АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ
РЕСПУБЛИКИ КАЗАХСТАН

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРОКУРАТУРЫ: ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ПРАКТИКА ПРИМЕНЕНИЯ В ГОСУДАРСТВАХ-УЧАСТНИКАХ СНГ

АСТАНА, 2025

Академия правоохранительных органов
при Генеральной прокуратуре Республики Казахстан

Межведомственный научно-исследовательский институт

Технологии искусственного интеллекта в деятельности органов прокуратуры: правовое регулирование и практика применения в государствах-участниках СНГ

Монография

Астана, 2025

УДК 004.08
ББК 32.813
Т 38

Рецензенты:

Бессонов Алексей Александрович – ректор ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева», доктор юридических наук, доцент;

Сейтенов Калиолла Кабаевич – первый проректор Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, доктор юридических наук, профессор, почетный академик Национальной академии наук Республики Казахстан.

Технологии искусственного интеллекта в деятельности органов прокуратуры: правовое регулирование и практика применения в государствах-участниках СНГ / Коллектив авторов. – Астана: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2025. – с.171.

В монографии представлен обзор текущего состояния и развития информационно-аналитических систем, а также технологий искусственного интеллекта в деятельности органов прокуратуры отдельных государств-участников СНГ, подготовленный на основе материалов, представленных членами авторского коллектива.

Проанализированы нормы международного и национального законодательства, регламентирующего вопросы правового регулирования технологий искусственного интеллекта. Исследованы научно-теоретические и прикладные аспекты развития информационных технологий, а также перспективы внедрения искусственного интеллекта в деятельность органов прокуратуры.

Монография может быть полезна для практических работников органов прокуратуры государств-участников СНГ и их образовательных учреждений.

Рекомендовано к публикации Учебно-методическим советом
Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан.

ISBN 978-601-82311-6-2

УДК 004.08
ББК 32.813

БЛАГОДАРНОСТЬ

Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан выражает благодарность Секретариату Координационного совета генеральных прокуроров государств-участников СНГ, членам авторского коллектива Научно-практического центра укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь, Генеральной прокуратуре Кыргызской Республики, Университету прокуратуры Российской Федерации, Генеральной прокуратуре и Правоохранительной академии Республики Узбекистан за содействие в проведении исследования, предоставление эмпирических и практических материалов.

ОГЛАВЛЕНИЕ

Обозначения и сокращения 6

Глоссарий 7

Введение 9

ГЛАВА 1. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМУ ПРОКУРОРСКОГО НАДЗОРА 13

§ 1.1 Понятие и правовая природа технологий искусственного интеллекта в контексте прокурорского надзора 13

§ 1.2 Функциональный анализ возможностей искусственного интеллекта в контексте задач и полномочий органов прокуратуры 25

§ 1.3 Международные стандарты, принципы и ограничения применения искусственного интеллекта в правоохранительной деятельности 42

Выводы главы 1 56

ГЛАВА 2. СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОКУРОРСКОЙ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВ СНГ 58

§ 2.1 Анализ действующего законодательства и правоприменительной практики в сфере искусственного интеллекта 58

§ 2.2 Сравнительное исследование институциональных моделей внедрения искусственного интеллекта в прокуратурах СНГ 66

§ 2.3 Выявление проблем правового регулирования и практические вызовы цифровизации 89

Выводы главы 2 95

ГЛАВА 3. ПРАВОВЫЕ ГАРАНТИИ И МЕХАНИЗМЫ КОНТРОЛЯ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОКУРОРСКОЙ ДЕЯТЕЛЬНОСТИ И ПЕРСПЕКТИВЫ 98

§ 3.1 Защита персональных данных и обеспечение конфиденциальности при работе с системами искусственного интеллекта 98

§ 3.2 Участие прокурора в электронном судопроизводстве: применение технологий искусственного интеллекта 123

§ 3.3 Стратегические направления перспективного развития применения искусственного интеллекта в органах прокуратуры государств СНГ 141

Выводы главы 3 155

Заключение 158

Приложение 166

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС	Автоматизированная информационная система
АЦ	Аналитический центр
ГУ	Государственное учреждение
ЕРАП	Единый реестр административных правонарушений
ЕРДР	Единый реестр досудебных расследований
ЕРП	Единый реестр правонарушений
ЕРСОП	Единый реестр субъектов и объектов проверок
ЕС	Европейский Союз
ИИ	Искусственный интеллект
ИКТ	Информационно-коммуникационные технологии
ИС	Информационная система
КСГП	Координационный совет генеральных прокуроров государств-участников СНГ
КСОНР	Координационный совет руководителей органов налоговых (финансовых) расследований государств-участников СНГ
МЦРИАП	Министерство цифрового развития и аэрокосмической промышленности Республики Казахстан
НРПА	Национальный реестр правовых актов
ОДКБ	Организация Договора о коллективной безопасности
ООН	Организация Объединенных Наций
СЕ	Совет Европы
СНГ	Содружество Независимых Государств
УК	Уголовный кодекс
УПК	Уголовно-процессуальный кодекс
ШОС	Шанхайская организация сотрудничества

ГЛОССАРИЙ

Искусственный интеллект (Artificial intelligence, AI) – комплекс технологических решений, имитирующий когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и позволяющий при выполнении задач достигать результаты, как минимум сопоставимые с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает информационно-коммуникационную инфраструктуру, программное обеспечение, в котором в том числе используются методы машинного обучения, процессы и сервисы по обработке данных и выработке решений.

Генеративный ИИ (Generative AI) – система искусственного интеллекта, который изучает представление артефактов из данных и использует его для создания совершенно новых, полностью оригинальных артефактов, сохраняющих сходство с исходными данными.

Информация (Information) – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная система (Information system) – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач.

Информационные технологии (Information technologies) совокупность средств и методов сбора, обработки и передачи первичной информации (информационных ресурсов) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта) на основе применения средств вычислительной техники.

Информационная безопасность (Information security) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Нейротехнологии (Neural technologies) – технологии, которые используют или помогают понять работу мозга, мыслительные процессы, высшую нервную деятельность, в том числе технологии по усилению, улучшению работы мозга и психической деятельности.

Нейросети (**Neural networks)** – сеть примитивных обрабатывающих элементов, соединенных взвешенными связями с регулируемыми весами, в которой каждый элемент выдает значение, применяя нелинейную функцию к своим входным значениям, и передает его другим элементам или представляет его в качестве выходного значения.

Интернет (The Internet) – всемирная система объединенных сетей телекоммуникаций и вычислительных ресурсов для передачи электронных информационных ресурсов.

