

2. Сурнин И.Н. Вопросы использования искусственного интеллекта в органах прокуратуры Российской Федерации // Молодой ученый. – 2024. – № 46 (545). – С. 216-219.

3. Ястреб Н.А. «Как проблема персональных данных меняет этику искусственного интеллекта?» // Философские проблемы информационных технологий и киберпространства. – 2020. – № 1 (17). – С. 29-44.

Лисицкая Снежана Александровна¹

Студентка 3 курса Института международного права и правосудия
Московского государственного лингвистического университета

lisitskaia134@gmail.com

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Аннотация. Статья исследует проблему дистанционного мошенничества в условиях цифровой трансформации. Анализируется эволюция мошеннических схем - от простого социального инжиниринга до сложных технологических методов (фишинг, поведенческие манипуляции). Рассматривается неэффективность традиционных профилактических мер, обусловленная когнитивными особенностями уязвимых групп и применением преступниками методов психологического воздействия. В качестве решения предлагается внедрение систем искусственного интеллекта для выявления преступных мошеннических действий. Проводится правовой анализ новых нормативно-правовых актов, выявляющий противоречие между необходимостью усиления контроля и защитой персональных данных. Делается вывод о необходимости комплексного подхода, сочетающего технологии искусственного интеллекта, совершенствование правового регулирования, развитие цифровой грамотности населения.

¹ Воронин Михаил Юрьевич, заведующий кафедрой национальной безопасности и правоохранительной деятельности, директор института международного права и правосудия Московского государственного лингвистического университета, доктор юридических наук, профессор

Ключевые слова: преступность, цифровое пространство, мошенничество, искусственный интеллект, нормативный правовой акт.

Lisitskaya Snezhana Alexandrovna

3rd year student at the Institute of International Law and Justice

Moscow State Linguistic University

COUNTERING CRIME IN THE DIGITAL SPACE

Annotation. The article explores the problem of remote fraud in the context of digital transformation. The evolution of fraudulent schemes is analyzed - from simple social engineering to complex technological methods (phishing, behavioral manipulation). The inefficiency of traditional preventive measures is considered, due to the cognitive characteristics of vulnerable groups and the use of psychological influence methods by criminals.

As a solution, it is proposed to implement artificial intelligence systems to detect criminal fraudulent activities. A legal analysis of new regulatory legal acts is carried out, revealing the contradiction between the need to strengthen control and personal data protection. The conclusion is made about the need for an integrated approach combining artificial intelligence technologies, improving legal regulation, and developing digital literacy among the population.

Keywords: crime, digital space, fraud, artificial intelligence, regulatory legal act.

Сегодня цифровое пространство — это наша обыденность. В 2024 году число россиян, ставших пользователями сети Интернет стало более 130 млн. человек. Речь идет как о его повседневном бытовом использовании, так и о применении сети Интернет для рабочей сферы, например внедрение во многих организациях электронного документооборота предоставило возможность не только получить доступ к информационным ресурсам, но и вести свою повседневную деятельность дистанционно.

Однако за всеми этими преимуществами скрываются и опасности, которые связаны с противоправными деяниями, совершаемыми с использованием информационно-телекоммуникационных технологий. Одной из остро стоящих проблем стало мошенничество, совершаемое дистанционно с использованием возможностей информационно-коммуникационных технологий. Начинается все с ежедневного обзвона сотен людей в целях поиска жертв, готовых назвать код из СМС.

Мы полагаем, что на сегодняшний день полностью искоренить данный вид преступлений просто невозможно. Идет постоянное совершенствование как информационно-коммуникационных технологий, так и технологий социальной инженерии. Если 15 лет назад преступники говорили потерпевшим, что кто-то из их родственников попал в аварию, то сегодня констатируется большое число новых мошеннических схем, включающих обращения от псевдодоставщиков цветов, до псевдосотрудников деканата, от псевдосотрудников банков, ФСБ, включая и создание фишинговых сайтов. В структуре преступных посягательств с использованием возможностей информационно-коммуникационных технологий мошенничества в 2023 году составили 70,2 процента.

Статистика отражает и резкий рост числа преступных деяний, связанных с неправомерным доступом к компьютерной информации, число в 2024 году выросло до 105773, учитывая, что 2023 году зарегистрировано 37101 преступления.

Названные факторы обусловили разработку и утверждение Концепции государственной системы противодействия противоправным деяниям, совершенным с использованием информационно-коммуникационных технологий. В качестве цели создания и деятельности государственной системы является защита интересов государства, общества и граждан от противоправных деяний в указанной сфере. Достижение поставленной цели возможно посредством реализации комплекса задач государственной системы, включающего широкий спектр деятельности начиная от прогнозирования и заканчивая укреплением международного сотрудничества в исследуемой сфере.

Нормативное правовое регулирование сферы противодействия преступлениям в цифровом пространстве находит свое развитие в Федеральном законе от 01 апреля 2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации». В первую очередь этот федеральный закон направлен на создание государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий.

Федеральным законом вносятся изменения и дополнения в ряд федеральных законов, например, в Федеральный закон от 02.12.1990 N 395-1 (ред. от 28.02.2025) «О банках и банковской деятельности»; Закон РФ от 07.02.1992 № 2300-1 (ред. от 08.08.2024) «О защите прав потребителей»; Федеральный закон от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»; Федеральный закон от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности»; Федеральный закон от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности» и ряд других.

