3. ВЦИОМ: результаты опроса о восприятии россиянами интернета и о возможности его ограничения [Электронный ресурс] // Сайт Всероссийского центра изучения общественного мнения. 22.03.2021 [Электронный ресурс]. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-i-deti-vozmozhnosti-i-ugrozy#:~:text=%D0%94%D0%B5%D1%82%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5,%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5%20(81%25)

4. Магдилова Л. В. Правовые основы обеспечения информационной безопасности несовершеннолетних // Сайт научной электронной библиотеки КиберЛенинка. 2017. 10.21779/2224-0241-2017-23-3-104-108

5. Сколько времени в день ребенку можно проводить в Интернете? // Сайт Лиги безопасного Интернета. 13.02.2023. [Электронный ресурс]. – URL: https://ligainternet.ru/skolko-vremeni-v-den-rebenku-mozhno-provodit-v-internete/

6. Сустина Т. К вопросу об интернет-безопасности детей // «Адвокатская газета». – 2022. – № 5.

7. Угрозы для детей в цифровой среде [Электронный ресурс] // Сайт Центра правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ». 2023. – URL: https://4people.grfc.ru/faq/detskaya-bezopasnost-v-internete-na-chto-sleduet-obraschat-vnimanie/

8. 56 % детей постоянно находятся в Сети [Электронный ресурс] // По материалам сайта kaspersky.ru. [Электронный ресурс] – URL: http://security.mosmetod.ru/internet-zavisimosti/99-56-detej-postoyanno-nakhodyatsya-v-seti

Г. Г. Егоров,
кандидат юридических наук, доцент,
Волгоградский государственный университет
(Волжский филиал)

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ ДЛЯ МОНИТОРИНГА ПРОТИВОПРАВНЫХ ОТНОШЕНИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статья рассматриваются перспективны использование современных машинных комплексов анализа правовых отношений на предмет соответствия современному действующему законодательству. Выделяются основные направление противоправных действий, выявление которых становится возможным при использовании графологических нейронных сетей (GNN) основанных на логике асинхронного анализа правонарушений основанных на нарушения финансового оборота. В качестве практической составляющей использовался опыт апробации данных комплексов в Китайской народной республики, при этом проводится анализ как технических так и правовых особенностей внедрения тождественных систем в контрольную сфере Российской Федерации. Определя-

ются основные сложности по внедрению цифровых систем контроля и перспективы по их адаптации к Российским условиям.

Ключевые слова: нейронные графологические сети, контроль за правомерностью отношений, технические средства выявление правонарушений, федеральный контроль за цифровой безопасностью, правовой статус информации, цифровой контроль.

USING NEURAL NETWORKS FOR MONITORING ILLEGAL RELATIONS IN THE RUSSIAN FEDERATION

Abstract. The article considers the prospects of using modern machine complexes for analyzing legal relations for compliance with current legislation. The main areas of illegal actions are identified, the identification of which becomes possible with the use of graphological neural networks (GNN) based on the logic of asynchronous analysis of offenses based on violations of financial turnover. The experience of testing these complexes in the People's Republic of China was used as a practical component, while an analysis of both technical and legal features of the implementation of identical systems in the control sphere of the Russian Federation is carried out. The main difficulties in the implementation of digital control systems and prospects for their adaptation to Russian conditions are determined.

Keywords: neural graphological networks, control over the legality of relations, technical means of identifying offenses, federal control over digital security, legal status of information, digital control.

Введение. В условиях стремительного развития цифровых технологий и финансовых инноваций, возникает необходимость переосмысления подходов к обработке данных в сфере ПОД/ФТ.

Постоянно увеличивающийся поток данных и необходимость оперативного анализа рисков отмывания денег требуют внедрения и развития искусственного интеллекта в системы противодействия финансовым преступлениям [7].

Повышенный интерес к технологиям искусственного интеллекта (далее – ИИ) обусловлен эволюцией преступных схем, использованием ИИ злоумышленниками, необходимостью обработки огромных объемов данных в финансовой разведке и развитием экспертных систем в сфере противодействия отмыванию денег.

Научная база для изучения ИИ в сфере ПОД/ФТ пока еще находится в стадии формирования. Существующие исследования в основном сосредоточены на рисках злоупотребления ИИ для отмывания денег, проблемах регулирования и внедрения ИИ в системы ПОД/ФТ, а также на потенциале ИИ в финансовой сфере [6].

Основная часть. В 2022–2023 годах ИИ все чаще используется в преступных целях. Одной из самых серьезных угроз стали фейковые видео, аудио и изображения, созданные нейросетями. Люди склонны верить видео, поэтому дипфейки, поддельные видео с реальными людьми, представляют особую опасность. Примеры таких преступлений включают вымогательства с использовани-

ем поддельных видео с руководителями или родственниками, а также мошеннические схемы с использованием фальшивых рекламных роликов.

ИИ используется банками для биометрической идентификации пользователей по лицу при входе в мобильные приложения, в то время как преступники применяют нейросети для создания новых наркотиков, улучшения взрывчатых веществ и разработки более опасных видов оружия.

ИИ-сервисы все чаще используются для получения советов по незаконному обналичиванию денег и усовершенствованию схем отмывания денег. Пользователей интересуют правила финансового контроля, а также деятельность регуляторов в этой области. Параллельно с этим, резко увеличилось количество поддельного контента, созданного с помощью искусственного интеллекта, который используется для пропаганды и вербовки преступников. Ежедневно создаются миллионы фальшивых изображений.

