



Организация по безопасности и
сотрудничеству в Европе

ИСПОЛЬЗОВАНИЕ
НОВЫХ
ТЕХНОЛОГИЙ
**ДЛЯ ПОВЫШЕНИЯ
ЭФФЕКТИВНОСТИ
АНАЛИЗА
ПРЕСТУПНОСТИ**

ИТОГОВЫЙ ДОКЛАД ПО РЕЗУЛЬТАТАМ
ЭКСПЕРТНОГО КРУГЛОГО СТОЛА В
СЕКРЕТАРИАТЕ ОБСЕ В ВЕНЕ, АВСТРИИ
(22-23 ОКТЯБРЯ 2024 Г.)

Отказ от ответственности: В настоящем документе обобщены материалы круглого стола, проведенного в соответствии с «правилом Четэм-хауса». Представленные здесь взгляды, мнения и выводы отражают обобщение обсуждений за круглыми столами и не обязательно отражают официальную позицию Организации по безопасности и сотрудничеству в Европе (ОБСЕ) и/или ее государств-участников. Цель настоящего документа — передать суть дискуссии без указания конкретных участников или их принадлежности к тем или иным организациям. ОБСЕ не поддерживает и не проверяет достоверность отдельных утверждений, высказанных в ходе круглого стола. Читателям следует рассматривать данный документ как отражение многообразия точек зрения, озвученных в ходе мероприятия, а не как авторитетное заявление по обсуждавшимся темам.

© ОБСЕ 2025

Все права защищены. Содержимое данной публикации может свободно использоваться и копироваться в образовательных и других некоммерческих целях при условии, что любое такое воспроизведение будет сопровождаться признанием ОБСЕ в качестве источника.

Секретариат ОБСЕ
Департамент по противодействию
транснациональным угрозам
Отдел стратегических вопросов
полицейской деятельности
Валльнерштрассе 6
1010 Вена, Австрия

Эл. почта: SPMU@osce.org
www.osce.org/policing

Введение

Новые и развивающиеся технологии преобразовали практически все сферы человеческой жизни. От анализа больших данных и алгоритмов машинного обучения, через «интернет вещей», «умные» датчики и автономные беспилотные аппараты — вплоть до искусственного интеллекта (ИИ): нынешние темпы технологических инноваций беспрецедентны. На фоне такого развития событий начались дискуссии относительно преимуществ и рисков, связанных с применением новых технологий в различных профессиональных областях.

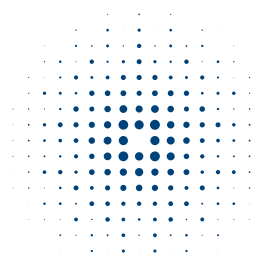
В контексте борьбы с преступностью и полицейской деятельности значительная часть дискуссий сосредоточена на опасениях, связанных с угрозами, которые могут исходить от подобных технологий — в особенности с возможностью их неправомерного использования в преступных целях. Тем не менее, потенциал этих технологий произвести революцию в работе правоохранительных органов, повысив как их результативность, так и эффективность, имеет не меньшее значение.

Существуют широкие и разнообразные возможности для интеграции новых и перспективных технологий в деятельность правоохранительных структур. Например, они могут способствовать анализу тенденций и закономерностей, мониторингу угроз и рисков безопасности, содействовать выявлению подозреваемых и раскрытию преступлений, а также

оптимизировать различные административные процессы и процедуры. В то же время обеспечение баланса между использованием технологических достижений и защитой прав и основных свобод человека представляет собой важную задачу, порождающую вопросы этического, правового и практического характера.

В этой связи, Отделом стратегических вопросов полицейской деятельности Департамента по противодействию транснациональным угрозам при Секретариате ОБСЕ была организована серия экспертных круглых столов по вопросам применения правоохранительными органами новых и перспективных технологий. Цель данных дискуссий заключается в том, чтобы выявить возможности использования правоохранительными органами новых и перспективных технологий для поддержки своей деятельности, способствовать выработке рекомендаций по вопросам политики, а также изучить потенциальные направления поддержки со стороны ОБСЕ в области наращивания потенциала в данной области.

