УДК 343.9.01

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРЕСТУПНОСТЬ: ИСПОЛЬЗОВАНИЕ ИИ ДЛЯ СОВЕРШЕНИЯ И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ

***Ищенко Н.Е.*[1]**

студент юридического института, 4 курс

ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

Россия, г. Белгород

Аннотация

Актуальность данной статьи заключается в цифровизации общества и связанных с этим рисках, таких как высокотехнологичная преступная деятельность и киберугрозы. Искусственный интеллект занимает двойную позицию: одну, где ИИ обретает союзников в правоохранительных органах, и другую, где он становится новым оружием в арсенале преступных умов.

Ключевые слова: Дипфейки, искусственный интеллект, преступная деятельность, специализированные системы, интеграция.

ARTIFICIAL INTELLIGENCE AND CRIME: USING AI TO COMMIT AND PREVENT CRIMES

Ishchenko N.E.

Law Institute student, 4th year

[1] ***Научный руководитель: Алейникова Валерия Андреевна,*** *Ассистент кафедры уголовного права и процесса,* *ФГАОУ ВО «Белгородский государственный национальный исследовательский университет», Россия, г. Белгород*

Aleynikova Valeria Andreevna, *Assistant Professor of the Department of Criminal Law and Procedure, Belgorod State National Research University, Belgorod, Russia*

Belgorod State National Research University
Belgorod, Russia

Annotation
The relevance of this article lies in the digitalization of society and the associated risks, such as high-tech criminal activity and cyber threats. AI occupies a dual position: one where AI finds allies in law enforcement, and the other where it becomes a new weapon in the arsenal of criminal minds.
Keywords: Deepfakes, artificial intelligence, criminal activity, specialized systems, integration.

Преступники часто используют новые методы и технологии, что усложняет работу правоохранительных органов. Например, для организации своих действий они применяют алгоритмы машинного обучения и искусственный интеллект. Технологическая сложность искусственного интеллекта, сложности установления намерений и вопросы юрисдикции могут сделать существующие правовые рамки неэффективными против новых угроз, во многом из-за повторяющихся проблем с решением вопросов юрисдикции и сложности определения намерений.[1] Использование искусственного интеллекта для предотвращения преступности вызывает серьезные этические проблемы, особенно в условиях, когда приоритет отдается алгоритмической дискриминации, вторжению в частную жизнь и прозрачности эффекта черного ящика. Согласно определению, черным ящиком (ЧЯ) называют объект, внутреннее устройство которого либо неизвестно, либо слишком сложно для того, чтобы можно было по свойствам его составных частей и структуре связей между ними делать выводы о поведении объекта.[2]

Целью данной статьи является тщательный анализ того, как искусственный интеллект может применяться в современных преступных

операциях как средство как инициирования, так и прекращения уголовных преступлений.

Искусственный интеллект, как многообещающее средство содействия прогрессу, также предлагает новые способы криминализации преступлений, которые раньше были невозможны. Модернизация обычных преступных схем и создание принципиально новых угроз позволяют злоумышленникам использовать способность использовать себя, большие наборы данных и самообучение для принятия обоснованных решений, как видно из опции «ландшафтного ландшафта», которая предоставляет злоумышленникам возможность использовать существующие преступные методы и использовать уязвимости. Рост адаптивных вредоносных программ и вирусов является серьезной проблемой в киберпространстве из-за роста онлайн-сообществ, которые используют их для нанесения ущерба. Злоумышленники теперь внедряют ИИ непосредственно во вредоносное ПО, позволяя ему действовать разными способами. При попадании в новую среду такое вредоносное ПО обучается, анализирует систему безопасности и меняет свое поведение, чтобы избежать стандартных методов обнаружения.

