```
# Малювання графа
nx.draw_networkx_nodes(G, pos, node_color="#AED6F1", node_size=3000)
nx.draw_networkx_edges(G, pos, arrows=True, arrowstyle='-|>', edge_color='gray')
labels = nx.get_node_attributes(G, 'label') # Мітки вузлів
nx.draw_networkx_labels(G, pos, labels, font_size=10)
edge_labels = nx.get_edge_attributes(G, 'label') # Мітки ребер (умови)
nx.draw_networkx_edge_labels(G, pos, edge_labels=edge_labels, font_color='red', font_size=9)
plt.title("TTS-процес з умовами успіху/помилки генерації голосу", fontsize=14)
plt.axis('off')
plt.show()
plt.show()
```

Подяка. Дана стаття підготована завдяки грантової підтримки Національного Фонду Досліджень України, реєстраційний номер проєкту 33/0012 від 3/03/2025 (2023.04/0012) «Розроблення інформаційної системи автоматичного виявлення джерел дезінформації та неавтентичної поведінки користувачів чатів» за конкурсом «Наука для зміцнення обороноздатності України».

Список використаних джерел

1. Формальні мови, граматики та автомати : механізми виявлення дезінформації, фейкових новин та пропаганди : навчальний посібник / О. О. Марків, В. А. Висоцька, О. В. Лозинська. – Львів : «Новий Світ-2000», 2025. – 269 с. ISBN 978-966-418-542-1
2. Лозинська О. В., Марків О. О., Висоцька В. А. Метод виявлення джерел дезінформації на основі ансамблевих моделей машинного навчання // Біоніка інтелекту. – 2025. – № 1 (102). – С. 11–19.
3. Jurafsky, D., & Martin, J. H. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition (3rd ed.). – 2023

DOI 10.70286/ISU-15.10.2025.006

АНАЛІЗ ДАНИХ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ ДЛЯ УПРАВЛІННЯ БАНКІВСЬКИМИ РИЗИКАМИ

Кісь Ярослав Петрович
кандидат технічних наук, доцент
Сироветник Богдан Юрійович
аспірант
Кафедра інформаційних систем та мереж
Національний університет «Львівська політехніка», Україна

Мета полягає у побудові промислових моделей для ймовірності дефолту, виявлення шахрайства, операційного ризику і раннього попередження про зсуви портфельної якості з інтеграцією результатів у процеси скорингу, лімітування й

резервування. Очікуваний прикладний ефект виражається у скороченні частки проблемних активів на нуль цілих вісім десятих до одного цілих дві десятих відсоткового пункту, зниженні витрат на фрод на двадцять п’ять до сорока відсотків та прирості чистого портфельного доходу на два до чотирьох відсотків рік у рік.

Дані формуються з транзакційних потоків, профілів клієнтів, бюро кредитних історій, журналів інцидентів і телеметрії IT. Типовий набір містить від п’яти до п’ятнадцяти мільйонів позик і платежів за три роки, з двохсот до восьмисот ознак після відбору. Частка позитивного класу у задачі PD зазвичай від одного до трьох відсотків, у задачі фроду нижче однієї десятої відсотка, що вимагає спеціальних стратегій навчання.

Підготовка даних включає нормалізацію сум, дедуплікацію і часову синхронізацію. Пропуски обробляються мішаною стратегією, де до п’ятдесяти відсотків дірок закривається статистичними імпутерами, решта маркується бінарними індикаторами відсутності. Викиди коригуються вінзоризацією на рівнях перший і дев’яносто дев’ятий перцентил. Для транзакцій встановлюється вікно спостереження дев’яносто днів, для наслідків сто вісімдесят днів, що забезпечує незалежність часових зрізів і відтворюваність метрик [1].

Інженерія ознак спирається на частотні та монетарні агрегати, коефіцієнти сезонності, ковзні медіани і дисперсії, ентропію призначень платежів, графові характеристики зв’язності рахунків. Приклади корисних показників включають індекс концентрації витрат топ три категорій, співвідношення готівкових зняттів до безготівкових операцій, темп падіння залишків за останні тридцять днів, середню затримку оплати комунальних послуг у днях, розмір найбільшої одноразової транзакції за шістдесят днів, кількість нічних сесій логіну. Для мережевих ознак застосовується центральність за ПейджРенк з обрізанням рідкісних зв’язків. Для послідовностей будуються токени подій і n грам структури.

