



ИНТЕЛЛЕКТУАЛЬНО-ЦИФРОВЫЕ ИННОВАЦИИ И ПРОФИЛАКТИКА ПРАВОНАРУШЕНИЙ: ТОЧКИ СОПРИКОСНОВЕНИЯ

З.Ш.Шаумаров

Старший преподаватель кафедры Деятельность профилактики
правонарушений Академии МВД Республики Узбекистан,
подполковник

А.Насимов

Курсант 336-группы 3-курса Академии МВД Республики
Узбекистан,

<https://doi.org/10.5281/zenodo.15395927>

ARTICLE INFO

Qabul qilindi: 05-May 2025 yil

Ma'qullandi: 10-May 2025 yil

Nashr qilindi: 13-May 2025 yil

KEY WORDS

профилактика
правонарушений,
искусственный интеллект
(ИИ), цифровизация,
кибербезопасность,
предиктивный анализ,
информационные технологии
(ИТ).

ABSTRACT

в статье рассматриваются возможности интеграции инновации ИИ и цифровизации в систему профилактики правонарушений, с акцентом на заблаговременное предотвращение преступлений и обеспечение общественной безопасности с помощью нейросети, искусственного интеллекта (ИИ) и информационных технологий (ИТ). В условиях использования индивидами цифровых технологий с противоправными намерениями, а также глобальных изменений в правовом и социальном контексте, зарубежный опыт применения интеллектуальных систем в США, КНДР, Великобритании и других странах практики рода «системы предиктивного патрулирования на основе ИИ и исторических данных о преступности» и «системы видеонаблюдения с распознаванием лиц и алгоритмы анализа поведения» подчёркивают высокую эффективность таких подходов. Рассматриваются перспективы использования цифровых инструментов для профилактики правонарушений, однако, одновременно выявляются возможные риски, связанные с пресечением прав и свобод граждан, что требует особого внимания к обеспечению конфиденциальности данных и сведений. Подчёркивается, что успешная интеграция искусственного интеллекта и других инноваций в

В современном этапе развития Республики Узбекистан особое внимание уделяется цифровизации всех сфер общественной жизни¹, в том числе и системы профилактики правонарушений. Традиционные методы контроля и учёта уступают место инновационным технологиям, позволяющим более эффективно управлять общественным порядком, предупреждать правонарушения и обеспечивать безопасность граждан. На сегодняшний день в стране активно внедряются цифровые платформы, такие как «E-Mahalla», «E-Xonadon», «E-Jarima», которые направлены на автоматизацию мониторинга, сбора, анализа и обработки информации в реальном времени. Это позволяет не только оперативно реагировать на потенциальные угрозы, но и формировать устойчивую цифровую базу для принятия превентивных мер. Таким образом, можно говорить о начале становления интеллектуально-цифровой модели профилактики правонарушений в Узбекистане. Несмотря на то, что процесс цифровой трансформации находится на начальной стадии, уже наблюдаются позитивные изменения в правоприменительной практике. Это, в свою очередь, создаёт предпосылки для более глубокой интеграции искусственного интеллекта и других интеллектуальных систем в деятельность правоохранительных органов. Несмотря на активную государственную политику в направлении цифровизации управления и правоохранительной деятельности, а также наличие стратегических программ и целевых инвестиций в ИТ-сферу, уровень технологического развития преступной среды зачастую опережает официальные институты. Это обусловлено тем, что криминальные элементы действуют вне бюрократических процедур, гибко адаптируются к новым цифровым реалиям и быстро осваивают новейшие технологические решения — от использования зашифрованных мессенджеров до внедрения криптовалют, VPN-туннелей, фейковых идентичностей и автоматизированных схем мошенничества. В то время как государственные структуры сосредоточены на модернизации технической инфраструктуры, создании единых баз данных, цифровизации документооборота и интеграции межведомственных систем (в рамках проектов типа «E-Mahalla», «E-Xonadon», «E-Jarima»² и других), преступный мир эффективно осваивает те же цифровые ресурсы, но с противоправными целями³ — оставаясь мобильным, анонимным и трансграничным. Это порождает ситуацию, при которой государство, несмотря на объективные усилия, вынуждено вести реактивную политику, постоянно догоняя новые формы цифровых правонарушений. Таким образом, на фоне роста киберпреступности, социальной инженерии, цифрового экстремизма и анонимной интернет-активности, становится очевидным: необходим не просто технологический апгрейд, а глубокая реформа парадигмы профилактики, в основе которой должно лежать проактивное применение технологий искусственного интеллекта, машинного обучения, больших данных и интеллектуального видеонаблюдения. Эффективная борьба с цифровыми формами преступности невозможна без переосмысления роли государства как не только надзорного, но и прогностического субъекта, способного действовать на опережение, выстраивать

систему анализа рисков, выявления поведенческих отклонений и цифровых следов противоправной активности ещё до момента совершения правонарушения.

