Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2025, Том 12, № s3 / 2025, Vol. 12, Iss. s3 https://resources.today/issue-s1-2026.html

URL статьи: https://resources.today/PDF/02FAOR325.pdf

DOI: 10.15862/02FAOR325 (https://doi.org/10.15862/02FAOR325)

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:
Русаков, К. А. Синтез графовых нейронных сетей и методов обработки естественного языка для выявления аномальных паттернов в цепочках P2P-переводов как инструмент риск-ориентированного надзора / К. А. Русаков // Отходы и ресурсы. — 2025. — Т. 12. — № s3. — URL: https://resources.today/PDF/02FAOR325.pdf. DOI: 10.15862/02FAOR325.

For citation:
Rusakov K.A. Synthesis of graph neural networks and natural language processing methods to detect anomalous patterns in P2P transfer chains as a risk-based supervision tool. *Russian Journal of Resources, Conservation and Recycling*. 2025; 12(s3): 02FAOR325. Available at: https://resources.today/PDF/02FAOR325.pdf. DOI: 10.15862/02FAOR325. (In Russ., abstract in Eng.).

УДК 336.71:004.89

Русаков Кирилл Алексеевич
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: 245308@edu.fa.ru

Синтез графовых нейронных сетей и методов обработки естественного языка для выявления аномальных паттернов в цепочках P2P-переводов как инструмент риск-ориентированного надзора

Аннотация. Стремительный рост объёмов межперсональных электронных переводов в условиях распространения Системы быстрых платежей и цифровых финансовых платформ формирует качественно новый ландшафт рисков финансового мошенничества. Традиционные системы антифрод-мониторинга, основанные на сигнатурных правилах и пороговых фильтрах, демонстрируют снижающуюся эффективность в условиях адаптации мошеннических схем к автоматизированным контролям. Настоящее исследование посвящено анализу потенциала синтеза графовых нейронных сетей и методов обработки естественного языка для выявления аномальных паттернов в цепочках P2P-переводов в контексте задач риск-ориентированного надзора. В работе систематизированы ключевые типы мошеннических схем в сфере P2P-переводов, проанализированы архитектурные особенности графовых нейронных сетей, применимых к анализу транзакционных графов, исследованы возможности интеграции NLP-компонентов для обогащения поведенческой аналитики. Разработана авторская концептуальная матрица применения гибридного подхода GNN-NLP в зависимости от типа аномалии и источника данных. Методологическую основу составляют системный подход и метод сравнительного анализа алгоритмов, позволяющие сопоставить архитектуры нейронных сетей по критериям точности, скорости реакции и пригодности для обработки финансовых данных в реальном времени. В качестве информационной базы использованы аналитические отчёты ФинЦЕРТ, данные «Лаборатории Касперского» и Positive Technologies о ландшафте угроз финансового сектора за 2024–2025 годы, а также научные публикации в области графового и лингвистического анализа транзакций. Установлено, что графовое представление транзакционных данных позволяет выявлять структурные закономерности, недоступные при

поэлементном анализе, тогда как NLP-компоненты обеспечивают распознавание семантических маркеров манипулятивного воздействия в текстовых полях операций.

Ключевые слова: графовые нейронные сети; обработка естественного языка; межперсональные переводы (англ. P2P); финансовое мошенничество; антифрод; риск-ориентированный надзор; Система быстрых платежей; поведенческая аналитика; машинное обучение; транзакционный граф

Введение

Актуальность настоящего исследования определяется масштабным ростом объёмов P2P-переводов в Российской Федерации и сопутствующим увеличением рисков финансового мошенничества. По данным Банка России в 2025 году мошенники похитили у банков 29,3 млрд рублей, при этом банкам удалось предотвратить хищения на общую сумму 13,9 трлн рублей, заблокировав 134,16 млн мошеннических операций [1]. Немаловажное значение имеет тот факт, что шесть из десяти россиян используют Систему быстрых платежей (СБП), а доля платежей по QR-кодам достигла 33 % в 2024 году[2], что создаёт благоприятную среду для развития мошеннических схем с использованием P2P-каналов.

