ДОСЛІДЖЕННЯ МЕТОДІВ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСТВА

***Афанасьєва І.В.**, к.т.н., доцент, кафедра ПІ, ХНУРЕ*
***Скримінський Н.О.**, магістр, кафедра ПІ, ХНУРЕ*

У сучасну цифрову епоху, коли шахраї знаходять і реалізують все більш витонченні методи, бізнес постійно шукає інноваційні методи виявлення та запобігання шахрайству. Одним з таких методів, що привертає значну увагу, є використання нейромережевих алгоритмів для виявлення шахрайства.

Нейронні мережі не тільки можуть виявляти відомі типи шахрайства, але й мають здатність адаптуватися та навчатися на нових шаблонах, що робить їх безцінними у боротьбі з постійно розвиваючимися методами шахрайства.

Зі збільшенням кількості цифрових транзакцій шахрайство в Інтернеті стало серйозною проблемою для бізнесу. Традиційні системи виявлення шахрайства в основному покладаються на системи, засновані на правилах, і перевірці вручну, які можуть забирати багато часу і давати багато хибних результатів. Більше того, оскільки шахраї постійно вдосконалюють свою тактику, звичайні методи часто виявляються недостатніми [1]. Шахраї оновлюють свої знання та розробляють витончені методи обману системи, часто використовуючи складні ланцюжки транзакцій, щоб уникнути виявлення. Тому традиційні системи на основі правил та машинного навчання (ML) з такими методами як SVM і XGBoost, часто можуть розглядати лише безпосередні межі транзакції (хто кому відправив гроші), часто пропускаючи шахрайські схеми з більш складним контекстом. Системи, що базуються на правилах, також потребують ручного налаштування з часом, оскільки шахрайські схеми змінюються і з'являються нові вразливості. Отже, потреба в більш досконалих, адаптивних методах, таких як ті, що пропонує штучний інтелект, є першочерговою.

Нейронні мережі мають здатність до навчання і ця здатність полягає в тому, що нейромережі здатні фіксувати і відображати складні взаємозв’язки між вхідними і вихідними даними. Нейронні мережі імітують людський мозок і тому вони можуть набути знань за допомогою навчання. Дані нейромережі зберігаються у вагах та параметрах моделі. Головна перевага нейронних мереж полягає в їх здатності представляти як лінійні, так і нелінійні зв'язки, а також в їх здатності вивчати ці зв'язки безпосередньо з даних, що моделюються. Традиційні лінійні моделі просто не підходять для моделювання даних, які містять нелінійні характеристики. На сьогодні більшість використовують графову нейронну мережу (GNN) як основу для виявлення шахрайства. Графові нейронні мережі побудовані на концепції представлення локального структурного та функціонального контексту безпосередньо в моделі. Інформація від ребер та властивостей вузлів поширюється за допомогою агрегації та передачі повідомлень сусіднім вузлам [2].

Коли виконується багатошарова згортка графа, це призводить до того, що стан вузла містить деяку інформацію від вузлів, розташованих на декількох

рівнях, що фактично дозволяє GNN мати сприйнятливе поле вузлів або ребер, розташованих на відстані декількох кроків від вузла або ребра. В контексті проблеми виявлення шахрайства, це велике сприйнятливе поле GNN може пояснити більш складні або довші ланцюжки транзакцій, які шахраї можуть використовувати для заплутування. Крім того, зміна шаблонів може бути врахована шляхом ітеративного перенавчання моделі.

Використання нейронних мереж для виявлення шахрайства має ще декілька переваг над традиційними методами. Однією з переваг є їхня здатність обробляти великі та складні набори даних. Нейронні мережі призначені для обробки величезних обсягів даних і виявлення складних закономірностей, що дозволяє їм виявляти навіть найприхованіші шахрайські дії. З появою нових шахрайських схем нейромережі можуть швидко оновлювати свої моделі, щоб виявляти та запобігати цим новим загрозам. Така адаптивність робить нейромережеві методи високоефективними у боротьбі з шахрайськими методами, що постійно розвиваються. Аналізуючи кілька змінних одночасно, нейромережі можуть виявляти складні взаємозв'язки і розкривати шахрайські дії, які можуть бути приховані в даних.

Хоча нейронні мережі пропонують значні переваги для виявлення шахрайства, вони також мають свої власні проблеми та обмеження. Однією з головних проблем є потреба у великих обсягах позначених даних для навчання. Шахрайські транзакції зустрічаються відносно рідко порівняно зі справжніми, що ускладнює отримання збалансованого набору даних. Нестача мічених даних може призвести до надмірної адаптації або поганого узагальнення нейромережевої моделі. Ще однією проблемою є інтерпретованість нейромережевих моделей. Нейронні мережі часто називають моделями "чорної скриньки", оскільки буває важко зрозуміти, як вони роблять свої прогнози. Відсутність інтерпретованості може ускладнити пояснення причин прийняття певного рішення, що може бути необхідним у певних галузях [3].

Методи нейронних мереж стали потужним інструментом для виявлення шахрайства в сучасну цифрову епоху. Їх здатність аналізувати величезні обсяги даних, адаптуватися до нових шахрайських схем і виявляти складні взаємозв'язки робить їх безцінними в боротьбі з шахрайськими діями. Незважаючи на те, що існують певні проблеми та обмеження, постійні дослідження та вдосконалення методів нейронних мереж обіцяють подолати ці перешкоди та ще більше вдосконалити системи виявлення шахрайства. Також технології штучного інтелекту з використанням машинного навчання можуть забезпечити більш точні та швидкі результати, ніж традиційні методи.

Список літератури

1. Unlocking Fraud Detection: Applications of Large Language Models. https://medium.com/@andrew_johnson_4/unlocking-fraud-detection-applications-of-large-language-models-f4bc5f01c5a7.

2. Sardana, A., Yilmaz, O., & Kranen, K. (2022). Optimizing Fraud Detection in Financial Services with Graph Neural Networks and NVIDIA GPUs. https://developer.nvidia.com/blog/optimizing-fraud-detection-in-financial-services-with-graph-neural-networks-and-nvidia-gpus/.

3. Roscher, R., Bohn, B., Duarte, M., & Garcke, J. (2020). Explainable Machine Learning for Scientific Insights and Discoveries, R. Roscher, B. Bohn, M-F. Duarte, and J. Garcke. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9007737.