

**Ссылка для цитирования этой статьи:**

Долгова И.В., Жамборов А.А. Использование возможностей искусственного интеллекта для борьбы с преступностью // Human Progress. 2025. Том 11, Вып. 7. С. 27. URL: [http://progress-human.com/images/2025/Tom11\\_7/Dolgova.pdf](http://progress-human.com/images/2025/Tom11_7/Dolgova.pdf) DOI 10.46320/2073-4506-2025-7a-24.

УДК 343.85

## **ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ БОРЬБЫ С ПРЕСТУПНОСТЬЮ**

**Долгова Ирина Владимировна**

кандидат социологических наук,  
доцент кафедры Менеджмента и предпринимательского права,  
Северо-Кавказский институт,  
Российская академия народного хозяйства и государственной службы  
при Президенте Российской Федерации,  
г. Пятигорск, Российская Федерация

**Жамборов Анзор Анатольевич**

кандидат юридических наук,  
доцент кафедры Огневой подготовки,  
Северо-Кавказский институт повышения квалификации (филиал),  
Краснодарский университет МВД России,  
г. Нальчик, Российская Федерация

**Аннотация.** В статье раскрывается потенциал методов искусственного интеллекта для выявления и предотвращения преступлений. Представлена характеристика методов искусственного интеллекта и рассмотрен опыт применения их в практике российских правоохранительных органов. Обозначены вызовы и ограничения, затрудняющие использование искусственного интеллекта в деятельности органов правопорядка.

Авторами делается акцент на том, что искусственный интеллект обладает огромным потенциалом в области выявления и предотвращения преступлений, эффективность этих инструментов зависит от способности профессионалов эффективно их использовать. Поэтому, имеется необходимость в наличии постоянных образовательных и обучающих программ, которые позволят сотрудникам правоохранительных органов быть в курсе новейших технологий и методик искусственный интеллект. При этом, в качестве одной из основных целей реализации данных программ должно быть - устранение разрыва между традиционными методами расследования и современными цифровыми инструментами, обеспечивая

беспрепятственную интеграцию искусственного интеллекта в повседневную деятельность правоохранительных органов.

**Ключевые слова:** искусственный интеллект, методы, нейросети, правоохранительные органы, борьба с преступностью.

Стремительное развитие информационных технологий открывает новые горизонты для всех аспектов общественной жизни, однако одновременно предоставляет криминальным элементам современные инструменты для совершения правонарушений. Это создает дополнительные угрозы для безопасности граждан, бизнеса и общества в целом. Правоохранительным органам необходимо быть готовыми к противодействию «интеллектуальным» преступлениям, особенно тем, которые представляют опасность для личной или общественной безопасности. Использование искусственного интеллекта (ИИ), в частности технологий машинного обучения, позволяет повысить уровень осведомленности о текущих и потенциальных угрозах, а также оптимизировать процесс принятия сложных решений в борьбе с преступностью [1].

Искусственный интеллект (ИИ) представляет собой «программный комплекс, который способен воспроизводить человеческие навыки: планировать, решать проблемы, давать советы, а также обучаться и улучшать свою работу в процессе выполнения задач» [2].

Понятия «искусственный интеллект» и «нейросеть» часто путают, воспринимая их как одно и то же, но они не тождественны.

Искусственный интеллект – это «более широкая область информатики, которая занимается созданием систем, (распознавание речи, принятие решений, планирование, обучение и многое другое)» [3, с. 22].

Нейросети же являются лишь одной из технологий в арсенале ИИ, наряду с другими подходами, такими как логические системы или статистические методы, и не охватывают всю область ИИ. Нейросеть по сути – это математическая модель, состоящая из множества взаимосвязанных узлов (нейронов), организованных в слои, которые обрабатывают входные данные, преобразуют их и выдают результат [4, с. 31]. Нейросети обучаются на больших объемах данных, выявляя закономерности и корреляции, что позволяет им решать задачи, такие как распознавание изображений, обработка текстов или прогнозирование.

Другими словами, нейросеть - это инструмент или метод внутри ИИ, который наиболее хорош для задач, требующих обработки больших данных и выявления сложных закономерностей (например, компьютерное зрение). ИИ, в свою очередь, может решать задачи без нейросетей, используя правила, логику или другие алгоритмы.

Сегодня применение технологий искусственного интеллекта охватило практически все сферы деятельности - это транспорт и логистика, торговля и финансы, культура и здравоохранение, военная промышленность и судебная системы и др. Использование ИИ дает возможность не только автоматизировать любой процесс, но и настроить его в соответствии с конкретной задачей человека, ведомства или производства. В каждой из этих областей есть свои цели, задачи и неопределённости.