Преступники научились создавать с помощью искусственного интеллекта стандартные комментарии, которые распространяются через ботов в социальных сетях, разжигая рознь, экстремизм и провокации. В 2023 году количество мошенничеств с использованием ИИ резко возросло. Например, на Филиппинах таких случаев стало в 45 раз больше по сравнению с предыдущим годом, а во Вьетнаме, США и Японии – в 30–28 раз [8].

Искусственный интеллект необходим финансовой разведке для обработки огромных массивов неструктурированных данных, их очистки и улучшения качества. Социальные сети и мессенджеры являются ценным источником информации о фигурантах финансовых расследований. Помимо пропаганды и вербовки преступников, эти платформы используются для сбора и перевода незаконно полученных средств, а также для легализации преступных доходов [5].

Анализ данных из соцсетей в финансовой разведке проводится в рамках общей системы обработки информации с использованием искусственного интеллекта. Росфинмониторинг получает данные о финансовых операциях, от государственных органов, иностранных финансовых разведок, СМИ и пользователей. Вся информация хранится и очищается с помощью машинного обучения. Далее проводится углубленный анализ данных: создаются списки, модели поведения и профили риска [12].

В результате обработки данных получаем ответы на запросы, инициативно предоставляем информацию государственным органам, спецслужбам и банкам, уведомляем в соответствии с законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (ст. 8 Федерального закона от 07.08.2001 № 115-ФЗ) и информируем зарубежные финансовые разведки [1].

Сбор, обработка, анализ и распространение информации о террористических и экстремистских группах в интернете – это работа с большими данными. В Росфинмониторинге для поиска в социальных сетях используется российская поисковая система с учетом смысла слов. В системе реализована оценка риска сообщений и автоматическое создание отчетов по новостям и социальным сетям. Сейчас данные переносятся на российское программное обеспечение.

Одновременно с этим в базе данных Росфинмониторинга обрабатываются данные о банковских картах, включая обязательные для контроля и подозрительные операции, которые также относятся к большим данным. Информация из онлайн-платформ объединяет структурированные и неструктурированные данные из множества источников, таких как тексты, изображения, видео, аудио и геолокация, образуя огромные массивы информации [4].

В основе автоматического поиска и анализа данных о террористических и экстремистских группах лежит анализ ключевых слов и объединение полученной информации. Пользователи системы могут использовать как готовые списки слов, так и создавать свои собственные.

Обработка данных осуществляется как автоматически, так и вручную. Ручная обработка требует много времени и ресурсов. Автоматизированные системы, такие как «СЕУС», «Георгий Победоносец», «Крибрум», «Сапфир», «Дарвин» и другие, позволяют быстро обрабатывать большие объемы информации в режиме реального времени [6]. Систему можно легко настроить под конкретные запросы пользователя. Помимо анализа интернет-ресурса, количества подписчиков и публикаций, программы определяют содержание сообщений и оценивают уровень вовлеченности пользователей. Некоторые системы также отслеживают изменения в профилях.

Особую значимость имеет функция сравнения адресов аккаунтов и сообществ с реестром запрещенных сайтов и списком экстремистских материалов. Человек необходим для оценки настроения сообщений, изменений взглядов и поведения пользователей, а также для уточнения их данных. Системы позволяют экспортировать данные в разных форматах.

Анализ данных с помощью искусственного интеллекта позволяет находить закономерности и тенденции, распределять данные по группам, выявлять исключения, определять связи между пользователями и их роли, собирать информацию из профилей и искать конкретных пользователей. Анализ текстов помогает выявить темы обсуждений, их эмоциональную окраску и основные направления.

Росфинмониторинг внедрил систему, основанную на машинном обучении, которая умеет отличать реальные компании от тех, что созданы только для перевода денег [9]. Эта система ищет в больших объемах данных информацию, которая не соответствует обычным правилам. Например, она может найти компании с неправильным количеством цифр в ИНН или ОГРН, с буквами вместо цифр или с неверными датами рождения.

Модель запускается автоматически по расписанию. Сначала загружаются свежие данные из ЕГРЮЛ, затем проводится классификация компаний и физических лиц с помощью заранее подготовленных моделей. Результаты этой классификации сохраняются в системе Росфинмониторинга. Такой подход позволяет находить повторяющиеся данные и улучшать их качество.

Качество моделей зависит от внешних факторов и может меняться. На это влияют выбранные характеристики, настройки пороговых значений, недостаток примеров для обучения и экспертные правила. Эксперт должен следить за состоянием моделей. Моделирование используется для классификации текстов по ключевым словам и анализа социальных сетей.

Ключевыми игроками в онлайн-пространстве экстремизма и терроризма являются криминальные и колумбайнерские сообщества, движение «МКУ», ультраправые группировки. Их сетевой характер подтверждается единой символикой, названиями, тематикой, общими администраторами или участниками, различной географической принадлежностью, взаимной рекламой и финансовыми связями.

Правонарушения часто связаны с финансовыми взаимодействиями между людьми. Во многих странах уже созданы схемы для выявления таких незаконных действий. Китайские исследователи Юэ Тянь, Гуаньцзюнь Лю, Цзяцзюнь Ван и Мэнчу Чжоу предлагают использовать модифицированную графическую нейронную сеть для обнаружения подобных отношений [18].

Онлайн-платежи, которые скрывают свою истинную цель, привлекают как финансовых мошенников, так и других преступников, нанося огромный ущерб частным лицам и банкам. Глобальные потери от таких действий достигли 25 миллиардов долларов в 2018 году и продолжают расти. Согласно данным Nilson Report, в 2020 году убытки увеличились до 28,65 миллиарда долларов. В ответ на это финансовые учреждения приняли меры для предотвращения мошенничества [15].