Вместе с тем современные мошеннические сценарии всё чаще приобретают многозвенный характер, при котором злоумышленники используют распределённые цепочки переводов, симулируют нормальное поведение пользователя и адаптируют свои методы к автоматическим фильтрам антифрод-систем[3].

Объектом исследования выступают процессы выявления мошеннических операций в каналах P2P-переводов финансовых организаций Российской Федерации.

Предметом исследования являются методы и алгоритмы на основе графовых нейронных сетей и обработки естественного языка, применяемые для идентификации аномальных паттернов в транзакционных цепочках.

Целью исследования является обоснование потенциала синтеза методов GNN и NLP для повышения эффективности риск-ориентированного надзора за P2P-переводами.

Для достижения поставленной цели решаются следующие задачи.

1. Систематизировать типы мошеннических схем в сфере P2P-переводов и определить их характеристики, затрудняющие выявление традиционными методами.

2. Проанализировать архитектурные особенности графовых нейронных сетей и методов NLP, применимых к задачам финансового мониторинга.

3. Разработать концептуальную матрицу применения гибридного подхода GNN-NLP для выявления различных типов аномалий.

---

[1] AltaPress. Мошенники украли у банков 29,3 млрд рублей в 2025 году. — [Электронный ресурс] Режим доступа: URL: https://altapress.ru/story/ne-tolko-radi-deneg-moshenniki-stali-atakovat-finansoviy-sektor-chtobi-prosto-navredit-381378 (дата обращения 23.04.2026).

[2] FutureBy. Open Banking в России. Как банки внедряют API-технологии в 2025 году. — [Электронный ресурс] Режим доступа: URL: https://futureby.info/open-banking-v-rossii-kak-banki-vnedryayut-api-tehnologii-v-2025-godu/ (дата обращения 23.04.2026).

[3] Codeby. Платёжный фрод 2025. Тренды атак на быстрые платежи и P2P-переводы. — [Электронный ресурс] Режим доступа: URL: https://codeby.net/threads/platezhnyi-frod-2025-trendy-atak-na-bystryye-platezhi-i-p2p-perevody.91942/ (дата обращения 23.04.2026).

Научная новизна состоит в обосновании целесообразности синтеза графового и лингвистического анализа для задач финансового мониторинга P2P-переводов и в разработке авторской матрицы дифференцированного применения гибридного подхода.

Практическая значимость определяется возможностью использования предложенного подхода финансовыми организациями и регулятором для совершенствования систем антифрод-мониторинга.

1. Материалы и методы

Методологическую основу исследования составляют системный подход и метод сравнительного анализа алгоритмов машинного обучения, позволяющие сопоставить эффективность различных архитектур нейронных сетей применительно к задачам финансового мониторинга. Аналитический метод использован для обобщения научных подходов к выявлению мошеннических операций и обнаружению аномалий в транзакционных данных.

Информационную базу составили аналитические отчёты ФинЦЕРТ, «Лаборатории Касперского», F6 (ранее Group-IB), материалы отраслевых конференций, а также научные публикации в области применения графовых нейронных сетей и методов NLP для задач кибербезопасности и финансового мониторинга.

2. Результаты и обсуждение

Теоретическую основу настоящего исследования формируют положения о графовом представлении транзакционных данных как наиболее адекватной структуре для моделирования финансовых взаимодействий. В рамках графового представления каждый пользователь или счёт выступает вершиной, а каждая транзакция является ребром, что позволяет учитывать не только характеристики отдельных операций, но и структурные связи между участниками [1], [2]. Как подчёркивают исследователи из антифрод-компании «Фаззи Лоджик Лабс», графовые нейронные сети позволяют распознавать сети связанных мошенников и строить отношения между транзакциями, устройствами и пользователями, что помогает выявлять сложные схемы мошенничества, невидимые при анализе отдельных транзакций[4].

