Дата поступления рукописи в редакцию: 03.03.2026 г.
Дата принятия рукописи в печать: 14.04.2026 г.
DOI: 10.24412/2782-3830-2026-3-95-99

ДУНАЕВ Роман Алексеевич,
кандидат философских наук,
доцент кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института МВД России
имени И.Д. Путилина,
e-mail: rmndnv@yandex.ru

БОРИСЕНКО Александр Васильевич,
кандидат физико-математических наук,
старший преподаватель кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института МВД России
имени И.Д. Путилина,
e-mail: borisenko02.94@mail.ru

КОВАЛЕВА Екатерина Геннадьевна,
кандидат технических наук,
доцент кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института МВД России
имени И.Д. Путилина,
e-mail: kovalevazchs@yandex.ru

ПИРОЖЕНКО Юрий Анатольевич,
преподаватель кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института МВД России
имени И.Д. Путилина,
e-mail: pieibex@yandex.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ: ПРАВОВЫЕ И РЕГУЛЯТОРНЫЕ АСПЕКТЫ

Аннотация. *В связи с тем, что условиях все большей цифровизации традиционные методы борьбы с киберпреступностью, которая приобретает системный, трансграничный характер, не всегда позволяют справиться с современными угрозами. Все это создает серьезные проблемы для правоохранительных органов и правовых систем по всему миру. На помощь приходят достижения в области информационных технологий. В целях выявления, предотвращения и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, все более широко применяются технологии искусственного интеллекта и машинного обучения. В статье приводится анализ правовых и процессуальных проблем использования данных технологий при выявлении киберугроз. Особое внимание уделяется соотношению использования искусственного интеллекта требованиям уголовного и уголовно-процессуального законодательства, законодательства о защите персональных данных, а также формулируются предложения по совершенствованию правового регулирования.*

Ключевые слова: *искусственный интеллект, машинное обучение, киберпреступность, цифровые доказательства, кибербезопасность, уголовное право, правовое регулирование.*

DUNAEV Roman Alekseevich,
Candidate of Philosophical Sciences,
Docent of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

BORISENKO Alexander Vasilyevich,
Candidate of Physico-mathematical Sciences,
Senior lecturer of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

KOVALEVA Ekaterina Gennadievna,
Candidate of Technical Sciences,
Associate Professor of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

PIROZHENKO Yuri Anatolyevich,
lecturer of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: LEGAL AND REGULATORY ASPECTS

Annotation. *Due to the fact that with increasing digitalization, traditional methods of combating cybercrime, which is becoming systemic and cross-border in nature, do not always make it possible to cope with modern threats. All this creates serious problems for law enforcement agencies and legal systems around the world. Advances in information technology are coming to the rescue. Artificial intelligence and machine learning technologies are widely used in order to prevent and investigate crimes committed using information and communication technologies. The article provides an analysis of the legal and procedural problems of using these technologies in identifying cyber threats. The paper pays special attention to the correlation of the use of artificial intelligence with the requirements of criminal and criminal procedure legislation, legislation on the protection of personal data, and formulates proposals for improving legal regulation.*

Key words*: artificial intelligence, machine learning, cybercrime, digital evidence, cybersecurity, criminal law, legal regulation.*

Развитие цифровых технологий оказало существенное влияние на структуру и способы совершения преступлений. Мало того, в настоящее время формируется цифровое пространство – метавселенная, которая «постепенно становится основным компонентом промышленных и коммерческих процессов по всему миру. Хотя остается много вопросов, и некоторые из них вырисовываются все больше в приоритетах правительства и корпоративного сектора разных стран, тем не менее, у современных технологий цифрового пространства есть высокие шансы реорганизовать компании, отрасли, национальные экономики и даже масштабные инициативы экономического регионализма» [1] Вероятность роста данного «рынка» весьма высока, что открывает новые угрозы, ведущие к совершенно очевидным негативным последствиям.