Традиционно онлайн-транзакции проверяются на соответствие определенным правилам, составленным экспертами. Если транзакция вызывает подозрения, ее передают модели обнаружения мошенничества. Эта модель, используя огромный объем исторических данных о транзакциях, выявляет закономерности, характерные для мошеннических действий. Цель модели – найти транзакции, которые с высокой вероятностью преследуют незаконные цели.

Возможности систем обнаружения связей ограничены и плохо адаптируются к быстро меняющимся мошенническим схемам. Ученые стремятся выявлять все больше схем мошенничества, но сложные схемы и системы обнаружения создают своего рода «динамическую игру». Записи о транзакциях часто содержат дополнительную информацию, такую как местоположение, время и предмет, что может быть полезно для анализа.

Существующие методы машинного обучения для обнаружения мошеннических транзакций требуют ручного создания признаков и построения классификаторов, что не гарантирует стопроцентное автоматическое обнаружение новых схем мошенничества. Между транзакциями существует множество взаимосвязей, анализ которых позволяет глубже изучить характер транзакций.

С другой стороны, поведение пользователей при совершении транзакций постоянно меняется, что затрудняет создание эффективной системы представления данных для обнаружения мошеннических действий. Мошенники постоянно меняют свои методы, что снижает эффективность многих существующих систем обнаружения и делает их менее универсальными [14].

В последнее время графовые нейронные сети (GNN) стали применяться для автоматического создания представлений данных в различных задачах прогнозирования [16]. В отличие от традиционных методов машинного обучения, GNN обрабатывают данные, учитывая их взаимосвязи, что позволяет строить более глубокие представления данных и затем использовать нейронные сети для

классификации объектов и прогнозирования связей между ними. Такие методы позволяют захватывать сложные взаимозависимости между данными и избегать создания искусственных признаков, что часто является недостатком традиционных подходов [17].

Несмотря на потенциал графовых нейронных сетей, их прямое применение к обнаружению мошеннических транзакций сопряжено с трудностями. Такие методы не учитывают взаимосвязи между различными характеристиками транзакций и не способны адаптироваться к динамическим изменениям в поведении пользователей. Исследования, проведенные специалистами [18], показали, что популярные модели GNN, такие как GraphSAGE и GCN, не позволяют надежно различать мошеннические и законные транзакции, как видно из рис. 1.

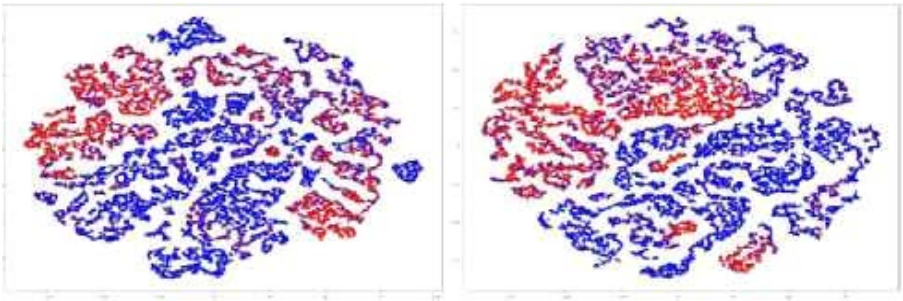

Рис. 1. Результаты визуализации GCN модели GNN. Красные узлы представляют собой мошеннические транзакции, а остальные – законные. (а) Перед обучением на наборе исходных финансовых данных. (б) После обучения на наборе адаптивных финансовых данных [18]

Кроме того, GNN сталкиваются с проблемой чрезмерного усреднения, когда представления узлов разных классов становятся слишком похожими. Эта проблема усиливается в контексте обнаружения мошенничества, где мошеннические узлы часто маскируются под законные, как показано на рис. 2. Такое смешивание классов данных еще больше затрудняет различение мошеннических и законных транзакций.

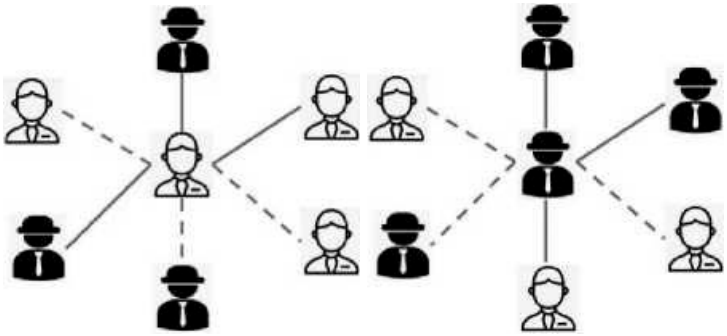

Рис. 2. Маскировка мошенников. Мошенники ослабляют свои подозрения, маскируя поведение держателей карт так, что система обнаружения считает, что это законные транзакции [18]

Для решения этой проблемы ряд авторов [18] предлагают использовать новый метод, названный ASA-GNN, основанный на адаптивной выборке и агрегации в графовых нейронных сетях для обнаружения мошеннических транзакций. Этот метод объединяет ранее предложенные авторами подходы. Сначала создается граф транзакций из необработанных данных, а затем, учитывая особенности мошеннических транзакций, анализируются взаимосвязи между различными характеристиками и динамические изменения в поведении пользователей.

Для отбора соседей, наиболее похожих на текущий узел, используется специальный алгоритм выборки, основанный на косинусной мере сходства и весе ребер. Этот алгоритм позволяет отфильтровать шумные соседи, сохраняя при этом структурную информацию графа. Для усиления эффекта отбора и уменьшения числа связей между мошенническими узлами предлагается увеличивать выборку подобных соседей.