К сожалению, в переходный период нашей страны из-за непросвещённости, низкой правовой культуры и образования некоторые молодые люди стали жертвами вербовок незаконных религиозных экстремистских организаций.

Профилактика религиозного экстремизма в Республике Узбекистан — это многогранный процесс, который требует комплексного подхода, включающего образование, профилактику, законодательство, а также активное участие гражданского общества. Важно, чтобы меры по борьбе с экстремизмом не нарушали права граждан, обеспечивали свободу вероисповедания и способствовали созданию устойчивого и безопасного общества.

Корни таких явлений, как экстремизм, радикализм и терроризм, маскирующихся под религиозные идеи, уходят в далекое прошлое. Однако в настоящее время они никогда не угрожали безопасности и стабильности стран так сильно, как сегодня.

Предотвращение подобных угроз, устранение факторов, способствующих их развитию и борьба с ними стали важнейшими задачами для каждой страны.⁴

С учётом трансформации угроз в цифровой плоскости и технологической эволюции как правомерной, так и преступной деятельности, настоящая работа ставит своей целью обоснование необходимости перехода к качественно новой парадигме профилактики⁵ правонарушений, основанной на глубокой интеграции интеллектуально-цифровых инноваций в систему обеспечения правопорядка. Для достижения поставленной цели предполагается рассмотреть и систематизировать задачи, решение которых критически необходимо для адаптации механизма профилактики к реалиям XXI века. Эти задачи охватывают три ключевых направления, это обеспечение общественной безопасности на новом технологическом уровне, противодействие цифровой преступности, а также, применение искусственного интеллекта и нейросетей в сфере цифровой аналитики и профилактики, которые требуют не просто реформ, а технологического скачка и институциональной переориентации.

Современная общественная безопасность невозможна без надёжного технологического фундамента. Здесь немаловажную роль играет взаимодействие структур и информационный обмен.

Взаимный информационный обмен считается наиболее распространенной формой сотрудничества, так как обмен информацией в основном рассматривается в процессе отношений между сторонами сотрудничества. Учитывая, что выводы, основанные на сборе, анализе и обмене информацией, влияют на взаимоотношения сотрудников правоохранительных органов с правонарушителем или лицом, склонным к правонарушению, некоторые ученые считают поиск и обмен информацией одной из основных технологий деятельности ОВД.⁶

Приоритетной задачей является модернизация технического и цифрового оснащения правоохранительных органов, что требует высокого уровня финансового,

кадрового и научного обеспечения. Речь идёт не просто об обновлении оборудования, а о внедрении интеллектуальных систем реального времени, таких как:

- автономные дроны с ИИ-навигацией и распознаванием ситуаций риска в городском пространстве;⁷

- комплексные системы “умного мониторинга”, интегрирующие анализ видеопотока с функциями распознавания лиц, поведения и аномалий;⁸

- биометрические идентификационные платформы, использующие распознавание по:

- лицу,
- отпечатку пальца,
- радужной оболочке глаза (зрачку),
- голосу и даже паттернам походки.

Все эти технологии формируют цифровой контур наблюдения и профилактики, способный фиксировать, анализировать и классифицировать потенциальные угрозы ещё на стадии их формирования.⁹

Следующий стратегический вектор — это борьба с высокоорганизованной, трансграничной и анонимной преступной деятельностью, перешедшей в киберпространство. Ключевые угрозы включают:

- использование VPN-туннелей и даркнета для сокрытия цифровой активности;¹⁰
- трансграничные кибератаки на информационные и критически важные инфраструктуры;
- кражу и утечку персональных данных граждан, а также государственной информации;
- фишинг и социальная инженерия, используемые для обмана пользователей и сотрудников организаций;
- бот-сети, применяемые для атак типа DDoS, дестабилизации информационных потоков и распространения фейковой информации.

Актуальной и практически неизбежной проблемой современности становится вмешательство в государственные информационные ресурсы, включая базы МВД, органов ЗАГС, ГНИ, а также манипуляции в системе электронного голосования и подделка цифровых удостоверений личности. В этих условиях цифровая профилактика должна включать в себя не только технические меры, но и гибкую правовую регламентацию, ориентированную на киберсуверенитет, правовое пресечение анонимности и защиту цифровых границ.