В сферах общественной безопасности, наблюдения, предотвращения преступлений и криминалистических расследований, а также в прогнозировании вероятности будущих преступных деяний использование ИИ особенно актуально, и работа по его внедрению и ведется очень активно.

Европейские страны и США начали использовать ИИ для борьбы с преступностью примерно с середины 2010-х годов, хотя эксперименты с предшествующими технологиями, такими как предиктивная аналитика, стартовали раньше.

В США пионером стало использование программы PredPol (Predictive Policing) в 2011 году в Лос-Анджелесе. Она анализировала данные о преступлениях для прогнозирования «горячих точек». К 2015 году алгоритмы ИИ, такие как COMPAS, активно применялись в судах для оценки рецидивизма. С 2017 года ФБР и полиция начали внедрять ИИ (например, технологии от Clearview AI) для анализа видеонаблюдения и распознавания лиц.

В Европе ИИ стал применяться чуть позже. В 2016 году полиция Великобритании запустила проект HART (Harm Assessment Risk Tool) для оценки рисков рецидивизма. В Нидерландах с 2017 года полиция использует CAS (Crime Anticipation System) для прогнозирования преступлений. Германия и Франция начали внедрять ИИ для анализа данных и распознавания лиц в 2018-2019 годах, но с ограничениями из-за строгих законов о конфиденциальности.

В России использование ИИ для борьбы с преступностью началось в конце 2010 -х гг. Одним из первых примеров является внедрение системы FindFace для распознавания лиц. Широкое практическое применение ИИ в российской правоохранительной деятельности началось в 2019 году, когда Указом Президента РФ № 490 от 10.10.2019 была утверждена Национальная стратегия развития ИИ до 2030 года [5]. Стратегия включает обеспечение национальной безопасности и правопорядка как приоритетные направления. Это стимулирует внедрение ИИ в правоохранительной деятельности.

Сегодня можно говорить о все более широком использовании возможностей ИИ в выявлении и предотвращении преступлений. Рассмотрим ряд методов, принятых на

вооружение органами охраны правопорядка различных государств, и отметим особенности их применения в России.

Правоохранительные органы могут осуществлять распознавание лиц и проводить видео аналитику, используя метод глубокого обучения - сверточные нейронные сети (CNN) для обработки видеопотоков с камер наблюдения и идентификации подозреваемых в реальном времени [6]. В крупных городах России, в частности, в Санкт-Петербурге, Казани, Сочи, а особенно в Москве, в рамках программы «Безопасный город» уже используются камеры с распознаванием лиц. В Северо-Кавказском федеральном округе система «Безопасный город» действует в Грозном, Махачкале, Нальчике, Пятигорске и др. При этом применяются алгоритмы компьютерного зрения. Технологические решения для МВД поставляют российские компании, такие как VisionLabs и NtechLab.

Алгоритм глубокого обучения, благодаря точной настройке, обеспечивает высокую достоверность прогнозирования при наличии необходимого набора данных о преступлениях в конкретной среде.

Искусственный интеллект может использовать модели машинного обучения для прогнозирования «горячих точек» преступности, используя данные о месте, времени, типе и обстоятельствах преступления. Полноценные системы предиктивной аналитики, такие как PredPol в США, в России пока ограничены из-за неравномерного доступа к данным в регионах. Вместе с тем, в Москве и других крупных городах данные с камер, геолокации и полицейских отчетов анализируются для оптимизации маршрутов патрулей. Также в некоторых регионах данные из системы «Безопасный город» используются для распределения полицейских сил. Полноценная реализация возможностей метода машинного обучения требует доступа к данным МВД, интеграции с системами «Безопасный город» и учета региональных различий в уровне преступности.

Кроме того, ИИ на основе моделей машинного обучения может разработать систему оценки, которая выявляет жертв торговли людьми в целях сексуальной эксплуатации в интернете.

Например, эта технология может применяться для выявления незаконной деятельности с помощью многофакторной системы оценки на основе искусственного интеллекта, а также для распознавания лиц жертв.

Искусственный интеллект способен раскрывать такие преступления, как продажа краденого имущества и отмывание денег, и потенциально может использоваться практически для любой незаконной деятельности, совершаемой в интернете.

Нейросети наиболее полезны для анализа текстов и выявления киберпреступлений с помощью обработки естественного языка (NLP) с целью мониторинга социальных сетей, форумов и даркнета на предмет незаконной деятельности (торговля наркотиками, экстремизм, мошенничество) [7].