Одним из крупных направлений являются дипфейки. Deepfake — это технология синтеза изображений, включающая машинное обучение и искусственный интеллект, в результате чего создается технология синтеза изображений. Границы между реальностью и вымыслом искажаются, оставляя после себя разделение между реальным и непреднамеренным. [3]. Для генерации дипфейка применяются алгоритмы машинного обучения, а именно — генеративные состязательные сети (GAN). Этот метод является одним из наиболее популярных подходов к созданию дипфейков. В структуру GAN входят две нейронные сети — генератор и дискриминатор, при этом каждый из этих компонентов выполняет собственную, уникальную роль в процессе генерации данных.[4]

Злоумышленники начали процесс интеграции ИИ во вредоносное ПО, которое затем может действовать как приманка и переключаться между реактивным интеллектом (ИИ) и адаптивным интеллектом (ИИ/вредоносное ПО). Внедряясь в новую систему, вредоносное ПО проникает внутрь, анализирует систему безопасности и перенастраивает свое поведение, чтобы пропустить стандартные методы обнаружения. Эксперты по информационной безопасности вынуждены иметь дело с гораздо большей сложностью, а не только с созданием сложных вредоносных программ, что упрощает процесс.

Если раньше злоумышленники преследовали в первую очередь финансовую выгоду и выбирали отдельные компании в качестве целей, то с 2022 года акценты сместились кардинально. Кибератаки все чаще направлены на государства и инфраструктуру целиком. В первой половине 2025 года государственные учреждения оказались жертвами 21% всех успешных атак на организации, и это максимальный показатель за последние годы. Основная цель таких кампаний состоит в дестабилизации: 68% атак на госструктуры имели задачу нарушить их работу, а 29% были направлены на причинение ущерба государственным интересам. В феврале 2025 года Роскомнадзор отразил 822 DDoS-атаки на государственные системы управления, а одна из них длилась 71 час подряд. В мае массированный DDoS одновременно вывел из строя сервисы ФНС, «Госключ», «Честный знак» и региональные платформы.

Правоохранительные органы всё чаще используют искусственный интеллект (ИИ) для предотвращения и расследования преступлений. Его функции охватывают широкий спектр функций, включая прогнозирование тенденций городской преступности и выявление современных киберугроз в даркнете. Использование этих технологий позволяет людям обойти возмездие за совершенные преступления и вместо этого работать над их предотвращением более быстрыми темпами. Предиктивная аналитика используется многими для выявления горячих точек преступности, и одним из наиболее заметных достижений является использование прогнозной аналитики. Анализируя

историческую статистику преступности и выявляя скрытые закономерности и временные зависимости, алгоритмы машинного обучения могут определять преступления. Следовательно, вероятность совершения преступлений в определенных районах в определенное время можно предсказать с высокой степенью точности. Исследование 120 научных работ с использованием моделей машинного обучения показало, что различные модели могут предсказать преступность. «PredPol» - это аналитический инструмент, который подсказывает сотрудникам полиции, на какой участок обратить особое внимание («горячая точка»), чтобы заранее «погасить» криминальную активность на территории подразделения правоохранительного органа, а также предоставляет обобщенные данные о состоянии преступности на участке.[4 p. 321] Система PredPol и модель Чикагского университета получили известность как надежные зарубежные образцы: система PredPol является наиболее точной с точностью примерно 90%, а южнокорейская система Дежавю является наиболее точной с точностью 82,8%. Это позволяет полиции лучше контролировать свои маршруты, повышать эффективность патрулирования и более эффективно распределять полицейские ресурсы.[5]

Российская Федерация привержена использованию технологий искусственного интеллекта в правоохранительной деятельности и активно занимается их внедрением. Обнаружение и расследование преступлений дополняется рядом специализированных систем, которые были разработаны для работы в различных областях обнаружения и расследования преступлений и эффективны в обнаружении и преследовании этих видов преступлений. Среди них такие системы, как «Спрут», которая идентифицирует лиц, совершивших преступления, на основе данных о преступных группировках и экономических факторах; «Маньяк», анализирующий серийные убийства и помогающий составить наиболее вероятную личность преступника; и «Криминалист», целью которого является выявление потенциальных преступников, групп и мест преступлений, а также предложение оптимальных решений

