Вестник Восточно-Сибирского института МВД России. 2025. № 3 (114). С. 157–166.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2025. Vol. no. 3 (114). Pp. 157–166.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья
УДК 343.985

ПРОБЛЕМА ПРЕСТУПНОГО ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА СЕРВИСАХ ИНТЕРНЕТ-ЗНАКОМСТВ

Гажаева Екатерина Ивановна
Краснодарский университет МВД России, Краснодар, Российская Федерация
Budylinakeit@yandex.ru

Введение: Современные информационно-телекоммуникационные технологии оказывают все большее влияние на различные сферы жизни общества. Одной из наиболее популярных форм коммуникации являются сервисы интернет-знакомств, которые предоставляют удобный интерфейс и платформу для поиска новых знакомств и общения. Однако вместе с очевидными преимуществами и удобствами такие онлайн-сервисы становятся благоприятной средой для совершения различных преступлений. Наряду с этим преступники стали активно осваивать и использовать современные инструменты, включая технологии искусственного интеллекта для реализации своих корыстных мотивов на сервисах интернет-знакомств. В данной статье рассматриваются способы использования искусственного интеллекта в преступных целях на сайтах для знакомств, а также вносится предложение о применении рекомендаций по методике выявления и пресечения правоохранительными органами фактов криминального использования технологий искусственного интеллекта на сервисах интернет-знакомств.

Материалы и методы. Основой для данного исследования послужили научные статьи ученых-криминалистов, нормы уголовного и уголовно-процессуального законодательства, результаты анкетных опросов и интервьюирования сотрудников следственных подразделений МВД России. Автором использовались общенаучные методы: анализ, синтез, индукция, дедукция, а также частнонаучные методы: сравнительно-правовой и формально-юридический.

Результаты исследования. В процессе анализа и изучения официальных статистических данных МВД России, научных статей на тему использования технологий искусственного интеллекта в преступных целях, а также по результатам анкетных опросов и интервьюирования сотрудников следственных подразделений МВД России, удалось

определить ряд способов преступного использования искусственного интеллекта на сервисах интернет-знакомств. В свою очередь, имея затруднения в процессе выявления использования искусственного интеллекта в преступных целях на сервисах интернет-знакомств, для правоохранительных органов предлагается последовательный алгоритм эффективного установления данных фактов.

Выводы и заключения. Проведенное исследование позволило сформулировать комплекс мер, направленных на эффективное выявление использования технологий искусственного интеллекта на сервисах для знакомств, а также уточнены способы, посредством которых субъект преступления реализует корыстный мотив.

Ключевые слова: искусственный интеллект, сервисы интернет-знакомств, преступное использование технологий искусственного интеллекта, нейросети, информационно-телекоммуникационные технологии, способы использования ИИ на сервисах для знакомств.

Для цитирования: Гажаева, Е. И. Проблема преступного использования технологий искусственного интеллекта на сервисах интернет-знакомств // Вестник Восточно-Сибирского института МВД России : науч.-практ. журн. Иркутск: Восточно-Сибирский институт МВД России. 2025. № 3 (114). С. 157–166.

5.1.4. Criminal law sciences (legal sciences)

Original article

THE PROBLEM OF CRIMINAL USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES ON ONLINE DATING SERVICES

Ekaterina I. Gazhaeva, Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russian Federation, Budylinakeit@yandex.ru

Introduction: Modern information and telecommunication technologies are having an increasing impact on various spheres of society. One of the most popular forms of communication is online dating services, which provide a user-friendly interface and platform for finding new acquaintances and communicating. However, along with the obvious advantages and amenities, such online services are becoming a favorable environment for the commission of various crimes. Along with this, criminals began to actively master and use modern tools, including artificial intelligence technologies, to realize their selfish motives on online dating services. This article discusses ways to use artificial intelligence for criminal purposes on dating sites, and also suggests developing minimally relevant recommendations on how law enforcement agencies can identify and prevent the criminal use of artificial intelligence technologies on online dating services.