Для борьбы с маскировкой мошенников вводится новая метрика разнообразия соседей, основанная на энтропии. Она позволяет оценить, насколько однородны или разнообразны соседи данного узла, отражая динамические изменения в поведении участников. Это помогает определить, приведет ли агрегирование информации от соседей к искажению представлений узла. Каждый узел получает свой коэффициент агрегации, позволяющий обеспечить компактность внутри классов и разделение между классами [3].

Исследователей предлагает новую модель для обнаружения мошеннических транзакций. Несмотря на существование множества методов, основанных на экспертных правилах и машинном обучении, которые успешно применяются в различных областях, включая обнаружение мошенничества, они имеют свои ограничения. Такие методы извлекают информацию из доступных данных для автоматического выявления признаков мошенничества, демонстрируя эффективность на известных типах мошенничества, однако они могут быть менее эффективны при обнаружении новых, неизвестных схем мошенничества [18].

Для решения этой проблемы эксперты обратились к методам глубокого обучения. Эти методы способны автоматически выявлять сложные взаимосвязи между различными характеристиками транзакций, обеспечивая более точное представление данных и позволяя эффективнее обнаруживать случаи мошенничеств. Одним из наиболее распространенных методов глубокого обучения в этой области является сверточная нейронная сеть (CNN).

Помимо анализа взаимосвязей между характеристиками транзакций, существующие методы также извлекают ассоциации между самими транзакциями для улучшения результатов обнаружения мошенничества. Одним из распространенных подходов является агрегирование данных. Этот метод объединяет транзакции в группы по определенным временным интервалам и затем вычисляет агрегированные признаки, такие как суммарная сумма транзакций в группе и количество транзакций.

Для повышения информативности о поведении пользователя, в качестве дополнительных признаков агрегации учитывались местоположение и код продавца. Это позволило расширить временной контекст анализа. Параллельно с этим, для изучения динамики транзакций во времени стали применяться ре-

куррентные нейронные сети (RNN). В частности, сети с долгой краткосрочной памятью (LSTM) позволяют эффективно улавливать эволюцию распределения данных во времени [18]. Учитывая постоянные изменения в распределении данных, предлагаются динамические методы для достижения более высоких показателей точности.

Для комплексного изучения различных взаимосвязей между транзакциями исследователи построили граф на основе имеющихся данных. Графовые нейронные сети (GNN) позволяют эффективно выявлять эти взаимосвязи и улучшать обнаружение мошенничества. Однако поскольку GNN обычно используют только один тип связи для построения графа, они могут упускать из виду множество других полезных признаков, характерных для мошеннических действий [11].

Большинство существующих методов не охватывают одновременно все аспекты взаимосвязи между транзакциями, взаимосвязи между их характеристиками и динамические изменения в поведении пользователей. Мы предлагаем использовать взвешенный мультиграф и графовые нейронные сети (GNN) для комплексного анализа этих взаимосвязей и динамики. Однако наш метод также имеет определенные ограничения.

GNN – это мощная структура, способная изучать представления графов путем моделирования связей данных в неевклидовых графах. Некоторые специалисты ранее рассматривали эту систему как совокупность операций свертки, аналогичных тем, что используются при обработке изображений, но применительно к данным графов. После этого было предложено и успешно применено множество методов, основанных на графах [18].

Большинство ранних алгоритмов строят представления узлов в два этапа: сначала определяют последовательность соседних узлов случайным образом, а затем используют модели машинного обучения для анализа топологической структуры графа и получения векторного представления для каждого узла. Несмотря на то, что эти алгоритмы учитывают топологическую структуру, они игнорируют атрибуты самих узлов.

Некоторые методы, работающие с графами, используют атрибуты узлов, основанные на текстовой и статистической информации. Например, Graph Convolutional Network (GCN) применяет спектральные графовые свертки для извлечения информации о признаках. Graph Attention Network (GAT) определяет важность различных соседей с помощью механизма внимания. GraphSAGE позволяет гибко обновлять представления узлов путем выборки и агрегирования соседних узлов. Метод сети реляционных графов (RGCN) способен моделировать данные с различными типами связей [18].

Последние исследования успешно применяли крупномасштабные графы, преодолевая вычислительные сложности. Учитывая разнообразие типов узлов и ребер в гетерогенных графах, а также их динамическую природу, были предложены гетерогенные GNN и динамические GNN. Параллельно с этим велись исследования по интерпретируемости и оптимизации структуры GNN.

Однако применение существующих GNN к обнаружению мошеннических транзакций не позволяет полностью использовать все доступные данные для по-

строения графов. В результате полученные графы могут не содержать важной информации. Метод конкурентных графовых нейронных сетей (CGNN) [18] использует гетерогенные графы для моделирования нормального и мошеннического поведения в электронной коммерции. Метод MAFI применяет трехмерный механизм пространственно-временных транзакций для анализа графов транзакций, основанных на геолокации. Кроме того, MAFI использует механизм внимания на уровне агрегации и уровне отношений для изучения информации о соседях и различных типах связей [13].

LGM-GNN использует локальную и глобальную информацию для создания более различимых представлений, улучшая точность прогнозирования. Однако эти методы не учитывают, что чрезмерная агрегация может привести к тому, что представления узлов разных классов станут слишком похожими и неразличимыми.

Это приводит к эффекту чрезмерного сглаживания в GNN. В контексте обнаружения мошеннических транзакций мошенники часто маскируют свою деятельность, имитируя поведение добросовестных пользователей. В результате, между узлами, связанными с мошенническими действиями, и легитимными узлами возникают сходства. Это усиливает негативное воздействие эффекта чрезмерного сглаживания.