Интеллектуальный робот (Intellectual robot) – автоматизированное устройство, совершающее определенное действие или бездействующее с учетом воспринятой и распознанной внешней среды.

Цифровая трансформация (Digital transformation) – комплекс мероприятий, включающий в себя внедрение цифровых технологий, реинжиниринг и использование данных.

Открытые данные (Open data) – данные, представленные в машиночитаемом виде и предназначенные для дальнейшего использования, повторной публикации в неизменном виде.

Большие данные (Big data) – большие массивы данных, отличающиеся такими характеристиками, как объем, разнообразие, скорость обработки и/или вариативность, которые требуют использования технологии масштабирования для эффективного хранения, обработки, управления и анализа.

Программное обеспечение (Software) – совокупность программ, программных кодов, а также программных продуктов с технической документацией, необходимой для их эксплуатации.

Персональные данные (Personal data) – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

Биометрические данные (Biometric data) – персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность.

Машинное обучение (Machine learning) – процесс автоматического обучения и совершенствования поведения системы искусственного интеллекта на основе обработки массива обучающих данных без явного программирования.

Глубинное обучение (Deep learning) – форма машинного обучения, которая использует вычислительные структуры, известные как «нейронные сети», для автоматического распознавания шаблонов в данных и предоставления подходящих выходных данных, таких как прогноз или доказательства для принятия решения.

Цифровая подпись (Digital signature) – цифровой код, получаемый в результате ключевого шифрования, который присоединяется к передаваемому документу в целях подтверждения аутентичности содержания и личности отправителя.

ВВЕДЕНИЕ

В условиях стремительного развития процессов глобальной цифровизации информационные технологии оказывают трансформирующее влияние на все сферы общественной и государственной деятельности. Современные технологические парадигмы, включая технологии обработки больших данных, облачные вычисления, распределенные реестры (блокчейн), механизмы обеспечения кибербезопасности и, в особенности, искусственный интеллект (далее – ИИ), формируют основу цифровой трансформации, способствуя интенсификации управленческих процессов, автоматизации деловых операций и повышению институциональной эффективности органов государственной власти.

На фоне нарастающих глобальных вызовов и факторов дестабилизации массовое внедрение указанных технологий и ускорение процессов роботизации приводят к усилению конкурентной динамики на международной арене и актуализируют широкий спектр социотехнологических, правовых и этических вопросов.

Цифровизация проникает в ключевые механизмы управления, контроля и регулирования с применением ИИ как центрального элемента современной технологической повестки, включая правоохранительную деятельность. Государственные институты систематически интегрируют решения на базе ИИ в инфраструктуру обеспечения правопорядка, национальной безопасности, уголовного правосудия и контроля миграционных потоков.

ИИ-системы применяются, в частности, как прогностические инструменты, способные обрабатывать и анализировать массивы исторически накопленных данных для проведения оценки вероятностных рисков и моделирования будущих сценариев. Также широкое распространение получают технологии интеллектуального видеонаблюдения, нательные регистраторы и системы биометрической идентификации, в том числе в рамках обеспечения безопасности при проведении массовых мероприятий.

Однако масштабная имплементация ИИ в правоохранительный сектор сопряжена с рядом значимых вызовов, включая вопросы этической легитимности, нормативной регламентации, алгоритмической подотчетности и угроз, связанных с возможными нарушениями прав человека, ростом киберпреступности и утечкой конфиденциальной информации.

Сегодня специалитстами IT-сферы наравне с учеными отмечается, что функционирование ИИ-алгоритмов носит вероятностный характер, что обусловливает присущую им неопределенность и потенциальное воздействие на фундаментальные права и свободы. ИИ не осуществляет точного предсказания, а лишь реализует процедуры экстраполяции на основании обучающих data set (набора данных). При этом многие алгоритмические модели функционируют как «черные ящики», где внутренняя логика принятия решений остается непрозрачной и недоступной для внешнего аудита.

В ответ на данные вызовы многие государства разворачивают процессы нормативного регулирования и институционального управления технологиями ИИ в правоохранительной сфере. Разрабатываются законодательные инициативы, стандарты технического регулирования и методические подходы, направленные на обеспечение транспарентности, правовой определенности и подотчетности алгоритмически поддерживаемых решений.

Примером такой деятельности служит инициатива, реализуемая Интерполом совместно с Межрегиональным научно-исследовательским институтом ООН по вопросам преступности и правосудия (ЮНИКРИ), в рамках которой был подготовлен «Инструментарий ответственных инноваций в сфере ИИ для правоохранительных органов»[1]. Документ предлагает рекомендации по законному, прозрачному и этичному применению ИИ в правоохранительной сфере, способствуя минимизации рисков и нарушений.

В этих условиях органы прокуратуры не могут оставаться в стороне от глобальных технологических изменений. Поэтому закономерно, что в последние годы в государствах-участниках Содружества Независимых Государств (СНГ) наблюдается тенденция цифровизации надзорной деятельности.

В ряде государств-участников СНГ органы прокуратуры внедряют аналитические платформы, системы обработки больших данных, автоматизированные системы надзора и прогнозирования преступности.

К примеру, в Российской Федерации внедряется платформа на основе ИИ для аналитической работы, прогнозирования роста преступности в отдельных регионах и анализа законопроектов[2].

В Казахстане 31 марта 2025 года запущена система «Цифровой надзор» с элементами ИИ, позволяющая автоматически распознавать беглых преступников, должников и пропавших без вести лиц[3]. Основной фокус системы направлен на сквозной надзор с момента поступления информации и до полного разрешения ситуации по ней с максимальной прозрачностью для всех участников процесса.

Однако, несмотря на существование отдельных инициатив, в целом подходы к внедрению информационных технологий в системы прокуратуры стран СНГ остаются несогласованными. Более того, на международном уровне также отсутствуют единое концептуальное понимание ИИ и единые стандарты его правового регулирования.

Эффективная интеграция технологий ИИ в органы прокуратуры государств-участников СНГ требует решения ряда фундаментальных вопросов. Прежде всего, необходимо формирование государственной стратегии, предусматривающей

[1] UNICRI and INTERPOL, «Toolkit for responsible AI innovation in law enforcement» / [Electronic resource] – Access mode: https://www.ai-lawenforcement.org/guidance/_(Access data: 20.05.2025).

[2] Генеральная прокуратура РФ начала внедрять в свою работу искусственный интеллект / [Электронный ресурс] – Режим доступа: https://tass.ru/politika/20634537 _(дата обращения:22.05.2025).