Materials and Methods. The research was based on scientific articles by criminologists, the norms of criminal and criminal procedure legislation, the results of questionnaires and interviews with employees of investigative units of the Ministry of Internal

Affairs of Russia. The author used general scientific methods: analysis, synthesis, induction, deduction, as well as private scientific methods: comparative law and formal law.

The Results of the Study. In the process of analyzing and studying official statistics of the Ministry of Internal Affairs of Russia, scientific articles on the use of artificial intelligence technologies for criminal purposes, as well as based on the results of questionnaires and interviews with employees of investigative departments of the Ministry of Internal Affairs of Russia, it was possible to identify a number of ways of criminal use of artificial intelligence on online dating services. In turn, having difficulties in the process of detecting the use of artificial intelligence for criminal purposes on online dating services, a consistent algorithm is proposed for law enforcement agencies to effectively establish these facts.

Findings and Conclusions. The conducted research allowed us to formulate a set of measures aimed at effectively identifying the use of artificial intelligence technologies in dating services, as well as clarifying the ways in which the subject of the crime implements a selfish motive.

Keywords: artificial intelligence, online dating services, criminal use of artificial intelligence technologies, neural networks, information and telecommunication technologies, ways of using AI on dating services.

For citation: Gazhaeva E.I. Problema prestupnogo ispol'zovaniya tekhnologij iskusstvennogo intellekta na servisah internet-znakomstv [The Problem of Criminal Use of Artificial Intelligence Technologies on Online Dating Services]. Vestnik Vostochno-Sibirskogo institute MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2025, no.3 (114), pp. 157–166.

Родоначальником механизма для решения сложных задач и искусственного интеллекта как теории принято считать философа и математика Раймонда Луллия в XIII веке [1, с. 130], но появление искусственного интеллекта как научного явления произошло только в XX веке.

Развитие технологий искусственного интеллекта (далее ИИ) и параллельный рост популярности сервисов для знакомств создают новые возможности для совершения преступлений с их использованием. Проблема преступного использования технологий ИИ на сервисах интернет-знакомств (далее СИЗ) является актуальной как для самих пользователей, так и для провайдеров этих платформ. Технологии ИИ значительно упрощают создание и поддержание множества поддельных профилей, повышают степень реалистичности подделок, создавая серьезные риски финансового и репутационного характера для пользователей сервисов. Как отмечает Р. И. Дремлюга, «использование интеллектуальных систем повышает эффективность, снижает издержки, минимизирует риски и позволяет повысить охват преступной деятельностью» [2, с. 161]. Мы, несомненно, разделяем мнение автора, так как в данном случае преступный результат достигается без активного вовлечения преступника. То есть субъект преступления обучил и запустил систему, что позволяет в дальнейшем пользоваться результатами ее работы.

Согласно Указу Президента РФ от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», «ИИ - это комплекс

технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека, превосходящие их»[1].

В свою очередь И. В. Понкин и А. И. Редькина в работе «Искусственный интеллект с точки зрения права» дают общее разъяснение термину ИИ, утверждая, что в его основе лежит автоматическое управление, при котором программные алгоритмы заранее не задаются, а формируются самой системой управления на основе формализованных описаний целей, знаний о возможных действиях и информации о текущих изменениях состояния внешней среды [3]. Исходя из определения авторов, можем сделать вывод о том, что данные технологии обладают потенциалом как для повышения эффективности во многих сферах общественной деятельности, так и для использования их преступниками в целях реализации корыстных мотивов.

Так как СИЗ стали неотъемлемой частью повседневной жизни миллионов людей, возникла проблема появления новых видов преступлений. Технологии ИИ, такие как чат-боты, алгоритмы машинного обучения и нейронные сети, в настоящее время часто используются в преступных целях, создавая угрозу безопасности пользователей онлайн-ресурсов. В связи с этим возникает необходимость детального анализа и изучения новейших технологий и выявления их использования в преступных целях на онлайн-сервисах.