Следует отметить, что киберпреступность характеризуется высокой латентностью и использованием весьма сложных технических средств, что существенно осложняет деятельность правоохранительных органов. Данная категория преступлений охватывается в частности статьями 159.6, 272, 273 и 274.1 Уголовного кодекса РФ (далее – УК РФ).

Традиционные методы выявления и расследования таких преступлений зачастую оказываются недостаточно эффективными в связи с обработкой значительных массивов цифровых данных. В этой связи особую актуальность приобретает использование искусственного интеллекта (ИИ) и машинного обучения (МО) позволяющих автоматизировать анализ информации и выявлять признаки противоправной деятельности и прогнозировать будущие атаки. При этом использование искусственного интеллекта привносит собственные риски, которые отличаются от традиционно рассматриваемых в кибербезопасности [2].

Внедрение искусственного интеллекта (ИИ) в сферу кибербезопасности произвело революцию в области обнаружения и устранения киберугроз, позволив справиться с растущей сложностью и изощренностью атак. В масштабном исследовании коллектива во главе с Абдулла Аль

Сиам [3] рассматривается эффективность ИИ в выявлении таких угроз, как вредоносное ПО, фишинг и уязвимости нулевого дня, а также в автоматизации реагирования на угрозы. Среди выводов можно отметить, что ИИ значительно повышает уровень кибербезопасности в пяти областях: обнаружение угроз, защита конечных устройств, обнаружение фишинга, сетевая безопасность и адаптивная аутентификация. Технологии ИИ улучшат возможности обнаружения угроз. Будущие исследования должны быть направлены на улучшение обнаружения в реальном времени, повышение масштабируемости и интеграцию различных источников данных для создания эффективных ИИ-решений.

Для современного правоохранителя понимание того, как собираются и оцениваются доказательства, становится весьма актуальным. Вместе с тем внедрение технологий в сферу уголовного судопроизводства порождает ряд проблем, связанных с допустимость доказательств, соблюдением процессуальных норм и защитой прав личности.

Взрывной рост технологий ИИ требует правового анализа их применения с учетом специфики уголовно-процессуального законодательства. Существующие научные работы преимущественно ориентированы либо на технические аспекты кибербезопасности, либо на общетеоретическое осмысление цифровизации права. Мы обосновываем положение о вспомогательном, а не самостоятельном характере технологий ИИ в механизме уголовного доказывания, соотнеся конкретную технологию с составами преступлений, предусмотренных статьями 159.6, 272, 273, 274.1 УК РФ. Также формулируем критерии допустимости и оценки данных полученных с применением ИИ и предложен комплекс мер по совершенствованию правового регулирования, направленных на обеспечение баланса между эффективностью противодействия киберпреступности и защитой прав личности. Практическое применение результатов может быть использовано в:

- при подготовке экспертных заключений в области компьютерной криминалистики и кибербезопасности;
- в деятельности органов предварительного расследования при оценке материалов, полученных с применением технологий ИИ;
- в судебной практике при решении вопросов допустимости, достоверности и оценки цифровых доказательств по делам о киберпреступлениях.

Современные системы кибербезопасности, основанные на искусственном интеллекте и машинном обучения, используют различные инструменты и методы для защиты компьютерной информации и выявления киберугроз. Отметим наиболее распространенные из них:

- анализ больших данных и распознавания закономерностей. Основной метод используемый для выявления отклонений от стандартных моделей поведения. Позволяет фиксировать аномалии, которые могут свидетельствовать о несанкционированном доступе к компьютерной информации, образующем состав преступления, предусмотренного статьей 272 УК РФ. Помимо непосредственно доступа к информации возникает проблема утечки, которые следует учитывать. Так, например, исследование компании, связанное с поведением персонала в связи с появлением инструмента генеративных моделей [4], говорит о том, что более половины сотрудников офиса вводили рабочую информации в ИИ.

Важным является понимание того, как собираются и подтверждаются доказательства с помощью систем на базе ИИ. Это могло бы помочь как обвинению, так и защите в делах, связанных с киберпреступлениями.

