УДК 343.85:004.8

СОВЕРШЕНСТВОВАНИЕ ПРОФИЛАКТИКИ ПРАВОНАРУШЕНИЙ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Зохид Саломов
самостоятельный исследователь.

https://doi.org/10.5281/zenodo.23744129

Аннотация. *В статье исследуются теоретико-правовые и организационные основы применения технологий искусственного интеллекта (ИИ) в деятельности по профилактике правонарушений в Республике Узбекистан. Проанализированы положения Закона Республики Узбекистан «О профилактике правонарушений», Стратегии развития технологий искусственного интеллекта до 2030 года, а также поправок в Закон «Об информатизации», впервые закрепивших легальное определение искусственного интеллекта. Рассмотрены основные направления использования ИИ в превентивной деятельности: прогнозная аналитика, интеллектуальное видеонаблюдение в рамках концепции «Безопасный город», анализ обращений граждан и цифровых следов, раннее выявление факторов социального риска на уровне махалли. На основе изучения зарубежного опыта (США, Европейский союз, Российская Федерация) выделены риски алгоритмической дискриминации, непрозрачности моделей и нарушения права на неприкосновенность частной жизни. Предложена трёхуровневая модель «ИИ-ассистированной профилактики» с обязательным участием человека в принятии решений, а также комплекс предложений по совершенствованию национального законодательства.*

Ключевые слова: *искусственный интеллект, профилактика правонарушений, прогнозная аналитика, предиктивная полиция, «Безопасный город», большие данные, алгоритмическая дискриминация, персональные данные, цифровая трансформация органов внутренних дел.*

Abstract. *The article examines the theoretical, legal and organizational foundations for the use of artificial intelligence (AI) technologies in crime and offence prevention in the Republic of Uzbekistan. The provisions of the Law «On Prevention of Offences», the Strategy for the Development of AI Technologies until 2030 and the recent amendments to the Law «On Informatization» are analyzed. The main areas of AI application in preventive activity are considered, along with the risks of algorithmic bias, opacity and privacy intrusion. A three-level model of «AI-assisted prevention» with mandatory human oversight and a set of legislative proposals are put forward.*

Keywords: *artificial intelligence, offence prevention, predictive analytics, predictive policing, Safe City, big data, algorithmic bias, personal data.*

Введение

Профилактика правонарушений традиционно рассматривается в отечественной и зарубежной криминологии как наиболее гуманное и экономически эффективное направление борьбы с преступностью. Предупредить правонарушение значительно проще и дешевле, чем расследовать его, привлекать виновного к ответственности, исполнять наказание и восстанавливать нарушенные права потерпевшего. Именно поэтому в Республике Узбекистан профилактика правонарушений возведена в ранг

самостоятельного направления государственной политики, а её правовой основой выступает Закон Республики Узбекистан от 14 мая 2014 года № ЗРУ-371 «О профилактике правонарушений» [2].

Вместе с тем классическая модель профилактики, основанная преимущественно на ручном сборе сведений, личном знании участковым инспектором обстановки на обслуживаемой территории и периодическом анализе статистической отчётности, в условиях цифровой трансформации общества обнаруживает существенные ограничения. Объём информации, значимой для предупреждения правонарушений, многократно возрос: это данные видеонаблюдения, обращения граждан через электронные платформы, сведения социальных реестров, информация о транспортных потоках, сообщения в социальных сетях. Обработать такие массивы традиционными методами невозможно, а значит, значительная часть сигналов о готовящихся или вероятных правонарушениях остаётся незамеченной.

Технологии искусственного интеллекта, способные выявлять закономерности в больших данных, классифицировать события, распознавать изображения и речь, прогнозировать развитие ситуаций, открывают качественно новые возможности для превентивной деятельности. Не случайно Постановлением Президента Республики Узбекистан от 14 октября 2024 года № ПП-358 утверждена Стратегия развития технологий искусственного интеллекта до 2030 года [4], а Законом от 21 января 2026 года № ЗРУ-1115 в Закон «Об информатизации» внесены поправки, впервые закрепившие легальное определение искусственного интеллекта и общие принципы его применения [5].

Одновременно использование ИИ в правоохранительной сфере сопряжено с серьёзными рисками: алгоритмической дискриминацией, непрозрачностью принимаемых решений, вторжением в частную жизнь, смещением ответственности с должностного лица на «машину». Зарубежный опыт показывает, что непродуманное внедрение так называемых систем «предиктивной полиции» может не только не снизить преступность, но и подорвать доверие населения к правоохранительным органам.