Согласно статистике МВД России, число преступлений, связанных с использованием сети Интернет, в том числе и на платформах для знакомств, продолжает расти. В 2024 году зарегистрировано более 40 тысяч случаев мошенничества в сети, что на 15% больше по сравнению с предыдущим годом. Около 10% из них связано именно с онлайн-знакомствами[2]. При этом значительное число преступлений остается незарегистрированным, поскольку потерпевшие не всегда осознают факт мошенничества. Однако отметим, что статистические данные о преступном использовании технологий ИИ на СИЗ отсутствуют в связи с тем, что процесс установления данных фактов затруднен, как и выявление субъекта преступления. Об этом же свидетельствуют результаты проведенного нами анкетирования 250 сотрудников следственных подразделений МВД России и интервьюирования 50 сотрудников: 96% респондентов указали на факт применения пользователями СИЗ в преступных целях технологии ИИ, но установить субъект преступления не представляется возможным, в связи с чем более 99% уголовных дел по данному факту приостановлены.

Рассматривая проблему преступного использования ИИ, В. Ю. Дроздов отмечал, что преступления в сфере информационно-телекоммуникационных технологий обладают высоким уровнем латентности, в связи с чем возникают дополнительные трудности у правоохранительных органов в процессе их установления и выявлении субъектов. Также автор обращает внимание на то, что ненадлежащее хранение и отсутствие архивов данных,

---

[1] Указ Президента РФ от 10.10.2019 N 490 "О развитии искусственного интеллекта в Российской Федерации" (с изменениями и дополнениями) ГАРАНТ. URL: https://base.garant.ru/72838946/?ysclid=m8mr6qxip72636380

[2] Официальный сайт статистики МВД России «Каждое четвертое преступление в России совершают через интернет». URL: https://мвд.рф/dejatelnost/statistics

используемых для обучения алгоритмов, может привести к созданию модифицированных версий ИИ [4]. Мы, несомненно, согласны с высказыванием В. Ю. Дроздова, так как криминальное использование технологий ИИ может привести к обходу систем безопасности и нанести колоссальный ущерб как гражданам, так и нашему государству.

Проанализировав работу технологий ИИ на сервисах для знакомств, мы пришли к выводу о том, что субъекты преступлений могут их использовать в корыстных целях следующими способами:

1. Фейковые профили и автоматизированные боты. Так, для автоматической генерации изображений с помощью нейросетей (например, GAN, This Person Does not Exist) преступники создают реалистичные, но несуществующие фотографии людей для маскировки своей реальной личности в целях поиска потенциальных жертв. Также преступники используют на сервисах для знакомств чат-боты, которые на основе ИИ способны автоматически отвечать на сообщения, используя сгенерированный стиль переписки, который приближен к «человеческому». Данный способ позволяет преступнику выстраивать долгосрочные коммуникации с потенциальными жертвами с минимальными затратами сил [5].

Deep fake-видео. Технологии замены лиц и синтеза речи позволяют создавать правдоподобные видео, в которых человек якобы участвует в реальной видеовстрече, или же преступники создают видео интимного характера с участием потенциальной жертвы. Что касается синтеза голоса, то преступники могут использовать сгенерированный голос, чтобы разговаривать по телефону от лица другого человека (например, wavel.ai).

Преступники, использующие фейковые профили и автогенерируемые сообщения, создают «схемы обмана», разыгрывают сценарии, целью которых является получение денежных средств от потенциальной жертвы. Также при помощи технологий ИИ преступники таргетированно подталкивают потенциальную жертву к переходу по вредоносным ссылкам, сбору конфиденциальной информации (пароли, номера карт и т. д). На сегодняшний день данное направление мошеннических схем определяется общим понятием - фишинг.

2. Манипуляции и социальная инженерия. В данном случае преступник выполняет действия поэтапно, а именно: 1) осуществляет сбор информации о потенциальной жертве (пол, возраст, предпочтения, модель поведения при переписке) и алгоритмически анализирует для эффективного дальнейшего воздействия; 2) автоматически сгенерированные сообщения могут быть адаптированы под эмоциональное состояние потенциальной жертвы с целью вызвать доверие и в последующем склонить к определенным действиям (например, финансовым переводам или передаче конфиденциальной информации и данных) [6].