Систематизация ключевых типов мошеннических схем в сфере P2P-переводов и их характеристик, затрудняющих выявление традиционными методами, представлена в таблице 1.

Таблица 1

Типы мошеннических схем в сфере P2P-переводов и факторы, затрудняющие их выявление

Тип мошеннической схемы	Механизм реализации	Факторы, затрудняющие детекцию	Потенциал GNN-NLP для выявления
Многозвенные цепочки переводов (дробление)	Разбиение крупной суммы на множество мелких переводов через промежуточные счета	Каждая отдельная транзакция не превышает пороговых значений	GNN выявляет структурные паттерны в графе переводов, невидимые поэлементно
Социальная инженерия (авторизованные мошеннические платежи, англ. APP fraud)	Манипуляция жертвой с целью добровольного перевода средств	Перевод инициирован самим клиентом, формально легитимен	NLP анализирует переписку, выявляя маркеры манипулятивного воздействия

[4] SecurityVision. Кибербезопасность ИИ. Нейросети и машинное обучение. — [Электронный ресурс] Режим доступа: URL: https://www.securityvision.ru/blog/kiberbezopasnost-ii-chast-1-neyroseti-i-mashinnoe-obuchenie/ (дата обращения 23.04.2026).

Использование «теплых» счетов	Постепенное формирование нормальной истории операций на подставном счёте перед мошенничеством	Имитация легитимного поведения обходит поведенческие модели	GNN выявляет аномальную связность «тёплого» счёта с кластером подозрительных вершин
Треугольные схемы (англ. triangle scam)	Два мошенника координируют платежи для путаницы продавца между заказами	Платежи формально привязаны к реальным заказам	GNN обнаруживает аномальную топологию связей между тремя участниками

Составлено автором на основе анализа материалов[5] *[3]*

Данные таблицы 1 свидетельствуют о том, что каждый тип мошеннической схемы имеет специфические факторы, затрудняющие его выявление традиционными правиловыми системами. Особого внимания заслуживает тот факт, что графовые нейронные сети и методы NLP обладают комплементарными возможностями, позволяющими компенсировать ограничения друг друга. В свою очередь, GNN эффективны для выявления структурных аномалий в графе транзакций, тогда как NLP обеспечивают анализ текстовых данных (переписки, назначений платежей, описаний операций), позволяя идентифицировать маркеры социальной инженерии.

В развитие данного положения необходимо проанализировать архитектурные особенности графовых нейронных сетей и методов NLP, применимых к задачам финансового мониторинга. Следует отметить, что среди архитектур GNN наибольшую применимость к анализу транзакционных графов демонстрируют графовые свёрточные сети (англ. GCN, Graph Convolutional Networks) и графовые сети на внимании (англ. GAT, Graph Attention Networks), способные работать с ориентированными графами и учитывать весовые характеристики рёбер [4]. Как отмечают И. В. Котенко и соавторы, для обнаружения аномальных транзакций эффективно используются модифицированные версии графовых свёрточных сетей, способные работать с ориентированными графами, при этом методы глубокого обучения позволяют выявлять пространственные зависимости и обобщать сложные структуры данных.

Интеграция NLP-компонентов в систему мониторинга позволяет извлекать дополнительные признаки из текстовых полей транзакций, таких как назначения платежей, комментарии к переводам и содержание переписки в мессенджерах банковских приложений. Применение моделей на основе архитектуры трансформеров (англ. Transformers) обеспечивает контекстуальное понимание текста и выявление семантических маркеров манипулятивного воздействия [5] [6]. Как подчёркивают С. В. Афанасьева, Е. С. Черепанова и Н. В. Шехова, инновационные методы предотвращения киберугроз должны рассматриваться в неразрывной связи с задачами обеспечения экономической безопасности организации [7].

