Юридические исследования
Правильная ссылка на статью:
Жужлов И.С. Возможности применения искусственного интеллекта в предупреждении преступлений // Юридические исследования. 2025. № 12. DOI: 10.25136/2409-7136.2025.12.76431 EDN: TZTBGV URL: https://nbpublish.com/library_read_article.php?id=76431

Возможности применения искусственного интеллекта в предупреждении преступлений

Жужлов Игорь Сергеевич

аспирант, кафедра уголовно-правовых дисциплин, Российская таможенная академия

140015, Россия, Московская обл., г. Люберцы, ул. Рождественская, д. 8, кв. 874

zhuzh.igor@yandex.ru

Статья из рубрики "Уголовный закон и правопорядок "

DOI:

10.25136/2409-7136.2025.12.76431

EDN:

TZTBGV

Дата направления статьи в редакцию:

26-10-2025

Аннотация: Предметом исследования выступают способы и методы применения искусственного интеллекта (далее ИИ) в процессе предупреждения преступлений. Цель статьи состоит в анализе возможностей применения ИИ для предупреждения преступлений, а также разработка рекомендаций по оптимизации и интеграции в российскую правоприменительную практику систем на базе ИИ. В статье исследуются различные подходы к определению искусственного интеллекта, его ключевые признаки и характеристики. Анализируется возможности внедрения методов и способов, основанных на технологиях с использованием ИИ, для предупреждения преступлений. Рассматриваются проблемы и сложности, которые могут возникнуть при использовании данных систем. Особый акцент делается на таких технологиях как: предиктивная аналитика, системы поддержки принятия решений, системы распознавания лиц и изображений, анализ цифровых улик, обработка естественного языка. Исследование сопровождается практическими примерами, иллюстрирующими возможности технологий ИИ в процессе предупреждения преступлений. В статье рассматривается как зарубежный, так и российский опыт использования технологий ИИ в процессе

предупреждения преступлений. Методология исследования опирается на фундаментальные научные принципы диалектики, историзма и объективности. В работе применяются общенаучные методы, такие как анализ и синтез, индукция и дедукция. Кроме того, используются частнонаучные методы: формально-юридический, системный и структурно-функциональный анализ. Также применен метод моделирования для мысленного создания возможных моделей по использованию технологий ИИ. Актуальность исследования обосновывается тем, что современные технологии ИИ, включая машинное обучение, анализ больших данных, обработку естественного языка, компьютерное зрение предоставляют новые возможности для анализа криминальных паттернов, предсказания потенциальных угроз и улучшения эффективности работы правоохранительных органов. Все эти технологии на данный момент активно внедряются и имеют большой потенциал для развития деятельности правоохранительных органов по предупреждению преступлений, а также для развития криминалистики как науки в целом. В результате исследования были рассмотрены подходы к пониманию ИИ, изучены способы и основные технологии на базе ИИ, которые используются или могут быть использованы для целей предупреждения преступлений, описаны способы применения и перспективы использования технологий на базе ИИ в практической деятельности правоохранительных органов.

Ключевые слова:

криминалистика, искусственный интеллект, нейронные сети, обработка естественного языка, предупреждение преступлений, расследование преступлений, цифровые следы, компьютерное зрение, машинное обучение, предиктивная аналитика

В последние десятилетия искусственный интеллект (далее ИИ) стал неотъемлемой частью множества сфер жизни и начал применяться как инструмент в большинстве научных областей, включая уголовно-правовые науки и в том числе в криминалистике. С развитием технологий и увеличением объемов данных, доступных для анализа, ИИ предлагает новые методы и инструменты для предупреждения преступлений и повышения уровня общественной безопасности. Применение криминалистических средств, поддерживаемых ИИ, позволяет не только более эффективно выявлять и предотвращать преступные действия, но и оптимизировать процесс расследования, минимизируя потенциально возможные ошибки и субъективность, вызванную человеческим фактором.

Методологическую основу исследования составили фундаментальные научные принципы диалектики, историзма и объективности. Принцип диалектики позволил показать, что процесс предупреждения преступлений в результате внедрения инновационных технологий находится в постоянном развитии. Наблюдается тенденция сближения и заимствования знаний из различных наук, которые в своем многообразии могут быть направлены на решение поставленных задач. Принцип историзма применялся для изучения эволюции компьютеризированных систем от строго алгоритмизированных до систем качественно другого уровня, предполагающих широкие возможности обучения. Принцип объективности позволил осветить различные мнения исследователей, взглянуть на анализируемые технологии как с позиции возможностей, так и с позиции потенциальных рисков. В исследовании были использованы общенаучные методы, такие как анализ и синтез, индукция и дедукция, и частно-научные методы, а именно формально-юридический, системный и структурно-функциональный анализ, метод

моделирования. Формально-юридический метод был использован для анализа и интерпретации нормативного определения ИИ и его признаков. Метод системного анализа применялся для рассмотрения групп различных технологий, составляющих в своей совокупности ИИ как систему. Структурно-функциональный анализ помог описать, какие именно задачи и функции способны выполнять рассматриваемые технологии в сфере предупреждения преступности. Метод моделирования позволил создавать мысленные модели и возможные потенциальные сценарии применения рассматриваемых технологий на базе ИИ.

ИИ можно определить как самостоятельную область компьютерных наук, которая занимается созданием систем, способных выполнять задачи, требующие интеллектуальных усилий, которые обычно ассоциируются с человеческим мышлением. Также под ИИ следует понимать саму способность машин выполнять задачи, аналогичные с мыслительными навыками человека. На текущий момент нормативное определение ИИ можно найти в Указе Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», в котором ИИ определяется как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и возможность получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их». Данное определение представляется достаточно широким, под него попадает большой спектр технологий, от простых алгоритмов до сложных систем, в свою очередь это позволяет с одной стороны регулировать ИИ на государственном уровне без слишком жёстких рамок, что важно для быстрого развития отрасли, но с другой стороны может породить противоречия в практике правоприменения. Отдельно стоит обратить внимание, что определение вводит понятие «когнитивные функции», но не раскрывает его полностью. Это важно поскольку возникает закономерный вопрос, что именно считать «когнитивными функциями», например, включает ли оно простые автоматизации, как калькуляторы, или предполагает только более сложные и «умные» системы.