Внесение изменений и дополнений в федеральные законы направлены на обеспечение создания государственной информационной системы и обеспечение эффективной работы этой системы. Вместе с тем мы предполагаем, что данный федеральный закон порождает и потенциальные правоприменительные проблемы, а именно конфликт с защитой персональных данных. Закон предполагает массовый сбор и анализ данных пользователей, что может вступить в противоречие с № 152-ФЗ «О персональных данных» и ст. 23–24 Конституции РФ (право на неприкосновенность частной жизни). Кроме того, № 41-ФЗ может породить проблемы с исполнением обязанностей IT-компаний по предоставлению информации, которые могут быть вызваны техническими сложностями — не все сервисы могут оперативно предоставлять данные (например, мессенджеры с шифрованием).

Основным недостатком названной выше Концепции государственной системы противодействия противоправным деяниям, совершенным с использованием информационно-коммуникационных технологий, и государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий является невнимание к такому, очень важному в настоящее время, аспекту – использованию искусственного интеллекта в области противодействия преступлениям в сфере информационно-коммуникационных технологий.

Например, возвращаясь к мошенничествам, мы констатируем, что мошенники — это не просто преступники, это в первую очередь отличные психологи. Многие потерпевшие говорят о том, что совсем не контролировали свои действия, а «отключив» голову, действовали по указаниям преступников, которые в свою очередь стараются работать очень быстро: не дают человеку сообщить о диалоге родственникам, сами выбирают адреса банков, в которых потерпевшие берут кредиты, причем если кредит не одобрили в одном банке, то мошенники могут вызвать такси потерпевшему неограниченное количество раз до любого отделения банка, пока сотрудники банка не осуществят выдачу кредита. В такой ситуации человек просто забывает о любых профилактических беседах и их содержании.

Необходим алгоритм действий, который будет учитывать все существующие мошеннические схемы, предопределять направления их совершенствования и предлагать механизм противодействия. Разработка этого алгоритма под силу искусственному интеллекту (далее – ИИ).

Когда мошенничество неизбежно, крайне важно выявить его как можно скорее, чтобы принять необходимые меры. Подлинность транзакции может быть определена только с помощью средств обнаружения мошенничества. Безусловно, человек не может вручную оценить каждую транзакцию для выявления

мошеннических операций. Именно поэтому необходимы автоматизированные решения для обнаружения мошенничества ¹.

Но мошенники орудуют не только посредством телефонных звонков. Многие совершают преступления в сфере электронной коммерции (торговли и предоставления услуг населению). Здесь ИИ тоже может внести свой вклад в предотвращение преступлений. Системы автоматического анализа способны обрабатывать информацию о покупателях и их действиях, чтобы выявлять потенциально мошеннические заказы. Опираясь на различные факторы, такие как взаимосвязь между покупателем и продавцом, историю покупок и другие данные, искусственный интеллект может обнаруживать попытки обмана и предотвращать возможные финансовые потери.

Важно отметить значимость искусственного интеллекта в области кибербезопасности. ИИ способен выявлять и предотвращать кибератаки, анализируя активность в цифровой среде. Он может распознавать угрозы и предлагать необходимые меры для их нейтрализации. С помощью ИИ разработчики могут создавать более защищённые онлайн-платформы, обеспечивая безопасность пользователей от потенциальных рисков.

Таким образом, повсеместное внедрение информационных технологий несет в себе не только преимущества, но и серьезные угрозы, связанные с появлением дистанционного мошенничества. Несмотря на активную профилактическую работу и новые законодательные меры, полностью искоренить этот вид преступлений пока не представляется возможным. В этих условиях ключевую роль в противодействии мошенничеству может сыграть искусственный интеллект, способный анализировать транзакции, выявлять подозрительные схемы и предотвращать финансовые потери в режиме реального времени.

¹ Нестерова В. А., Рыбакова В. А. Обзор использования искусственного интеллекта в обнаружении финансового мошенничества // Экономика и парадигма нового времени. 2024. №1 (22). URL: <https://cyberleninka.ru/article/n/obzor-ispolzovaniya-iskusstvennogo-intellekta-v-obnaruzhenii-finansovogo-moshennichestva> (дата обращения: 11.04.2025).

Принятые нормативно-правовые акты создают основу для системного противодействия киберпреступности, но их реализация должна сопровождаться четким регулированием и общественным контролем в целях избежания злоупотреблений со стороны правоохранительных органов и массовых нарушений прав граждан. Дальнейшее развитие технологий безопасности, международное сотрудничество в указанной сфере и повышение цифровой грамотности населения остаются важнейшими направлениями в борьбе с дистанционным мошенничеством. Только комплексный подход, сочетающий в себе технологические, правовые и просветительские меры, позволит минимизировать риски и сделать цифровую среду более безопасной.

Список литературы

1. Нестерова В. А., Рыбакова В. А. Обзор использования искусственного интеллекта в обнаружении финансового мошенничества // Экономика и парадигма нового времени. – 2024. – №1 (22). – URL: <https://cyberleninka.ru/article/n/obzor-ispolzovaniya-iskusstvennogo-intellekta-v-obnaruzhenii-finansovogo-moshennichestva> (дата обращения: 11.04.2025).

Нуруллин Никита Альбертович¹

Студент 2 курса Института государства и права
Тюменского государственного университета,
stud0000292053@study.utmn.ru

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АВТОМАТИЗАЦИИ ЮРИДИЧЕСКИХ ПРОЦЕССОВ

Аннотация. В данной статье проведен анализ вопросов касающихся развития искусственного интеллекта и его внедрения в юридические процессы. Основная цель анализа заключается в рассмотрении различных точек зрения, которые напрямую связаны с вопросами использования передовых технологий в

¹ Научный руководитель: **Калашников Никита Анатольевич**, ассистент кафедры теоретических и публично-правовых дисциплин.