В настоящем материале обобщены ключевые тезисы и результаты первого круглого стола, посвященного теме использования новых технологий для совершенствования анализа преступности и состоявшегося в Вене, Австрии, 22–23 октября 2024 года.



Анализ преступности в цифровую эпоху

Способность анализировать криминальные тенденции и закономерности приобретает все большее значение, поскольку современные правоохранительные органы стремятся решать все более сложные задачи в сфере безопасности в условиях ограниченных ресурсов. Анализ преступности способен внести существенный вклад в доказательное и упреждающее оперативное и стратегическое планирование, помогая повысить эффективность, результативность и оперативность полицейской деятельности.

Стремительное развитие цифровых технологий трансформировало сферу анализа преступности и открыло перед ней новые возможности. С одной стороны, цифровизация государственного сектора позволила правоохранительным органам получить более простой доступ к существующим массивам данных и информации, содержащимся в различных государственных системах и базах данных. Это значительно упростило и ускорило как доступ к таким данным и информации, так и их обработку. С другой стороны, цифровые технологии также постоянно генерируют новые данные о самых разнообразных видах человеческой деятельности. Постоянно растущий объем и разнообразие данных открывают новые перспективы для дальнейшего совершенствования анализа преступности, делая его более надежным, адресным и действенным.

Существует широкий консенсус в отношении того, что качественная аналитика данных способна

способствовать повышению эффективности работы полиции.

Таким образом, способность анализировать огромные объемы данных (так называемые «большие данные») в целях поддержки тактического, оперативного или стратегического планирования и принятия решений стала неотъемлемой частью современного анализа преступности. В то же время сбор, управление и анализ таких «больших данных» создают ряд практических сложностей для правоохранительных органов, а также поднимают важные вопросы, касающиеся защиты прав человека и основных свобод.

Эффективное применение искусственного интеллекта

Машинное обучение (МО) и искусственный интеллект (ИИ)¹ играют ключевую роль, помогая правоохранительным органам реализовать потенциал «больших данных» для существенного повышения качества анализа преступности.

[1] МО представляет собой подраздел ИИ, позволяющий компьютерам обучаться и совершенствоваться на основе данных без необходимости явного программирования. Оно дает машинам возможность автоматически учиться на прошлом опыте, выявлять закономерности и делать прогнозы при минимальном участии человека. ИИ — это более широкая технологическая область, ориентированная на создание компьютерных систем, способных имитировать когнитивные функции человека, такие как обучение, рассуждение и решение задач. Для простоты изложения в настоящем итоговом докладе мы будем использовать более широкий и обобщающий термин «ИИ».

Различные прикладные решения — особенно в области науки о данных — уже продемонстрировали потенциальную пользу этих технологий в контексте правоохранительной деятельности. К числу важных направлений, где ИИ уже доказывает свою высокую эффективность, относятся:

Автоматизация ручных задач: ИИ способен автоматизировать множество ручных задач или процессов, входящих в аналитическую работу, таких как расшифровка многочасовых аудиозаписей или извлечение конкретных ключевых слов и сведений из объемных текстов. Это высвобождает время аналитиков, позволяя им сосредоточиться на выполнении наиболее важных задач, включая запросы данных для более глубокого изучения темы, формирование взглядов, выявление закономерностей и тенденций. Тем не менее, проверка результатов автоматизированной работы по-прежнему требует вмешательства человека, поскольку ошибки возможны — и неизбежно будут возникать.

Управление данными: ИИ может оказывать содействие в управлении «большими данными», включая категоризацию и маркировку неструктурированных или слабоструктурированных данных, а также очистку массивов данных. Это позволяет аналитикам исследовать данные, использование которых иным способом было бы затруднительным или вовсе невозможным — например, данные, хранящиеся в устаревших (унаследованных) базах данных.

Анализ данных: ИИ способен анализировать данные гораздо быстрее и в значительно более

крупных масштабах, чем аналитики. В условиях постоянно растущего объема данных, использование ИИ для анализа крупных массивов информации станет насущной необходимостью. Это может повысить релевантность и качество аналитических продуктов.