[3] Прокуратура будет искать преступников, должников и пропавших без вести с помощью искусственного интеллекта / [Электронный ресурс] – Режим доступа: https://kz.kursiv.media/2024-08-06/zhrb-gen-ii-vidcam/ _(дата обращения: 25.05.2025).

целесообразность внедрения ИИ в деятельность государственных органов, а также оценка имеющихся ресурсов и инфраструктурных возможностей.

Ключевыми элементами успешной реализации данной стратегии являются: подготовка квалифицированных специалистов в области ИИ; создание мощных центров обработки и хранения данных; развертывание современных высокопроизводительных вычислительных систем.

Все эти компоненты требуют значительных финансовых вложений, что делает вопросы бюджетного планирования и привлечения инвестиций критически важными при разработке и реализации программ цифровой трансформации в правоохранительной деятельности.

Альтернативой может стать использование зарубежных решений, таких как ChatGPT[4], DeepSeek[5], GROK[6] и других аналогичных платформ. Однако важно учитывать, что загрузка данных в такие системы означает их потенциальную доступность владельцам платформ. Это создает риск утечки конфиденциальной и другой служебной информации, включая сведения, относящиеся к государственной тайне. В связи с этим специалисты отмечают, что использование ИИ в государственных органах требует локального развертывания платформ ИИ внутри страны. Это позволит минимизировать риски, связанные с передачей чувствительных данных за рубеж, и обеспечит соблюдение требований законодательства о защите государственной тайны и национальной безопасности.

Осознание необходимости системного подхода к внедрению ИИ в деятельность органов прокуратуры государств-участников СНГ стало одним из оснований для принятия на Координационном совете генеральных прокуроров в 2023 году решения о проведении научного исследования по данному вопросу.

Учитывая схожие правовые нормы законодательств государств-участников СНГ, общие исторические предпосылки развития постсоветских государств, в данном исследовании впервые предпринята попытка комплексно рассмотреть текущее состояние применения информационных технологий и уровень развития ИИ в органах прокуратуры в разрезе отдельных государств-участников СНГ.

Результаты проведенного исследования собраны и систематизированы в настоящей монографии, в которой наряду с обзором опыта ряда государств-участников СНГ отдельное внимание уделено вопросам правового регулирования, анализу международного опыта, выявлению потенциальных угроз, а также оценке возможностей и рисков применения ИИ в надзорной деятельности.

В монографию включены материалы, предоставленные членами авторского коллектива межгосударственного научного исследования – Научно-практическим центром укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь, Генеральной прокуратурой Кыргызской

---

[4] Чат-бот с генеративным искусственным интеллектом, разработанный Американской компанией «OpenAI» / [Электронный ресурс] – Режим доступа: https://chatgpt.com/ _(дата обращения: 24.05.2025).

[5] Чат-бот с генеративным искусственным интеллектом, разработанный Китайской компанией «Deep Seek» / [Электронный ресурс] – Режим доступа: https://www.deepseek.com/ _(дата обращения: 25.05.2025).

[6] Чат-бот с генеративным искусственным интеллектом, разработанный компанией Илона Маска «xAI» / [Электронный ресурс] – Режим доступа: https://grok.com/ _(дата обращения: 24.01.2025).

Республики, Университетом прокуратуры Российской Федерации и Правоохранительной академией Республики Узбекистан, а также сведения, полученные из открытых источников.

В связи со стремительным развитием информационных технологий, в частности искусственного интеллекта, выводы и предложения, изложенные в настоящей монографии, актуальны на день ее выпуска.

ГЛАВА 1. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМУ ПРОКУРОРСКОГО НАДЗОРА

§ 1.1 Понятие и правовая природа технологий искусственного интеллекта в контексте прокурорского надзора

Развитие ИИ привело к необходимости формирования правового регулирования, которое охватывает все сферы применения новых технологий.

Вместе с тем, как и многие ученые, полагаем необходимым разобраться в этимологии самого термина «интеллект».

Интеллект является одной из центральных и многогранных концепций в психологии, когнитивных науках и философии. На протяжении долгого времени ученые предлагали различные теории и определения, пытаясь охватить всю сложность этого феномена. В современном научном дискурсе интеллект рассматривается как совокупность когнитивных и эмоциональных способностей, обеспечивающих адаптацию, решение проблем и успешную интеграцию в социальную и природную среду.

В обобщенном виде интеллект можно определить, как совокупность когнитивных, эмоциональных и социальных способностей человека, которые обеспечивают его способность эффективно решать задачи, адаптироваться к изменениям окружающей среды, обучаться на основе собственного опыта и взаимодействовать с другими людьми. Интеллект включает в себя как аналитические и логические способности, так и творческие, эмоциональные и межличностные компоненты, что делает его многомерным и динамичным.

Основоположник теории когнитивного развития Жан Пиаже рассматривал интеллект как динамичный процесс адаптации человека к меняющимся условиям среды. В своей теории он выделял два основных механизма: «ассимиляцию» (интеграцию новых знаний в существующие когнитивные структуры) и «аккомодацию» (модификацию этих структур для усвоения новых знаний)[7].

Психолог Роберт Стернберг предложил модель тройного интеллекта, которая включает три компонента: «аналитический интеллект» (способность решать задачи с использованием логических рассуждений), «креативный интеллект» (способность генерировать оригинальные идеи и решения) и «практический интеллект» (умение применять знания в реальных жизненных ситуациях).

С учетом таких позиций, интеллект – это не только способность к решению абстрактных задач, но и широкий спектр навыков и умений, направленных на динамическую адаптацию и эволюцию систем в условиях постоянно меняющейся среды.

Анализируя природу ИИ в контексте прокурорского надзора, мы сравнили вышеназванную совокупность способностей человека с природой ИИ отметив

[7][Электронный ресурс] – Режим доступа: https://gtmarket.ru /librery/basis/3252/3255_(дата обращения:18.06.2025)

отсутствие у последнего эмоциональных и физических возможностей (сочувствие, жалость, радость, усталость и т.д.).

На сегодняшний день ученые-юристы, исследующие ИИ и возможности его применения, определяют ИИ не как обычный алгоритм, а как комплекс информационных технологий и программ, состоящий из ряда информационных объектов – программ, баз данных, алгоритмов, обучающих наборов данных.

Таким образом, мы видим ИИ как сложный информационный объект со специфическим правовым режимом в существующей системе права.

Для законного применения технологий с использованием ИИ в сфере прокурорского надзора возникает необходимость урегулирования следующих аспектов: правовой статус ИИ, этика и ответственность, защита данных и конфиденциальность, регулирование, стандарты, взаимодействие с другими органами.