правоохранительным органам путем определения названий и определения преступной деятельности.[6]

Практическая реализация этих технологий уже дает ощутимые результаты. Например, 24 августа 2025 года на сайте «Первого канала». В ней сообщалось, что с помощью искусственного интеллекта в Пермском крае удалось раскрыть несколько запутанных преступлений, давность которых исчислялась не одним десятком лет. Всего за несколько минут исследователи искусственного интеллекта потратили 30 минут, анализируя огромные объемы данных, анализируя, казалось бы, необъяснимые улики, раскрывая скрытые детали и используя отпечатки пальцев, чтобы создать приблизительную картину убийцы, используя компьютерные и машинные портреты. В январе 2024 года Президент РФ Владимир Путин утвердил «Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека». В одном из поручений было рекомендовано Верховному суду РФ совместно с Генеральной прокуратурой РФ, Следственным комитетом РФ, МВД и Минюстом России к 1 июля 2024 года проанализировать практику применения технологий искусственного интеллекта при расследовании преступлений и при необходимости представить предложения по её совершенствованию. [7]

В июне 2025 года сообщалось, что Минцифры России разработало законопроект, который вводит уголовную ответственность за преступления, совершённые с применением искусственного интеллекта (ИИ). Документ входит во второй пакет мер по противодействию мошенничеству и находится на межведомственном согласовании. В России развивается комплексный подход к интеграции передовых технологий в правоохранительную систему, который предполагает сочетание практического внедрения, анализа результатов и развития нормативной базы. Законопроект вносит поправки в несколько статей УК РФ. Так, в ст. 158 (кража), ст. 159 (мошенничество), ст. 163 (вымогательство), ст. 272 (злостное воздействие на информационную систему, информационно-телекоммуникационную сеть, компьютерную информацию или сеть

электросвязи) и ст. 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) УК РФ, вносятся отдельный вид преступлений, совершенных с помощью искусственного интеллекта.

Интеграция ИИ в российскую преступную деятельность связана с рядом серьезных этических и правовых проблем, которые требуют скорейшего понимания и создания соответствующих механизмов регулирования. Анализ текущего сценария и точек зрения экспертов позволяет нам систематизировать эти проблемы и разработать соответствующие стратегии для их решения. Системы искусственного интеллекта, основанные на исторических данных, обученные на прошлых событиях, несут риск увековечения существующих предрассудков и дискриминационных моделей в обществе, а также воспроизведения прошлых результатов. Идея о том, что определенный социальный класс или область необоснованно называют «криминогенными», потенциально может противоречить основному принципу, согласно которому все люди должны иметь равные шансы на участие в правосудии. Использование ИИ в правосудии требует хранения и обработки огромных объемов конфиденциальных данных, включая личную и биометрическую информацию, чтобы участники могли участвовать в судебных разбирательствах, а также участники, которые отточены в обработке и манипулировании этой информацией. Реальная возможность построения системы тотального понимания и отрицания секретности проистекает из реальной опасности. Использование таких данных может быть неэффективным и вредным из-за строгих запретов на их использование, но оно не должно регулироваться, создавая серьезные риски для прав потребителей.

Российская Федерация признает серьезность этих проблем и принимает меры по их решению. Предлагаемое законодательное предложение по включению искусственного интеллекта в будущий федеральный закон было разработано действующей рабочей группой при Государственной Думе, целью

которой является дать осмысленное определение искусственного интеллекта. По мнению специалистов, закон, предусматривающий прозрачность, этику и защиту данных, потребует включения этих принципов. Повышается уголовная ответственность за преступления, совершенные с использованием ИИ. Способность ИИ участвовать в правовой системе уже присутствует, но он ограничил юрисдикцию в отношении некоторых аспектов. Председатель Совета судей РФ Виктор Момотов заявил, что окончательное решение по судебным делам будет приниматься единолично человеком. К середине 2025 года ИИ уже использовался каждым третьим российским судом для подготовки проектов приговоров и анализа документов, но точнее в качестве помощника, а не лица, принимающего решения, как говорится в сгенерированных ИИ постановлениях Императорского суда естественного права.