Рассмотрим определения ИИ, которые предлагают ученые-правоведы, наиболее интересной представляется дефиниция Д. В. Бахтеева, по его мнению под ИИ стоит понимать «междисциплинарную область знаний о группе смежных технологий и создаваемое с ее помощью программное обеспечение, функционирующее нелинейно, способное ограниченно понимать причинность и выполнять задачи интеллектуального, эвристического характера с возможностью обучения, корректировки и уточнения за счет опыта принимаемых решений»[1, С. 27]. В контексте рассматриваемой темы, именно это определение представляется наиболее удачным поскольку сочетает в себе три наиболее важных качества в виде нелинейности, то есть без строгой алгоритмизации, эвристический характер, предполагающий направленность на решение задачи и получения нового знания путем выявления скрытых, неочевидных взаимосвязей и способность к самообучению, то есть возможность корректировки при получении новых сведений. Можно предположить, что именно эти качества лежат в основе способности прогнозирования, а следовательно, и предупреждения преступлений.

Стоит подчеркнуть, что понятие искусственный интеллект носит в определенной степени собирательный характер, поскольку данная область подразумевает совокупность технологий и направлений, которые в нее входят. В этот список можно включить: машинное обучение, нейронные сети, компьютерное зрение, технологии обработки и анализа данных (Big Data), робототехника, экспертные системы, обработка естественного языка, распознавание речи. При этом данные технологии имеют общее

основание в виде: наличия определенного программно-аппаратного комплекса, имеют возможность выполнять задачи схожие с интеллектуальными навыками человека, способны распознавать информацию, в разных ее проявлениях (звуковом, текстовом, в виде изображений), могут моделировать среду, принимать решения и исполнять их, а также способны на обучение и в определенной степени автономны.

Особенно важным представляется тот факт, что современные технологии позволяют ИИ обучаться на основе больших объемов данных, выявляя закономерности и делая предсказания, что является особенно полезным в контексте криминалистики. Стоит отметить, что именно на это качество обращают внимание многие исследователи, поскольку зачастую это служит ключевым отличием таких систем от традиционных строго алгоритмизированных программ. Так В. В. Бычков пишет, что «ИИ представляет собой компьютерно-программное обеспечение, используемое для раскрытия и расследования преступлений, способное не только решать задачи следственной деятельности, но и самосовершенствоваться с целью повышения эффективности деятельности правоохранительных органов» [2].

Значительную роль в криминалистике занимает процесс предупреждения преступлений. По своей сути он выражен в комплексе мер и методов, направленных на предотвращение преступных деяний с использованием научных и технических знаний в области криминалистики до непосредственного совершения преступления. Эти меры могут включать в себя различные подходы и технологии, которые помогают выявлять, анализировать и предотвращать преступления до их совершения. Как отмечал Р.С. Белкин существуют 3 группы криминалистических средств и методов предупреждения преступлений:

1) средства и методы установления причин и условий, способствовавших совершению или сокрытию преступлений;

2) средства и методы получения информации о готовящихся преступлениях;

3) средства и методы защиты различных объектов от преступных посягательств и создания благоприятных условий для возникновения доказательственной информации [3, С. 154].

Представляется, что включение ИИ в процесс предупреждения преступлений позволит расширить арсенал всех трех обозначенных групп. На сегодняшний день к технологиям на базе ИИ для предупреждения преступлений можно отнести: предиктивная аналитику, поддержку принятия решений, системы распознавания лиц и изображений, анализ цифровых улик, обработку естественного языка.

Термин предиктивная аналитика происходит от английского слова «predictive», которое означает «предсказательный» и подчеркивает стремление заглянуть в будущее и попытаться предугадать дальнейшее развитие событий. Данная технология опирается на анализ ретроспективных данных, и статистические выкладки, которые изучаются системами ИИ. Анализ, проводимый ИИ позволяет выявить определенные паттерны, характерные для анализируемых данных и экстраполировать их на будущие процессы. При этом такие модели фиксируют связи огромного числа факторов чтобы сделать оценку наиболее полной и точной. Фактически чем более объемной является информационная база, на которой обучается система, тем более точно она сможет анализировать информацию. Такая система позволяется работать с огромным массивом различной информации и искать взаимосвязи там, где человек будет видеть лишь набор

разрозненных данных.

Можно допустить, что технологии ИИ, предполагающие наличие способности к самообучению, могут решить множество прикладных криминалистических задач. В части предсказательной аналитики важно понимать, что «предсказания» система делает на основе анализа загруженной ранее информации, базы данных. При этом ранее использованные системы, характеризующиеся строго алгоритмизированным подходом, например автоматизированные информационно-поисковые системы (далее АИПС) позволяли следователям структурировать, искать и хранить информацию, но глубокого анализа этих данных и поиска скрытых взаимосвязей внутри нее не происходило. Так, рассматривая вопрос применения строго алгоритмизированных механизмов и технологий расследования Е. П. Ищенко пишет: «некоторые связи не могут быть использованы при алгоритмизации расследования, ибо не являются закономерными, либо такие закономерности пока еще не выявлены. Примером может служить связь между характеристиками преступления и потерпевшего, с одной стороны, и признаками личности преступника, с другой. Некая связь здесь действительно присутствует, но она очень осложнена элементом случайности» [4, С. 52]. Машинное обучение предполагает другой подход, в рамках этой технологии поиск решения идет не строго по заданному алгоритму (напрямую), а индуктивно, через процесс обучения на множестве сходных задач, которые можно именовать прецендентами. Это особенно полезно, когда стоит цель проанализировать множество различных параметров и переменных. ИИ на базе технологий машинного обучения способен изучать огромный массив информации и вычленять из этой информации статистические или вероятностные сигналы о наличии тех или иных причинно-следственных связей [5].