Даркнет – это теневой сегмент интернета, который скрыт из общего доступа [8]. В даркнете обычно покупают и продают запрещённые товары. Кроме того, даркнет часто используется для кражи личных данных. Часто преступники продают украденную личную информацию, в том числе номера свидетельств социального страхования, данные кредитных карт и другие сведения. Алгоритмы кластеризации и классификации могут выявлять подозрительные сообщения.

Также ИИ может отслеживать Telegram-каналы или ВКонтакте для выявления схем мошенничества или вербовки в экстремистские группы.

Выявление преступного поведения с помощью технологий – сложная задача. Часто правоохранные органы ограничены в своих возможностях из-за бюджетных ограничений и недостаточной подготовки в области программного обеспечения для искусственного интеллекта. Однако правоохранные органы могут сотрудничать с технологическими компаниями, которые освоили технологии машинного обучения, необходимые для предотвращения преступлений.

В сфере киберкриминалистики ИИ осуществляет анализ цифровых следов, помогая восстанавливать удаленные файлы, анализировать логи или выявлять хакерские атаки. Позволяет отслеживать незаконные финансовые операции. С помощью анализа метаданных определяет время и место создания цифровых улик.

В России для выявления кибератак и защиты критической инфраструктуры (банки, госуслуги) от DDoS-атак или утечек данных ФСБ и МВД сотрудничают с частными IT-компаниями (например, Kaspersky, Group-IB). При этом используются алгоритмы обнаружения аномалий, нейронные сети для анализа трафика. Рост киберпреступности требует увеличения инвестиций в ИИ и подготовки специалистов.

Искусственный интеллект может использоваться в криминалистической экспертизе при проведении анализа ДНК, отпечатков пальцев, баллистических данных или почерка с использованием компьютерного зрения и алгоритмов кластеризации. ИИ ускоряет сравнение генетических материалов и помогает выявлять совпадения в базах данных [9]. Также может классифицировать следы обуви, шин или орудий преступления.

В России разработана система «Криминалист», которая позволяет анализировать данные из баз данных МВД, ФСБ, ФСИН, СКР, ФНС, Росфинмониторинга и др.

«Криминалист» может обнаруживать потенциальных преступников, группировки, места совершения преступлений, а также предлагать оптимальные решения для правоохранителей [10].

Для использования этих возможностей в российской практике необходима модернизация баз данных МВД и внедрение стандартизированных ИИ-решений в регионах [11].

Стоит отметить, что Министерство внутренних дел РФ активно работает в направлении интеграции искусственного интеллекта в правоохранительную практику. В текущем году предполагается создать ИИ-системы «Клон» и «Конъюнктура». Система «Клон» будет предназначена для обнаружения фальсификации видеоизображений в целях поддержки деятельности правоохранительных органов, а «Конъюнктура» - для предвидения негативных событий и нештатных ситуаций, а также имитации сценариев реагирования на них. [12].

Таким образом, ИИ в России уже применяется для обработки улик, особенно в видеоаналитике, киберкриминалистике и анализе документов. Однако масштабы внедрения варьируются по регионам, и технологии чаще используются в крупных городах (Москва, Подмосковье). Национальная стратегия и поддержка государства способствуют развитию, но этические, юридические и технические ограничения требуют дальнейшей работы.

Очевидно, что ИИ может представлять опасность для общества и влиять на права человека, если используется неправильно. С точки зрения этики необходимо учитывать риск предвзятости алгоритмов (например, при распознавании лиц или профайлинге). Также следует обеспечить соответствие использования ИИ законам о защите данных и конфиденциальности.

В качестве ограничений следует отметить неравномерное развитие технологий в регионах России, что может затруднить внедрение методов ИИ. Кроме того, недостаточно высокий уровень доверия к правоохранительным органам может осложнить восприятие ИИ-решений: по оценке ВЦИОМ, почти 27% россиян не доверяют сотрудникам правоохранительных органов [13].

В будущем необходимо обеспечить безопасность ИИ, чтобы гарантировать его этичное использование, а также обеспечить прозрачность и общественный контроль за использованием ИИ в правоохранительной деятельности. Использование ИИ должно регулироваться, особенно по мере развития технологий.