Цель настоящей статьи – на основе анализа национального законодательства, правоприменительной практики и зарубежного опыта обосновать концептуальную модель применения технологий искусственного интеллекта в профилактике правонарушений и сформулировать предложения по совершенствованию правового регулирования в данной сфере.

Для достижения поставленной цели решаются следующие задачи: определить понятие и содержание «ИИ-ассистированной профилактики»; систематизировать направления использования ИИ в превентивной деятельности; выявить риски и правовые ограничения; разработать предложения по совершенствованию законодательства и организации работы субъектов профилактики.

Материалы и методы исследования

Методологическую основу исследования составили общенаучный диалектический метод познания, а также частнонаучные методы: формально-юридический, сравнительно-правовой, системно-структурный, метод анализа документов и метод моделирования.

Формально-юридический метод применялся при анализе норм Конституции Республики Узбекистан, законов «О профилактике правонарушений», «Об информатизации», «О персональных данных», указов и постановлений Президента Республики Узбекистан, определяющих приоритеты цифровой трансформации.

Сравнительно-правовой метод использовался для сопоставления национальных подходов с регулированием Европейского союза (Регламент (ЕС) 2024/1689 об искусственном интеллекте), практикой США и Российской Федерации. Метод моделирования позволил сформулировать архитектуру системы ИИ-ассистированной профилактики.

Эмпирическую базу исследования составили официальные документы, публикации государственных органов о реализации концепции «Безопасный город», научные труды отечественных и зарубежных исследователей в области криминологии, уголовной политики и права информационных технологий, а также результаты опубликованных полевых экспериментов по применению прогнозных алгоритмов в полицейской деятельности.

Результаты исследования

1. Понятие и сущность профилактики правонарушений на основе искусственного интеллекта

Закон «О профилактике правонарушений» определяет профилактику как систему правовых, социальных, организационных и иных мер, направленных на выявление, изучение, устранение причин правонарушений и условий, способствующих их совершению, а также на предупреждение правонарушений. Законом выделяются общая, специальная, индивидуальная и виктимологическая профилактика, а также определяется широкий круг субъектов – от органов внутренних дел и прокуратуры до органов самоуправления граждан.

Анализ этой системы показывает, что её эффективность напрямую зависит от качества информационного обеспечения. Общая профилактика требует понимания структуры и динамики преступности на конкретной территории; специальная – знания о группах риска и криминогенных факторах; индивидуальная – достоверных сведений о конкретном лице и его окружении; виктимологическая – информации о потенциальных жертвах и ситуациях виктимизации. Каждая из этих задач по своей природе является аналитической, а следовательно, может быть существенно усилена средствами искусственного интеллекта.

Законодатель в Законе № ЗРУ-1115 определил искусственный интеллект как комплекс технологических решений, позволяющих имитировать знания и навыки человека, самостоятельно обучаться, находить решения и получать результаты, сопоставимые с результатами интеллектуальной деятельности человека при выполнении конкретных задач [5]. Принципиально важно, что тем же законом установлен запрет принимать юридически значимые решения, затрагивающие права и свободы человека, исключительно на основании выводов информационных систем, функционирующих на базе ИИ.

С учётом изложенного предлагается следующее авторское определение: профилактика правонарушений на основе искусственного интеллекта (ИИ-ассистированная профилактика) – это деятельность субъектов профилактики по выявлению, прогнозированию и устранению причин и условий правонарушений, осуществляемая с использованием систем искусственного интеллекта в качестве инструмента аналитической поддержки, при сохранении за уполномоченным должностным лицом исключительного права принятия решений и персональной ответственности за них.

Ключевым элементом данного определения является принцип «человек в контуре

принятия решений» (human-in-the-loop). Искусственный интеллект не заменяет участкового инспектора, инспектора по делам несовершеннолетних или представителя махалли, а расширяет их возможности, освобождая время от рутинной обработки информации и концентрируя внимание на наиболее значимых рисках.

2. Правовые и организационные предпосылки внедрения ИИ в профилактику в Республике Узбекистан

В Республике Узбекистан сложилась достаточно развитая нормативная и организационная база для внедрения технологий искусственного интеллекта в правоохранительную деятельность.