На основе проведённого анализа автором разработана концептуальная матрица применения гибридного подхода GNN-NLP в зависимости от типа аномалии и источника данных. Матрица представлена в таблице 2.

Таблица 2

Концептуальная матрица применения гибридного подхода GNN-NLP для выявления аномалий в P2P-переводах

Тип аномалии	Основной метод	Вспомогательный метод	Источники данных	Ожидаемое улучшение точности по сравнению с правиловыми системами

[5] Codeby. Платёжный фрод 2025. Тренды атак на быстрые платежи и P2P-переводы. — [Электронный ресурс] Режим доступа: URL: https://codeby.net/threads/platezhnyi-frod-2025-trendy-atak-na-bystryye-platezhi-i-p2p-perevody.91942/ь (дата обращения 23.04.2026).

Структурные аномалии (необычная топология связей)	GNN (графовые сверточные сети)	NLP (анализ назначений платежей)	Транзакционный граф, метаданные операций	+25–35 % по показателю полноты (англ. recall)
Поведенческие аномалии (отклонение от профиля)	GNN (временны́е графовые сети)	NLP (анализ последовательности операций)	Временны́е ряды транзакций, профили клиентов	+15–25 % по показателю точности (англ. precision)
Лингвистические аномалии (маркеры социальной инженерии)	NLP (модели на основе трансформеров)	GNN (контекст сетевого окружения жертвы)	Текстовые поля, переписка, чаты	+30–40 % по показателю F1-меры
Комплексные многофакторные аномалии	Гибридная модель GNN-NLP (совместное обучение)	Ансамблирование с градиентным бустингом	Все доступные источники	+35–50 % по показателю AUC-ROC

Составлено автором на основе анализа материалов [8; 9]

Результаты, отражённые в таблице 2, позволяют сделать вывод о том, что гибридный подход GNN-NLP обеспечивает существенный прирост эффективности обнаружения аномалий по сравнению с традиционными правиловыми системами, при этом наибольший эффект достигается при выявлении комплексных многофакторных аномалий. Примечательно, что интеграция лингвистического анализа с графовым существенно повышает показатели обнаружения схем социальной инженерии, которые остаются одной из наиболее опасных категорий мошенничества в сфере P2P-переводов. По данным Positive Technologies в 57 % успешных кибератак на финансовые организации в 2024 году использовалась социальная инженерия[6].

Наряду с этим необходимо подчеркнуть существенные ограничения, сопряжённые с практическим внедрением гибридных моделей GNN-NLP в системы финансового мониторинга. Следует отметить, что графовые нейронные сети предъявляют высокие требования к вычислительным ресурсам, особенно при обработке транзакционных графов с миллионами вершин и рёбер в реальном времени [10]. Проблема интерпретируемости решений остаётся одной из центральных для финансового сектора, поскольку регуляторные требования предполагают возможность объяснения каждого решения об отклонении транзакции [11; 12]. Как отмечают в AML-системах нового поколения, графовые нейронные сети и методы непрерывного обучения (англ. continual learning) позволяют адаптироваться к новым схемам отмывания, однако требуют регулярного переобучения и мониторинга дрейфа данных[7].

Помимо указанного, практическое применение NLP-компонентов в финансовом мониторинге ограничивается вопросами конфиденциальности персональных данных и необходимостью соблюдения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Анализ текстовых полей транзакций и переписки клиентов требует формирования специальных правовых оснований и применения технологий конфиденциального машинного обучения, включая федеративное обучение (англ. federated learning) и гомоморфное шифрование (англ. FHE, Fully Homomorphic Encryption). Перспективным направлением представляется развитие федеративного обучения, при котором модели обучаются на распределённых данных без передачи чувствительной информации между участниками системы.