- алгоритмы классификации применяются для выявления фишинговых сообщении, вредоносных файлов и поддельных ресурсов, что имеет непосредственное значение для расследования преступлений, предусмотренных статьей 159.6 УК РФ. Обнаружение дипфейков на основе инструментов ИИ могут оценивать видео/изображения на предмет манипуляций [5], позволяет выявлять контент, что важно в случаях, связанных с клеветой и политическими манипуляциями.
- технологии обработки естественного языка (NLP), которые позволяют анализировать информацию для выявления признаков социальной инженерии и мошенничества. NLP используется для обнаружения вредоносных программ для анализа больших объемов данных и обнаружения закономерностей, которые можно пропустить с помощью традиционных инструментов безопасности [6].
- кластеризация используется для обнаружения сетей ботов и координированных атак, также выявление групп фейковых аккаунтов на платформах социальных сетей, что может быть связано с преступлениями, предусмотренными статьей 273 УК РФ.
- прогностическая аналитика применяется для защиты критически важной информационной инфраструктуры и предупреждения преступлений, предусмотренных по ста-

тье 274.1 УК РФ. Подвергая алгоритмы машинного обучения широкому спектру реальных атак и сопоставляя их с обычными действиями пользователей можно сформировать решение, способное выявлять как известные, так и возникающие угрозы [7].

С точки зрения уголовного процесса технологии ИИ не могут рассматриваться как самостоятельные субъекты доказывания. Они выполняют вспомогательную функцию, обеспечивая обработку и систематизацию следов преступной деятельности. Результаты работы таких систем включаются в материалы уголовного дела посредством заключений экспертов или иных процессуальных документов. В соответствии со статьями 74 и 80 УК РФ доказательствами по уголовному делу являются сведения, полученные в предусмотренном законе порядке. Данные, полученные с применением ИИ, приобретают доказательственное значение только после их процессуального оформления и оценки судом.

Ключевой проблемой является проблема допустимости и достоверности данных, полученных с использованием алгоритмов машинного обучения [8]. Существенную сложность представляет ограниченная объяснимость многих ИИ-моделей, особенно основанная на технологиях глубокого обучения. В условиях состязательности уголовного процесса сторона защиты должна иметь реальную возможность оспорить доказательства. В этой связи экспертные заключения основанные на применении ИИ, должны содержать сведения о принципах функционирования системы, уровне точности, возможных ошибках и ограничениях применяемых алгоритмов. Отсутствие таких разъяснений может повлечь сомнения в достоверности доказательств и их недопустимость.

Применение ИИ в кибербезопасности предполагает обработку значительных объемов персональных данных. Данная деятельность регулируется Федеральным Законом №152 «О персональных данных». Особое значение приобретает вмешательство в частную жизнь, соразмерность этого вмешательства. Использование технологий мониторинга должно быть ограничено целями обеспечения кибербезопасноти и не приводить к неоправданному ограничению конституционных прав граждан.

Киберпреступления очень часто совершаются с использование инфраструктуры, расположенной за пределами РФ и группами граждан, находящихся в разных юрисдикциях. Несмотря на эффективность применения ИИ с точки зрения технической составляющей в выявлении подобных преступлений, их расследование требует международного сотрудничества и согласования правовых подходов к использованию цифровых доказательств. Различия в правовых режимах регулирования ИИ осложняют оказание правовой помощи и обмена цифровыми доказательствами.

На основании проведенного анализа представляется целесообразным следующие рекомендации по совершенствованию правового регулирования:

1. Развитие профессиональной подготовке сотрудников правоохранительных органов. Речь не идет о том, что каждый должен быть программистом, но понимать каким образом ИИ формирует контент (доказательства), ставить под сомнение надежность этого источника, проверять факты – условие необходимое.
2. Установить требования прозрачности и проверяемости систем ИИ, используемых в сфере кибербезопасности.
3. Закрепить законодательно положение о вспомогательном характере технологии ИИ при формировании доказательств.
4. Разработать методические рекомендации по использованию и оценке данных, полученных с применением ИИ в уголовном делопроизводстве.