Правовой статус с каждым днем становится актуальным и важным аспектом ИИ. Согласно правовой позиции законодательных органов большинства стран, ИИ не имеет самостоятельной правосубъектности, так как окончательное решение должно оставаться за человеком. С учетом такой позиции в контексте прокурорского надзора необходимо учитывать, что ответственность за использование ИИ при принятии решений в работе прокурора ложится на должностное лицо, которое может объяснить выводы ИИ по принятому решению.

Этическим аспектом применения ИИ в работе прокурора является законность, прозрачность, справедливость, недискриминация. Соответственно, ИИ системы должны принимать решения объективно и без злоупотреблений, не нарушая чьи-либо права и соблюдая правопорядок.

Защита данных и конфиденциальность, требующиеся при обработке больших данных, должны выступать гарантией от утери персональных данных физических и юридических лиц, сведений по уголовным, гражданским и административным делам и другой чувствительной информации правоохранительного блока. Цифровые технологии должны соответствовать требованиям норм законов, направленных на соблюдение прав граждан, а прокуроры в свою очередь должны гарантировать их использование в интересах общества.

Еще один аспект – это разработка регуляторных стандартов по применению ИИ в работе прокурора, в ходе которой прокуратуре необходимо предусмотреть гарантии соблюдения законности и других технических регламентов, предусмотренных для ИИ-систем.

Немаловажным аспектом является безопасность взаимодействия органов прокуратуры через цифровые каналы с другими органами, внедряющими или использующими ИИ-системы.

Для более широкого применения ИИ в работе прокурора мы должны быть полностью уверены в полной адаптации сложной конструкции работы ИИ под не менее сложные функции прокурорского надзора, куда также входят нормы

права, судебная практика и практика правоохранительных и специальных органов. Для этого необходима прозрачность принятия решений ИИ. Сторона по делу должна иметь возможность обжалования решения, а разработчик систем ИИ и прокурор должны понимать – как ИИ приняло то или иное решение, уметь объяснить алгоритм принятия решения, не ограничиваясь введением материалов и задач для «черного ящика» и получением на выходе «непрозрачного результата».

Этот вопрос в научном мире остается открытым.

Применение ИИ в любой сфере, начиная от правоохранительных органов и судебных систем до экономики и здравоохранения, требует четкого определения понятий и концепций, это обязательное условие при разработке нормативных актов, регулирующих использование ИИ. В этой связи предлагается рассмотреть определения ИИ, закрепленные в законодательных актах, рекомендациях и других документах как ряда стран СНГ, так и стран дальнего зарубежья.

Выработка определений ИИ, его правового статуса и ответственности за его возможные ошибки сегодня в международно-правовом и научно-теоретическом мире сопровождается множеством дискуссий и споров. Однако единого унифицированного определения ИИ на сегодня не сформировано, нет и общего согласия по вопросу правосубъектности ИИ, в то же время он активно внедряется в деятельность правоохранительных и судебных органов.

Значительное влияние на создание стандартов в формировании правового регулирования ИИ оказывают нормы и рекомендации таких международных организаций, как Европейский Союз, ЮНЕСКО, ОЭСР, ОДКБ и других организаций, которые могут стать основой для разработки национальных законодательств. При этом само понятие ИИ продолжает эволюционировать в ответ на развитие технологий.

Так, согласно **Рекомендациям ЮНЕСКО об этических аспектах искусственного интеллекта** (2021 г.), ИИ определяется как «технологические системы, способные обрабатывать данные и информацию способом, напоминающим разумное поведение и включающим, как правило, такие аспекты, как рассуждение, обучение, распознание, прогнозирование, планирование и контроль».

Это определение ориентируется на высокоуровневое представление ИИ, что является общепринятым в мировой практике, учитывая его широкий спектр применения в различных сферах.

При этом, как утверждает данная организация, она не имеет намерения ввести единственно правильное определение ИИ, мотивируя это тем, что с течением времени и развитием технологий такое определение потребовало бы изменений.

Разбирая приоритеты этой дефиниции, следует отметить, что она касается не только физической реализации систем ИИ, но и их функциональной роли в обществе. Иными словами, ИИ в данном случае трактуется не только как техническая система, но и как механизм, влияющий на процессы принятия решений, определяющий выбор людей и организаций. В этой связи данный

аспект приобретает определенное значение в деятельности органов прокуратуры, где необходимо учитывать этические и правовые ограничения в использовании таких технологий, где заключительное решение должен принимать человек.

Европейский Закон «Об искусственном интеллекте (2024 г.), известный также как **Регламент ЕС об ИИ,** не содержит прямого определения ИИ, но он трактуется как «система искусственного интеллекта», основанная на машинной технологии, разработанной для работы с различными уровнями автономности и способной демонстрировать адаптивность после развертывания, которая, имея явные или неявные цели, делает выводы на основе получаемых данных для генерации таких выходных результатов, как прогнозы, контент, рекомендации или решения, способные влиять на физическую или виртуальную среду.

Содержащиеся в данном законе нормы определяют системы ИИ как машинные системы, которые могут работать автономно и адаптироваться после развертывания, генерируя такие результаты как прогнозы и решения.

Регламент ЕС также устанавливает рамки для стран-участников по применению ИИ в разных сферах, подчеркивая адаптивность алгоритмов, акцентируя внимание на регулировании рисков, связанных с ИИ, а также необходимости обеспечения прав человека в условиях цифровых технологий.

Анализ определений ИИ, представленных в нормативных актах **Китайской Народной Республики**, показывает их различную направленность, в зависимости от сферы действия документа.

В «Положении о содействии развитию индустрии ИИ в Шанхае» (Shanghai AI Industry Development Promotion Regulations) дано определение искусственному интеллекту, где ИИ – это «система теорий, методов, технологий и программного обеспечения, использующая компьютеры и машины для симуляции, расширения и дополнения человеческого интеллекта, воспринимающая окружающую среду, обретая знания и используя их для достижения наилучших результатов».

Основными положениями данного нормативного документа является поддержка разработчиков ИИ, развитие науки и законодательства по регулированию ИИ.

Этот документ регулирует развитие индустрии ИИ в Китае, особенно в Шанхае, и поддерживает создание инновационной экосистемы для технологий ИИ. Однако основными нормативно-правовыми актами КНР в этой сфере являются **«Положение об управлении алгоритмическими рекомендациями информационных Интернет-сервисов» (Закон об управлении алгоритмами Китая)** (2022 г.), «Спецификация этики искусственного интеллекта нового поколения» (2021 г.) и другие государственные инициативы[8].