Во-первых, на стратегическом уровне цифровая трансформация закреплена Стратегией «Цифровой Узбекистан – 2030», утверждённой Указом Президента от 5 октября 2020 года № УП-6079 [3], и Стратегией «Узбекистан – 2030». Стратегия развития технологий ИИ до 2030 года предусматривает формирование нормативно-правовой базы для развития ИИ, совершенствование стандартов, развитие кадрового потенциала и доведение объёма программных продуктов и услуг на основе ИИ до 1,5 млрд долларов США [4].

Во-вторых, в стране последовательно реализуется концепция «Безопасный город», предполагающая создание единой платформы видеонаблюдения, ситуационных центров и интеграцию информационных систем правоохранительных и иных государственных органов. По официальным данным, на основании постановления Президента 2023 года данная концепция поэтапно реализуется в республиканском масштабе, а интегрированное использование единой платформы позволило сэкономить значительные бюджетные средства [10]. Инфраструктура «Безопасного города» фактически является технологическим фундаментом для внедрения аналитических моделей ИИ.

В-третьих, в системе профилактики сформирована уникальная для региона модель работы на уровне махалли («махаллабай»), включающая институт профилактических инспекторов, а также электронные социальные реестры, позволяющие учитывать семьи и лиц, нуждающихся в социальной поддержке. Эти данные, при условии их правомерной и защищённой обработки, могут служить источником для раннего выявления факторов социального неблагополучия – одной из ключевых причин правонарушений.

В-четвёртых, Законом Республики Узбекистан от 2 июля 2019 года № ЗРУ-547 «О персональных данных» [6] и поправками 2026 года в Закон «Об информатизации» заложены базовые гарантии защиты прав граждан: требования законности обработки персональных данных, административная ответственность за незаконную обработку персональных данных с применением ИИ и запрет на «полностью автоматизированные» юридически значимые решения [5].

Вместе с тем Закон «О профилактике правонарушений» до настоящего времени не содержит норм, прямо регламентирующих использование информационных технологий и систем искусственного интеллекта субъектами профилактики. Отсутствуют требования к качеству данных, к процедуре оценки воздействия алгоритмов на права граждан, к прозрачности и аудиту используемых моделей. Этот пробел создаёт правовую неопределённость как для правоприменителей, так и для граждан.

3. Основные направления применения ИИ в профилактике правонарушений

На основе анализа отечественной и зарубежной практики можно выделить пять основных направлений использования искусственного интеллекта в превентивной

деятельности.

Первое направление – пространственно-временное прогнозирование правонарушений (прогнозная аналитика «горячих точек»). Алгоритмы машинного обучения анализируют исторические данные о зарегистрированных правонарушениях, а также сопутствующие факторы (время суток, день недели, освещённость, наличие мест массового скопления людей, торговых объектов, остановок транспорта) и вычисляют вероятность совершения правонарушений определённого вида на конкретных участках территории. Результаты используются для оптимизации маршрутов патрулирования и распределения сил. В рандомизированном полевом эксперименте, проведённом в Лос-Анджелесе и Кенте, Дж. Молер и соавторы установили, что алгоритм прогнозирования на основе модели эпидемического типа точнее выявлял участки повышенного риска, чем аналитики-криминологи [11]. Метаанализ исследований полицейской деятельности в «горячих точках», выполненный А. Брагой и соавторами, подтверждает, что концентрация профилактических усилий на небольших участках с высокой концентрацией преступности даёт статистически значимое снижение преступности без существенного её смещения на соседние территории [13].

Важно подчеркнуть, что объектом прогноза здесь выступает не личность, а место и время. Такой подход в наименьшей степени затрагивает права конкретных граждан и потому представляется наиболее приемлемым для первоочередного внедрения.

Второе направление – интеллектуальное видеонаблюдение и видеоаналитика. Системы компьютерного зрения позволяют в режиме реального времени выявлять ситуации, требующие реагирования: скопление людей, драки, оставленные предметы, падение человека, дорожно-транспортные происшествия, нарушения правил дорожного движения. Для целей профилактики наиболее ценна именно событийная видеоаналитика, позволяющая предотвратить эскалацию конфликта или оказать своевременную помощь. Использование же технологии распознавания лиц должно быть ограничено законом, так как она связана с обработкой биометрических персональных данных и несёт наибольшие риски для частной жизни.