На сегодняшний день с помощью алгоритмов машинного обучения правоохранительные органы могут анализировать исторические данные о преступлениях и выявлять закономерности, которые помогают предсказать, где и когда могут произойти новые преступления. Это позволяет более эффективно распределять ресурсы и проводить профилактические мероприятия. Например, в некоторых странах уже используются системы, которые на основе анализа данных о преступлениях рекомендуют патрулирование конкретных районов в определенное время суток. Что позволяет высвободить ресурсы с тех районов, где наблюдается пониженная криминогенность. Алгоритмы искусственного интеллекта помогают определить, в каких областях необходимо увеличить ресурсы для борьбы с преступностью, а также выявить типы преступлений, на которые следует сосредоточить профилактические усилия. На основе этой информации разрабатывается стратегия противодействия правонарушениям. Кроме того, это позволяет оптимизировать внутренние процессы в борьбе с преступностью, включая улучшение привлечения и обучения сотрудников, составление графиков работы для каждого работника, разработку логистических моделей для поддержки правоохранительной деятельности [6, С. 280].

Для предотвращения преступлений также разрабатываются алгоритмы для анализа «горячих точек», то есть зон с высоким уровнем криминогенности. При таком подходе анализируется места совершений преступлений и накладываются на карту тем самым создавая области, которые являются более подверженными риску совершения там преступления. Яркий пример такой системы это Predictive Policing (PredPol), система на базе математики, прогностической аналитики и методов ИИ, разработанная в США и призванная обозначать такие «горячие точки». Данная система суммирует массив полицейских данных о совершенных преступлениях и анализируя его предоставляет карту города или конкретной области, разбитых на определенные квадраты, где путем

обработки данных выводится вероятностное значение возможности совершения там преступлений. В свою очередь это позволяет сконцентрировать силы полиции именно в этих точках, установить там регулярное патрулирование, тем самым обеспечить предупреждение преступления до момента его совершения. По оценкам, которые предоставляют эксперты данная система уже показала значительное снижение преступности в районах с активным использованием этого программного обеспечения [7].

Для целей предупреждения преступлений системы предиктивной аналитики могут интегрироваться с системами поддержки принятия решения. Такие системы в классическом их понимании представляют собой программно-аппаратные комплексы, которые созданы с целью хранения и поиска необходимой информации. Они позволяют правоохранительным органам быстро получать, сравнивать, анализировать информацию, в результате чего сотрудник может принимать более обоснованные решения. Классические примеры, которые получили практическое применение это информационные базы данных, направленные на решение конкретных задач. Так система «Маньяк» агрегирует информацию при расследовании серийных убийств на сексуальной почве. Система «Блок» обеспечивает информационное сопровождение расследования экономических преступлений. Система «Опознание», включает данные примет лиц, сбежавших от следствия и суда, находящихся в розыске, ранее судимых.

Представляется, что данные системы в их привычном исполнении имеют в своей основе реактивный подход, то есть применяются уже в ходе расследования, после факта преступления, но объединение их с системами способными глубоко анализировать информацию позволяет перейти к проактивному подходу, то есть к возможности прогнозирования предупреждения преступлений до их совершения.

Уже сегодня системы на базе ИИ могут применяться для формирования профилей преступников, исследуя данные о прошлых преступлениях и выявляя характерные особенности, которые могут быть полезны в расследованиях. Набор данных может составляться на основе баз правоохранительных органов используя различную информацию, например: историю правонарушений, личные данные (пол, возраст, образование, место жительства и социально-экономический статус), психологические характеристики (анализ личностных черт, мотивации и психических расстройств, если таковые имеются), социальные связи (информация о друзьях, семье и окружении, которые могут влиять на поведение преступника).

Такой анализ позволяет выявить паттерны и закономерности в лицах и их действиях чтобы создать определенные наиболее вероятностные шаблоны и экстраполировать их на будущее. Аналогичный анализ можно провести для виктимных групп, выявив наиболее общие черты для определенных групп населения стать жертвой преступления. Конечно, стоит отметить, что всегда возникает вопрос этичности и точности таких систем, особенно если изначальные базы данных, на которых обучается система являются некорректными, отличаются субъективностью или имеют характер предвзятости к той или иной категории населения.

Примером системы, которая работает на стыке АИПС и систем направленных на глубокий анализ данных служит разработанная в России программа «ФОРВЕР». Основное направление ее применения это расследование убийств. Система базируется на принципах математики и статистики. Программа «ФОРВЕР», проанализировав исходный набор данных, предлагает следователю перечень версий, упорядоченных по уровню их вероятности. С опорой на результаты этой программы, следователь поручает

оперативным работникам разыскать и проверить лиц, соответствующих конкретным описательным признакам, в соответствии с выводами системы [8]. Важной частью программы выступает криминалистическая характеристика преступления, которая представляет собой набор значимых с криминалистической точки зрения признаков, помогающих охарактеризовать само преступление и его исполнителя. Корреляционные взаимосвязи между признаками, обнаруженными при осмотре места происшествия, и характеристиками неустановленного преступника позволяют формулировать поисковые гипотезы. При выдвижении версии компьютерная программа позволяет осуществлять полный перебор вариантов, достигающий сотен возможных ответов [9].

Рассматривая подобные системы, нельзя не отметить их потенциал в практическом применении, представляется, что такая алгоритмизация отработки следственных действий позволит кратно ускорить процесс расследования за счет приоритезации проверки версий в зависимости от их вероятности. С точки зрения ценности прогнозирования и предупреждения преступлений можно предположить, что подтвержденные практическим применением результаты программы позволят сформировать определенные шаблоны взаимозависимости между преступлением и лицом его совершившим и применить их при проведении дальнейших расследований и профилактики преступлений.

При этом остаются вопросы относительно, наличия корреляционных взаимосвязей, всегда ли они присутствуют. Статистические методы могут содержать погрешности, особенно если обучающие данные не репрезентативны. Также при рассмотрении данной технологии, как и технологии предиктивной аналитики в целом следует подчеркнуть, что подобные системы генерируют исключительно вероятностные варианты развития событий. Такие прогнозы не дают точного видения будущего, а лишь моделируют возможные сценарии, реализация которых носит лишь потенциально возможный характер. Тем не менее, можно предположить, что с учетом возможных методов корректировки обучения таких систем и расширения базы данных, статистическая вероятность реализации предложенных гипотез будет только увеличиваться.