В «Положении об управлении алгоритмическими рекомендациями информационных Интернет-сервисов» не нет прямого определения понятия ИИ, но регулируются рекомендательные алгоритмы машинного обучения и

[8] [Электронный ресурс] – Режим доступа: https://rg.ru/2021/10/04/v-kitae-vypustili-kodeks-eticheskih-principov-dlia-iskusstvennogo-intellekta.html_(дата обращения:18.06.2025).

автоматизированного принятия решений, где основными положениями являются ограничения на алгоритмическую персонализацию контента (например, в социальных сетях), защита данных пользователей, запрет на манипуляции общественным мнением[9].

В «Спецификации этики искусственного интеллекта нового поколения» в Китае (2021 г.) ИИ описывается как «интеллектуальная технология, способная воспринимать, обучаться и адаптироваться и оказывающая влияние на общество». Основными принципами здесь являются: гармония с человеком (ИИ не должен заменять человеческую волю), справедливость и инклюзивность, безопасность и контроль. В спецификации акцент делается не только на технологической стороне ИИ, но и на его влиянии на социальные процессы.

Краткий сводный анализ рынка ИИ Китая описан в «**Белой книге развития ИИ»** (2021 г.), где последний рассматривается как «ключевая технология для цифровой трансформации экономики и других областей».

В Книге рассказывается о стимулировании инноваций, усилении госрегулирования, внедрении стандартов безопасности.

В целом, китайская политика в области ИИ представляет собой модель жесткого государственного регулирования (безопасность, контроль данных, управление алгоритмами) с одновременным активным стимулированием индустрии развития технологий, инвестиций, исследований.

Это отражается в сочетании мер по контролю над алгоритмами и защите общественных интересов с программами поддержки разработчиков, инвестициями в исследования и созданием инновационной экосистемы. Такой подход позволяет Китаю управлять рисками ИИ, минимизировать негативные социальные эффекты и одновременно ускорять технологический прогресс.

Если в Китае по законодательному регулированию применения новых технологий, в том числе ИИ, приняты «полномасштабные и решительные меры», то в ряде развитых стран к этому вопросу подходы более «осторожные».

К примеру, в **Великобритании** на сегодня еще нет общего законодательного регулирования ИИ**,** тогда как различные области права затрагивают вопросы регулирования ИИ на практике и, согласно информационным источникам, законодательная работа в этом направлении начата.

Подход Англии к регулированию ИИ опирается на существующие правовые рамки вроде законов о неприкосновенности частной жизни, защите данных и ответственности за качество продукции[10].

В программном документе правительства Великобритании 2023 года «Проинновационный подход к регулированию ИИ» системы ИИ, или технологии ИИ, описаны как «продукты и услуги, которые являются «адаптируемыми» и «автономными».

---

[9] FAQ по регулированию Китаем рекомендательных веб-сервисов / [Электронный ресурс] – Режим доступа: https://dorotenko.pro/ru/china-algorithmic-recommendations-regulations-faq/_(дата обращения: 29.09.2024).

[10] Как в Великобритании планируют регулировать искусственный интеллект / [Электронный ресурс] – Режим доступа: https://trends.rbc.ru/trends/industry/64b154ee9a794770e668094b_(дата обращения: 25.06.2024).

В свою очередь адаптируемость ИИ относится к системам ИИ, которые после обучения часто развивают способность использовать новых методы поиска закономерностей и связей в данных, которые напрямую не предусмотрены программистами-людьми. Автономность ИИ относится к некоторым системам ИИ, которые могут принимать решения без намерения или постоянного контроля со стороны человека[11].

Названный документ наглядно указывает на стремление к гибкому регулированию, поддержанию инноваций, отсутствию чрезмерного контроля по сдерживанию развития ИИ. В нем также подчеркивается риск-ориентированный подход, где регулирование зависит от сферы применения ИИ, а не от единого жесткого набора правил.

Конгресс Соединенных Штатов Америки в 2017 году в ходе научной деятельности описывает ИИ как технологии машинного обучения, роботы и умное программное обеспечение, способные действовать рационально, то есть планировать действия, выстраивать их последовательность, принимать решения, воплощать планы и обучаться.

Данные технологии включают следующие ключевые аспекты:

- технологии машинного обучения отражают основной подход к созданию ИИ-систем, которые используют данные для выявления закономерностей и адаптации;

- роботизация подчеркивает, что ИИ не ограничивается программным обеспечением, но также применяется в физических устройствах, автономных системах и киберфизических системах;

- умное программное обеспечение охватывает широкий спектр ИИ-решений, включая экспертные системы, чат-ботов и системы автоматизированного анализа данных, обеспечивая интеллектуальную поддержку в различных сферах деятельности.

С научной точки зрения, данное определение ИИ имеет ряд преимуществ: оно включает ключевые характеристики ИИ, такие как способность к планированию, обучению и принятию решений; охватывает как программные, так и аппаратные реализации; соответствует современному представлению об ИИ как адаптивной и рациональной технологии. Однако у него есть и недостатки: он упрощает концепцию рациональности, так как современные ИИ-системы не всегда действуют строго рационально без четко определенных целей; не упоминает глубокое обучение и нейросетевые подходы, которые стали ключевыми в развитии ИИ; а также не делает различия между слабым (узким) и сильным (общим) ИИ, что важно для точного регулирования и понимания границ технологий.

Как мы уже отмечали, сегодня в законодательстве Соединенных Штатов Америки отсутствует единое федеральное определение ИИ. Однако различные

[11] Глоссарий искусственного интеллекта / [Электронный ресурс] – Режим доступа: https://post.parliament.uk/artificial-intelligence-ai-glossary_(дата обращения: 25.06.2024).

государственные документы и инициативы предлагают описания и принципы, связанные с ИИ. Это следующие ключевые нормативные акты и документы, регулирующие сферу ИИ в США.

Национальный стратегический план исследований и разработок в области искусственного интеллекта (National Artificial Intelligence Research and Development Strategic Plan: 2019 Update)[12] (обновлен в 2023 г.) не дает конкретного определения ИИ, но он в документе понимается как междисциплинарная область компьютерных наук, где ИИ включает широкий спектр технологий и методов, которые позволяют машинам воспринимать информацию, анализировать данные, принимать решения и действовать для достижения поставленных целей. Его основные характеристики –автономность, адаптивность и способность к обучению**.**

Документ подчеркивает, что ИИ включает в себя не один конкретный метод, а представляет собой набор технологических подходов, таких как «Машинное обучение», «Обработка естественного языка», «Компьютерное зрение», «Автоматизированное планирование и автономные системы "Robototechnica-интегра"». Основной целью развития ИИ, согласно данному стратегическому плану, является создание умных автономных систем, способных воспринимать окружающую среду, обрабатывать и анализировать информацию, прогнозировать последствия и принимать решения и в целом обучаться и адаптироваться.