Третье направление – интеллектуальный анализ обращений граждан и информационных сообщений. Методы обработки естественного языка (NLP) позволяют автоматически классифицировать обращения, поступающие через телефон доверия, электронные приёмные, мобильные приложения, выявлять повторяющиеся сигналы с одного адреса (например, о семейно-бытовых конфликтах), оценивать срочность и направлять обращение уполномоченному субъекту. Это особенно важно для профилактики бытового насилия, где повторяемость обращений является одним из наиболее значимых предикторов тяжких последствий.

Четвёртое направление – раннее выявление факторов социального риска. Интеграция данных социальных реестров, сведений об образовании, занятости, о выявленных фактах безнадзорности несовершеннолетних позволяет формировать для органов самоуправления граждан и профилактических инспекторов «карты социального неблагополучия» территории. Подчеркнём, что речь должна идти не о «прогнозировании преступника», а о выявлении потребности в социальной поддержке – трудоустройстве молодёжи, помощи семьям в трудной жизненной ситуации, организации досуга подростков. Такой подход соответствует сути профилактики как устранения причин правонарушений.

Пятое направление – противодействие киберпреступности и мошенничеству. Модели машинного обучения выявляют аномальные транзакции, фишинговые ресурсы, массовые мошеннические рассылки, что позволяет банкам, операторам связи и правоохранительным органам блокировать противоправные действия до наступления ущерба. С учётом стремительного роста преступлений, совершаемых с использованием информационных технологий, данное направление приобретает особое значение для виктимологической профилактики: своевременное информирование потенциальных жертв о новых мошеннических схемах является эффективной превентивной мерой.

4. Зарубежный опыт и выявленные риски

Изучение зарубежного опыта позволяет выделить как положительные практики, так и важные уроки.

В США в 2010-е годы получили широкое распространение коммерческие системы прогнозирования преступности (PredPol и др.), а также системы оценки индивидуального риска. Однако ряд таких проектов был свёрнут. Так, Департамент полиции Чикаго в конце 2019 года отказался от использования «Списка стратегических субъектов» (Strategic Subject List), ранжировавшего лиц по вероятности их причастности к насилию с применением оружия, после критики со стороны независимых экспертов, указывавших на низкую эффективность и непрозрачность методики. К. Лам и У. Айзек на основе моделирования показали, что обучение прогнозных алгоритмов на данных о задержаниях, отражающих прежнюю интенсивность полицейского контроля, может воспроизводить и усиливать существующие перекосы, формируя замкнутый цикл: больше патрулей – больше выявленных нарушений – ещё больше патрулей [12]. Аналогичные выводы содержатся в фундаментальном исследовании Э. Фергюсона о «полиции больших данных» [14] и в аналитическом докладе корпорации RAND [15].

В Европейском союзе принят Регламент (ЕС) 2024/1689 об искусственном интеллекте [7], который устанавливает риск-ориентированный подход. Пункт «d» части 1 статьи 5 Регламента запрещает использование систем ИИ для оценки риска совершения физическим лицом уголовного правонарушения исключительно на основе профилирования или оценки его личностных черт и характеристик. При этом системы, поддерживающие оценку, проводимую человеком на основе объективных и проверяемых фактов, напрямую связанных с преступной деятельностью, под запрет не подпадают, но относятся к категории высокого риска с соответствующими требованиями к качеству данных, документированию, прозрачности и человеческому надзору.

В Российской Федерации активно развиваются системы «Безопасный город» с элементами видеоаналитики и распознавания лиц. В отечественной и российской научной литературе (В.С. Овчинский [8], Д.В. Бахтеев [9] и др.) обращается внимание как на высокий потенциал таких систем, так и на необходимость правовых гарантий против злоупотреблений.

Обобщение зарубежного опыта позволяет выделить следующие основные риски применения ИИ в профилактике:

– риск алгоритмической дискриминации, когда модель, обученная на смещённых данных, систематически завышает оценку риска для определённых территорий или социальных групп;

– риск непрозрачности («чёрного ящика»), затрудняющей проверку обоснованности выводов и их оспаривание;

– риск «автоматизационной предвзятости» (automation bias), при которой должностное лицо некритически следует рекомендации системы;

– риск чрезмерного вторжения в частную жизнь и «эффекта охлаждения» – самоограничения граждан в реализации прав под влиянием тотального наблюдения;

– риск утечки и неправомерного использования накопленных массивов персональных данных;

– риск стигматизации лиц, отнесённых алгоритмом к «группе риска», что противоречит принципу презумпции невиновности.