Исходя из описанного можно заключить, что способы применения правоохранительными органами систем предиктивной аналитики наиболее перспективны в следующих направлениях:

- генерация наиболее вероятностных сценариев совершения преступлений. В ходе такой генерации выдвигается прогноз о том, как и где могут произойти преступления на основе анализа исторических данных, таких как время, место и типы инцидентов;

- определение зон с повышенной криминогенностью с последующим наиболее рациональным распределением ресурсов в данные области;

- выявление паттернов и единых механизмов совершения преступления, выявление серийности;

- выявление организованной преступности через изучение отношений подозреваемых, посредством анализа общих контактов, мест или финансовых потоков;

- моделирование поведения преступника и его мышления для того, чтобы предсказать наиболее вероятностные варианты действий;

- моделирование поведения следователя и его мышления для целей анализа ошибок и выработки наиболее рациональных стратегий расследования;

- выявление мошеннических схем, включая анализ повторяющихся паттернов обмана, такие как поддельные сайты, телефонные аферы или финансовые пирамиды, на основе анализа транзакций и обращений;

- прогнозирование тенденций преступности, их качественных и количественных характеристик;

- интеграция в системы поддержки принятия решений.

Наибольшее практическое применение и развитие в перечне технологий на базе ИИ, которые могут быть использованы для целей предупреждения преступления, на текущим момент, получили системы распознавания изображений и лиц. Данная технология, иначе именуемая компьютерным зрением, обеспечивает взаимодействие между цифровой средой и материальной действительностью, позволяет получать и анализировать данные материального мира, переведенные в цифровую форму а также использовать их для решения конкретных задач с ограниченным участием человека. Технологии распознавания лиц, могут использовать нейронные сети и специальные механизмы обработки, посредством которых получается сопоставить два изображения: исходный образец и искомый объект или выявить наиболее похожие, а также осуществить поиск по общей базе данных. Важно отметить, что механизм нейронных сетей имеет в своей основе не просто полностью последовательно запрограммированную базу, а заложенный механизм обучения. Это важнейшее отличие и преимущество в сравнении с системами, предполагающими строгую алгоритмизацию. Нейросеть проводит анализ данных и пытается выявить определенные, повторяющиеся элементы. В этом процессе система делает множество ошибок, с каждым повторением ошибок становится все меньше, это происходит за счет того, что при каждой итерации нейросеть сравнивает свои результаты с правильными ответами и корректирует свои параметры. Такой процесс именуют обратным распространением ошибки. По итогу получается система, которая за счет обучения на множестве собственных ошибок постоянно совершенствуется и предоставляет все более и более точные результаты.

Задачи, для которых используется технология можно разделить на несколько категорий. Во-первых, распознавание, то есть возможность понять присутствует какой-либо объект на изучаемом изображении или видеозаписи, а также возможность понять обладает ли этот объект какими-либо качествами и параметрами. Например, в контексте расследования важно понять находится ли на изображении человек или другой искомый объект, а также какими визуальными характеристиками он обладает. Во-вторых, классификация, то есть возможность группировки объектов по определенному признаку или отнесению их к определенной группе. Это имеет важное значение поскольку зачастую мало определить, что человек запечатлен на фото или видеозаписи, но и важно понять, что он относится к определенной группе, выделяющей его из остальных людей, например, находится в розыске. В-третьих, улучшение или восстановление изображений и видеозаписей, которые имеют плохое качество для того, чтобы придать изучаемому объекту более четкую форму, избавить от лишних шумов и помех, препятствующих его изучению. Например, часто фиксация камерами наружного наблюдения осуществляется в темное время суток или плохую погоду из-за чего качество изображения падает, в свою очередь нейросети анализируют данные, восстанавливают недостающие элементы и устраняют недостатки, опираясь на примеры из своего обучения.

Пример системы распознавания изображений и лиц программный комплекс под названием Clearview AI. Эта система распознавания лиц использует обширную базу

данных изображений, собранных из открытых источников, таких как социальные сети. Правоохранительные органы могут загружать фотографии подозреваемых, и система ищет совпадения в своей базе данных, что позволяет быстро идентифицировать личность. Системы распознавания лиц способны идентифицировать подозреваемых по видеозаписям с камер наблюдения, что значительно ускоряет расследование. Задачи, которые ставятся перед таким программным комплексом следующие: идентификация подозреваемых, свидетелей и жертв, поиск пропавших людей, контроль доступа. При этом стоит отметить, что система вызвала большой общественный резонанс в связи со спором в отношении законности использования таких систем и нарушения ими конфиденциальности людей, прав пользователей и законов о защите персональных данных [10].

Похожая система под названием FindFace Security от компании NtechLab была разработана в России и применяется на железнодорожных станциях в целях управления пассажиропотоком, розыска преступников и пропавших людей. Данная программа является интеллектуальной видеоаналитикой, основанной на распознавании лиц. Лица в режиме реального времени выделяются из видеопотока специализированной системой, сверяются со списками мониторинга и, в случае обнаружения совпадения, система отправляет уведомление о наличии совпадения с определенным лицом в имеющейся базе. [11].

Системы фото и видеофиксации в совокупности с системами ИИ способны фиксировать паттерны поведения преступников, определять их эмоции и даже предполагать намерения. Так, ученые из Китая разработали новый функционал системы распознавания преступников, который используется в общественных местах. Эта система работает следующим образом: анализируются записи с камер видеонаблюдения, и сопоставляется поведение людей на этих записях с характерными паттернами преступников. Исследователи выделили 11 различных категорий действий в видеоданных, алгоритм способен распознавать, как потенциальные правонарушители сердятся, оглядываются, курят, бегают, прыгают, наносят удары, ходят и какие позы принимают люди, готовые к совершению преступления и так далее. Аналогичные системы, получившие название «Безопасный город», в последние годы активно внедряются и в крупных городах России [12].