Документ предусматривает инвестиции в фундаментальные исследования, направленные на продвижение этических и социальных аспектов ИИ, анализ и смягчение потенциальных рисков, связанных с его внедрением, а также использование ИИ для решения юридических и социальных проблем. Кроме того, в нем подчеркивается необходимость оценки широкомасштабных последствий развития и применения ИИ.

Таким образом, ИИ в данном документе понимается не как единая технология, а как целая экосистема методов, подходов и решений, интеллектуально управляемых машинами в различных средах.

Проект США «Билль о правах ИИ» (Blueprint for an AI Bill of Rights, 2020)[13] устанавливает принципы защиты прав граждан при использовании автоматизированных систем. Документ включает положения о безопасности и надежности ИИ, требуя, чтобы системы были устойчивыми и предсказуемыми, а также о защите от алгоритмической дискриминации, предотвращающей несправедливое обращение и негативное влияние на людей. Он также подчеркивает важность конфиденциальности данных, гарантируя защиту личной информации пользователей, и требует уведомления и объяснения, чтобы люди были осведомлены о применении ИИ и могли понимать его решения. Кроме того,

[12][Электронный ресурс] – Режим доступа: https://d-russia.ru/wp-content/uploads/2023/05/national-artificial-intelligence-research-and-development-strategic-plan-2023-update.pdf /_(дата обращения: 18.10.2024).

[13][Электронный ресурс] – Режим доступа: https://ai.gov.ru/knowledgebase/normativnoe-regulirovanie-ii/2022_proekt_billya_o_pravah_iskusstvennogo_intellekta_the_blueprint_for_an_ai_bill_of_rights_the_white_house/_(дата обращения: 15.09.2024).

проект предусматривает человеческие альтернативы и контроль, обеспечивая возможность выбора взаимодействия с человеком вместо ИИ.

Исполнительный указ о безопасном, защищенном и заслуживающем доверия искусственном интеллекте (2023 г.) направлен на управление рисками и укрепление лидерства США в области ИИ-технологий. Документ предусматривает разработку стандартов безопасности, требуя от разработчиков предоставлять данные об испытаниях, а также защиту конфиденциальности, призывая к принятию закона о защите данных. Он акцентирует внимание на борьбе с алгоритмической дискриминацией, продвижении равенства и гражданских прав, а также анализе влияния ИИ на рынок труда для защиты работников. Указ дополнительно поддерживает инновации и конкуренцию, расширяя возможности для высококвалифицированных специалистов, и требует разработки руководств для государственных агентств, обеспечивая ответственное использование ИИ в управлении.

Таким образом, хотя в США нет единого официального определения ИИ на федеральном уровне, существующие документы и инициативы устанавливают рамки и принципы для разработки и использования ИИ, акцентируя внимание на безопасности, этике и защите прав граждан.

Следующий пример – **определение Отчета Организации экономического сотрудничества и развития** (ОЭСР, 2019 г.), не являющееся юридически обязательными, но влияющее на создание стандартов политики государств-участников (38 стран).

Согласно указанному Отчету, ИИ определяется как «системы, которые воспринимают окружающую среду, обрабатывают информацию и принимают решения с целью достижения поставленных задач». Это определение ставит акцент на целеустремленности ИИ и его способности действовать в интересах пользователей. ОЭСР подчеркивает, что ИИ должен быть направлен на решение конкретных задач.

В **Европейской хартии искусственного интеллекта** (2020 г.) ИИ определяется как «системы, которые могут выполнять задачи, требующие человеческого интеллекта, включая восприятие, обработку информации, принятие решений и обучение». Это определение близко к тем, что предложены ЮНЕСКО и ОЭСР, с акцентом на обучаемость систем и их способность решать задачи аналогично человеческому интеллекту.

На территории государств-участников СНГ правовые определения ИИ также находятся на стадии формирования. Однако в ряде стран, таких как Россия, Узбекистан и Казахстан, были предприняты первые шаги в области правового регулирования ИИ.

18 апреля 2025 года на 58 пленарном заседании Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств принят

Модельный закон СНГ «О технологиях искусственного интеллекта», направленный на регулирование ИИ в государствах-участниках СНГ[14].

Модельный закон разработан учеными Объединенного института проблем информатики Национальной академии наук совместно с заинтересованными организациями Беларуси.

По мнению генерального директора Объединенного института проблем информатики Национальной академии наук Республики Беларусь Сергея Кругликова, ключевой проблемой при разработке закона оказалось отсутствие общепринятого определения самого понятия ИИ.

В данном законе дано свое понятие ИИ, под которым подразумевается комплекс технологических решений, включающих информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе такое, в котором используются методы машинного обучения), процессы и сервисы обработки данных и поиска решений, позволяющих имитировать когнитивные функции человека (включая поиск решения без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека, или превосходящие их.

Определение отражает современный прикладной и инженерный подход к ИИ – системный, ориентированный на практическую эффективность, технологическую комплексность и способность к адаптации. Одной из особенностей определения мы считаем акцент на техническую архитектуру, имитацию разумности и критерии результативности, что делает его созвучным с подходами, встречающимися в международной практике, в частности в документах ЕС, ISO.

Межпарламентская Ассамблея СНГ также еще в 2023 году разработала Рекомендации по нормативному регулированию использования искусственного интеллекта, включая этические стандарты для исследований и разработок. Документ направлен на формирование системы законов в сфере ИИ на территории Содружества[15].

В данной инициативе акцентируется внимание на этическом регулировании ИИ, подчеркивая необходимость обеспечения благополучия и безопасности человека, запрета на причинение вреда, подконтрольности ИИ человеку и недопустимости манипуляций поведением людей.

Ранее **Федеральным законом Российской Федерации** от 24 апреля 2020 года **«О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта»** дано следующее определение ИИ: «Искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при

[14]Модельный закон «О Технологиях искусственного интеллекта принят Межпарламентской Ассамблеей СНГ» / [Электронный ресурс] – Режим доступа: https://uiip.basnet.by/rus/news/438/_(дата обращения: 02.07.2025).
[15][Электронный ресурс] – Режим доступа: https://iacis.ru/baza_dokumentov/modelnie zakonodatelnie_akti_i_ rekomendatcii_mpa_sng/rekomendatcii/10_(дата обращения: 18.06.2025).

выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека».

Стоит отметить, что в странах СНГ часто даются более ограниченные и конкретизированные определения, ориентированные на практическое использование технологий в различных отраслях, включая правоохранительные органы.

Например, **в Республике Узбекистан в рамках Стратегии цифровой экономики** (2020 г.) ИИ определяется как «система, которая анализирует данные и использует их для автоматического принятия решений или классификации, имитируя когнитивные способности человека». Это определение отражает более прагматичную точку зрения на ИИ, ориентированную на практическое использование в сфере административных решений и регулирования.

В проекте **Закона Республике Казахстан «Об искусственном интеллекте»** (2025 г.) искусственный интеллект определяется как «информационно-коммуникационная технология, позволяющая имитировать или превосходить когнитивные функции человека, с целью выполнения интеллектуальных задач и поиска решений».

Одно из любопытных положений здесь — разделение систем ИИ по степени независимости в принятии решений и воздействия на пользователя. На основе этих критериев выделяются:

- вспомогательные (помощники) – системы, в которых ИИ выполняет функции помощи пользователю и окончательные решения принимаются только пользователем;

- полуавтономные – системы, которым собственником (владельцем) или пользователем предоставлены ограниченные права на автоматизированное принятие решения в рамках заранее заданных параметров, при этом лицо, предоставившее права на принятие решения, может вмешиваться в процесс принятия решений или изменять результаты деятельности системы;

- полностью автономные – системы, которые принимают решения вне зависимости от заранее заданных параметров и не поддаются контролю со стороны собственника (владельца) данной системы[16].

Вместе с тем, в период разработки Закона об ИИ высказывались мнения против его необходимости. Так,казахстанский эксперт в области информационных технологий Арман Абдрасилов полагает, что в Казахстане не нужен отдельный закон об ИИ и нет необходимости выделять ИИ внутри Закона РК «Об информатизации». Более того, принятие Цифрового кодекса РК повлечет за собой отмену закона об ИИ. Эксперт, приводя в обоснование своей позиции пример отсутствия отдельного закона по регулированию IP технологий, 5G и т.д.,

[16]Искусственному интеллекту запретят манипулировать казахстанцами / Анастасия Прилепская 05.02.2025 / [Электронный ресурс] – Режим доступа: https://orda.kz/iskusstvennomu-intellektu-zapretjat-manipulirovat - kazahstancami-397718/_(дата обращения: 05.03.2025).

утверждает, что ИИ это очередная технология, которая не подлежит регулированию отдельным законом[17].

Между тем один из авторов законопроекта, депутат Мажилиса Парламента Е.М. Смышляева полагает, что, хотя в цифровом законодательстве мы стараемся соблюдать принцип технологической нейтральности, то есть не посвящать отдельным технологиям законы или нормы, в данном случае технология настолько особенная, что порождает вокруг себя особый тип общественных отношений. Их и будет регулировать настоящий закон[18].

Анализ представленных определений ИИ раскрывает несколько ключевых аспектов, которые характеризуют все системы ИИ:

- *восприятие*. Все определения, включая разработанные ЮНЕСКО, ОЭСР, в Казахстане, России и других странах, подчеркивают способность ИИ воспринимать окружающую среду. Это предполагает использование датчиков, камер и других технологий для сбора данных;

- *обработка информации*. Все определения указывают на способность ИИ обрабатывать информацию. Это включает ее анализ, обработку и интерпретацию для принятия решений;

- *принятие решений*. Важным аспектом всех определений является способность ИИ принимать решения. Это является основой для использования ИИ в различных сферах, таких как правоохранительная деятельность, экономика и здравоохранение;

- *обучение*. Ряд определений акцентирует внимание на обучении ИИ. Это делает системы ИИ адаптивными и способными улучшать свою работу на основе полученного опыта.

В большинстве нормативных актов и рекомендаций ИИ определяется как система, обладающая рядом значимых функций: восприятие окружающей среды, обработка информации, принятие решений и обучение. Эти элементы являются основными для понимания правового и этического вопроса использования ИИ в различных областях.

Однако существующие определения в разных странах и международных организациях не всегда совпадают, что затрудняет создание унифицированных стандартов для регулирования ИИ. К примеру, страны СНГ только начинают вводить термин ИИ в свои нормы права, и эти определения будут развиваться по мере актуализации законодательства.

Международные организации, такие как ЮНЕСКО, ОЭСР и Европейский Союз, предлагают более универсальные определения ИИ, что способствует гармонизации мировых стандартов. Однако для эффективного правового

[17]Причина в деньгах: эксперт по информтехнологиям раскритиковал законопроект об ИИ /Анжела Ким 22.05.2024 г. / [Электронный ресурс] – Режим доступа: https://cmn.kz/prichina-v-dengah-expert-po-informtehnologiyam-raskritikoval-zakonoproekt-ob-ii/_(дата обращения: 18.01.2025).

[18]В Мажилисе презентовали законопроект об искусственном интеллекте / Екатерина Елисеева 12.09.2024 г. / [Электронный ресурс] – Режим доступа: https://www.zakon.kz/obshestvo/6469053-v-mazhilise-prezentovali-zakonoproekt-ob-iskusstvennom-intellekte.html_(дата обращения: 12.09.2024).

регулирования необходимо учитывать особенности всех юрисдикций, уделяя внимание вопросам этики и безопасности применения ИИ.

В дальнейшем, при необходимости унификации норм необходимо стремиться к выработке общих принципов и стандартов для регулирования ИИ, которые будут соответствовать как международным, так и национальным требованиям.

С учетом всех рассмотренных определений ИИ в различных странах и международных организациях можно предложить новое, более универсальное определение, которое будет отражать ключевые аспекты ИИ, учитывая его сложность и многообразие применения. При этом необходимо принимать во внимание, что в условиях использования ИИ в государственных органах, особенно в прокуратуре и суде, важным аспектом является этическое и правовое регулирование этого процесса. В этом случае ИИ должен быть не только эффективным инструментом, но и строго регулируемым, минимизирующим риски нарушения прав граждан и гарантирующим соблюдение этических норм.

По основе имеющихся на сегодня в международных и национальных документах ряда стран определениях ИИ мы скомпилировали определение термина ИИ с фокусом на его практическое применение.