Сталкиваясь с проблемой маскировки мошенников, метод CAmouflage-RESistant GNN (CARE-GNN) вводит метрику сходства с учетом меток, используя расстояние N для выбора соседей. Однако он фокусируется исключительно на сходстве меток. Расстояние N становится менее эффективным в многомерном пространстве и неспособно описать сложное сходство поведения. Транзакционный граф (TG), построенный в схеме, способен уловить взаимосвязи между динамическим поведением транзакций, статическими атрибутами транзакций и самими транзакциями [18].

Однако он не учитывает, что мошенники избегают взаимодействовать с другими мошенниками. Более того, он не решает проблему чрезмерного сглаживания. Авторы предлагают использовать косинусное сходство и взвешивание ребер для устранения этих недостатков, а также фокусируются на оценке негативного влияния агрегации окрестностей на проблему чрезмерного сглаживания.

Структура ASA-GNN представлена на рис. 3. Ее ключевые компоненты – выборка соседей и агрегация соседей. На этапе выборки соседей, чтобы отсеять шумных соседей и сохранить структурную информацию, мы вводим новую стратегию выборки соседей, основанную на косинусном сходстве и весе ребер. В процессе агрегации соседей важность различных соседей определяется механизмом внимания. Затем применяется метрика разнообразия, чтобы контролировать степень агрегации. В заключение, функция softmax вычисляет вероятность мошеннической транзакции.

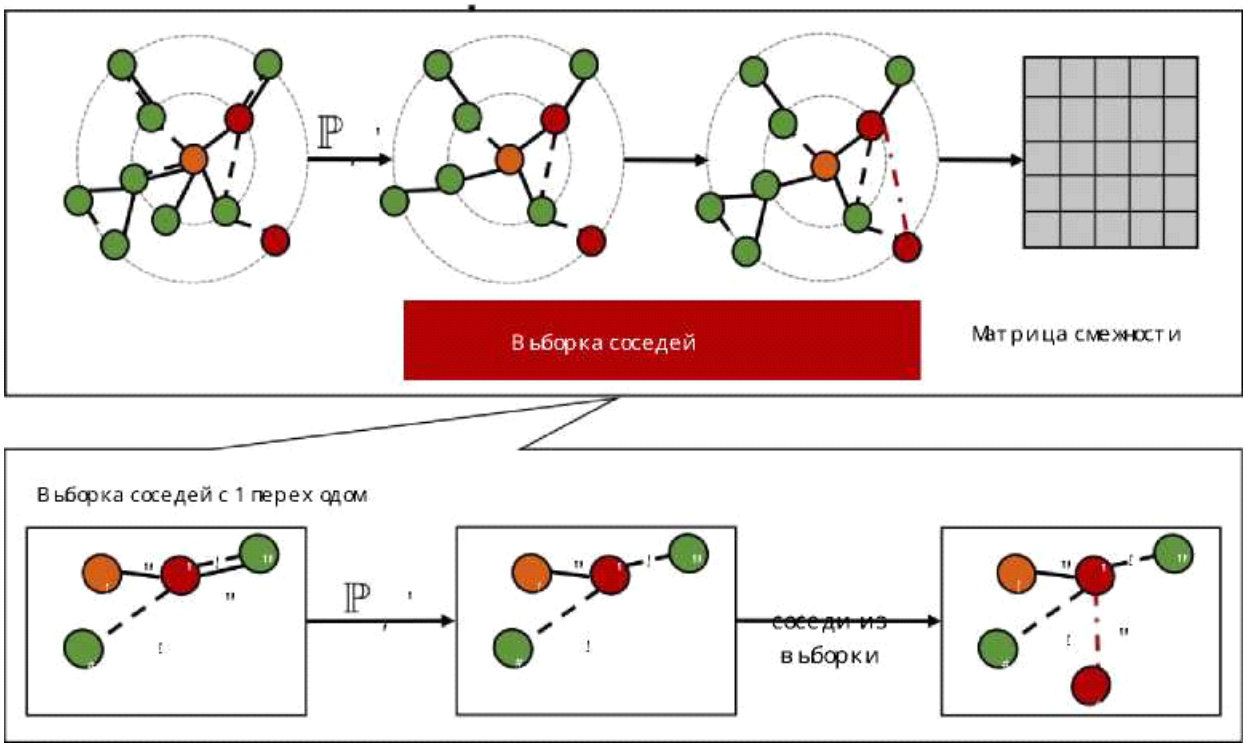

Рис. 3. Обзор ASA-GNN: 1) Выборка соседей на уровне узла, при которой соседи Top-z выбирают информацию о шуме фильтра каждого узла, а затем производят избыточную выборку соседей для мошеннических узлов. 2) Расчет показателя внимания и степени агрегации для изучения представлений. 3) Сценка вероятности того, что транзакция будет предсказана как мошенническая на уровне обнаружения [18]

GNN используют информацию о соседних узлах для построения более точных представлений. Существующие методы, такие как GraphSAGE, применяют случайный выбор соседей, исходя из предположения, что похожие узлы связаны между собой. Однако это не учитывает качество информации, предоставляемой соседями. Некоторые соседи могут быть бесполезными и вводить шум в процесс обучения, что затрудняет различение узлов разных классов. Другие соседи могут содержать много полезной информации, которую важно не упустить. Поэтому мы предлагаем новую стратегию выбора соседей, которая учитывает как степень сходства между узлами (косинусное сходство), так и силу связи между ними (вес ребра). Это позволяет отбирать наиболее информативных соседей и повысить качество полученных представлений [18].