Третья и наиболее перспективная задача — интеграция ИИ и нейросетевых моделей в комплекс превентивных и аналитических механизмов правопорядка. Искусственный интеллект способен взять на себя не только функции мониторинга, но и:

- автоматическое выявление правонарушений по видеопотоку и аудиопотоку в общественных местах;

- предиктивную аналитику, способную прогнозировать вероятность совершения преступления на основе поведенческих паттернов, геоданных и социальных факторов;
- оценку рецидивного риска у условно-досрочно освобождённых лиц;¹¹
- анализ больших массивов данных из открытых и закрытых источников (в т.ч. соцсетей, мессенджеров, форумов) для выявления скрытых признаков экстремизма, агрессии, подготовки преступлений;
- автоматизированную сортировку обращений граждан по уровню риска, срочности и категории;
- моделирование криминологических сценариев и оценку эффективности оперативных мер.

В ближайшей перспективе ИИ сможет принимать условно-автономные решения, предлагать оперативные меры реагирования органам правопорядка и даже участвовать в формировании доказательственной базы по цифровым следам правонарушений.

Мировая практика демонстрирует устойчивую тенденцию к использованию интеллектуальных цифровых технологий в сфере обеспечения общественной безопасности и профилактики преступности. Развитые государства уже реализуют масштабные инициативы по внедрению искусственного интеллекта, нейросетей, Big Data и автоматизированных систем прогнозирования в правоприменительную деятельность, что позволяет говорить о глобальной трансформации подходов к превентивной политике.

США стали одним из первопроходцев в области применения предиктивного полицейского анализа. Широко используется система PredPol (Predictive Policing),¹² основанная на алгоритмах ИИ и исторических данных о преступности. Она позволяет определять географические зоны с повышенным риском преступлений и направлять туда патрулирование до момента совершения правонарушения. Дополнительно применяются:

- ShotSpotter — акустическая система ИИ-анализа выстрелов в городской среде;¹³
- Real-Time Crime Centers — центры обработки цифровых сигналов, включая видео, соцсети и дорожные сенсоры;¹⁴
- Распознавание лиц и регистрация поведения в реальном времени через умные камеры с нейросетями.

США остаются одним из мировых лидеров в сфере искусственного интеллекта, активно развивая как стратегическую, так и инвестиционную составляющие. В 2023 году был обновлён Национальный стратегический план по ИИ, где акцент сделан на безопасность, прозрачность и подотчётность ИИ-систем. Однако в 2025 году администрация США отменила указ №14110, ранее обязывавший компании раскрывать информацию о своих ИИ-системах, что отражает смену подхода к регулированию отрасли. В рамках нового инвестиционного проекта Stargate США планируют вложить до \$500 млрд в развитие ИИ-инфраструктуры, включая дата-центры и энергетические объекты в Техасе. В дополнение, Microsoft заявила о

намерении инвестировать \$80 млрд в ИИ-дата-центры,¹⁵ из которых более половины будет направлено на территорию США. Научно-исследовательский потенциал США также остаётся значительным. Страна продолжает лидировать по количеству публикаций в области ИИ, но сталкивается с конкуренцией со стороны Китая по числу патентов и объёмам инвестиций. В 2023 году была озвучена инициатива создания общедоступной исследовательской инфраструктуры ИИ, что должно помочь демократизировать доступ к вычислительным ресурсам, данным и экспертизе. Тем не менее, несмотря на масштабные инвестиции, США сталкиваются с рядом вызовов:

- зависимость от зарубежных поставок микрочипов,
- необходимость модернизации энергетической инфраструктуры,
- недостаточная прозрачность и объяснимость ИИ-систем, что снижает общественное доверие.

В Великобритании реализуется концепция “predictive justice” — цифровая аналитика в судебной и правоохранительной системах. Полиция Лондона использует HunchLab, аналог PredPol, для прогнозирования инцидентов. Д. Хассабис, Г. Хинтон утверждают что в 2024 году британские исследователи получили Нобелевские премии за развитие искусственных нейронных сетей и создание системы AlphaFold, которая предсказывает структуру белков, что укрепляет позиции Великобритании в сфере ИИ.¹⁶

М. Бауер, П. Голдер отмечают что Великобритания запустила AI Opportunities Action Plan, который включает создание AI Growth Zones для привлечения инвестиций и развитие инфраструктуры, с общей суммой инвестиций в £14 млрд.¹⁷

Великобритания уверенно продвигается в развитии искусственного интеллекта, стремясь стать одним из мировых лидеров в этой области. В 2025 году правительство представило амбициозный AI Opportunities Action Plan, включающий 50 чётких рекомендаций по стимулированию инноваций. В рамках плана создаются AI Growth Zones — зоны роста, где сосредоточено внимание на инфраструктуре и привлечении инвестиций. Общая сумма частных и государственных вложений должна составить £14 млрд, а это — более 13 000 новых рабочих мест.