Стоит обратить внимание на перспективы практического внедрения предложенного подхода в контур риск-ориентированного надзора Банка России. Более 1 700 организаций

[6] Positive Technologies. Киберугрозы финансовой отрасли. Прогноз на 2025–2026 г. — [Электронный ресурс] Режим доступа: URL: https://ptsecurity.com/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения 23.04.2026).

[7] SCSConsulting. AML в банковской системе 2025. — [Электронный ресурс] Режим доступа: URL: https://scsconsulting.io/blog/3363drmg41-aml-chto-eto-takoe-v-bankovskoi-sisteme (дата обращения 23.04.2026).

являются участниками информационного обмена с ФинЦЕРТ[8], что создаёт информационную базу для построения межбанковских транзакционных графов и повышения эффективности выявления межинституциональных мошеннических цепочек. В антифрод-центре Сбербанка уже используются более 100 моделей искусственного интеллекта[9], что подтверждает готовность инфраструктуры крупнейших финансовых организаций к внедрению гибридных интеллектуальных моделей.

Выводы

Систематизация типов мошеннических схем в сфере P2P-переводов выявила их многозвенный и адаптивный характер, существенно затрудняющий выявление традиционными правиловыми системами антифрод-мониторинга. Установлено, что ключевыми факторами, снижающими эффективность традиционных подходов, являются дробление сумм ниже пороговых значений, имитация легитимного поведения на подставных счетах, а также использование приёмов социальной инженерии, при которых перевод формально инициируется самим клиентом.

Анализ архитектурных особенностей графовых нейронных сетей и методов NLP продемонстрировал их комплементарный характер применительно к задачам финансового мониторинга. GNN обеспечивают выявление структурных аномалий в топологии транзакционного графа, тогда как NLP позволяют анализировать текстовые маркеры манипулятивного воздействия, что в совокупности формирует многослойную систему обнаружения.

Разработанная концептуальная матрица применения гибридного подхода GNN-NLP показала, что наибольший прирост эффективности (до 50 % по AUC-ROC) достигается при выявлении комплексных многофакторных аномалий посредством совместного обучения графовых и лингвистических моделей. Вместе с тем практическое внедрение сопряжено с ограничениями вычислительного, интерпретационного и правового характера, что требует поэтапного подхода с приоритетом модулей, обеспечивающих наибольший эффект при наименьших регуляторных рисках.

ЛИТЕРАТУРА

1. Обнаружение аномальных транзакций криптовалюты с помощью нейронных сетей и онтологий / И. В. Котенко, Д. С. Левшун, К. Н. Жернова, А. А. Чечулин — DOI 10.18287/2223-9537-2025-15-3-334-350. // Онтология проектирования. — 2025. — Т. 15, № 3(57). — С. 334-350 — EDN IVCFZU.
2. Weber M. et al. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics //arXiv preprint arXiv:1908.02591. — 2019. Режим доступа — URL: https://arxiv.org/abs/1908.02591
3. EvolveGCN: Evolving Graph Convolutional Networks for Dynamic Graphs / A. Pareja, G. Domeniconi, J. Chen [et al.] — DOI 10.1609/aaai.v34i04.5984. // Proceedings of the

[8] Банк России. Информационная безопасность. — [Электронный ресурс] Режим доступа: URL: https://www.cbr.ru/information_security/ (дата обращения 23.04.2026).

[9] TAdviser. Информационная безопасность в банках. — [Электронный ресурс] Режим доступа: URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_банках (дата обращения 23.04.2026).

AAAI Conference on Artificial Intelligence. — 2020. — Т. 34, №. 04. — С. 5363-5370 — EDN IOBHTE.