5. Трёхуровневая модель ИИ-ассистированной профилактики

С учётом изложенного предлагается модель внедрения ИИ в профилактику правонарушений, состоящая из трёх взаимосвязанных уровней.

Первый уровень – информационный (уровень данных). Он включает интеграцию данных из информационных систем органов внутренних дел, платформы «Безопасный город», электронных обращений граждан, социальных реестров. Обязательными условиями функционирования данного уровня являются: правовое основание обработки каждого вида данных; минимизация данных (использование только сведений, необходимых для конкретной цели); обезличивание данных при решении аналитических задач, не требующих идентификации лица; контроль качества и репрезентативности данных для предотвращения смещений.

Второй уровень – аналитический (уровень моделей). На этом уровне функционируют модели прогнозирования «горячих точек», событийной видеоаналитики, классификации обращений, выявления социальных рисков и мошеннических схем. Каждая модель до ввода в эксплуатацию должна проходить процедуру оценки воздействия на права человека, тестирование на наличие дискриминационных смещений, а также регистрацию в специальном реестре систем ИИ, применяемых в правоохранительной сфере. Предпочтение следует отдавать интерпретируемым моделям, позволяющим объяснить, какие факторы повлияли на результат.

Третий уровень – управленческий (уровень решений). Результаты работы моделей поступают должностным лицам в виде рекомендаций, а не обязательных указаний. Решение о проведении профилактического мероприятия, особенно индивидуального характера, принимается должностным лицом самостоятельно, с указанием оснований и с возможностью его последующего обжалования. Предусматривается обратная связь: результаты профилактических мероприятий используются для оценки эффективности и переобучения моделей.

Сквозным элементом модели выступает независимый контроль: периодический аудит алгоритмов, публичная отчётность об используемых системах и их эффективности, участие представителей гражданского общества и научного сообщества в оценке.

Реализацию модели целесообразно осуществлять поэтапно. На первом этапе (пилотном) предлагается апробировать модели прогнозирования «горячих точек» и классификации обращений граждан в одном-двух районах г. Ташкента, где инфраструктура «Безопасного города» развита в наибольшей степени. На втором этапе, по итогам независимой оценки результатов пилотного проекта, – распространить апробированные решения на областные центры с одновременной доработкой нормативной базы. На третьем этапе – обеспечить интеграцию аналитических модулей в единую информационную систему профилактики правонарушений с доступом для всех

субъектов профилактики в пределах их компетенции.

6. Критерии оценки эффективности применения ИИ в профилактике

Внедрение технологий искусственного интеллекта не является самоцелью; оно оправдано лишь в том случае, если приводит к измеримому улучшению состояния правопорядка без несоразмерного ограничения прав граждан. Поэтому необходимо заранее определить систему критериев, по которым будет оцениваться эффективность внедряемых систем.

Представляется, что такая система должна включать четыре группы показателей.

Первая группа – криминологические показатели: динамика числа зарегистрированных правонарушений на территориях, где применялись модели ИИ, в сравнении с сопоставимыми контрольными территориями; доля правонарушений, совершённых в прогнозированных зонах риска; отсутствие либо наличие смещения преступности на соседние территории; динамика повторных правонарушений, в том числе в сфере семейно-бытовых отношений.

Вторая группа – управленческие показатели: сокращение времени реагирования на сообщения о правонарушениях; доля обращений граждан, правильно классифицированных и направленных уполномоченному субъекту; высвобождение рабочего времени участковых и профилактических инспекторов для непосредственной работы с населением.

Третья группа – правозащитные показатели: число жалоб граждан на действия должностных лиц, связанные с применением систем ИИ; результаты проверок на наличие дискриминационных смещений в работе моделей; число выявленных инцидентов неправомерного доступа к персональным данным.

Четвёртая группа – социальные показатели: уровень доверия населения к органам внутренних дел и чувство безопасности граждан, измеряемые посредством регулярных социологических опросов, в том числе на уровне махалли.

Важно, чтобы оценка проводилась с использованием научно обоснованных методов, позволяющих отделить эффект от применения ИИ от влияния иных факторов, – в идеале посредством рандомизированных или квазиэкспериментальных исследований по аналогии с упомянутыми зарубежными полевыми экспериментами [11; 13]. Только при наличии подтверждённого положительного эффекта по совокупности указанных групп показателей система может быть рекомендована к широкому внедрению.