Однако на фоне этих достижений Великобритания сталкивается и с рядом серьёзных вызовов. Несмотря на существование обязательного государственного реестра ИИ-систем, в него занесены лишь 9 из всех применяемых ИИ-решений в секторе госуправления, включая социальные и полицейские службы, что вызывает критику за недостаточную прозрачность.

Дополнительный удар по доверию нанёс отказ нового правительства от ранее обещанных £1,3 млрд инвестиций в экзаскейл-суперкомпьютер и сопутствующие исследовательские ресурсы, которые были запланированы для поддержки масштабных ИИ-проектов.

Таким образом, несмотря на масштабные вложения, продуманные стратегические шаги и сильную научную базу, Великобритания сталкивается с вызовами в реализации

ИИ-политики, особенно в вопросах прозрачности и долгосрочной финансовой стабильности проектов.

КНР демонстрирует наиболее масштабную и централизованную модель цифрового контроля, основанную на глубокой интеграции ИИ, видеонаблюдения, биометрии и “социального рейтинга”. Ключевые компоненты: Система “Skynet” — более 600 миллионов камер с ИИ-распознаванием лиц; ¹⁸ ИИ-оценка общественного поведения с помощью “социального кредита”;

Реализация системы раннего выявления лиц с девиантным поведением; Использование искусственного интеллекта для анализа интернет-активности, чатов, звонков, транзакций.

Китайская модель, несмотря на критику в адрес тотального надзора, демонстрирует высокую эффективность в предупреждении массовых беспорядков, уличной преступности и террористических угроз.

П.Э. Струкова отмечает что Китай активно развивает индустрию искусственного интеллекта, стремясь занять лидирующие позиции в мире. В 2017 году была утверждена государственная стратегия, согласно которой страна планирует стать мировым лидером в области ИИ к 2030 году¹⁹. Уже к 2020 году в Китае насчитывалось 1398 ИИ-компаний, что является третьим показателем в мире после США и Великобритании. Китай занимает первое место по количеству научных публикаций в области ИИ, хотя пока уступает США по качественным показателям, таким как уровень цитируемости.²⁰

ИИ также активно применяется в здравоохранении, образовании, промышленности и управлении «умными городами». Однако, несмотря на стремительное развитие и масштабную интеграцию технологий, Китай продолжает сталкиваться с рядом проблем: высокой зависимостью от зарубежных микрочипов, отсутствием прозрачности алгоритмов и неразрешёнными этическими вопросами, связанными с массовым цифровым контролем.

Согласно обобщённым данным Министерства внутренних дел Республики Узбекистан, специализированные подразделения по борьбе с киберпреступностью ведут активную деятельность по выявлению и пресечению цифровых правонарушений. Тем не менее, статистика свидетельствует о стремительном росте преступности в онлайн-среде. Так, по сравнению с 2021 годом, когда было зарегистрировано 2 280 случаев, в 2022 году этот показатель вырос на 89%, достигнув 4 332. В 2023 году число киберпреступлений увеличилось ещё на 27%, составив 5 500 случаев. Наиболее резкий скачок зафиксирован в 2024 году — почти 59 000 зарегистрированных преступлений, что составляет рост более чем на 970% по сравнению с 2023 годом. При этом более 97% всех нарушений были связаны с хищением персональных и финансовых данных граждан. Дополнительно отмечен рост количества заявлений о мошенничестве — на 34% за год. Эти данные подчёркивают, что, несмотря на усилия МВД, преступный элемент стремительно адаптируется к

цифровой среде, что требует коренной модернизации превентивных механизмов и опережающего технологического реагирования.

Несмотря на существующие вызовы, связанные с финансовыми затратами и киберугрозами, очевидно, что Узбекистан движется в стратегически верном направлении по пути цифровой трансформации сферы профилактики правонарушений. Уже сегодня закладывается прочный нормативно-правовой фундамент, обеспечивающий возможность поэтапной интеграции интеллектуально-цифровых инноваций в деятельность правоохранительных органов. В частности, законодательство о кибербезопасности, цифровой экономике, электронном управлении и защите персональных данных формирует целостную правовую рамку, позволяющую внедрять современные технологии — от биометрических платформ до предиктивной аналитики — с соблюдением баланса между эффективностью и правами личности.

