ілюструє, як антифрод-система може використовувати кластеризацію для автоматичного виявлення шахрайських дій та аномальної поведінки, що значно підвищує безпеку транзакцій та мінімізує втрати.

Таке представлення функціонування, як кластеризація даних за допомогою алгоритму k-means, може суттєво полегшити взаємодію з нейронними мережами в контексті побудови антифрод-систем завдяки кільком ключовим аспектам.

По-перше, попереднє групування даних у кластери дозволяє зменшити складність моделі нейронної мережі, оскільки вона працює вже з сегментованими наборами даних, що спрощує процес навчання. Це особливо актуально у випадках із великими багатовимірними даними, коли нейронна мережа може витрачати значні ресурси на обробку нерівномірних чи хаотично структурованих даних.

По-друге, використання кластеризації може забезпечити додатковий рівень інтерпретованості даних для нейронної мережі. Кластери, отримані через k-means, можуть слугувати як попередні мітки для наглядового навчання або створювати структуру, яка підвищує точність моделі за рахунок обмеження простору можливих результатів. Наприклад, замість навчання моделі на всіх даних одночасно, кожен кластер може оброблятися окремо, що підвищує локальну адаптивність і дозволяє нейронній мережі краще враховувати специфіку даних у межах кожного сегменту.

По-третє, кластеризація спрощує процес виявлення аномалій, які є важливими для антифрод-систем. Нейронні мережі, як правило, добре працюють із типізованими та частими патернами поведінки, проте кластеризація дозволяє виділити точки, які не відповідають жодному кластеру. Ці аномалії можуть бути передані в спеціалізовані підмережі для глибшого аналізу, що знижує ймовірність пропуску шахрайських дій.

Крім того, кластеризація покращує управління даними для багатоканальних систем. У крос-платформній антифрод-системі дані часто мають

різні джерела та структуру, що ускладнює їх обробку нейронними мережами. Попередня кластеризація дозволяє нейронній мережі отримати стандартизований, упорядкований набір даних із попередньо виявленими взаємозв'язками, що знижує обчислювальні витрати та підвищує продуктивність.

Нарешті, використання кластеризації сприяє розробці більш стійких до змін систем. У випадку появи нових шахрайських сценаріїв, які змінюють характер транзакцій, нейронна мережа може швидко адаптуватися за рахунок оновлення кластерів і локального навчання в межах змінених сегментів, що дозволяє підтримувати високий рівень точності без необхідності повного перенавчання.

Таким чином, інтеграція алгоритмів кластеризації, таких як k-means, у взаємодію з нейронними мережами створює більш ефективну та гнучку систему для боротьби з шахрайством у цифровій економіці.

Висновки. Крос-канальні антифрод-системи є потужним інструментом для забезпечення безпеки цифрової економіки завдяки використанню сучасних технологій, таких як машинне навчання, кластеризація, аналіз великих даних, прогнозування та адаптація до нових загроз. Вони інтегрують багатоканальні дані, включаючи транзакційну активність, поведінкові патерни та геолокацію, створюючи цілісні профілі користувачів. Такі системи забезпечують реакцію в реальному часі, мінімізують кількість хибнопозитивних результатів і дозволяють прогнозувати шахрайські дії, що є ключовими факторами для зменшення економічних втрат.

Кластеризація, зокрема алгоритм k-means, відіграє важливу роль у роботі таких систем, оскільки дозволяє сегментувати транзакції та виявляти аномалії. Це спрощує аналіз і забезпечує ефективну взаємодію з нейронними мережами, які можуть використовувати результати кластеризації для покращення точності та зниження складності моделі. Кластери допомагають виділяти типові, ризикові та підозрілі операції, дозволяючи оптимізувати ресурси системи та підвищувати якість її роботи.

Крос-платформні антифрод-системи також покращують обробку багатоканальних даних, стандартизуючи їх та інтегруючи в єдину модель. Це забезпечує високу ефективність навіть у складних умовах зростання обсягів операцій. Крім того, кластеризація спрощує управління адаптацією системи до нових загроз і сценаріїв шахрайства, дозволяючи швидко оновлювати моделі без втрати якості роботи.

Таким чином, крос-канальні антифрод-системи демонструють високу ефективність у боротьбі з шахрайством завдяки комплексному підходу до аналізу даних, використанню кластеризації, прогнозних алгоритмів і адаптації до нових викликів. Це робить їх незамінними інструментами для забезпечення стабільності та безпеки цифрової економіки.