Исходя из описанного можно выделить следующие ключевые направления использования систем распознавания изображений и лиц в процессе предупреждения преступлений:

- сравнение лиц с информацией в базах данных (например, фото из паспортов, криминальных архивов или баз розыска);

- поиск и оперативное оповещение правоохранительных органов о наличие того или иного искомого объекта;

- мониторинг общественных пространств, посредством интеграции с системами видеонаблюдения для контроля за местами общего пользования такими как аэропорты, метро или улицы;

- обработка больших объемов данных для выявления паттернов поведения, таких как подозрительные перемещения, необычное поведение;

- контроль доступа для безопасности важных объектов. Использование система распознавания лиц в системах охраны для верификации личности при входе в

защищённые зоны, для целей несанкционированного проникновения;

- комбинация с другими биометриями (отпечатки пальцев, голос) для создания комплексных профилей, с целью повышения точности идентификации.

Учитывая широкое распространение компьютеризации в различных областях, в криминалистике все большую актуальность приобретает такое направление, как форензика. Данная область знаний изучает методы и способы раскрытия и предупреждения преступлений, связанных с компьютерной информацией. Важная часть этого учения - это цифровые улики или цифровые следы. По своей сути это информация, собранная из электронных устройств и систем, которая может быть использована в качестве доказательства в процессе расследования преступлений. По мнению Е. Р. Россинской цифровой след представляет собой: «криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [13]. Цифровые следы могут включать: данные с компьютеров и мобильных устройств, логи (текстовые файлы фиксирующие действия пользователя в программе) интернет-активностей, сообщения и электронные письма, данные из социальных сетей, информация из облачных хранилищ, информация об отчетах или финансовых транзакциях пользователей.

Анализ цифровых улик, проводимый системами на базе ИИ, также может использоваться для предотвращения преступлений. Например, такие системы действуют в сфере мониторинга киберугроз. Так анализ сетевого трафика и поведения пользователей может помочь выявить потенциальные угрозы, такие как попытки незаконного проникновения в личные данные пользователей, попытки проведения незаконных переводов с целью легализации средств, полученных преступным путем или террористической деятельности, регулярный просмотр информации, который может свидетельствовать о противоправных мотивах лица.

Анализ цифровых улик позволяет осуществлять обнаружение схем мошенничества с использование интернет-банкинга. Современные системы анализа данных могут выявлять аномалии в финансовых транзакциях, то есть система может видеть, когда финансовые операции отличаются от регулярных паттернов и сигнализировать это человеку, который в свою очередь проводит детальную проверку, запрашивает дополнительные документы или блокирует такую операцию.

Примером такой системы может служить, разработанный компанией IBM программный комплекс Watson for Cyber Security. Он представляет собой суперкомпьютер, оснащенный системой ИИ. Watson for Cyber Security использует искусственный интеллект и машинное обучение для улучшения безопасности информационных систем и защиты от киберугроз. Путем анализа больших объемов данных, он выявляет аномалии и автоматизирует процессы реагирования на инциденты [14]. В российских банках действуют специальные антифрод системы, построенные на анализе большого количества данных с применением ИИ. Принцип работы сконцентрирован на оценке действий клиента и информировании об аномалиях. При обнаружении таких подозрительных действий система блокирует операцию, препятствуя возможности преступника совершить противоправное действие. [15]

Говоря о системах, работающих с цифровыми уликами, нельзя не отметить важность технологии обработки естественного языка. Технологии обработки естественного языка и анализа цифровых улик довольно близки в контексте изучаемого вопроса поскольку

объектом изучения систем обработки языка зачастую являются текстовые файлы, которые непосредственно могут выступать в виде цифровой улики.

Системы обработки естественного языка позволяют создавать инструменты способные распознавать и анализировать текстовые данные, по аналогии с тем, как человек способен считывать языковые символы и понимать их смысл. Анализ заключается в выявлении скрытых связей между сообщениями, интерпретация текста, нахождение определенных слов. Например, слов, свидетельствующих или указывающих на возможность приготовления к совершению преступления.

Все это приобретает особую актуальность в современных реалиях, где все большее количество преступлений, подготавливаются, координируются и совершаются посредством интернет-сервисов обмена сообщениями, иначе именуемых социальными сетями или мессенджерами [16]. Представить, что весь объем данных, проходящих через такие сети, может быть анализирован человеком крайне сложно, но такая задача по силам системам обработки естественного языка, построенным на базе ИИ. Так посредством анализа сообщений в социальных сетях может быть найдены готовящиеся угрозы и направлены силы для предотвращения еще до момента фактического совершения преступления.

Системы ИИ с использованием технологии обработки естественного языка осуществляют мониторинг и помогают выявлять подозрительные активности, которые могут вызывать опасения. В таких случаях программа должна немедленно блокировать устройство или процесс, происходящий в сети, после чего правоохранительные органы уведомляются для проведения проверки данной деятельности. Например, автоматизированные системы могут эффективно искать запрещенный контент, блокировать информацию, направленную на торговлю запрещенными веществами, сигнализировать о сообщениях, призывающих к незаконной деятельности [17].

Обобщая сказанное можно выделить следующие основные способы применения систем обработки естественного языка и анализа цифровых улик для целей предупреждения преступлений:

- анализ социальных сетей и сообщений для обнаружения рисков терроризма, экстремизма или криминальных замыслов путем отслеживания публикаций, чатов, а также распознавания шаблонов в общении для определения фраз, указывающих на мошенничество, шантаж или киберпреступления;

- извлечение данных с устройств путем восстановления удаленных файлов, сообщений или истории браузера из смартфонов, компьютеров или жестких дисков для подтверждения преступлений;

- анализ сетевого трафика для мониторинга и реконструкции онлайн-активности, включая IP-адреса, логи и метаданные;

- идентификация цифровых следов путем их поиска в облачных хранилищах, базах данных.