Проведенное исследование позволяет сделать вывод о двойственной роли искусственного интеллекта в современной преступности. С одной стороны, ИИ стал мощным инструментом в арсенале злоумышленников, усугубляя киберугрозы за счет создания адаптивного вредоносного ПО, изощренных схем мошенничества с использованием дипфейков и масштабных атак на критическую инфраструктуру. Это создает беспрецедентные вызовы для правоохранительных органов, связанные с технологической сложностью, установлением вины и вопросами юрисдикции. Искусственный интеллект показал себя чрезвычайно успешным в предотвращении преступности и раскрытии преступлений. Предиктивная аналитика, анализ больших данных с помощью искусственного интеллекта, прогнозная аналитика, подобная той, которую используют «Спрут», «Маньяк» и «Криминалист», а также использование машинного обучения для анализа больших данных — все это способствовало значительному повышению эффективности и точности работы правоохранительных органов, о чем свидетельствуют практические результаты, в том числе в Пермском крае. Применение ИИ в правоохранительной практике связано с этическими и правовыми рисками, такими как алгоритмическая

дискриминация, вторжение в частную жизнь и непоследовательность в принятии решений («эффект черного ящика»). Вызовом, создаваемым этими препятствиями, является инициативное создание нормативной базы, примером чего является предложенный Минцифры России законопроект о введении уголовной ответственности за преступления, совершенные с использованием ИИ. Будущее борьбы с преступностью в условиях цифровизации характеризуется сочетанием технологических достижений и строгого правового регулирования. Ключ к успеху в обеспечении баланса между эффективным использованием искусственного интеллекта и безоговорочным уважением фундаментальных прав и свобод человека при сохранении конечной роли человека при принятии судебных и следственных решений.

Библиографический список:

1) Бхатт Н. Преступления в эпоху искусственного интеллекта: гибридный подход к ответственности и безопасности в цифровую эру // Journal of Digital Technologies and Law. 2025;3(1):65–88. https://doi.org/10.21202/jdtl.2025.3. EDN: rtolza

2) Прохоров А. М. Большая советская энциклопедия : в 30-ти т. / гл. ред. А. М. Прохоров. 3-е изд. - М. : Советская энциклопедия, 1969-1978.

3) Агеева, А. С. Дипфейк: технология создания и применение в современной киноиндустрии / А. С. Агеева. — Текст : непосредственный // Молодой ученый. — 2025. — № 2 (553). — С. 8-9. — URL: https://moluch.ru/archive/553/121597.

4) Применение генеративных адверсариальных сетей (GANs) для синтеза данных. — Текст: электронный //Хабр: [сайт]. — URL: https://habr.com/ru/companies/otus/articles/754978/

5) Williams M. L., Burnap P., Sloan L. Crime sensing with big data: The affordances and limitations of using open source communications to estimate crime patterns // British Journal of Criminology. - 2016. -No 57. - P. 320-340.

6) Шах, Н., Бхагат, Н. и Шах, М. Прогнозирование преступности: подход к прогнозированию и предотвращению преступлений с использованием машинного обучения и компьютерного зрения // Vis. Comput. Ind. Biomed. Art 4, 9 (2021). https://doi.org/10.1186/s42492-021-00075-z

7) Афонин В.Н. Повышение достоверности обработки информации в информационно-телекоммуникационных системах органов внутренних дел // Труды Академии управления МВД России. - 2009. - №1. - С. 62..

8) Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утвержден Президентом Российской Федерации 14.01.2024) (опубликован 17.01.2024 www.kremlin.ru)

Оригинальность 75%