Выявление закономерностей и тенденций: ИИ может стать чрезвычайно мощным инструментом для выявления конкретных закономерностей или тенденций в данных — особенно при условии предоставления четко сформулированных и точно определенных критериев поиска. В то же время ИИ способен помогать в обнаружении новых корреляций в крупных наборах данных — таких, которые аналитики могли бы упустить из виду. И хотя наличие корреляции не означает автоматически наличие причинно-следственной связи и требует дополнительной проверки, подобные находки могут открывать новые направления для дальнейших исследований, а также способствовать формированию новых выводов и углублению понимания изучаемых вопросов.

Распознавание изображений и голоса: ИИ может способствовать оперативному выявлению лиц или объектов в огромных массивах аудиовизуальных данных, оказывая помощь в отслеживании подозреваемых, поиске пропавших без вести или анализе обстановки на месте преступления. Кроме того, ИИ может использоваться для классификации изображений, исходя из их основного содержания или присутствующих на них объектов. Например, ИИ уже применяется для анализа спутниковых

снимков с целью отслеживания посевов культур, используемых для производства наркотических средств.

Выявление угроз и раннее

предупреждение: ИИ может использоваться для обнаружения различных видов противоправного онлайн-контента, а также дезинформации и «дипфейков». Его также можно использовать для выявления признаков новых криминальных тенденций (например, новых сленговых названий наркотиков, набирающих популярность в интернете) и для обеспечения ранних предупреждений. Аналитики уже применяют генеративный ИИ для разработки сценариев и гипотез в рамках текущих уголовных расследований. Полезность ИИ для этих и других целей будет лишь возрастать по мере развития соответствующих технологий.

Прогностическая полицейская

деятельность: ИИ способен обрабатывать огромные объемы как структурированных, так и неструктурированных данных, обеспечивая тем самым более глубокий и всесторонний анализ, необходимый для совершенствования прогностических моделей, предсказывающих места концентрации преступлений и криминальные тенденции. Поскольку прогностическая полицейская деятельность базируется на применении сложных статистических методов для извлечения новых знаний из различных видов исторических данных, технологии МО и ИИ способны сделать такой анализ более надежным и достоверным. В настоящее время исследователи изучают возможность

использования технологий ИИ для устранения потенциальных скрытых смещений в данных, используемых для прогнозирования, а также для минимизации риска получения дискриминационных результатов.

Административные задачи:

ИИ может оказывать содействие в выполнении множества административных задач. Например, инструменты обработки естественного языка позволяют расшифровывать аудиозаписи интервью, резюмировать объемные документы, переводить тексты с иностранных языков или составлять отчеты. Они также могут помогать в управлении графиками работы и распределении ресурсов, а также в контроле за соблюдением процессуальных требований. Снижая административную нагрузку, эти инструменты не только экономят время, но и способны повысить точность и последовательность при выполнении рутинных задач, тем самым способствуя повышению общей операционной эффективности.

Обучение, подготовка и

тестирование: генеративный ИИ может использоваться для создания совершенно нового контента, включая текст, изображения, видео или аудио. Подобные «синтетические данные» могут быть полезны для обучения и подготовки новых аналитиков. Кроме того, их можно использовать в качестве входных данных для обучения новых моделей ИИ, а также для тестирования и проверки функциональности существующих систем или инструментов.

Эти примеры демонстрируют широкий спектр потенциальных областей

применения и сценариев использования данной технологии в контексте анализа преступности. Однако полезность и эффективность инструментов ИИ в значительной степени зависят от качества исходных данных и надежности используемых алгоритмов. Иными словами, низкое качество данных неизбежно приведет к низкому качеству результатов (согласно принципу «мусор на входе — мусор на выходе»). Эффективное применение инструментов ИИ также во многом зависит от способности пользователей понимать логику обработки информации искусственным интеллектом, что необходимо для обеспечения прозрачности получаемых результатов.

Есть также значительная разница между использованием возможностей уже существующих больших языковых моделей, обученных на общих данных из интернета, и обучением совершенно новой модели на более уникальных и специализированных наборах данных. Уже сейчас существует возможность задействовать локальных ИИ-агентов, обученных исключительно на локальных или внутренних данных; это позволяет сделать результаты их работы гораздо более точными и адаптированными к конкретным потребностям или требованиям.