В то же время для сбора данных, на который у людей ушло бы слишком много времени, требуется больше ресурсов и инструментов искусственного интеллекта. ИИ способен собирать данные в текущий момент времени, а также проводить анализ данных, которые отражают прошлые события, тенденции и угрозы. Например, исторические данные о

кибератаках могут помочь понять, какие виды атак были наиболее распространены в разные периоды времени, какие методы защиты были наиболее эффективны, какие последствия имели атаки для жертв и злоумышленников, какие законы были приняты для борьбы с киберпреступностью [14]. При этом необходимо гарантировать добросовестное использование данных.

Хотя ИИ обладает огромным потенциалом в области выявления и предотвращения преступлений, эффективность этих инструментов зависит от способности профессионалов эффективно их использовать. Требуются постоянные образовательные и обучающие программы, которые позволят сотрудникам правоохранительных органов быть в курсе новейших технологий и методик ИИ. Эти программы могут быть разработаны таким образом, чтобы устранить разрыв между традиционными методами расследования и современными цифровыми инструментами, обеспечивая беспрепятственную интеграцию ИИ в повседневную деятельность правоохранительных органов.

### Список литературы

1. Walczak S. (2021) Predicting Crime and Other Uses of Neural Networks in Police Decision Making. *Front. Psychol.* URL: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.587943/full>.
2. Лапушкин А. Сферы применения систем искусственного интеллекта. URL: <https://maff.io/media/sfery-primeneniya-sistem-iskusstvennogo-intellekta/?ysclid=m9h1aua4ao261732347>.
3. Рассел С. Искусственный интеллект: современный подход: [перевод с английского] / Стюарт Рассел, Питер Норвиг. 4-е изд. Москва: Диалектика; Санкт-Петербург: Диалектика, 2021. Т. 1: Решение проблем: знания и рассуждения. 2021. 704 с.
4. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с англ. А.А. Слинкина. 2-е изд., испр. М.: ДМК Пресс, 2018. 652 с.
5. Nacional'naya strategiya. URL: <https://ai.gov.ru/national-strategy/>.
6. Bhalla, S., Kumar Singh, R. (2021). Exploration of Crime Detection Using Deep Learning. In: Singh, J., Kumar, S., Choudhury, U. (eds) Innovations in Cyber Physical Systems. Lecture Notes in Electrical Engineering, vol 788. Springer, Singapore. URL: [https://doi.org/10.1007/978-981-16-4149-7\\_26](https://doi.org/10.1007/978-981-16-4149-7_26).
7. Альбицкая И., Косяков А. Искусственный интеллект для юристов // Юридический справочник руководителя. № 1. 2022. URL: <https://delo-press.ru/journals/law/lichnyu-interes/60129-iskusstvenny-intellekt-dlya-yuristov/>.

8. Даркнет – опасен ли теневой интернет, и что вам нужно о нем знать URL: <https://www.kaspersky.ru/resource-center/threats/deep-web>.
9. Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2 (104). URL: <https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-kriminalistike-sostoyanie-i-perspektivy-ispolzovaniya>.
10. Как искусственный интеллект используется в борьбе с преступностью. URL: <https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu>.
11. Гордеев А. Ю. Перспективы развития и использования искусственного интеллекта и нейросетей для противодействия преступности в России (на основе зарубежного опыта) // Научный портал МВД России. 2021. № 1 (53). URL: <https://cyberleninka.ru/article/n/perspektivy-razvitiya-i-ispolzovaniya-iskusstvennogo-intellekta-i-neyrosetey-dlya-protivodeystviya-prestupnosti-v-rossii-na-osnove>.
12. МВД решило применить нейросети для поиска фейков и прогнозирования URL: <https://www.rbc.ru/society/11/01/2024/659f82459a7947ef6a4f54e5>.
13. Доклад о состоянии гражданского общества в Российской Федерации за 2024 год. URL: <https://report2024.oprf.ru/ru-RU/2024-the-main-thing-in-russian-civil-society.html>.
14. Исторические данные. URL: [https://www.securitylab.ru/glossary/istoricheskie\\_dannye/utm\\_referrer=https%3A%2F%2Fya.ru%2F](https://www.securitylab.ru/glossary/istoricheskie_dannye/utm_referrer=https%3A%2F%2Fya.ru%2F).