Принятые государственные стратегии, такие как «Цифровой Узбекистан — 2030», законы о кибербезопасности и информационной защите, а также постановления, направленные на развитие электронного правительства и защиту критической инфраструктуры, создают не просто декларативные, а практически применимые условия для технологической модернизации системы правопорядка. На практике это выражается во внедрении Ситуационного центра при МВД, функционирующего на базе ИИ-алгоритмов, в создании цифровых платформ, таких как E-Mahalla, E-Xonadon и E-Jarima, и в масштабном оснащении территорий видеонаблюдением, обслуживаемым инспекторами профилактики. Именно на уровне местной профилактической работы постепенно формируются точки соприкосновения между технологиями и исполнением закона.

Инспектор профилактики в ближайшем будущем станет не просто субъектом административного реагирования, а полевым оператором цифровой безопасности, взаимодействующим с нейросетевыми системами, анализирующим сигналы угроз и реализующим превентивные меры в реальном времени. Это знаменует собой переход к новой модели правопорядка, в которой сливаются аналитика, прогноз и профилактика, а инновации становятся неотъемлемым инструментом охраны общественной стабильности.

Современная система профилактики правонарушений переживает глубокую трансформацию, обусловленную развитием цифровых технологий и интеллектуальных решений. Уже недостаточно просто фиксировать правонарушения — необходимо предвидеть их, выстраивая систему реагирования на основе предиктивного анализа, поведенческих индикаторов и анализа цифровых следов. В этом контексте именно профилактика становится тем направлением, где проявляются наибольшие точки соприкосновения между правом и технологией, между превенцией и искусственным интеллектом.

Анализ практики показывает, что большая часть правонарушений, совершенных несовершеннолетними, не наказывается, а к ним применяется мера предупреждения. Потому что несовершеннолетний – это лицо, который в первую очередь нуждается в воспитании и защите. Поэтому в отношении данной категории лиц профилактический эффект в большинстве случаев оказывают не наказания, а методы убеждения и

предупреждения.²¹

Инспектор профилактики, ранее рассматривавшийся преимущественно как субъект махаллинской семёрки, сегодня превращается в активного участника цифровой безопасности — оператора, способного взаимодействовать с нейросетями, анализировать данные из видеонаблюдения и биометрических систем, распознавать модели риска и выносить оперативные суждения. Однако такие технологии не ограничиваются лишь профилактикой: они уже находят применение и в следственной практике, криминалистике²², оперативно-розыскной и разведывательной деятельности, а также в служебной психологии и системе исполнения наказаний. Это говорит о фундаментальном переосмыслении самой логики функционирования правоохранительных органов, где ИИ всё чаще становится не просто инструментом, а самостоятельным субъектом анализа и прогнозирования.

Мировой опыт подтверждает эффективность подобного подхода. Однако он также демонстрирует и обратную сторону цифровизации: риски нарушения прав, угрозы кибератак, этические конфликты, связанные с автономией ИИ. Поэтому успешная цифровая трансформация возможна лишь при наличии надёжного правового сопровождения, прозрачных алгоритмов и гарантии защиты конфиденциальных данных граждан.²³ В этом контексте нормативная база Узбекистана — законы о кибербезопасности, цифровом управлении, персональных данных — формирует необходимый фундамент, но требует динамического обновления, синхронизации с глобальными стандартами и технологическими реалиями. Следовательно, цифровая профилактика — это не просто технологическое обновление, а переход к новой правовой и институциональной парадигме, где безопасность определяется не числом патрулей, а скоростью обработки данных, не масштабом контроля, а точностью прогноза. Узбекистан, формируя эти подходы, получает шанс не догонять глобальные тренды, а формировать собственную модель правопорядка будущего — гибкую, интеллектуальную и ориентированную на опережение.

Использованная литература:

1. Указ Президента Республики Узбекистан от 5 октября 2020 г. № УП-6079 «О стратегии развития “Цифровой Узбекистан — 2030” и мерах по её реализации» // Сборник законодательства Республики Узбекистан, 2020. — № 41.
2. Закон Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 «О кибербезопасности» // Национальная база данных законодательства, 16.04.2022, № 03/22/764/0367.
3. Закон Республики Узбекистан от 30 августа 2019 г. № ЗРУ-547 «О персональных данных» (в редакции от 2022 г.) // Национальная база данных законодательства, 31.08.2019, № 03/19/547/3710.
4. Постановление Президента Республики Узбекистан от 28 апреля 2020 г. № ПП-4699 «О мерах по широкому внедрению цифровой экономики и электронного правительства» // Сборник законодательства Республики Узбекистан, 2020. — № 19.