Проблемы при внедрении искусственного интеллекта

Использование ИИ для повышения эффективности анализа преступности также ставит перед правоохранительными органами ряд специфических вызовов.

Выделение достаточных технических ресурсов

Во-первых, для обучения и развертывания систем ИИ требуются соответствующие технические ресурсы. Обучение сложных моделей ИИ на внутренних или локальных данных требует значительных вычислительных мощностей и объемов хранения, особенно в тех случаях, когда из соображений конфиденциальности и безопасности приходится ограничиваться решениями, развернутыми на собственной инфраструктуре. Многие правоохранительные органы не располагают необходимой высокопроизводительной вычислительной инфраструктурой для разработки подобных инструментов.

Эту проблему можно решить за счет использования облачных решений, которые позволяют правоохранительным органам получать доступ к высокопроизводительным ресурсам без необходимости создавать и поддерживать собственную инфраструктуру. Кроме того, облачные платформы предоставляют передовые инструменты и сервисы на базе ИИ, обеспечивая ускоренное обучение моделей, обработку данных в режиме реального времени и эффективное управление хранением информации. Фактически, для того чтобы в полной мере раскрыть потенциал ИИ, использование облачных систем является необходимым условием.

Однако, облачные решения сопряжены и с определенными трудностями — в частности, в вопросах

конфиденциальности и суверенитета данных.² Поскольку данные, находящиеся в распоряжении правоохранительных органов, зачастую содержат конфиденциальную персональную или засекреченную информацию, возникают серьезные опасения по поводу хранения таких данных в облаке. И хотя существуют технические решения, позволяющие минимизировать потенциальные риски безопасности (например, шифрование и различные механизмы контроля доступа), они могут не решать в полной мере вопросы, касающиеся защиты конфиденциальности данных.

Государства применяют различные подходы к решению этих проблем. В некоторых юрисдикциях действуют нормативные акты, ограничивающие трансграничную передачу определенных категорий данных, что усложняет использование глобальных облачных платформ. Другие страны пришли к выводу, что преимущества, предлагаемые глобальными облачными платформами, перевешивают риски, связанные с вопросами конфиденциальности и суверенитета.

Некоторые страны могут принять решение о создании собственной национальной облачной инфраструктуры, предназначенной специально для работы с конфиденциальными данными государственного сектора (например, в сферах правоохранительной

деятельности, обороны или здравоохранения). Еще одним возможным путем развития может стать использование гибридных решений, при которых конфиденциальные данные хранятся локально, а облачные ресурсы задействуются для выполнения менее критичных задач; либо же партнерство с надежными поставщиками облачных услуг с целью создания безопасных систем, соответствующих всем требованиям.

Доступность и качество данных

Вторая серьезная проблема связана с доступностью и качеством данных, используемых для обучения моделей ИИ. Анализ преступности часто опирается на данные из широкого спектра государственных баз данных; некоторые из них представляют собой устаревшие унаследованные системы, созданные без соблюдения каких-либо единых стандартов управления данными. Такие наборы данных могут содержать неполную, противоречивую или устаревшую информацию, а также различные внутренние искажения (предвзятости), что в совокупности может негативно сказаться на точности и надежности моделей ИИ. Кроме того, правоохранительные органы зачастую используют разрозненные базы данных и системы, что затрудняет интеграцию и стандартизацию данных, необходимых для их эффективной обработки средствами ИИ.

Обеспечение операционной совместимости различных баз данных на национальном уровне на протяжении многих лет — задолго до появления ИИ — оставалось одной из главных проблем в сфере

[2] К числу других проблем, связанных с использованием облачных решений, могут относиться риски безопасности, «привязка к поставщику» (зависимость от одного поставщика), долгосрочные финансовые затраты, необходимость соблюдения правовых и этических норм, а также обеспечение совместимости с унаследованными системами.