Подводя итоги, отметим следующие значимые положения. На данный момент в мире наблюдает широкая трансформация, вызванная масштабным внедрением компьютерных технологий. Одни из важнейших таких технологий, системы на базе ИИ. ИИ представляет собой одну из наиболее перспективных технологий, которая на сегодняшний день повсеместно внедрятся в практику как российской, так и зарубежной

правоохранительной деятельности. ИИ по своей природе представляет собой совокупность технологий, которые имитируют когнитивные навыки человека. При этом по сравнению с системами алгоритмизированными, системы ИИ обладают способностью к самообучению, что добавляет неоспоримое преимущество в возможности прогнозирования и обработки информации.

Рассмотренные в рамках статьи технологии не заменяют традиционные методы работы правоохранительных органов, но усиливают и расширяют возможности текущих. Системы на базе искусственного интеллекта способны решать несколько ключевых задач, которые сегодня ослабляют эффективность правоохранительных органов. В частности, они помогают преодолеть дефицит кадров и физическую невозможность для человека анализировать постоянно растущий объем информации, позволяют нивелировать ошибки, вызванные субъективным фактором. Системы мониторинга способны заменить человека в анализе многочисленного объема данных, позволяют реагировать точечно и распределять ресурсы исходя из реальной потребности, а также способны освободить человека от выполнения рутинных и повторяющихся операций, с которыми может более эффективно справить машина или программа.

Использование систем на базе ИИ требует формирования нового типа мышления у сотрудников правоохранительных органов, при котором системы ИИ воспринимаются как неотъемлемый инструмент в их работе. В свою очередь, это предполагает необходимость повышения уровня квалификации для обеспечения правильного взаимодействия с такими системами.

Важно, что на данный момент инструмент не лишен недостатков. Среди которых стоит выделить следующие дискуссионные моменты. Возможные ошибки технического характера, которые присущи любой сложной технической системе, в том числе возможность ошибки в изначально заложенных параметрах и алгоритмах программного кода, а также некорректная база данных, на которой проводится обучение модели ИИ. Так как ИИ не работает в вакууме ему необходим объем данных и чем он больше, тем лучше, в связи с этим всегда возникает вопрос безопасности такой базы данных. Нарушение ее целостности несет угрозу приватности и безопасности личной информации, которой потенциально могут воспользоваться преступники. Стоит также заметить, что грани и возможности использования ИИ находятся только в процессе становления и познания, что ведет к тому, что в дальнейшем неминуемо появятся вопросы и проблемы требующие разрешения, скрытые от нас на текущий момент.

Представляется, что уже сейчас растущее применение систем искусственного интеллекта остро ставит вопрос правового регулирования этих систем, особенно с позиции защиты базовых прав человека. В связи с чем представляется необходимым выработка законодательных и этических норм, описывающих границы возможного применения этих технологий. В противном случае имеется существенный риск, когда системы, которые должны противодействовать преступности и прогнозировать ее сами создают прецеденты нарушающие нормы права. Анализируя системы распознавания лиц и анализа цифровых улик, возникает множество вопросов этического характера, например, на сколько допустимо проводить мониторинг социальных сетей и обмена сообщениями внутри них со стороны систем ИИ, не ставит ли это под сомнение право на неприкосновенность частной жизни и тайну переписки.

Исследование показывает, что несмотря на множество дискуссионных вопросов применение искусственного интеллекта в области криминалистики и предупреждения преступлений открывает новые горизонты для правоохранительных органов и

специалистов в области безопасности. Интеграция систем на базе ИИ в классические криминалистические средства предупреждения преступлений позволяет значительно повысить эффективность расследований, улучшить анализ данных и предсказать возможные угрозы. Сегодня системы, использующие машинное обучение и анализ больших данных, способны выявлять закономерности и аномалии, которые могут указывать на потенциальные преступления, тем самым позволяя правоохранительным органам действовать на опережение. Системы обработки естественного языка позволяют считывать огромный массив информации неподдающийся человеческому анализу и информировать о потенциальных угрозах. Технологии распознавания лиц на базе компьютерного зрения уже давно используются в практической деятельности правоохранительных органов и служат действенным инструментом раскрытия, расследования и предупреждения преступлений, путем распознавания криминальных элементов и попыток совершения преступных действий.

Библиография

1. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы: монография. М.: Проспект, 2025. 176 с. EDN: GKWMZB.
2. Бычков В. В. Искусственный интеллект в сфере раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей // Российский следователь. 2022. № 1. С. 3-6. DOI: 10.18572/1812-3783-2022-1-3-6. EDN: VHGGPK.
3. Белкин Р. С. Курс криминалистики: Общая теория криминалистики. В 3-х томах. Т. 1. Москва: Юристъ, 1997. 408 с.
4. Алгоритмизация следственной деятельности: монография / Е. П. Ищенко, Н. Б. Водянова; под ред. Е. П. Ищенко. Москва: Юрлитинформ, 2010. 303 с. EDN: QRTFJX.
5. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2 (104). С. 43-47. EDN: XSESHB.
6. Братко А. Г. Искусственный разум, правовая система и функции государства: монография. Москва: ИНФРА-М, 2021. 280 с. DOI: 10.12737/1064996. EDN: TZZXBK.
7. Костенко Р. В., Ильяшенко А. Н. Будущее уголовного правосудия: роль искусственного интеллекта в предиктивной аналитике // Вестник Санкт-Петербургского университета МВД России. 2024. № 3 (103). С. 200-206. DOI: 10.35750/2071-8284-2024-3-200-206. EDN: FAGBUC.
8. Фесик П. Ю. Технология использования криминалистической характеристики в раскрытии убийств: дис. … канд. юрид. наук. Н. Новгород, 2011. 239 с. EDN: QFEGXZ.
9. Васкэ Е. В., Толстолуцкий В. Ю. Методологические основы комплексного корреляционно-смыслового подхода к составлению розыскного профиля неизвестного преступника // Вестник Пермского университета. Юридические науки. 2014. № 4. С. 166-171. EDN: TGKPHR.
10. Кухарев Г. А., Мауленов К. С., Щеголева Н. Л. Защита изображений лиц от распознавания в социальных сетях: способы решения и их перспективы // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 5. С. 755-766. DOI: 10.17586/2226-1494-2021-21-5-755-766. EDN: KTXDER.
11. Гусенкова А. А. Применение систем видеонаблюдения и автоматизированных систем биометрической идентификации человека при производстве портретных экспертиз и исследований (на примере аппаратно-программного комплекса "Безопасный город") // Вестник Московского университета МВД России. 2021. № 6. С. 86-90. DOI: 10.24412/2073-0454-2021-6-86-90. EDN: LGARSO.