Технологии ИИ и машинного обучения является важным инструментом противодействия киберпреступности в РФ. Современный юристы могут использовать широкий спектр инструментов ИИ, не имея технической подготовки, но при этом необходимый минимум понимания включающий анализ угроз, как системы выявляют признаки мошенничества или незаконную деятельность, сканирование файлов на наличие вредоносного ПО, проверка подозрительных файлов, полученных в результате доказательств по делу, использование инструментов для сохранения целостности, например, хэширование. Вместе с тем использование указанных инструментов в уголовном судопроизводстве требует строгого соблюдения принципов законности, процессуальной строгости и защиты прав личности. Совершенствование нормативного регулирования и правоприменительной практики является необходимым условием эффективной интеграции данных технологий в систему уголовной юстиции.

Список литературы:

[1] Петров П. К., Денисович В. В. Преступность в виртуальном пространстве: криминологическая характеристика //Проблемы права. – 2025. – №. 1 (97). – С. 66-70.

[2] Намиот Д. Е. О кибератаках с помощью систем Искусственного интеллекта //International journal of open information technologies. – 2024. – Т. 12. – №. 9. – С. 132-141.

[3] Al Siam A. et al. A comprehensive review of AI's current impact and future prospects in cybersecurity //IEEE Access. – 2025. – Т. 13. – С. 14029-14050.

[4] Намиот Д. Е. Искусственный интеллект в кибербезопасности. Хроника. Выпуск 4 // International Journal of Open Information Technologies. – 2026. – Т. 14. – №. 1. – С. 81-94.

[5] Неренц Д. В. Дипфейк как одна из главных информационных угроз XXI века //Филология: научные исследования. – 2025. – №. 9. – С. 96-111.

[6] Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности //Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2023. – №. 3 (326). – С. 65-72.

[7] Кузьминов Я., Кручинская Е. Потенциал генеративного искусственного интеллекта для решения профессиональных задач //Форсайт. – 2024. – Т. 18. – №. 4. – С. 67-76.

[8] Павлычев А. В., Стародубов М. И., Галимов А. Д. Использование алгоритма машинного обучения Random Forest для выявления сложных компьютерных инцидентов //Вопросы кибербезопасности. – 2022. – №. 5 (51). – С. 74-81.

References:

[1] Petrov P. K., Denisovich V. V. Crime in the virtual space: criminological characteristics //Legal issues. – 2025. – No. 1 (97). – pp. 66-70.

[2] Namiot D. E. On cyberattacks using artificial intelligence systems //International journal of open information technologies. – 2024. – Vol. 12. – No. 9. – pp. 132-141.

[3] Al Siam A. et al. A comprehensive review of AI's current impact and future prospects in cybersecurity //IEEE Access. – 2025. – T. 13. – pp. 14029-14050.

[4] Namiot D. E. Artificial intelligence in cybersecurity. The chronicle. Issue 4 //International Journal of Open Information Technologies. – 2026. – Vol. 14. – No. 1. – pp. 81-94.

[5] Namiot D. E. Artificial intelligence in cybersecurity. The chronicle. Issue 4 //International Journal of Open Information Technologies. – 2026. – Vol. 14. – No. 1. – pp. 81-94.

[6] Kozlova N. S., Dovgal V. A. Analysis of the application of artificial intelligence and machine learning in cybersecurity //Bulletin of the Adygea State University. Series 4: Natural, mathematical and technical sciences. – 2023. – No. 3 (326). – pp. 65-72.

[7] Kuzminov Ya., Kruchinskaya E. The potential of generative artificial intelligence for solving professional problems //Foresight. – 2024. – Vol. 18. – No. 4. – pp. 67-76.

[8] Pavlychev A.V., Starodubov M. I., Galimov A.D. Using the Random Forest machine learning algorithm to identify complex computer incidents // Cybersecurity issues. – 2022. – №. 5 (51). – pp. 74-81.