Розглянуті системи відкривають нові можливості для забезпечення безпеки цифрової економіки, але їх впровадження супроводжується викликами. Одним із ключових питань є конфіденційність даних, які обробляються в межах антифрод-систем. Зокрема, споживачі цифрових послуг можуть висловлювати занепокоєння щодо обсягу та типу даних, які збираються. Крім того, адаптивність алгоритмів машинного навчання є критично важливою, але нові шахрайські сценарії можуть залишатися нерозпізнаними на ранніх етапах. Впровадження таких систем також є ресурсомістким, що може обмежувати їхню доступність для малих цифрових підприємств.

Підсумок. Шахрайство у цифровій економіці стає дедалі серйознішою загрозою, оскільки фінансові втрати через кіберзлочини зростають експоненційно. Розвиток технологій створює нові можливості для зловмисників, одночасно викликаючи потребу у впровадженні інноваційних антифрод-систем. Ефективність таких систем багато в чому визначається їхньою здатністю використовувати сучасні методи аналізу даних, алгоритми машинного навчання та штучний інтелект.

Як стверджують Smith і Brown [8, с. 45–67], адаптивність алгоритмів машинного навчання дозволяє швидко реагувати на нові загрози. Водночас вони наголошують на важливості якісних даних, адже без їхньої достатньої кількості навіть найсучасніші методи втрачають свою ефективність.

Сфера електронної комерції є особливо чутливою до шахрайства, адже великі обсяги транзакцій створюють додаткові ризики для компаній і споживачів. Johnson [9, с. 34–56] акцентує увагу на тому, що сучасні антифрод-рішення допомагають зменшити кількість хибнопозитивних блокувань, що є надзвичайно важливим для збереження лояльності клієнтів. Проте впровадження таких систем залишається дорогим задоволенням, особливо для малих і середніх підприємств. Таким чином, розробка доступних і масштабованих рішень є одним із ключових викликів, що вимагає уваги дослідників.

Іншим важливим аспектом ефективних антифрод-систем є інтеграція даних із багатоканальних платформ. Як зазначають Lee і Kim [10, с. 78–91],

поведінкова аналітика відіграє важливу роль у створенні динамічних профілів користувачів, які дозволяють виявляти аномалії в транзакціях. Використання даних із мобільних додатків, веб-платформ, фізичних точок продажу та інших каналів сприяє підвищенню точності систем. Однак такий підхід потребує значних обчислювальних ресурсів та ретельного налаштування алгоритмів для забезпечення їхньої ефективності.

Водночас проблема конфіденційності даних є ще одним важливим викликом, адже збір і аналіз великих обсягів інформації про користувачів викликає занепокоєння щодо їхнього захисту. Забезпечення балансу між ефективністю антифрод-систем і дотриманням прав на приватність є одним із ключових питань сучасних досліджень. Крім того, висока складність і обчислювальні витрати, необхідні для реалізації передових алгоритмів, можуть стати перешкодою для їх масштабного впровадження.

Перспективи подальших досліджень у цій галузі є надзвичайно широкими. Інтеграція багатоканальних даних, розробка дешевших рішень для малого бізнесу, а також підвищення точності алгоритмів за одночасного зниження їхньої складності є ключовими напрямками роботи. Сучасні технології відкривають унікальні можливості для адаптації антифрод-систем до нових загроз, однак успіх їхньої реалізації залежить від здатності знайти баланс між ефективністю, доступністю та конфіденційністю.

У підсумку, боротьба з шахрайством у цифровій економіці вимагає міждисциплінарного підходу, який поєднує технічну досконаліть із дотриманням етичних стандартів. Інтеграція штучного інтелекту, поведінкової аналітики та багатоканального підходу дозволяє не лише підвищити ефективність протидії кіберзагрозам, а й створити стійкі технологічні рішення, які відповідають викликам сучасного світу.

Список літератури:

1. Tax N., de Vries K. J., de Jong M., Dosoula N., van den Akker B., Smith J., Thuong O., Bernardi L. Машинне навчання для виявлення шахрайства в електронній комерції: дослідницький порядок денний. У Deployable Machine Learning for Security Defense. Springer, 2021, с. 30–54. URL: https://doi.org/10.1007/978-3-030-87839-9_2 (дата звернення: 18.12.2024).