Для табличних наборів як базові використовуються багатошарові перцептрони з пакетною нормалізацією і дропаутом, табнет з масками уваги на рівні ознак, градієнтні бустинги як бенчмарк. Для послідовностей подій застосовуються CNN і трансформери з довжиною контексту від сто двадцять вісім до п’ятсот дванадцять кроків. Для аномалій на безміткових даних навчаються автоенкодери і варіаційні автоенкодери з вузьким латентним простором від вісім до шістнадцять. У задачі фроду ефективні гібридні ансамблі, де таблична гілка поєднується з послідовною через пізнє злиття логітів [2].

Стратегії боротьби з дисбалансом включають вагові коефіцієнти класів, фокальні втрати, синтетичне збагачення важкими негативами і часово узгоджений негативний семплінг. Для PD доцільне таргетне недосемплювання більшості до співвідношення один до десяти, для фроду один до п’ятдесят, з подальшим коригуванням порогів на валідації. Навчання виконується пакетами по тридцять дві тисячі рядків з косинусним планом навчальної ставки від три на десять у мінус третій до три на десять у мінус четвертій [3].

Через рідкість позитивів AUC ROC завищує очікування, тому пріоритет віддається площі під PR кривою, KS статистиці, топ ліст метрикам і стабільності децильних бригадувань. Цільові орієнтири для PD включають PR AUC від тридцять п’ять до сорок п’ять відсотків, KS не нижче двадцять п’ять, монотонне зростання дефолт рейту від першого до десятого децилю з кроком не менше нуль цілих дві десятих відсоткового пункту. Для фроду орієнтиром є захоплення дев’яносто відсотків шахрайських подій у топ п’яти відсотках алертів при частці хибно позитивних нижче два відсотки.

Калібрування переводить скор у ймовірність для коректного резервування і ціноутворення. Використовуються ізотонічна регресія і плац калібрування з перевіркою на ковзних вікнах довжиною тридцять днів. Прийнятною вважається похибка калібрування не більше плюс мінус два відсоткові пункти на кожному децилі і не більше один відсотковий пункт інтегрально. Для стабілізації ймовірностей запроваджується температурне масштабування і блендинг із простою логістичною регресією.

Інтерпретованість і контроль упереджень забезпечуються шляхом глобальних та локальних пояснень. Застосовується шеп для топ ста ознак з регулярним моніторингом дрейфу важливостей. Проводяться тести стабільності метрик для груп за віком, статтю і регіоном з максимально допустимими відхиленнями не більш ніж два відсоткові пункти у чутливості та точності. Виявлені проксі ознаки замінюються більш етичними сурогатами з незначною втратою якості [4].

Переміщення порогу прийняття для PD, що підвищує відмову на два відсоткові пункти у верхніх децилях ризику, за умови середнього лосу у дефолті сорок відсотків і середньої маржі десять відсотків, зменшує очікувані збитки на сім до дев’ять базисних пунктів портфеля і дає приріст чистого доходу на нуль цілих сім десятих відсоткового пункту. Для фроду зменшення хибно позитивної ставки з три до два відсотків при незмінній повноті дев’яносто підвищує пропускну здатність чесних операцій на один відсотковий пункт, що у мережевих платежах масштабу мільйон транзакцій на день означає додатково десять тисяч успішних операцій без ручної перевірки.

Робастність до зсувів контролюється індексами стабільності популяції для ознак і таргетів. Пороги тривоги встановлюються на рівні нуль цілих нуль п’ять для PSI по ключових ознаках і нуль цілих два для інтегрального показника. Перевищення порогу запускає позачергову перевірку калібрування і часткове перенавчання на останніх два до чотири тижнів даних з пріоритетним бустингом останніх подій.

Сценарії включають підвищення базової ставки на двісті базисних пунктів, падіння доходів домогосподарств на десять відсотків, локальні відключення платіжних сервісів на сімдесят дві години, сезонні піки трафіку на п’ятдесят відсотків. Для кожного сценарію оцінюється приріст очікуваних кредитних збитків і потреба у капіталі. Допустиме відхилення від плану збитків не більше п’ять відсотків квартал до кварталу.

MLOps контур організовано у вигляді конвеєрів. Виділено шари фічстору, навчання, перевірок, реєстру моделей і сервінгу. Час побудови ознак для одного батчу нижче п’ятнадцять секунд, латентність онлайнового рішення нижче п’ятдесят мілісекунд при навантаженні до п’яти тисяч запитів за секунду. Ведеться журнал усіх інференсів з версією моделі, хешем фіч, часом і результатом для повного аудиту і відтворюваності.