## USING THE CAPABILITIES OF ARTIFICIAL INTELLIGENCE TO FIGHT CRIME

**Dolgova Irina Vladimirovna**

Ph.D. of Sociological Sciences,  
Associate Professor at the Department of Management and Business Law,  
North Caucasus Institute-Branch,  
Russian Academy of National Economy and Public Administration,  
Pyatigorsk, Russian Federation

**Zhamborov Anzor Anatolyevich**

Ph.D. of Juridical Sciences  
Associate Professor at the Department of Fire Training,  
North Caucasus Institute of Advanced Training (branch),  
Krasnodar University of the Ministry of Internal Affairs of Russia,  
Nalchik, Russian Federation

**Abstract.** The article reveals the potential of artificial intelligence methods for detection and prevention of crimes. The article presents a characteristic of artificial intelligence methods and considers the experience of their application in the practice of Russian law enforcement agencies. Challenges and limitations hindering the use of AI in the activities of law enforcement agencies are outlined.

The authors emphasize that artificial intelligence has enormous potential in the field of detecting and preventing crimes, the effectiveness of these tools depends on the ability of professionals to use them effectively. Therefore, there is a need for ongoing educational and training programs that will allow law enforcement officers to be aware of the latest technologies and methods of artificial intelligence. At the same time, one of the main goals of the implementation of these programs should be to eliminate the gap between traditional investigative methods and modern digital tools, ensuring the seamless integration of artificial intelligence into the daily activities of law enforcement agencies

**Key words:** Artificial intelligence, methods, neural networks, law enforcement, crime fighting

### References

1. Walczak S. (2021) Predicting Crime and Other Uses of Neural Networks in Police Decision Making. *Front. Psychol.* URL: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.587943/full>.
2. Lapushkin A. Areas of application of artificial intelligence systems. URL: <https://maff.io/media/sfery-primeneniya-sistem-iskusstvennogo-intellekta/?ysclid=m9h1aua4ao261732347>.
3. Russell S. Artificial Intelligence: A Modern Approach: [translated from English] / Stuart Russell, Peter Norvig. 4th ed. Moscow: Dialectika; St. Petersburg: Dialectika, 2021. T. 1: Problem Solving: Knowledge and Reasoning. 2021. 704 p.
4. Goodfellow, J., Bengio, I., Courville, A. Deep Learning / translated from English by A.A. Slinkin. 2nd ed., corrected. Moscow: DMK Press, 2018. 652 p.
5. National Strategy. Available at: <https://ai.gov.ru/national-strategy/>.
6. Bhalla, S., Kumar Singh, R. (2021). Exploration of Crime Detection Using Deep Learning. In: Singh, J., Kumar, S., Choudhury, U. (eds) Innovations in Cyber Physical Systems. Lecture Notes in Electrical Engineering, vol 788. Springer, Singapore. Available at: [https://doi.org/10.1007/978-981-16-4149-7\\_26](https://doi.org/10.1007/978-981-16-4149-7_26).
7. Albitskaya I., Kosyakov A. Artificial Intelligence for Lawyers // Legal Handbook of the Manager. No. 1. 2022. URL: <https://delo-press.ru/journals/law/lichnyy-interes/60129-iskusstvennyy-intellekt-dlya-yuristov/>.
8. Darknet: Is the Shadow Internet Dangerous, and What You Need to Know About It? URL: <https://www.kaspersky.ru/resource-center/threats/deep-web>.
9. Bakhteyev D.V. Artificial Intelligence in Forensic Science: Status and Prospects of Use // Russian Law: Education, Practice, Science. 2018. No. 2 (104). URL: <https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-kriminalistike-sostoyanie-i-perspektivy-ispolzovaniya>.
10. How Artificial Intelligence is Used in the Fight Against Crime. URL: <https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu>.
11. Gordeev A. Yu. Prospects for the Development and Use of Artificial Intelligence and Neural Networks to Combat Crime in Russia (Based on Foreign Experience) // Scientific Portal of the Ministry of Internal Affairs of Russia. 2021. No. 1 (53). URL: <https://cyberleninka.ru/article/n/perspektivy-razvitiya-i-ispolzovaniya-iskusstvennogo-intellekta-i-neyrosetey-dlya-protivodeystviya-prestupnosti-v-rossii-na-osnove>.
12. The Ministry of Internal Affairs decided to use neural networks to detect fakes and make predictions. URL: <https://www.rbc.ru/society/11/01/2024/659f82459a7947ef6a4f54e5>.
13. Report on the state of civil society in the Russian Federation for 2024. URL: <https://report2024.oprf.ru/ru-RU/2024-the-main-thing-in-russian-civil-society.html>.

---

14. Historical data. URL:  
[https://www.securitylab.ru/glossary/istoricheskie\\_dannye/utm\\_referrer=https%3A%2F%2Fya.ru%2F](https://www.securitylab.ru/glossary/istoricheskie_dannye/utm_referrer=https%3A%2F%2Fya.ru%2F)  
F.