5. Постановление Кабинета Министров Республики Узбекистан от 5 мая 2021 г. № 242 «О мерах по развитию системы электронного управления» // Национальная база данных законодательства, 06.05.2021, № 09/21/242/0583.
6. Пшиченко Д.В. Использование искусственного интеллекта в противодействии преступности // Полиция и право. – 2023. – № 4. – С. 34–42.
7. Югай Л.Ю. Биометрическая идентификация личности по изображению лица человека: опыт Республики Узбекистан // Ensuring Women's Rights in Uzbekistan. – 2023. – № 2. – С. 244.
8. Репин И.С. Перспективные направления использования искусственного интеллекта в оперативно-розыскной деятельности // Журнал правовых и экономических исследований. – 2023. – № 3. – С. 87–96.
9. Палиева О.Н., Семенцова И.А. Использование искусственного интеллекта и информационных технологий в ходе расследования уголовных дел // Вестник Московского университета им. С.Ю. Витте. Серия 2: Юридические науки. – 2021. – № 2 (28). – С. 22–30.
10. Петров И.В. Использование возможностей искусственного интеллекта в сфере оперативно-розыскной деятельности // Военно-юридический журнал. – 2023. – № 6. – С. 14–21.
11. Кондрашечкин Р.В. Правовое обеспечение применения технологий искусственного интеллекта в оперативно-розыскной деятельности // Вестник ВИПК МВД России. – 2023. – № 2. – С. 56–63.
12. Чебуранова С.Е., Зубрик Д.А. Использование искусственного интеллекта в оперативно-розыскной деятельности // Информационные технологии и право: правовая информатизация. – 2021. – № 6. – С. 45–53.
13. Смирнов С.В., Иванова Т.А. Технологии искусственного интеллекта и дополненной реальности в экспертно-криминалистической деятельности органов внутренних дел // Advances in Law Studies. – 2022. – Т. 10, № 4. – С. 101–110.
14. Зуев С.В., Бахтеев Д.В. (ред.) Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде: монография. – М.: Юрлитинформ, 2023. – 256 с.
15. Тухтамирзаев Ш.Б. Исследование применения искусственного интеллекта в уголовном розыске // Международный педагогический портал «Солнцесвет». – 2023. – С. 12–19.
16. Иванова Л.А. Цифровизация – современный тренд развития правоохранительных органов // Право и цифровая реальность. – 2022. – № 1. – С. 15–24.
17. Космачёв С.В. Адаптация деятельности правоохранительных органов к цифровой трансформации преступной среды // Журнал прикладной криминологии. – 2023. – Т. 2, № 3. – С. 40–52.
18. Рахматова Г.Ж. Профилактика правонарушений в условиях цифровизации (на примере Узбекистана) // Вестник социологии и права. – 2023. – № 4. – С. 77–85.
19. Петров И.В. Предиктивная аналитика в работе органов внутренних дел: возможности и ограничения // Журнал государственной безопасности. – 2022. – № 2. – С. 102–110.

20. Селимова А.В. Биометрические системы в системе обеспечения общественной безопасности // Информационные технологии в правоохранении. – 2021. – № 5. – С. 33–41.
21. Таршева М.Н., Вастьянова О.Д. Искусственный интеллект в борьбе с преступностью: уголовно-процессуальный и криминалистический аспекты // Научный вестник Орловского юридического института МВД России. – 2024. – № 3 (100). – С. 266–275.
22. Степаненко Д.А., Бахтеев Д.В., Евстратова Ю.А. Использование систем искусственного интеллекта в правоохранительной деятельности // Цифровые технологии в современной криминологии. – 2020. – Т. 14, № 2. – С. 206–214.
23. Чебуранова С.Е., Зубрик Д.А. Нейросетевые технологии в оперативно-розыскной деятельности // Правовая информатизация. – 2021. – № 6. – С. 45–53.
24. Палиева О.Н., Семенцова И.А. ИИ и ИТ в расследовании уголовных дел // Вестник МУВ им. С.Ю. Витте. Серия 2: Юридические науки. – 2021. – № 2 (28). – С. 22–30.