3. Сбор конфиденциальных данных. Преступники, используя технологии ИИ, могут анализировать способы общения потенциальной жертвы, время отклика, любимые темы для незаметного составления ее психологического портрета. Еще одна из возможностей технологий ИИ, которую применяют преступники в корыстных целях, – это распознавание лиц. Анализ фотографий на СИЗ, поиск совпадений в социальных сетях, сопоставление с открытыми базами данных. Подобным образом преступники находят реальные аккаунты, контакты и адреса пользователей без их согласия.

По нашему мнению, причинами частого криминального использования технологий ИИ на СИЗ является доступность технологий. С развитием облачных сервисов и

появлением открытых библиотек машинного обучения (например, Tensor Flow, Py Torch и др.) построение и обучение моделей стало гораздо проще. Таким образом, преступнику не обязательно обладать набором познаний в сфере нейронных сетей, поскольку он может получить готовые решения и адаптировать их под свои корыстные мотивы. Причиной также является широкая аудитория и анонимность СИЗ, ведь они становятся привлекательны для преступников ввиду большого количества потенциальных жертв, а также возможности быстрой смены учетных записей и низкого риска разоблачения, что, несомненно, повышает их интерес к использованию данных платформ.

На сегодняшний день актуальной задачей для криминалистической науки является разработка научно обоснованных методических рекомендаций по выявлению и пресечению преступного использования технологий ИИ на СИЗ. Вследствие чего нами предлагаются рекомендации, способствующие своевременному и эффективному выявлению фактов криминального использования технологий ИИ в преступных целях.

1. Лингвистический анализ или семантический анализ текстов. Современные генераторы текстов на базе технологий ИИ (например, крупные языковые модели) довольно-таки качественно имитируют стиль и лексику реальных людей. Однако при глубоком лингвистическом анализе можно обнаружить определенные признаки автоматической генерации:

а) слишком правильная или однообразная грамматика;

б) статистически «редкие» сочетания слов, которые не часто встречаются в обычной речи носителей языка;

в) отсутствие индивидуальных стилистических особенностей, присущих реальному человеку.

Следовательно, правоохранительные органы могут использовать вышеуказанный метод для выявления подобных моделей на сервисах для знакомств. Также при расследовании данных видов преступлений необходимо осуществить сбор эталонов преступного общения (сообщения, шаблонные фразы). В этом случае, машинное обучение помогает автоматически сопоставлять текст новых подозрительных аккаунтов с «базой мошенников», определяя степень совпадений по ключевым словам и структуре.

2. Анализ изображений и выявление дипфейков и генеративных изображений. Сотрудники правоохранительных органов могут использовать программные инструменты, которые анализируют метаданные фото, проверяют цифровые артефакты и аномалии пикселей. У дипфейков часто присутствуют неестественные детали (размытые края ушей, асимметрия лица, неправильное расположение теней, несоответствие фона и освещения). Специальные нейросети, обученные распознавать признаки синтетического контента, эффективно помогают при решении этой задачи. Для выявления поддельных профилей сотрудники правоохранительных органов могут проводить обратный поиск по изображению через популярные поисковые системы, например, такие как *OSINT* [7]. Если фотография найдена в базе стоковых изображений, на личных страницах других людей или на сайтах с дипфейк-контентом, это может указывать на фальсифицированный профиль. Ввиду этого анализ изображений с аккаунта СИЗ будет способствовать эффективному установлению сгенерированных фотографий. Отметим, что данные действия будут результативны лишь во взаимодействии сотрудников правоохранительных органов с модераторами платформ.

3. Анализ аномалий поведения. Профили, в которых используются технологии ИИ, нередко взаимодействуют со множеством пользователей в короткий промежуток времени.

Например, бот может почти мгновенно отвечать на сообщения, либо рассылать большое количество одинаковых приветствий. Алгоритмы мониторинга выявляют подобную интенсивность, сигнализируя о возможном бот-аккаунте. Относительно же анализа временной активности, то благодаря ему часто можно обнаружить неестественные схемы (например, профиль активен круглосуточно без перерывов). Так как для нормального человека характерны перерывы во времени активности (сон, работа и т.д.), а ИИ-бот может работать 24/7 [8].