12. Тарасов А. В., Темзоков А. Р. Криминалистические аспекты использования искусственного интеллекта в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2023. № 10. С. 12-16. DOI: 10.24158/tipor.2023.10.33. EDN: AVYVYC.
13. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под ред. Е. Р. Россинской. М.: Проспект, 2022. 256 с.
14. Беспалова Н. В., Корчагин С. А., Сердечный Д. В., Селиверстов В. В. Анализ зарубежного опыта применения интеллектуальных методов в задачах защиты объектов критической информационной инфраструктуры финансового сектора // ИВД. 2024. № 5 (113). С. 1-7.
15. Дазмарова Т. Н. Искусственный интеллект в банковском секторе // Государственная служба и кадры. 2024. № 4. С. 5-7. DOI: 10.24412/2312-0444-2024-4-88-91. EDN: EPYWMO.
16. Соловьев В. С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Всероссийский криминологический журнал. 2016. № 1. С. 60-71. DOI: 10.17150/1996-7756.2016.10(1).60-72. EDN: VPBFZR.
17. Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде: монография / под ред. С. В. Зуева, Д. В. Бахтеева. М.: Юрлитинформ, 2022. 216 с.

Результаты процедуры рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Предмет исследования настоящей статьи не является уникальным. По указанной проблематике имеется достаточное количество работ. Особенно большое количество замечаний вызывает обозначенная тема. Рассматривая искусственный интеллект как криминалистическое средство, в заголовке статьи автор отделяет его от этих средств. Можно отметить непонимание автором технической терминологии, которая используется сегодня специалистами по информационным технологиям в сфере искусственного интеллекта. Так, автор выделяет две основные задачи искусственного интеллекта в криминалистике: это распознавание и идентификация и дифференциация. Фактически это смежные пересекающиеся понятия, и, если бы в данной ситуации автор использовал круги Эйлера, он смог бы для себя подтвердить этот вывод. Вызывает замечания и названная новой «предсказательная функция» алгоритмов, используемых в технологиях искусственного интеллекта. Следует отметить, что такая технология давно реализуется и была применена еще со времен «казанского феномена». Удивительно, что автор не исследовал советские и современные российские разработки по этому направлению, делая акцент на американских. В то же время, если бы он посвятил время изучению этого вопроса, то был бы приятно удивлен тем результатам, которые достигли советские ученые Академии наук СССР при разработке отечественного компьютера и возможностей использования его в прогнозировании.
Методология исследования ограничена лишь описанием, какой автор и что заявил, а также приведен обзор зарубежных компьютерных технологий. Ни один метод свойственный для современной правовой науки в статье не использован. Фактически статья является компиляцией отдельны отрывков, что характеризует текст как рваный. В статье не использованы ни научные методы анализа и синтеза, ни один из частно-

правовых методов.
Актуальность статьи вызывает сомнения. Во-первых, по причине того, что автором не исследован отечественный опыт. А во-вторых, потому что само название статьи содержит логические ошибки исходя из текста представленного научного труда.
Научная новизна в статье отсутствует. В тексте представленного материала содержится лишь отрывочное перечисление мнений и существующих технологий.
Стиль, структура, содержание поставлены в зависимость от вышеописанных проблем научного метода, который надлежало использовать в статье. Например, целесообразно было провести сравнительно-правовое исследование, а не только обозреть технологии, которые есть за рубежом. Так, автору следовало описать не техническую сторону, а обратиться к зарубежным нормативным правовым документам, которые регламентируют применение искусственного интеллекта в криминалистике в зарубежных странах.
Библиография вызывает замечания, поскольку в ней не приведены современные диссертационные исследования (коих очень много) по рассматриваемому вопросу, не приведены и зарубежные источники.
Апелляция к оппонентам полностью отсутствует. Автор просто перечисляет точки зрения других авторов не подвергая их критическому анализу.
Выводы, интерес читательской аудитории. Данная статья имеет характер газетной публицистики, в связи с чем должна быть переработана и направлена заново.

Результаты процедуры повторного рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Рецензия на статью
«Возможности применения искусственного интеллекта в предупреждении преступлений»

Статья посвящена изучению возможностей применения искусственного интеллекта (далее по тексту – ИИ) в предупреждении преступлений, подчеркивая важность новых методов и инструментов, направленных на повышение уровня общественной безопасности. Автором рассматриваются ключевые направления использования ИИ в криминалистике, среди которых выделяются предиктивная аналитика, поддержка принятия решений, системы распознавания лиц и изображений, анализ цифровых доказательств и обработка естественного языка.
Предметом исследования являются функционально-технологические возможности ИИ применительно к практике предотвращения правонарушений. Центральное внимание уделено правомерности и обоснованию внедрения указанных технологий. Однако недостатком текста является отсутствие четкого описания методологической базы проведенного исследования, что рекомендовано восполнить посредством введения соответствующих пояснений о выбранных методах и процедурах.
Исследование актуально ввиду стремительного развития технологий и возрастающего количества доступных для анализа данных, позволяющих эффективнее выявлять и предотвращать преступные деяния. Особенное значение имеет вклад современных

криминалистических средств, основанных на искусственном интеллекте, которые способствуют оптимизации процесса выявления преступлений и снижению ошибок человеческого фактора.