Обсуждение

Полученные результаты позволяют сформулировать ряд дискуссионных положений.

Во-первых, вопрос о допустимости индивидуального прогнозирования. Ряд исследователей полагает, что прогнозирование вероятности совершения правонарушения конкретным лицом несовместимо с принципами презумпции невиновности и равенства граждан перед законом. Представляется, что в национальной правовой системе следует занять взвешенную позицию, близкую к европейской: запретить оценку риска совершения правонарушения исключительно на основе профилирования и личностных характеристик, допуская использование ИИ лишь в качестве вспомогательного инструмента при наличии объективных, проверяемых фактов, установленных в порядке, предусмотренном законом (например, в отношении лиц, уже состоящих на профилактическом учёте по основаниям, указанным в Законе «О профилактике правонарушений»).

Во-вторых, вопрос об ответственности. Внедрение ИИ не должно приводить к «размыванию» ответственности. Если должностное лицо приняло решение на основании рекомендации системы, ответственность за такое решение несёт именно оно. Одновременно необходимо закрепить ответственность разработчиков и операторов систем за качество моделей и соблюдение установленных требований.

В-третьих, вопрос о кадровом обеспечении. Эффективность ИИ в профилактике определяется не только качеством алгоритмов, но и готовностью сотрудников критически оценивать их выводы. Поэтому в образовательные программы Академии МВД Республики Узбекистан и других профильных вузов целесообразно включить дисциплины по основам анализа данных, цифровой криминологии и этике искусственного интеллекта.

В-четвёртых, вопрос о доверии общества. Профилактика правонарушений, особенно на уровне махалли, основана на взаимодействии с населением. Скрытое использование систем ИИ способно подорвать это доверие. Напротив, открытость в отношении того, какие системы применяются, с какой целью и с какими гарантиями, способствует легитимности профилактической деятельности.

В-пятых, вопрос о межведомственном обмене данными. Эффективность ИИ-ассистированной профилактики во многом определяется полнотой и качеством исходных данных, которые сосредоточены в информационных системах различных ведомств: органов внутренних дел, органов социальной защиты, образования, здравоохранения, занятости, органов самоуправления граждан. В настоящее время обмен такими данными нередко осуществляется на основе разрозненных соглашений, без единых стандартов форматов и требований к защите информации. Представляется необходимым закрепить в законодательстве перечень сведений, которые могут передаваться субъектам профилактики для аналитической обработки, цели их использования, сроки хранения и порядок обезличивания. Это позволит одновременно повысить качество моделей и снизить риски неправомерного использования персональных данных.

В-шестых, вопрос о новых угрозах, порождаемых самим искусственным интеллектом. Генеративные модели уже используются злоумышленниками для создания поддельных аудио- и видеозаписей (дипфейков), автоматизации мошеннических рассылок, подделки документов. Следовательно, профилактика правонарушений должна учитывать двойственную природу ИИ: он выступает одновременно инструментом предупреждения правонарушений и средством их совершения. Введённое Законом № ЗРУ-1115 требование о маркировке контента, созданного с помощью ИИ, и административная ответственность за незаконную обработку персональных данных с его применением [5] являются важными шагами в этом направлении, однако требуют дополнения мерами виктимологической профилактики – прежде всего, повышением цифровой грамотности населения.

На основании проведённого исследования предлагается:

1) дополнить Закон Республики Узбекистан «О профилактике правонарушений» статьёй «Применение информационных технологий и систем искусственного интеллекта в профилактике правонарушений», закрепив в ней: цели и допустимые направления применения ИИ; принцип обязательного участия человека в принятии решений; запрет на применение профилактических мер в отношении лица исключительно на основании выводов систем ИИ; требования к качеству данных и недопущению дискриминации; право гражданина на получение информации о применении в отношении него систем ИИ;

2) поручить МВД совместно с Министерством цифровых технологий и Национальным центром по правам человека разработать Положение о порядке оценки воздействия систем искусственного интеллекта, применяемых в правоохранительной деятельности, на права и свободы человека;

3) создать ведомственный реестр систем ИИ, используемых субъектами профилактики, с публикацией обобщённых сведений о них;

4) на первом этапе внедрять преимущественно «территориальные» и «событийные» модели (прогноз «горячих точек», событийная видеоаналитика, классификация обращений), не связанные с индивидуальным профилированием;

5) обеспечить ежегодный независимый аудит эффективности и справедливости используемых алгоритмов с публикацией его результатов;

6) включить в программы подготовки и повышения квалификации сотрудников органов внутренних дел и профилактических инспекторов курсы по цифровой криминологии и этике ИИ.