В процессе выявления криминального использования технологий ИИ на СИЗ, сотрудникам правоохранительных органов необходимо проверить информацию: 1) с какими аккаунтами вступает в контакт подозрительный профиль; 2) как быстро устанавливаются «дружеские связи»; 3) насколько разнообразна география знакомств. Слишком быстрое увеличение количества друзей, одинаковые сообщения, напоминающие «сеть ботов» указывают на искусственное продвижение профиля.

4. Сотрудничество правоохранительных органов с модераторами СИЗ. Важным для правоохранительных органов при расследовании подобных видов преступлений становится взаимодействие с модераторами сервисов [9]. Ведь именно у модераторов платформ находятся журналы событий и внутренняя статистика, которая позволяет установить следующее:

а) видеть изменения в профиле (смена фотографий, описаний);

б) фиксировать IP – адреса, геолокацию и другие технические данные;

в) отслеживать схожие аккаунты, принадлежащие одному лицу;

г) выявлять массовую регистрацию профилей с одних и тех же платежных инструментов.

При наличии постановления суда или в рамках оперативно розыскных мероприятий правоохранительные органы могут запросить эти данные и выявить субъект преступления.

5. Технические инструменты отслеживания ИИ – активности. Существуют онлайн-сервисы и локальные приложения (AI – детекторы) текста, которые по определенным признакам могут оценивать, создан ли тот или иной текст при помощи ИИ. Эти технологии постоянно совершенствуются, повышая вероятность точного определения оригинального текста. Отметим, что в настоящее время сотрудникам правоохранительных органов необходимо использовать фильтрацию геолокационных аномалий в связи с тем, что преступники стали активно использовать VPN или прокси-сервисы для сокрытия своего реального местонахождения. Аналитические системы, включая системы, использующие ИИ, способны выявлять аномальные схемы подключения: резкие скачки IP-адресов в разных странах, использование подозрительных хостингов и т. д [10].

Также немаловажным является анализ устройств и технических параметров, так как иногда для автоматизации массовых рассылок и контроля ботов, преступники используют эмуляторы мобильных устройств. Сотрудникам правоохранительных органов необходимо проверять «цифровые следы» таких эмуляторов: когда при подключении к СИЗ выдаются нехарактерные комбинации параметров (версия операционной системы, User-Agent браузера и т. д.), тогда данные могут свидетельствовать о преступном профиле.

В связи с вышеизложенным можем сделать вывод о том, что использование ИИ на СИЗ несет в себе как позитивные, так и негативные аспекты. Так как, с одной стороны, ИИ помогает в работе добропорядочным пользователям: подбирает подходящих партнеров, осуществляет фильтрацию оскорбительного контента и заблаговременно блокирует его. С другой стороны, именно технологии ИИ открывают преступнику новые инструменты для

создания поддельных профилей, посредством которых субъект преступления способен обмануть даже опытных пользователей.

Подводя итоги нашей научной статье, можно сделать следующие выводы:

1. В связи с появлением новейших технологий и разработкой алгоритмов искусственного интеллекта повысился спрос на их применение в преступных целях. Конкретно в случаях с СИЗ и криминальным использованием технологий ИИ на данных платформах, отмечаем, что преступники научились создавать фейковые профили и чат-боты, генерируя достаточно реалистичные фото. А при помощи технологий замены лиц и синтеза речи создают правдоподобные видео, в которых человек якобы участвует в реальной видеовстрече для реализации своих корыстных целей.

2. С помощью алгоритмов искусственного интеллекта преступник может создавать план построения диалога, а также осуществлять сбор конфиденциальной информации, что позволяет ему находить реальные аккаунты, контакты и адреса пользователей без их согласия, используя их в последующем в преступных целях.

3. Предлагаем правоохранительным органам рекомендации, способствующие своевременному и эффективному выявлению фактов криминального использования технологий ИИ на СИЗ в преступных целях.