эффективного анализа преступности. В прошлом объединение старых и новых систем оказывалось чрезвычайно сложной задачей; в современной практике, как правило, эти системы сохраняют разделенными, добавляя лишь специальный абстракционный уровень, позволяющий использовать данные как из новых, так и из старых систем. В этом контексте ИИ открывает новые возможности, поскольку он особенно хорошо приспособлен для работы как со структурированными, так и с неструктурированными данными из различных источников. Однако это потребует переноса различных наборов данных в облако, что, как упоминалось выше, сопряжено со своими сложностями и вызывает определенные опасения.

Дополнительной сложностью при рассмотрении возможностей использования потенциала ИИ для анализа преступности на региональном или международном (глобальном) уровне становится обеспечение функциональной совместимости между национальными и международными базами данных. В данном случае технические трудности, связанные с объединением данных из различных предметных областей и измерений, усугубляются проблемами политического и правового характера, касающимися вопросов государственного суверенитета и различий в национальных законодательных базах. Тем не менее, вполне можно представить ситуацию, при которой в определенных сферах борьбы с преступностью, представляющих взаимный интерес, правительства ряда стран могли бы договориться об обмене конкретными наборами данных в аналитических целях.

Образование и профессиональная подготовка

Еще одна задача связана с образованием и профессиональной подготовкой сотрудников правоохранительных органов, которым необходимо будет освоить навыки и компетенции, требуемые для эффективного использования возможностей, предоставляемых ИИ, при сохранении при этом содержательного человеческого контроля над результатами его работы.

Для обучения и внедрения систем ИИ потребуются технический персонал, обладающий надлежащей квалификацией; это обуславливает необходимость для правоохранительных органов либо нанимать новых сотрудников, либо повышать квалификацию уже имеющегося штата.

Интеграция ИИ в аналитическую работу повлечет за собой повышение требований к подготовке аналитиков — особенно в таких областях, как наука о данных, принципы функционирования и ограничения алгоритмов ИИ, статистика и прогностическое моделирование, а также вопросы соблюдения прав человека и верховенства закона. Специалисты, использующие инструменты ИИ для анализа преступности, должны обладать фундаментальным пониманием принципов работы ИИ, его ограничений, а также уметь распознавать ошибки в выходных данных — в том числе те, которые

обусловлены «галлюцинациями»³ и предвзятостью алгоритмов. Кроме того, могут возникнуть новые должности и профессиональные профили по мере того, как вспомогательному персоналу полиции будет поручаться выполнение все более технических и специализированных функций. Аналитикам потребуется тесно взаимодействовать с этими новыми категориями сотрудников, включая специалистов по науке о данных, ИТ-специалистов и других сотрудников правоохранительных органов. В целом, роль аналитика преступности, вероятно, станет более междисциплинарной, сочетая традиционные экспертные знания в области криминологии с навыками в сфере науки о данных и ИТ.

Наконец, важнейшее значение будет иметь также профессиональное развитие других участников правоохранительного сообщества, включая руководителей высшего звена. Работа с большими данными и инструментами ИИ должна быть интегрирована в стандартные программы профессиональной подготовки и обучения сотрудников полиции — точно так же, как обучение обращению с оружием или навыкам вождения. Особую важность при этом будут приобретать критическое мышление, осведомленность в вопросах прав человека, а также

[3] «Галлюцинации» ИИ — это феномен, при котором большая языковая модель (LLM) — зачастую в лице чат-бота на базе генеративного ИИ или инструмента компьютерного зрения — распознает несуществующие или неразличимые для человеческого глаза закономерности либо объекты, в результате чего формируются выходные данные, лишенные смысла или полностью недостоверные.

базовое понимание принципов работы моделей ИИ и их ограничений. Многие из упомянутых выше проблем можно решить посредством эффективного управления изменениями, учитывающего как технические, так и кадровые требования, которые неизбежно повлечет за собой подобный сдвиг в возможностях и потенциале правоохранительных органов. Это, в частности, предполагает адаптацию программ профессионального развития к динамичному характеру технологий ИИ, а также обеспечение непрерывного обучения, позволяющего идти в ногу с технологическим прогрессом.