Предлагается новая стратегия выбора соседей, учитывающая расстояние между узлами (вычисляемое с помощью косинусной меры сходства, часто применяемой в анализе пользовательского поведения) и вес ребра, соединяющего эти узлы. Такой подход позволяет более точно выбирать соседей и решает проблему, связанную с неэффективностью случайного выбора соседей в существующих методах.

Используемый в исследовании набор данных содержит 5 133,5 миллионов финансовых транзакций, осуществленных клиентами китайской компании во

втором квартале 2017 года. Все транзакции были предварительно классифицированы профессиональными следователями китайского банка на мошеннические и легальные [18]. Для устранения дисбаланса в данных, перед началом анализа была проведена пониженная выборка легитимных транзакций.

Для обработки данных использовалось горячее кодирование дискретных признаков и нормализация min-max для непрерывных. Учитывая высокую вычислительную сложность CARE-GNN, для экспериментов был выбран небольшой подвыбор данных (PR02), включающий последние 10 000 транзакций, что позволило ускорить процесс тестирования.

Набор данных TC1, предоставленный компанией Orange Finance, включает 160 764 транзакции, из которых 44 982 классифицированы как мошеннические, а 115 782 – как законные. Для создания обучающих и тестовых выборок данные были разделены по времени совершения транзакций. Транзакции одной недели формируют обучающую выборку, а следующей – тестовую. Таким образом, набор TC1 был разбит на три подвыборки: TC12, TC23 и TC34. К этим подвыборкам применялись те же методы предобработки, что и к наборам данных PR01 и PR02. Набор данных XF, выделенный из iFLYTEK2, содержит 20 000 записей и включает пять типов информации: основные данные, мультимедийные данные, временные данные, информацию об IP-адресах и информацию об устройствах. Набор XF сбалансирован по классам. Для обработки дискретных и непрерывных признаков применялись те же методы, что и для наборов данных PR01 и PR02. При построении графа транзакции рассматривались как узлы, а различные логические связи между ними – как ребра. Такой подход учитывает, что мошенники часто используют разнообразные схемы взаимодействия для создания сложных моделей мошенничества [18].

Наиболее ярким и масштабным примером организации криминальной субкультуры служит экстремистское движение «АУЕ» (его модель копируют аналогичные молодежные группировки).

Мониторинг российской соцсети VK в 2022 году выявил 91 559 сообществ, пропагандирующих криминальные субкультуры, активных в России, Беларуси, Казахстане, Азербайджане, Армении, Грузии и на Украине. Особую опасность представляют молодежные сетевые движения террористической направленности, проповедующие идеи «естественного отбора», «биомусора» и «человеконенавистничества». Характерными примерами таких движений являются «Колумбайн» («Скулшутинг») и «МКУ» (True Crime Community) [9].

Идеология «Колумбайн» (скулшутинг) пропагандирует массовые убийства в образовательных учреждениях, совершаемые учениками или посторонними лицами. Эта идеология основана на идеях собственного превосходства над другими, сравнивая себя с богом, на концепции естественного отбора, где часть людей считается «биомусором», и на оправдании насилия и убийств как способа восстановления справедливости.

После запрета движения в России в 2022 году последовала массовая блокировка связанных с ним пабликов, что привело к значительному сокращению их аудитории. Поскольку мониторинг деструктивных сообществ ведется по ключе-

вым словам, администраторы групп стали скрывать запрещенные названия, используя другие формулировки.

В ходе мониторинга социальных сетей и мессенджеров неоднократно фиксировалось использование российскими сторонниками террористического движения «Колумбайн» иностранных символов и иероглифов в качестве никнеймов и названий деструктивных сообществ. Цель такого подхода – маскировка запрещенного контента и затруднение мониторинга, выявления и блокировки опасных аккаунтов. Значительная часть пользователей перешла в закрытые группы и телеграм-каналы, где распространяется более радикальный и жесткий контент.

С субкультурой колумбайна тесно связано движение «МКУ», пропагандирующее убийства и насилие. Онлайн-сообщества «МКУ» в социальных сетях являются открытыми и содержат информацию о серийных убийцах, маньяках и террористах.

Учитывая запрет «МКУ» в России в 2023 году, открытые МКУ-сообщества стали активно ссылаться на закрытые ресурсы с экстремистскими материалами, включая видеоинструкции по изготовлению взрывных устройств, переделке оружия и проведению диверсий. Несмотря на пресечение деятельности более 150 сторонников «МКУ» в 50 регионах России в 2021–2022 годах, попытки организации диверсий на транспортной инфраструктуре и поджогов государственных зданий продолжаются [9].

С началом СВО появилась новая угроза – деятельность диверсионных сообществ и одиночек, финансирующих терроризм и экстремизм. Росфинмониторинг активно противодействует этой угрозе, включив в 2023 году в Перечень террористов и экстремистов 87 диверсантов.

Поиск исполнителей для диверсий ведется через телеграм-каналы, где заинтересованным лицам предлагают поджечь объекты за вознаграждение. После выполнения задания и предоставления фото- или видеодоказательств, исполнителю перечисляют деньги. В социальных сетях преобладают аккаунты, связанные с неонацистской идеологией, что свидетельствует о радикализации ультраправых групп.

Ультраправые группы отличаются геопривязкой к Украине и большим количеством подписчиков. Они открыто пропагандируют неонацистские идеи и терроризм в описаниях своих каналов и пабликов. Многие такие группы ведут открытую деятельность. Важнейшим способом противодействия распространению деструктивных идей в сети является тщательный анализ интернет-активности пользователей.