Представляется, что предлагаемые нами решения будут активно способствовать предупреждению преступлений в отношении пользователей СИЗ, что в результате повлечет за собой снижение преступности в сфере информационно-телекоммуникационных технологий и сделает виртуальное пространство безопасней. Безусловно, по мере развития технологий схемы преступников на СИЗ будут становиться все более качественными, однако при взаимодействии сотрудников правоохранительных органов и модераторов СИЗ уровень рисков обмана в цифровом пространстве значительно снизится.

СПИСОК ИСТОЧНИКОВ

1. Боровская, Е. В., Давыдова, Н. А. Основы искусственного интеллекта: учебное пособие /. 4-е изд., электрон. М.: Лаборатория знаний, 2020. 130 с;

2. Дремлюга, Р. И. Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. №3. URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-v-prestupnyh-tselyah-ugolovno-pravovaya-harakteristika;

3. Понкин, И. В., Редькина, А. И. Искусственный интеллект с точки зрения права // Вестник РУДН. Серия: Юридические науки. 2018. №1. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-s-tochki-zreniya-prava;

4. Дроздов, В. Ю. Детерминанты преступности в сфере искусственного интеллекта // Закон и право. 2024. №10. URL: https://cyberleninka.ru/article/n/determinanty-prestupnosti-v-sfere-iskusstvennogo-intellekta;

5. Кавеева, А.Д., Гурин, К.Е. Искусственные профили «В Контакте» и их влияние на социальную сеть пользователей // ЖССА. 2018. №2. URL: https://cyberleninka.ru/article/n/iskusstvennye-profili-vkontakte-i-ih-vliyanie-na-sotsialnuyu-set-polzovateley;

6. Вакалова, Д. Е. Искусство манипуляции: как социальная инженерия ставит под угрозу нашу безопасность // Вестник науки. 2024. №11 (80). URL: https://cyberleninka.ru/article/n/iskusstvo-manipulyatsii-kak-sotsialnaya-inzheneriya-stavit-pod-ugrozu-nashu-bezopasnost;

7. Дворянкин, О. А. OSINT, PENTEST и нетсталкинг - информационные технологии интернета // НАУ. 2022. №84-2. URL: https://cyberleninka.ru/article/n/osint-pentest-i-netstalking-informatsionnye-tehnologii-interneta;

8. Саенко, И. Б., Котенко, И. В., Аль-барри, М. Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. 2022. №2 (48). URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennyh-neyronnyh-setey-dlya-vyyavleniya-anomalnogo-povedeniya-polzovateley-tsentrov-obrabotki-dannyh;

9. Федоренко, С. П. Электронные платформы взаимодействия правоохранительных органов и гражданского общества как средство защиты правопорядка // Вестник юридического факультета Южного федерального университета. 2020. №3. URL: https://cyberleninka.ru/article/n/elektronnye-platformy-vzaimodeystviya-pravoohranitelnyh-organov-i-grazhdanskogo-obschestva-kak-sredstvo-zaschity-pravoporyadka;

10. Гладков, Э. А. Применение методов искусственного интеллекта для мониторинга состояния инфраструктуры // Вестник науки. 2024. №12 (81). URL: https://cyberleninka.ru/article/n/primenenie-metodov-iskusstvennogo-intellekta-dlya-monitoringa-sostoyaniya-infrastruktury.

REFERENCES

1. Borovskaya E. V., Davydova N. A. Osnovy iskusstvennogo intellekta [Fundamentals of artificial intelligence]. Moscow, Laboratory of Knowledge, 2020, 130 p;

2. Dremlyuga R. I. Ispol'zovanie iskusstvennogo intellekta v prestupnyh celjah: ugolovno-pravovaja harakteristika [The use of artificial intelligence for criminal purposes: criminal and legal characteristics]. Aziatsko-Tihookeanskij region: jekonomika, politika, pravo. - Asia-Pacific region: economics, politics, law. 2021, no.3. URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-v-prestupnyh-tselyah-ugolovno-pravovaya-harakteristika;

3. Ponkin I.V., Redkina A.I. Iskusstvennyj intellekt s tochki zrenija prava [Artificial intelligence from the point of view of law]. Vestnik RUDN. Serija: Juridicheskie nauki. - Vestnik of the RUDN University. Series: Legal Sciences. 2018, no.1. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-s-tochki-zreniya-prava;