Влияние на права человека

Использование ИИ правоохранительными органами для анализа преступности открывает как новые возможности, так и создает определенные вызовы в контексте обеспечения полицейской деятельности в строгом соответствии с правами человека. При условии продуманного внедрения, ИИ способен повысить эффективность работы правоохранительных органов, одновременно обеспечивая уважение прав личности — а в некоторых случаях даже способствуя их укреплению. Однако без тщательного планирования, а также надлежащих механизмов управления и защитных мер его использование может усугубить существующее неравенство и посягнуть на основные свободы, создавая тем самым значительные практические и правовые проблемы.

Укрепление прав человека посредством использования ИИ

При рассмотрении потенциального позитивного влияния ИИ можно выделить четыре ключевые области. Во-первых, грамотно спроектированные системы ИИ, обученные на высококачественных данных, способны помочь в нейтрализации человеческих предубеждений в процессе анализа и принятия решений, опираясь при этом на выводы, полученные на основе объективных данных. Эмпирические исследования продемонстрировали негативное влияние человеческих когнитивных искажений на нашу способность воспринимать окружающий мир и принимать решения — особенно в сложных ситуациях. Сотрудники правоохранительных органов, в том числе аналитики преступности, не застрахованы от подобных искажений — особенно когда перед ними стоит задача по обработке и интерпретации колоссальных объемов данных и информации. Использование ИИ в анализе преступности открывает перспективы для снижения негативного воздействия человеческих когнитивных искажений на процессы аналитической работы и принятия решений. Более того, в тех случаях, когда выявляются определенные недостатки или вводятся новые правила и нормативы, обновить или усовершенствовать алгоритмы для обеспечения их полного соответствия новым требованиям зачастую гораздо проще, чем проводить переподготовку аналитиков.

Во-вторых, автоматизированные процессы способны повысить уровень прозрачности, подотчетности и

справедливости — при условии, что используемые алгоритмы являются интерпретируемыми, надлежащим образом документированными и поддающимися аудиту. Они могут способствовать укреплению принципов надлежащей правовой процедуры и соблюдения процессуальных норм за счет сокращения случаев произвольного или несоразмерного вмешательства, повышения обоснованности принимаемых решений (на основе фактических данных), минимизации процессуальных задержек, а также выявления закономерностей, свидетельствующих о наличии системной дискриминации или недостатков.

Кроме того, надлежащим образом спроектированные системы ИИ, оснащенные адекватными механизмами защиты, способны обеспечить более надежную реализацию права на неприкосновенность частной жизни. Например, они могут повысить уровень защиты данных, ограничивая доступ людей к конфиденциальной информации посредством автоматизированной обработки данных и ведения журналов доступа. Также они позволяют осуществлять гораздо более адресный и соразмерный поиск конфиденциальной персональной информации, гарантируя, что доступ предоставляется лишь к тем данным, которые имеют непосредственное отношение к конкретным задачам полицейской деятельности.

Наконец, аналитики преступности могут использовать ИИ для выявления и анализа недостоверной информации и «дипфейков»; это может помочь правоохранительным органам

разрабатывать более эффективные меры реагирования и формировать контрнарративы. Подобная практика может внести позитивный вклад в обеспечение свободы слова, способствуя формированию более информированной и заслуживающей доверия коммуникационной среды, а также выявляя и нейтрализуя распространение ложного или сфальсифицированного контента. В результате, использование ИИ в анализе преступности может способствовать сохранению целостности общественных дискуссий, защите граждан от обмана и снижению пагубного воздействия кампаний по распространению недостоверной информации.

Риски для прав человека, связанные с применением ИИ

В то же время использование ИИ для анализа преступности, безусловно, таит в себе и потенциальную угрозу для прав человека. Действительно, именно те сферы, которые должны получить пользу от внедрения систем ИИ, одновременно могут столкнуться и со значительными рисками, порождаемыми этими технологиями. Например, если должным образом спроектированные системы ИИ, обученные на высококачественных данных, способны помочь в смягчении некоторых предвзятостей, то модели, обученные на данных низкого качества — таких как предвзятые исторические данные, — могут закреплять или даже усиливать существующие предвзятости, что приводит к дискриминационным результатам. Профилирование и прогностическая полицейская деятельность, основанные на результатах анализа таких предвзятых данных, могут непропорционально

затрагивать определенные сообщества — например, приводя к их стигматизации или чрезмерному полицейскому контролю.