Заключение

Проведённое исследование позволяет сделать вывод о том, что технологии искусственного интеллекта обладают значительным потенциалом для повышения эффективности профилактики правонарушений. Они позволяют перейти от реактивной модели, ориентированной на реагирование на уже совершённые правонарушения, к проактивной модели, основанной на своевременном выявлении рисков и адресном устранении их причин.

В Республике Узбекистан созданы важные предпосылки для такого перехода: принята Стратегия развития технологий искусственного интеллекта до 2030 года, законодательно определено понятие искусственного интеллекта и установлен запрет на принятие юридически значимых решений исключительно на основе выводов ИИ, реализуется концепция «Безопасный город», действует система профилактической работы на уровне махалли.

Вместе с тем зарубежный опыт убедительно свидетельствует, что внедрение ИИ без надлежащих правовых гарантий чревато алгоритмической дискриминацией, нарушением права на неприкосновенность частной жизни и утратой доверия населения. Поэтому ключевым условием успешного внедрения является сочетание технологических инноваций с правовыми гарантиями: принципом участия человека в принятии решений, требованиями прозрачности и подотчётности, независимым аудитом алгоритмов.

Предложенная трёхуровневая модель ИИ-ассистированной профилактики и комплекс законодательных предложений направлены на достижение баланса между эффективностью превентивной деятельности и защитой прав и свобод человека. Дальнейшие исследования целесообразно сосредоточить на разработке методик оценки эффективности конкретных моделей ИИ в условиях Узбекистана, а также на криминологическом анализе новых видов правонарушений, совершаемых с использованием самих технологий искусственного интеллекта.

Список использованной литературы

1. Конституция Республики Узбекистан (новая редакция, принята на референдуме 30 апреля 2023 г.) // Национальная база данных законодательства. – URL: https://lex.uz.

2. Закон Республики Узбекистан от 14 мая 2014 г. № ЗРУ-371 «О профилактике правонарушений» // Национальная база данных законодательства. – URL: https://lex.uz/docs/2387359.

3. Указ Президента Республики Узбекистан от 5 октября 2020 г. № УП-6079 «Об утверждении Стратегии “Цифровой Узбекистан – 2030” и мерах по её эффективной реализации» // Национальная база данных законодательства. – URL: https://lex.uz.

4. Постановление Президента Республики Узбекистан от 14 октября 2024 г. № ПП-358 «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года» // Национальная база данных законодательства. – URL: https://lex.uz/docs/7158606.

5. Закон Республики Узбекистан от 21 января 2026 г. № ЗРУ-1115 «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с регулированием отношений, возникающих с применением искусственного интеллекта» // Национальная база данных законодательства. – URL: https://lex.uz.

6. Закон Республики Узбекистан от 2 июля 2019 г. № ЗРУ-547 «О персональных данных» // Национальная база данных законодательства. – URL: https://lex.uz.

7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. – 2024. – L series.

8. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. – М.: Норма, 2018. – 352 с.

9. Бахтеев Д.В. Искусственный интеллект: этико-правовые основы: монография. – М.: Проспект, 2021. – 176 с.

10. Президент ознакомился с деятельностью службы охраны города Ташкента // Портал государственных услуг gov.uz. – 28.01.2026. – URL: https://gov.uz/ru/news/view/125037.

11. Mohler G.O., Short M.B., Malinowski S., Johnson M., Tita G.E., Bertozzi A.L., Brantingham P.J. Randomized controlled field trials of predictive policing // Journal of the American Statistical Association. – 2015. – Vol. 110, No. 512. – P. 1399–1411.

12. Lum K., Isaac W. To predict and serve? // Significance. – 2016. – Vol. 13, No. 5. – P. 14–19.

13. Braga A.A., Turchan B., Papachristos A.V., Hureau D.M. Hot spots policing of small geographic areas effects on crime // Campbell Systematic Reviews. – 2019. – Vol. 15, No. 3. – e1046.

14. Ferguson A.G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. – New York: NYU Press, 2017. – 272 p.

15. Perry W.L., McInnis B., Price C.C., Smith S.C., Hollywood J.S. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. – Santa Monica: RAND Corporation, 2013. – 189 p.