В рамках интеллектуального анализа данных ключевыми направлениями являются: изучение аномалий, то есть выявление отклонений от нормального поведения, и отслеживание динамики аккаунтов, позволяющее выявить процесс радикализации и вовлечения пользователей в преступную деятельность.

Современные интернет-технологии в сфере борьбы с противоправным контентом должны сочетать автоматический поиск с ручной проверкой отдельных аккаунтов и пользователей. Сегодня эта работа ведется вручную, что требует значительных ресурсов. Единой государственной системы с искусственным ин-

теллектом для решения этой задачи пока нет, хотя отдельные ведомства и компании разрабатывают свои решения.

В рамках ПОД/ФТ необходимо детально изучать особенности финансирования, отслеживать финансовые потоки и связи между участниками. Сбор средств осуществляется через закрепленные в профилях или ссылках платежные реквизиты, с использованием различных платформ и криптовалют. Собранные средства переводятся на иностранные счета через зарубежные сервисы.

В преступной деятельности, особенно в сфере незаконного оборота наркотиков, широко применяются боты, выполняющие функции обменников криптовалют. Эти инструменты позволяют быстро обменять рубли на различные виды цифровых валют, используя при этом миксеры для сокрытия следов финансовых операций.

В Росфинмониторинге для отслеживания таких транзакций применяется программа «Прозрачный блокчейн», которая автоматически создает связи между владельцами криптокошельков, их финансовыми операциями и партнерами по сделкам [9]. В период с 2020 по 2023 годы эта программа успешно использовалась для борьбы с отмыванием денег, полученных от онлайн-продаж наркотиков.

Разработка экспертных систем и баз знаний является неотъемлемой частью искусственного интеллекта. В России создание экспертных систем в сфере ПОД/ФТ основывается на национальных и секторальных оценках рисков, разрабатываемых Росфинмониторингом. Эти документы содержат всесторонний анализ существующих угроз, схем преступной деятельности, тенденций и прогнозов развития системы ПОД/ФТ, созданный экспертами в данной области.

Все схемы отмывания денег классифицируются по этапам: создание незаконного дохода, ввод этих денег в легальный оборот, перемещение средств, обналичивание, вывод капитала за рубеж и использование легализованных средств. Существует около 70 основных способов отмывания денег.

В отличие от данных в базах данных, экспертные оценки способов отмывания денег описывают не отдельные случаи, а повторяющиеся наборы характеристик целых групп схожих действий, то есть определенные шаблоны поведения [10]. Эксперты ФАТФ считают, что искусственный интеллект может частично или полностью автоматизировать анализ рисков и предложить новые способы их выявления.

Использование технологий искусственного интеллекта в этой области позволит создать общие и специфические модели преступной деятельности, обнаружить новые виды преступлений, автоматизировать проверку подозрительных операций. При создании этих моделей ключевую роль играют данные, полученные от экспертов. Экспертные системы в сфере ПОД/ФТ могут применяться для анализа данных, мониторинга, обучения, предоставления рекомендаций аналитикам и службам комплаенса. Такие системы способны выдвигать стандартные версии событий, устанавливать связи между лицами и организациями, а также поддерживать принятие решений.

Будущее российской системы противодействия отмыванию денег заключается в создании самообучающихся интеллектуальных систем, постоянно совершенствующихся на новых данных и знаниях. Эти системы позволят значи-

тельно сократить ручную работу аналитиков, обеспечивая быструю обработку сообщений о подозрительных финансовых операциях и предоставляя рекомендации и прогнозы для подразделений финансовой разведки, банков и других участников системы ПОД/ФТ.

Заключение. Перспективными направлениями использования ИИ в сфере ПОД/ФТ являются: семантический анализ текстов, аудио-, фото- и видеоматериалов в соцсетях с применением нейросетей для обнаружения экстремистского контента, предложений о продаже запрещенных товаров и финансовых данных; классификация и анализ постов в соцсетях для выявления пропаганды, призывов к терроризму и легализации доходов; автоматизированный анализ стримов и онлайн-трансляций; выявление ботов, распространяющих фейки и дипфейки; автоматизация мультивалютных расследований с криптовалютами.

Необходимо регулировать использование ИИ в сфере ПОД/ФТ. По аналогии с операторами связи, нужно получать информацию от разработчиков нейросетей о пользователях, интересующихся незаконными финансовыми операциями. Следует закрепить использование инновационных технологий для проверок, применять инструменты обработки естественного языка и биометрию для идентификации клиентов, а также использовать поисковые модели для выявления манипуляций на финансовых рынках.

Необходимо включить отдельный раздел об искусственном интеллекте в Концепцию развития национальной системы противодействия легализации доходов, полученных преступным путем, и финансированию терроризма (утверждена Президентом РФ 30.05.2018) [2]. Концепцию можно дополнить обсуждением рисков, связанных с преступлениями, использующими технологии ИИ, а также мерами по внедрению ИИ в Единую информационную систему ПОД/ФТ.

Внедрение искусственного интеллекта в систему противодействия отмыванию денег – это не самостоятельный процесс, изолированный от всего остального. Многие руководители недостаточно осведомлены о возможностях ИИ и о том, как его можно использовать для решения различных задач. Также отсутствуют единые стандарты для тестирования и внедрения инструментов искусственного интеллекта.

Искусственный интеллект – дорогостоящий инструмент, требующий высококвалифицированных специалистов и развитой технической инфраструктуры. Недостаток кадров в области анализа данных и ИИ, а также сложность интерфейсов программ могут препятствовать их эффективному использованию. Применение сложных алгоритмов должно быть сбалансировано с необходимостью оперативного проведения финансовых расследований [5].