Сложные или непрозрачные системы ИИ также могут препятствовать обеспечению прозрачности и подотчетности, затрудняя отслеживание, понимание или оспаривание решений, принятых под влиянием этих технологий. Опора на ошибочные результаты работы таких систем может привести к неправомерным арестам, задержаниям или иным нарушениям прав на надлежащую правовую процедуру. Чрезмерно сложные или непрозрачные системы также создают дополнительные возможности для злоупотреблений.

Кроме того, внедрение систем ИИ без надлежащих защитных механизмов может привести к ущемлению прав на неприкосновенность частной жизни и защиту персональных данных. Например, инструменты наблюдения на базе ИИ — такие как системы распознавания лиц или голоса — могут легко нарушать право граждан на частную жизнь в отсутствие четких защитных механизмов. Аналогичным образом, если сбор больших объемов данных для обучения моделей ИИ осуществляется без надлежащего согласия или контроля, это может привести к навязчивому мониторингу, ставящему под угрозу неприкосновенность частной жизни как в общественных, так и в частных пространствах.

Наконец, использование систем ИИ для выявления и мониторинга недостоверной информации или «дипфейков» может легко стать инструментом злоупотреблений, если их внедрение не будет сопровождаться соответствующими защитными мерами и механизмами контроля. Например, применение таких инструментов для мониторинга конкретной группы лиц — скажем, политических оппонентов или представителей меньшинств — может нарушить права на свободу мысли, слова и собраний, а также принцип недискриминации. Кроме того, эти инструменты могут быть легко использованы не по назначению — например, для осуществления цензуры или надзора за законной деятельностью граждан.

В конечном счете, то, будет ли ИИ укреплять или подрывать права человека, зависит от того, как эти технологии будут внедряться и использоваться правоохранительными органами. В этом отношении ключевыми являются тщательное планирование, надлежащее управление и адекватные гарантии, а также необходимое понимание и экспертные знания в правоохранительных органах. Контроль за тем, чтобы использование ИИ не нарушало права человека, имеет важное значение не только для соблюдения международного и национального права, но и для поддержания общественного доверия, критически важного для эффективной работы полиции. Чрезмерная зависимость от инструментов ИИ без четкой коммуникации или надзора может подорвать доверие общественности к правоохранительным органам, особенно в сообществах, уже

скептически настроенных по отношению к полиции.

Выводы и программные рекомендации

Стремительное развитие новых и перспективных технологий — в частности, ИИ — открывает широкие возможности для использования потенциала «больших данных» и позволяет существенно повысить актуальность и результативность анализа преступности. В то же время, внедрение подобных технологий сопряжено с рядом специфических вызовов, в том числе в сфере прав человека и основных свобод. Многие из этих вызовов можно преодолеть посредством эффективного управления изменениями, с учетом как технических, так и кадровых требований, которые неизбежно повлечет за собой подобная трансформация возможностей и потенциала правоохранительных органов. В данном контексте для государств-участников ОБСЕ целесообразно рассмотреть следующие программные рекомендации.

Внедрение ИИ для анализа преступности

- Содействовать налаживанию регулярного междисциплинарного диалога и сотрудничества между аналитиками преступности, специалистами по обработке данных, экспертами в области права и ИТ-специалистами, с тем чтобы сформировать более глубокое понимание потенциальных преимуществ и вызовов, связанных

с использованием ИИ в процессе анализа преступности.

- Разработать национальные нормативно-правовые основы, регулирующие создание и применение систем ИИ в правоохранительной деятельности, обеспечив их соответствие национальному законодательству, международным соглашениям и применимым международным стандартам в области прав человека.
- Обеспечить сохранение значимого участия человека в процессе принятия решений с использованием ИИ, гарантируя, что никакие критически важные действия не будут предприниматься исключительно на основе рекомендаций ИИ. Создать каналы для информирования общественности о применении ИИ в правоохранительной сфере, включая предоставление четких разъяснений относительно целей использования таких систем, их преимуществ, а также мер защиты от злоупотреблений.