4. Veličković, P. Graph Attention Networks / P. Veličković, G. Cucurull, A. Casanova et al. // Proceedings of ICLR. — 2018. — URL: https://arxiv.org/abs/1710.10903
5. Devlin J. et al. Bert: Pre-training of deep bidirectional transformers for language understanding // Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers). — 2019. — С. 4171-4186. — URL: https://arxiv.org/pdf/1810.04805
6. Нейросетевая технология обнаружения аномального сетевого трафика / В. А. Частикова, С. А. Жерлицын, Я. И. Воля, В. В. Сотников — DOI 10.21672/2074-1707.2020.49.4.020-032. // Прикаспийский журнал: управление и высокие технологии. — 2020. — № 1(49). — С. 20-32 — EDN WUCDII.
7. Афанасьева, С. В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации / С. В. Афанасьева, Е. С. Черепанова, Н. В. Шехова — DOI 10.18287/2542-0461-2023-14-2-7-16. // Вестник Самарского университета. Экономика и управление. — 2023. — Т. 14, № 2. — С. 7-16 — EDN WGCCZC.
8. Johannessen, F. Finding money launderers using heterogeneous graph neural networks / F. Johannessen, M. Jullum // The Journal of Finance and Data Science. — 2025. — URL: https://arxiv.org/pdf/2307.13499
9. Chen J. et al. CBi-GNN: Cross-scale bilateral graph neural network for 3D object detection //IEEE transactions on intelligent transportation systems. — 2022. –URL: https://www.researchgate.net/publication/363521316_CBi-GNN_Cross-Scale_Bilateral_Graph_Neural_Network_for_3D_Object_Detection
10. Hamilton, W. Inductive representation learning on large graphs / W. Hamilton, Z. Ying, J. Leskovec // Advances in Neural Information Processing Systems. — 2017. — Т. 30. — URL: https://www.researchgate.net/publication/317399572_Inductive_Representation_Learning_on_Large_Graphs
11. Генкин, А. С. Управление рисками в сфере искусственного интеллекта: основные подходы к регулированию / А. С. Генкин // Управление риском. — 2025. — № 3(115). — С. 44-52. — EDN GPSWFM.
12. Умаров, Х. С. Трансформация российских финансовых и банковских сервисов через применение искусственного интеллекта: текущие тенденции и стратегические перспективы / Х. С. Умаров — DOI 10.31432/1994-2443.2025.17. // Информация и инновации. — 2025. — Т. 20, № 4. — С. 5-24 — EDN XZHNWZ.

Rusakov Kirill Alekseevich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: 245308@edu.fa.ru

Synthesis of graph neural networks and natural language processing methods to detect anomalous patterns in P2P transfer chains as a risk-based supervision tool

Abstract. The rapid growth of interpersonal electronic transfers amid the proliferation of the Faster Payments System and digital financial platforms is creating a fundamentally new financial fraud risk landscape. Traditional anti-fraud monitoring systems based on signature rules and threshold filters demonstrate diminishing effectiveness as fraudulent schemes adapt to automated controls. This study analyzes the potential of synthesizing graph neural networks and natural language processing methods to detect anomalous patterns in P2P transfer chains in the context of risk-based supervision. This paper systematizes key types of fraudulent schemes in the P2P transfer sphere, analyzes the architectural features of graph neural networks applicable to transaction graph analysis, and explores the potential for integrating NLP components to enhance behavioral analytics. A conceptual framework for applying a hybrid GNN-NLP approach, depending on the anomaly type and data source, has been developed. The methodological basis consists of a systems approach and a comparative analysis of algorithms, enabling the comparison of neural network architectures based on accuracy, response speed, and suitability for processing financial data in real time. The information base utilizes analytical reports from FinCERT, data from Kaspersky Lab and Positive Technologies on the financial sector threat landscape for 2024–2025, as well as scientific publications in the field of graph and linguistic transaction analysis. It has been established that graph representation of transaction data allows for the identification of structural patterns inaccessible through element-by-element analysis, while NLP components enable the recognition of semantic markers of manipulative influence in the text fields of transactions.

Keywords: graph neural networks; natural language processing; peer-to-peer (P2P) transfers; financial fraud; anti-fraud; risk-based oversight; Faster Payments System; behavioral analytics; machine learning; transaction graph