2. Damayanti R., Adrianto Z. Машинне навчання для виявлення шахрайства в електронній комерції. Журнал облікових і бізнес-досліджень Airlangga, 2023, том 2, вип. 2, с. 1562–1577. URL: https://doi.org/10.31093/jraba.v2i2.48559 (дата звернення: 18.12.2024).

3. Alomari Y. R. M., Sulaiman N. B., Ali S. H. Пояснювальне машинне навчання для виявлення шахрайства в реальному часі. У Explainable Artificial Intelligence in the Digital Sustainability. Springer, 2023, с. 1–15. URL: https://doi.org/10.1007/978-3-031-63717-9_1 (дата звернення: 18.12.2024).

4. Fintech Insider. Кібершахраї стають активнішими в Україні та світі. Які інструменти вони використовують та як захиститися? 2023. URL: https://fintechinsider.com.ua/kibershahrayi-stayut-aktyvnishymy-v-ukrayini-ta-sviti-yaki-instrumenty-vony-vykorystovuyut-ta-yak-zahystytysya/ (дата звернення: 18.12.2024).

5. Tranzzo. Все про безпеку платежів: система антифрод та PCI DSS. 2023. URL: https://tranzzo.com (дата звернення: 18.12.2024).

6. Website Rating. 50+ статистик та тенденцій кібербезпеки на 2024 рік. 2023. URL: https://www.websiterating.com/uk/blog/research/cybersecurity-statistics-facts/ (дата звернення: 18.12.2024).

7. EMA. Матриця платіжного шахрайства. Перезавантаження: аналіз, тренди та прогнози 2022–2023. 2023. URL: https://www.ema.com.ua/news/matricja-platizhnogo-shahrajstva-perezavantazhennja-analiz-trendi-ta-prognozi-2022-2023/ (дата звернення: 18.12.2024).

8. Smith J., Brown L. Розширені методи виявлення шахрайства в цифровій економіці. Журнал запобігання шахрайству, 2023, том 19, вип. 3, с. 45–67.

9. Johnson R. Машинне навчання у запобіганні шахрайству для електронної комерції. Аналітика електронної комерції, 2022, том 15, вип. 2, с. 34–56.

10. Lee H., Kim S. Аналітика поведінки для багатоканальних платформ у цифровій економіці. Огляд цифрової економіки, 2021, том 10, вип. 4, с. 78–91.

Zvieriev V.P., Bushkov V.H. CROSS-CHANNEL ANTI-FRAUD SYSTEMS AS A TOOL FOR COMPREHENSIVE PROTECTION OF ELECTRONIC COMMUNICATIONS IN THE DIGITAL ECONOMY

The article addresses the problem of ensuring the security of electronic communications in the digital economy, which is associated with the growing number of fraudulent activities in the financial sector. The active proliferation of cyber fraud necessitates the development of modern anti-fraud systems capable of effectively preventing fraud in real-time. The main focus is placed on the use of cross-channel anti-fraud

systems that integrate machine learning, big data analytics, graph models, and time series analysis to achieve maximum efficiency.

The analysis in the article includes modern approaches to fraud detection, among which are clustering methods (k-means, DBSCAN), forecasting algorithms (ARIMA, LSTM), and graph models (PageRank) for analyzing structured data. Special attention is given to the integration of multi-channel data coming from mobile applications, web platforms, and physical points of sale. This approach allows for the creation of a unified user profile, enabling more accurate anomaly detection. Emphasis is also placed on optimizing algorithms, reducing the number of false positives, and improving system scalability, which are critical criteria for their effectiveness.

The concept of a cross-channel anti-fraud system is proposed, which uses data from various sources, integrating them into a unified analytical space. The system implements the functionality of analyzing relationships between transactions, enabling the identification of hidden patterns, behavioral anomalies, and the prediction of potential risks. This is achieved through time series analysis, which accounts for behavioral patterns and evaluates changes in transaction dynamics.

The results of the study show that such systems significantly reduce financial losses from fraud, enhance the accuracy of identifying suspicious activities, and minimize the number of false blocks. Additionally, the system demonstrates flexibility and the ability to adapt to varying data volumes and new threats emerging in the digital environment.

The research makes a significant contribution to solving the problem of combating fraud in the digital economy. It is valuable for financial institutions, software developers, cybersecurity specialists, and researchers working in this field.

Key words: *anti-fraud system, cross-channel security, digital economy, machine learning, biometric authentication, digital threats.*