Подготовка и образование

- Ввести обязательное обучение для всего личного состава правоохранительных органов — в том числе для руководящего звена — по вопросам, касающимся принципов работы, сфер применения и ограничений технологий ИИ.
- Разработать специализированную учебную программу по вопросам ИИ для аналитиков преступности, охватывающую такие темы, как основы науки о данных,

функционирование и ограниченности алгоритмов ИИ, статистика и прогностическое моделирование, а также применение национальных и международных правовых норм и стандартов в области прав человека.

- Включить развитие навыков критического мышления во все образовательные программы для сотрудников правоохранительных органов — от курсантов полицейских учебных заведений до высшего руководящего состава.

Государственно-частное партнерство

- Наладить партнерские отношения между правоохранительными органами и технологическими компаниями, являющимися лидерами в области инноваций в области ИИ, с целью совместной разработки решений, адаптированных к конкретным потребностям полицейской деятельности.
- Содействовать разработке систем ИИ на основе принципов прав человека, требуя от субъектов частного сектора соблюдения соответствующих правовых стандартов при создании инструментов для правоохранительных органов, а также поощряя внедрение добровольных механизмов защиты прав человека в процессе разработки и применения ИИ для анализа преступлений.
- Установить партнерские отношения с надежными поставщиками облачных услуг для разработки

специализированных облачных решений, адаптированных к потребностям правоохранительных органов.

- Содействовать осуществлению совместных инвестиций в инфраструктуру ИИ, научные исследования и профессиональную подготовку с целью снижения затрат и наращивания потенциала для внедрения передовых технологий.

Подотчетность и прозрачность

- Поддерживать разработку моделей «объяснимого ИИ», которые поддаются интерпретации и оснащены четкими механизмами аудита и обеспечения подотчетности.
- Ввести обязательное требование о проведении регулярных оценок рисков и аудитов систем ИИ для подтверждения их функционирования по назначению, и выявления и устранения любых непредусмотренных последствий.
- Сделать обязательным документирование алгоритмов, обеспечивая интерпретируемость и доступность информации об их функциях и процессах принятия решений для соответствующих заинтересованных сторон, включая надзорные органы.
- Рассмотреть возможность создания специального независимого надзорного органа, конкретной задачей которого станет мониторинг внедрения и использования технологий ИИ в государственном секторе (в том числе в правоохранительных органах).

- Обеспечить доступные механизмы, позволяющие гражданам оспаривать решения, принятые системами ИИ или сформированные под их влиянием, гарантируя тем самым справедливость и подотчетность.

Соблюдение прав человека

- Ввести обязательное требование об использовании высококачественных наборов данных для обучения моделей ИИ, а также о регулярной оценке потенциальных предвзятостей в обучающих данных с целью минимизации риска закрепления дискриминационных результатов.
- Обеспечить, чтобы все системы ИИ, используемые правоохранительными органами, проходили оценку воздействия на права человека перед вводом в эксплуатацию, а впоследствии подвергались периодическому аудиту на предмет наличия предвзятостей.
- Приоритизировать защиту конфиденциальности путем внедрения надежных мер по защите данных, включая шифрование, контроль доступа и методы анонимизации.
- Разработать четкие руководящие принципы и операционные процедуры, гарантирующие, что использование систем ИИ будет соразмерно поставленным целям и не повлечет за собой неоправданного нарушения права на неприкосновенность частной жизни или иных фундаментальных прав.

Дополнительные материалы

Council of Europe (2024): *HUDERIA - Risk and Impact Assessment of AI Systems*, <https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>

Daniel Bing Andersen, Nina Sunde, Kyle Porter (2025): *Tool induced biases? Misleading data presentation as a biasing source in digital forensic analysis*, Forensic Science International: Digital Investigation, <https://doi.org/10.1016/j.fsidi.2025.301881>

Europol (2024): *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*, <https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf>

INTERPOL and UNICRI (2024): *Toolkit for Responsible AI Innovation in Law Enforcement*, <https://unicri.it/Publication/Toolkit-for-Responsible-AI-Innovation-in-Law-Enforcement-UNICRI-INTERPOL>

Accountability Principles for Artificial Intelligence, <https://ap4ai.eu/>



Организация по безопасности и сотрудничеству в Европе