4. Drozdov V.Y. Determinanty prestupnosti v sfere iskusstvennogo intellekta [Determinants of crime in the field of artificial intelligence]. Zakon i pravo - Law and legal 2024, no.10. URL: https://cyberleninka.ru/article/n/determinanty-prestupnosti-v-sfere-iskusstvennogo-intellekta;

5. Kaveeva A.D., Gurin K.E. Iskusstvennye profili «V Kontakte» i ih vlijanie na social'nuju set' pol'zovatelej [Artificial VKontakte profiles and their impact on the social network of users]. ZHSSA. 2018, no.2. URL: https://cyberleninka.ru/article/n/iskusstvennye-profili-vkontakte-i-ih-vliyanie-na-sotsialnuyu-set-polzovateley;

6. Vakalova D. E. Iskusstvo manipuljacii: kak social'naja inzhenerija stavit pod ugrozu nashu bezopasnost'[The art of manipulation: how social engineering endangers our security]. Vestnik nauki - Vestnik of Science. 2024, no. 11 (80), URL: https://cyberleninka.ru/article/n/iskusstvo-manipulyatsii-kak-sotsialnaya-inzheneriya-stavit-pod-ugrozu-nashu-bezopasnost;

7. Dvoryankin O.A. OSINT, PENTEST i netstalking - informacionnye tehnologii interneta [OSINT, PENTEST and netstalking - information technologies of the Internet].

NAU. 2022, no. 84-2. URL: https://cyberleninka.ru/article/n/osint-pentest-i-netstalking-informatsionnye-tehnologii-interneta;

8. Saenko I.B., Kotenko I.V., Al-barry M.H. Primenenie iskusstvennyh nejronnyh setej dlja vyjavlenija anomal'nogo povedenija pol'zovatelej centrov obrabotki dannyh [The use of artificial neural networks to detect abnormal behavior of users of data centers]. Voprosy kiberbezopasnosti - Cybersecurity issues. 2022, no. 2 (48), URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennyh-neyronnyh-setey-dlya-vyyavleniya-anomalnogo-povedeniya-polzovateley-tsentrov-obrabotki-dannyh;

9. Fedorenko S.P. Jelektronnye platformy vzaimodejstvija pravoohranitel'nyh organov i grazhdanskogo obshhestva kak sredstvo zashhity pravoporjadka [Electronic platforms for interaction between law enforcement agencies and civil society as a means of protecting law and orde]. Vestnik juridicheskogo fakul'teta Juzhnogo federal'nogo universiteta - Vestnik of the Faculty of Law of the Southern Federal University. 2020, no.3. URL: https://cyberleninka.ru/article/n/elektronnye-platformy-vzaimodeystviya-pravoohranitelnyh-organov-i-grazhdanskogo-obschestva-kak-sredstvo-zaschity-pravoporyadka;

10. Gladkov E. A. Primenenie metodov iskusstvennogo intellekta dlja monitoringa sostojanija infrastruktury [Application of artificial intelligence methods for monitoring the state of infrastructure]. Vestnik nauki - Vestnik of Science. 2024, no.12 (81), URL: https://cyberleninka.ru/article/n/primenenie-metodov-iskusstvennogo-intellekta-dlya-monitoringa-sostoyaniya-infrastruktury.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Гажаева Екатерина Ивановна, адъюнкт. Краснодарский университет МВД России, Россия, 350005, Российская Федерация, Краснодар, улица Ярославская, 128.

INFORMATION ABOUT THE AUTHOR

Gadzhaeva Ekaterina Ivanovna, postgraduate student. Krasnodar University of the Ministry of Internal Affairs of Russia, 128 Yaroslavskaya Street, Krasnodar, 350005, Russian Federation.

Статья поступила в редакцию 19.04.2025; одобрена после рецензирования 22.05.2025; принята к публикации 28.07.2025.
The article was submitted 19.04.2025; approved after reviewing 22.05.2025; accepted for publication 28.07.2025.