Список литературы

1. Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 08.08.2024) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изм. и доп., вступ. в силу с 01.09.2024) // Российская газета. – № 151–152. – 09.08.2001.

2. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утв. Президентом РФ 30.05.2018) // СПС «КонсультантПлюс: Законодательство».

3. Егоров Г. Г. Перспективы развития современного гражданского права в условиях внедрения нейросетевых комплексов // В сборнике: Стратегия развития гражданского права в поисках ответов на вызовы XXI века (цифровые перспективы и действительность). Материалы II Международной научно-практической конференции. Волгоград, 2024. – С. 69–78.

4. Егоров Г. Г. Правовые формы обеспечения информационной безопасности в сети Интернет // Правовая парадигма. 2022. Т. 21. № 4. С. 70-76.

5. Егоров Г. Г. Нормативно-правовой оборот цифровых прав в России // В сборнике: Цифровые технологии и право. сборник научных трудов II Международной научно-практической конференции В 6 т. – Казань, 2023. – С. 154–168.

6. Красинский В. В., Леонов П. Ю., Морозов Н. В. Применение искусственного интеллекта в сфере противодействия отмыванию денег и финансированию терроризма // Современное право. – 2024. – № 5. – С. 75–82.

7. Казанцева С. Ю., Казанцев Д. А. Практика применения и перспективы развития технологий ИИ и робототехники в сфере финансового контроля // Вопросы инновационной экономики. – 2021. – № 2. – С. 553–564.

8. Красинский В. В. Цифровые технологии в антитеррорe // Современное право. – 2020. – № 6. – С. 123–129. – DOI: 10.25799/NI.2020.93.13.009.

9. Красинский В. В. Противодействие финансированию терроризма с использованием криптовалют // Современное право. – 2022. – № 9. – С. 108–116. – DOI: 10.25799/NI.2022.58.84.018

10. Шатских С. И. Методология оценки рисков ОД/ФТ как возможная основа инженерии знаний и искусственного интеллекта в контрольно-надзорной деятельности // Финансовая безопасность. – 2023. – № 39. – С. 60 – 65.

11. Khazane A., Rider J., Serpe M., Gogoglou A., Hines K., Bruss C. B., Serpe R. Deeptrax: Embedding graphs of financial transactions // 18th IEEE International Conference On Machine Learning And Applications (ICMLA). – IEEE. – 2019. – Pp. 126–133.

12. Leonov P. Y., Sushkov V.M., Krasinsky V.V. [at al] Detecting Money Laundering Patterns through Cash Flow Analysis a Neural Network-Based Approach // IEEE International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE). – Novosibirsk, 2023. – Pp. 1390 – 1393. – DOI: 10.1109/APEIE59731.2023.10347735

13. N. Jiang, F. Duan, H. Chen, W. Huang, and X. Liu, “Mafi: Gnn-based multiple aggregators and feature interactions network for fraud detection over heterogeneous graph // IEEE Transactions on Big Data. – 2021. – Vol. 8, № 4. – Pp. 905–919.

14. S. Yin, G. Liu, Z. Li, C. Yan, and C. Jiang, “An accuracy-and-diversitybased ensemble method for concept drift and its application in fraud detection,” in 2020 International Conference on Data Mining Workshops (ICDMW). IEEE, 2020. – Pp. 875–882.

15. The Nilson Report. [Online]. – URL: https://nilsonreport.com/mention/1313/1link/

16. X. Hou, K. Wang, C. Zhong, and Z. Wei, “ST-Trader: A Spatial-Temporal Deep Neural Network for Modeling Stock Market Movement,” IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 5, pp. 1015–1024, 2021.

17. Dou Y., Liu Z., Sun L., Deng Y., Peng H., Yu P. S. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters // Proceedings of the 29th ACM International Conference on Information & Knowledge Management, 2020. – Pp. 315–324.

18. Yue Tian, Guanjun Liu, Jiacun Wang, Mengchu Zhou Transaction Fraud Detection via an Adaptive Graph Neural Network // JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2021. Pp. 1–10

Т. Э. Кылчыкбаев,
кандидат юридических наук, доцент,
Кыргызский национальный университет
имени Ж. Баласагына

ПОНЯТИЕ КИБЕРБЕЗОПАСНОСТИ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

Аннотация. В современном цифровом мире понятие кибер-угрозы все больше проникает в нашу жизнь. Кибербезопасность становится важной проблемой для всех, от отдельных лиц до мировых компаний, корпораций и стран. В данной статье на основе анализа законодательных инициатив и практических мер органов исполнительной власти в сфере информационной безопасности Кыргызской Республики рассматриваются возможности государства по противодействию современным кибер-угрозам и формированию культуры личной информационной безопасности.

Ключевые слова: информационные технологии, кибербезопасность, цифровая информация, защита личных данных, законодательное регулирование

THE CONCEPT OF CYBERSECURITY IN THE KYRGYZ REPUBLIC

Abstract. In today's digital world, the concept of a cyber threat is increasingly penetrating our lives. Cybersecurity is becoming an important issue for everyone, from individuals to global companies, corporations and countries. This article, based on an analysis of legislative initiatives and practical measures of executive authorities in the field of information security of the Kyrgyz Republic, examines the state’s capabilities to counter modern cyber threats and create a culture of personal information security.

Key words: information technology, cybersecurity, digital information, personal data protection, legislative regulation

Введение. Цифровая революция, которая началась в конце XX века, продолжает стремительно развиваться, оказывая глубокое влияние на все сферы жизни современного общества. По данным Международного союза электросвязи