На портфелі роздрібного кредитування приріст PR AUC з тридцять два до сорок один відсоток і KS з двадцять один до двадцять дев’ять забезпечив зменшення частки дефолтів у виданих заявках на нуль цілих дев’ять десятих відсоткового пункту і зниження обсягу створених резервів на шість відсотків рік у рік. У задачі фроду перехід на гібридну нейромережеву архітектуру знизив втрати на двадцять дев’ять відсотків при скороченні ручних перевірок на тридцять шість відсотків без погіршення рівня захоплення шахрайських подій [5].

Говернанс і відповідність. Для кожної моделі зберігаються картки з описом призначення, даних, обмежень, зон застосування, метрик тренування і продакшену, процедурами відкату і планом декомісії. Проводиться щоквартальна ревізія справедливості рішень і повторне узгодження політик із кредитним комітетом. У виробничих політиках закріплені порогові дії. Високий ризик призводить до зниження лімітів і вимоги додаткових документів. Середній ризик тягне за собою посилену верифікацію. Низький ризик використовується для кроспродажів і підвищення лояльності.

Обмеження і подальша робота. Якість вхідних даних і повнота бюро впливають на стелю метрик. Необхідно нарощувати покриття альтернативними даними, уніфікувати логіку відкладених міток для PD і стабілізувати затримки таргетів. Доцільно впровадити активне навчання з добором складних прикладів, регуляризацію розподілів для стійкості до спуфінгу фроду і онлайн калібрування з динамічними порогами на рівні сегментів.

Нейронні мережі, поєднані з якісною інженерією ознак, правильним калібруванням і суворими MLOps практиками, стабільно підвищують керованість банківських ризиків. Критичними є контроль дисбалансу класів, економічна валідація кожного зсуву порога, моніторинг дрейфів і говернанс рішень. За дотримання цих умов досягається вимірюваний фінансовий ефект у грошових показниках, зменшуються втрати і підвищується швидкість прийняття рішень без компромісів із безпекою та справедливістю.

Список використаних джерел

1. Ткачук, Н. (2022). Діджиталізація фінансово-економічної сфери в Україні: стан та перспективи розвитку. Економічний часопис Волинського національного університету імені Лесі Українки, (3), 18–28.
2. Кльоба, Л. Г. (2018). Цифровізація як інноваційний напрям розвитку банківської системи. Ефективна економіка, (12). http://www.economy.nayka.com.ua/?op=1&z=6741

3. Пантєлєєва, Н. М. (2019). Технології штучного інтелекту в антикризовому управлінні банком. Науковий вісник Херсонського державного університету. Серія: Економічні науки, (33), 193–197.
4. Дроботя, Я. А., & Бражник, Л. В. (2021). Діджиталізація банківської діяльності та платіжних систем: сучасні виклики і тенденції. Гроші, фінанси і кредит. Інфраструктура ринку, (51), 261–267.
5. Зянько, В., & Нечипоренко, Т. (2024). Цифрова трансформація банківського сектору: сучасні тренди та вектори розвитку. Innovation and Sustainability, (4), 6–11.

КІБЕРЗАГРОЗИ У ВИДАВНИЧІЙ ІНДУСТРІЇ: АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМ ЕЛЕКТРОННОГО РОЗПОВСЮДЖЕННЯ КОНТЕНТУ

Карпин Анна
старший викладач
Кафедра фізики та інформаційних систем,
Дрогобицький державний педагогічний університет
імені Івана Франка,
м. Дрогобич, Україна,
Банько Олександра
здобувачка вищої освіти бакалаврського рівня
Національний університет «Львівська Політехніка»
м. Львів, Україна

У сучасному цифровому середовищі видавнича індустрія все активніше переходить до електронних форматів розповсюдження контенту. Це відкриває нові можливості для авторів, видавців та читачів, але водночас створює значні ризики у сфері кібербезпеки. Наявність вразливостей у системах електронного книговидання може призвести до витоку персональних даних, незаконного копіювання творів та фінансових втрат видавництв.

Серед основних кіберзагроз, характерних для видавничої сфери, можна виокремити: піратство та нелегальне копіювання матеріалів, DDoS-атаки на онлайн-бібліотеки та видавничі ресурси, фішинг і соціальну інженерію, а також зловмисні дії, спрямовані на викрадення даних авторів і користувачів. Додатковим викликом є інтеграція хмарних технологій, що при неналежному захисті створює нові точки доступу для потенційних атак.

Типові вразливості систем електронного розповсюдження контенту можна поділити на технічні (недостатній рівень шифрування, відсутність багатофакторної автентифікації, слабкий захист API), організаційні (відсутність чіткої політики інформаційної безпеки у видавництвах, слабкий моніторинг загроз) та людські (низький рівень обізнаності персоналу у сфері кібербезпеки).