УДК 343.72

Коржова Ксения Андреевна, студентка лечебного факультета ФГБОУ ВО «Курский государственный медицинский университет» Минздрава России.

e-mail: korzovaksenia0@gmail.com

Научный руководитель: Сергеева Наталия Митрофановна, кандидат фармацевтических наук, доцент кафедры организации и менеджмента фармации ФГБОУ ВО «Курский государственный медицинский университет» Минздрава России

МОШЕННИЧЕСКИЕ СХЕМЫ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация: в статье отмечается, что искусственный интеллект является не только новым и эффективным инструментом развития национальной экономики, но и инструментом мошенников для совершения различных преступлений. В работе рассмотрены основные направления применения мошенниками искусственного интеллекта и способы защиты от них.

Ключевые слова: искусственный интеллект, мошеннические схемы, национальная стратегия.

Korzhova Kseniya Andreyevna, a student of the Faculty of Medicine of Kursk State Medical University

e-mail: korzovaksenia0@gmail.com

Supervisor: Natalia Mitrofanovna Sergeeva, Candidate of Pharmaceutical Sciences, Associate Professor, Department of Organization and Management of Pharmacy, Kursk State Medical University, Ministry of Health of Russia

FRAUDULENT SCHEMES USING ARTIFICIAL INTELLIGENCE

Abstract: The article notes that artificial intelligence is not only a new and effective tool for the development of the national economy, but also a tool for fraudsters to commit various crimes. The paper examines the main areas of artificial intelligence use by fraudsters and methods of protection against them.

Keywords: artificial intelligence, fraudulent schemes, national strategy.

Искусственный интеллект является одной из самых важных технологий, которые доступны человеку в настоящее время: уже сейчас благодаря искусственному интеллекту происходит рост мировой экономики, ускорение инноваций во всех областях науки, повышение качества жизни населения, доступности и качества медицинской помощи, качества образования, производительности труда и качества отдыха [1]. Однако, искусственный интеллект (ИИ) является не только новым и эффективным инструментом цифровизации деятельности в современном обществе, но и «оружием» злоумышленников для совершения киберпреступлений [6].

Цель исследования - обзор современных методов мошенничества, основанных на использовании искусственного интеллекта и способов защиты от них. Работа выполнена на основании анализа научных публикаций ученых и экспертов по проблемам мошенничества с использованием искусственного интеллекта.

Анализ научных публикаций позволил выделить основные направления применения мошенниками искусственного интеллекта в процессе создания мошеннических схем [2,4]:

1. Фишинг, т.е. интернет-мошенничество, совершаемое с целью получения доступа к конфиденциальной информации пользователей.
2. Deepfake (глубокие подделки) – создание фальшивых видео и аудио. Такие подделки применяются для дезинформации или манипуляций.
3. Таргетирование - анализ больших объемов данных с помощью ИИ в целях выявления потенциальных жертв и адаптации мошеннического контента к конкретным слабостям человека.

4. Чат-боты с поддержкой ИИ используются для общения с потенциальными жертвами мошенничества в рамках процесса манипулирования ими для вымогательства.

5. Инвестиционные мошенничества – создание поддельных платформ с ИИ, имитирующих реальные финансовые операции и отзывы клиентов для обмана инвесторов.

6. Рассылка мошеннических электронных писем, СМС-сообщений.

7. Поддельные интернет-сайты платежных сервисов, торговых центров и т.д.

8. Подделка голоса и фотографий лица.

9. Взломы. Алгоритмы ИИ могут ускорить процесс взлома паролей, более эффективно прогнозируя и тестируя комбинации на основе утечек данных и распространенных моделей использования.

Отдельные авторы отмечают, что в настоящее время с помощью искусственного интеллекта появились и особенно активно используются мошенниками такие мошеннические схемы, как подделка документов и голосовых сообщений, организация сбора денежных средств на благотворительные цели с использованием поддельных видео- и фотодокументов, созданных искусственным интеллектом [5]. Получать образцы голоса мошенники могут из различных источников: голосовых сообщений, обычных звонков и т.д. [3].

В «Национальной стратегии развития искусственного интеллекта на период до 2030 года» отмечена недопустимость использования искусственного интеллекта в целях умышленного причинения вреда гражданам и организациям [1]. Однако эффективная борьба с мошенничеством требует комплексного подхода, включающего активное взаимодействие различных государственных структур, бизнеса и населения в целом, применение современных технологий, а также постоянное повышение финансовой грамотности населения.

Таким образом, в ходе исследования рассмотрены основные направления применения мошенниками ИИ и комплексный подход к решению рассматриваемой проблемы, который позволит минимизировать риски и обеспечить безопасное развитие цифрового общества в эпоху искусственного интеллекта.

Список использованных источников:

1. Российская Федерация. Указы Президента. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 г. № 490: послед. ред. // Официальные сетевые ресурсы Президента России: [сайт]. – URL: http://www.kremlin.ru/acts/bank/44731/page/1 (дата обращения: 30.09.2025)

2. Казаченко, И.С. Искусственный интеллект и мошенничество: новые угрозы и способы противодействия / И. С. Казаченко // Вестник науки. – 2025. – Т. 3, № 7(88). – С. 135-139.

3. Медведева, И.В. Новые виды мошенничества с использованием искусственного интеллекта / И. В. Медведева // Правовая среда в современной России: проблемы и перспективы развития : сборник научных статей II межвузовской научно-практической конференции, Саратов, 22 февраля 2024 года. – Саратов: Саратовский военный ордена Жукова Краснознаменный институт войск национальной гвардии, 2024. – С. 84-88].

4. Орлов, П.Р. Современные модели ИИ и новые виды мошенничества / П. Р. Орлов // V Международная научная конференция по междисциплинарным исследованиям : сборник статей V Международной научной конференции по междисциплинарным исследованиям, Екатеринбург, 15 апреля 2024 года. – Екатеринбург: Общество с ограниченной ответственностью "Институт Цифровой Экономики и Права", 2024. – С. 368-373.

5. Осипова, Д.В. Мошенничество, совершенное с использованием искусственного интеллекта: криминалистическая характеристика / Д. В. Осипова, Д. Д. Паутова // Современность в творчестве начинающего исследователя : материалы Всероссийской научно-практической конференции, Иркутск, 27 марта 2025 года. – Иркутск: Восточно-Сибирский институт МВД России, 2025. – С. 283-288.

6. Санина, Л.В. Особенности расследования мошенничества, совершенные с помощью искусственного интеллекта / Л. В. Санина, В. В. Коломинов // Право и государство: теория и практика. – 2024. – № 8(236). – С. 355-359.