Научная новизна исследования проявляется в постановке ряда важных тезисов. Во-первых, отмечается перспективность повсеместного распространения ИИ в рамках правоохранительной деятельности, как отечественной, так и международной практики. Во-вторых, указывается на решение основных проблем, стоящих перед органами правопорядка, путем автоматизации обработки большого массива данных, уменьшения зависимости от субъективных факторов и освобождения сотрудников от рутинных процессов.

Структурная организация текста соответствует научным стандартам, изложение ясно и доступно, что способствует легкому восприятию материала читателями различной профессиональной направленности. Тематический охват полный и систематизированный, стилистическое оформление соответствует требованиям академического стиля. Между тем отдельные положения требуют дополнительной эмпирической поддержки и статистического подкрепления, особенно в части рисков предвзятости алгоритмов и негативных последствий ошибочных прогнозов.

Библиографический список отличается полнотой и разнообразием, включающим труды известных ученых-криминалистов и юристов-процессуалистов, таких как Бахтеев Д.В., Белкин Р.С., Россинская Е.Р., Зуев С.В. и др. (Бахтеев Д. В. Искусственный интеллект: этико-правовые основы: монография. М.: Проспект, 2025. 176 с., он же – Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2 (104). С. 43-47; Белкин Р. С. Курс криминалистики: Общая теория криминалистики. В 3-х томах. Т. 1. Москва: Юристъ, 1997. 408 с.; Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под ред. Е. Р. Россинской. М.: Проспект, 2022. 256 с.; Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде: монография / под ред. С. В. Зуева, Д. В. Бахтеева. М.: Юрлитинформ, 2022. 216 с. и прочее). Это свидетельствует о глубине проведенной исследовательской работы и высоком уровне теоретической подготовки автора.

Тем не менее, вызывает сожаление отсутствие развернутого критического осмысления позиций цитируемых авторов, что снижает аргументированность выводов. Несмотря на это, выводы соответствуют содержанию и представляются интересными для научных кругов, педагогов-юристов и практикующих следователей.

Выводы статьи в целом отражают содержание работы и представляют интерес для научного сообщества, преподавателей юридических вузов и практических сотрудников органов предварительного расследования. Исследование показывает, что несмотря на множество дискуссионных вопросов применение искусственного интеллекта в области криминалистики и предупреждения преступлений открывает новые горизонты для правоохранительных органов и специалистов в области безопасности. Интеграция систем на базе ИИ в классические криминалистические средства предупреждения преступлений позволяет значительно повысить эффективность расследований, улучшить анализ данных и предсказать возможные угрозы. Сегодня системы, использующие машинное обучение и анализ больших данных, способны выявлять закономерности и аномалии, которые могут указывать на потенциальные преступления, тем самым позволяя правоохранительным органам действовать на опережение.

Таким образом, статья «Возможности применения искусственного интеллекта в предупреждении преступлений» затрагивает важную и актуальную проблему правоохранительной деятельности, в частности криминалистического предупреждения

преступлений. Автор демонстрирует хорошее понимание темы и способность к системному анализу. Вместе с тем, статья рекомендуется к дальнейшему совершенствованию без обязательного дополнительного рецензирования, хотя и предполагает рекомендации по углублению методологического аппарата и расширению полемики вокруг использования технологий ИИ в правовой сфере.

Результаты процедуры окончательного рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Статья «Возможности применения искусственного интеллекта в предупреждении преступлений» посвящена комплексному анализу возможностей, пределов и рисков применения технологий искусственного интеллекта (ИИ) в сфере криминологического прогнозирования и предупреждения преступлений. Предмет исследования рассмотрен многоаспектно, включая технологическую составляющую криминологическую эффективность, а также ключевые правовые и этические ограничения.
Методологическая база исследования является междисциплинарной и комплексной: основу исследования составили фундаментальные научные принципы диалектики, историзма и объективности; обще-научные методы анализа и синтеза, индукция и дедукция, и частно-научные методы, а именно формально-юридический, системный и структурно-функциональный анализ, сравнительно-правовой и нормативный анализ, метод моделирования для описания принципов работы прогнозных алгоритмов и сценариев их внедрения. Такой подход обеспечивает всесторонность и глубину исследования.
Актуальность темы обусловлена стремительной цифровизацией всех сфер жизни, включая правоохранительную деятельность, и глобальным запросом на технологии "умной" безопасности, балансом между безопасностью и приватностью, эффективностью и дискриминацией. Статья дает научно обоснованный ответ на эти вызовы, что делает её крайне востребованной.
Новизна работы в синтезе технологического и гуманитарного знания: автор не ограничивается описанием технологий, а делает акцент на их социально-правовых последствиях; предложена четкая и аргументированная классификация рисков внедрения ИИ, что является вкладом в методологию оценки подобных систем; подчеркивается необходимость сохранения за человеком роли лица, принимающего окончательные решения, что предлагает конструктивный путь интеграции ИИ как инструмента.
Статья написана ясным, логичным и терминологически выверенным научным языком. Структура логична: введение формулирует проблему, основной текст последовательно раскрывает потенциал, анализирует риски и предлагает регуляторные подходы, , заключение содержит взвешенные выводы. Содержание демонстрирует высокий уровень эрудиции автора. Стиль, глубина анализа и практическая значимость выводов соответствуют стандартам научной публикации.
Автор демонстрирует высокую степень научной рефлексии, последовательно рассматривая аргументы сторонников технократического подхода и его категоричных

противников, что усиливает убедительность и объективность работы.

Выводы статьи являются логичным завершением проведенного анализа. Они сбалансированы, конкретны и носят прикладной характер. Автор обоснованно утверждает, что потенциал ИИ в предупреждении преступлений реален, но может быть раскрыт только при условии приоритета права и этики над технологическим утилитаризмом.

Исследование показывает, что применение ИИ в области криминалистики и предупреждения преступлений открывает новые горизонты для правоохранительных органов и специалистов в области безопасности. Интеграция систем на базе ИИ в классические криминалистические средства предупреждения преступлений позволяет значительно повысить эффективность расследований, улучшить анализ данных и предсказать возможные угрозы

Статья представляет собой своевременное методологически зрелое исследование. Статья рекомендуется к публикации в научном журнале.