Вариант 1. Искусственный интеллект – это совокупность систем и технологий, способных воспринимать окружающую среду, обрабатывать полученные данные, обучаться на основе опыта и принимать решения аналогичных тем, что выполняет человек, с целью оптимизации процессов и повышения эффективности в различных сферах деятельности, включая экономику, право, медицину и другие области.

Такое определение ИИ не только охватывает все ключевые аспекты, упомянутые в нормативных актах разных стран и международных организациях, но и подчеркивает важность практической стороны применения ИИ в различных областях. Оно достаточно гибкое для применения в разных юрисдикциях, и в то же время дает четкое представление о функционале и возможностях ИИ в правовом регулировании.

Вариант 2. Искусственный интеллект – это совокупность технологий, методов и систем, способных автоматически воспринимать, анализировать и интерпретировать данные, а также обучаться, адаптироваться и принимать решения с целью выполнения задач, традиционно требующих человеческого интеллекта. ИИ включает как программные, так и аппаратные решения, охватывает машинное обучение, нейросетевые подходы, обработку естественного языка, компьютерное зрение и робототехнику.

Данные определения предполагают практически автономное функционирование систем, но в сотрудничестве с человеком на стадии принятия решений, учитывающее при этом этические, правовые и социальные аспекты, обеспечение безопасности, прозрачности, конфиденциальность данных и защиту прав пользователей.

§ 1.2 Функциональный анализ возможностей искусственного интеллекта в контексте задач и полномочий органов прокуратуры

Цифровая трансформация деятельности органов прокуратуры не сводится лишь к вопросам повышения административной эффективности или внедрения новых технических решений. Напротив, она представляет собой сложный социально-философский процесс, затрагивающий основы функционирования государственной власти, механизмов юридической ответственности и самого понимания справедливости в условиях алгоритмического посредничества. Информационные технологии становятся не просто инструментами, а участниками принятия решений, влияющих на судьбы людей, что требует особой критической рефлексии со стороны науки и правоприменителя.

Использование интеллектуальных систем в прокуратуре предполагает переосмысление традиционных категорий юридического мышления: меняется структура правовой субъектности, усложняется рамка взаимодействия между человеком и системой, возникает потребность в новых критериях легитимности и нормативной верификации алгоритмических решений. Эти изменения затрагивают фундаментальные понятия доверия, автономии, подотчетности и институциональной справедливости.

В своей работе Ш.Ён-Джин и К.Сын-Тэ исследуют концепцию электронного правительства сквозь призму трех ключевых подходов – экономического развития, социального детерминизма и технического детерминизма. Эти теоретико-методологические рамки, предложенные для государственной администрации, обладают высоким эвристическим потенциалом и могут быть продуктивно экстраполированы на сферу надзорной деятельности органов прокуратуры, позволяя глубже осмыслить институциональные, технологические и социальные последствия цифровизации в правоприменительной практике[19].

С точки зрения социального детерминизма, цифровизация надзорной функции прокуратуры становится не просто вопросом автоматизации процессов, а элементом организационно-культурной реконфигурации. Новые цифровые инструменты – будь то платформы для электронного реагирования на обращения граждан, алгоритмы первичной фильтрации и анализа поступающей информации, либо системы предикативного контроля исполнения прокурорских актов – требуют пересмотра логики внутренней коммуникации, перераспределения функциональных обязанностей между сотрудниками, а также пересоздания символического образа прокурора как публичного участника.

Таким образом, информационные технологии здесь не формируют новые структуры вертикально, а внедряются, так как существует общественный и институциональный запрос на повышение транспарентности, подотчетности, эффективности и открытости прокуратуры. Смена парадигмы управления «от

[19] Young-Jin S., Seang-Tae K. E-Government Concepts, Measures, and Best Practicies //Global e-government: theory, applications and benchmarking. – IGI Global, 2007. – С. 340-369.

реакции к проактивности» диктуется не самими технологиями, а динамикой правового сознания и ожиданий со стороны общества.

Особый интерес представляет то, как алгоритмизация деятельности органов прокуратуры влияет на институциональную идентичность и восприятие легитимности. В условиях, когда прокурорские действия все чаще опосредуются цифровыми интерфейсами, возрастает риск отчуждения субъекта от функции, и потому требуется сохранение баланса между технологической рациональностью и гуманистическим содержанием публичной службы. Именно общественное ожидание справедливости, а не технические параметры систем, должно определять границы и формы цифрового внедрения.

Таким образом, философия социального детерминизма позволяет рассматривать цифровую трансформацию прокуратуры не как односторонний технологический проект, а как социально обусловленный процесс адаптации публичного института к меняющимся условиям коммуникации, правосознания и нормативных ориентиров. Это понимание требует не только технической подготовки, но и высокой институциональной чувствительности, междисциплинарного подхода и этической рефлексии.

Согласно логике **технического детерминизма**, именно развитие технологий детерминирует вектор и глубину трансформации социальных институтов, включая формы управления, способы организации труда и даже когнитивные модели профессионального мышления. Технология в этой оптике выступает не как инструмент, адаптируемый под социальный запрос, а как автономная сила, продуцирующая структурные сдвиги в логике функционирования институтов — в том числе правовых.

Применительно к прокурорской системе это означает, что цифровизация не ограничивается автоматизацией второстепенных процедур или ускорением документооборота. Она становится структурообразующим фактором, задающим новые нормативы эффективности, прозрачности, интерпретации и даже легитимности. Интеллектуальные платформы, способные осуществлять предиктивный анализ, выявлять процессуальные дефекты, ранжировать дела по степени значимости или сложности, начинают формировать новую реальность надзорной деятельности, в которой исходной точкой анализа выступает не правовая норма, а алгоритмически выявленная аномалия.

Так, например, системы машинного обучения, интегрированные в аналитические блоки органов прокуратуры, способны автоматически выделять дела, содержащие признаки нарушений процессуального закона, либо выстраивать вероятностные модели поведения фигурантов. Кроме того, технологии видеоаналитики и распознавания моделей поведения в судебных залах могут использоваться для фиксации отклонений в регламенте, которые ранее были доступны только профессиональному наблюдению.

Тем не менее, данная логика несет в себе существенные философско-правовые риски. Смещение эпицентра прокурорской деятельности с субъекта, обладающего правовым сознанием и профессиональным суждением, на

алгоритмическую подсказку создает угрозу редукции нормативного мышления до уровня технической целесообразности. Возникает проблема границ: где заканчивается помощь, улучшающая качество правоприменения, и начинается подмена волевого и ответственного решения автоматическим выбором, лишенным моральной и юридической субъектности.

Таким образом, позиция технического детерминизма позволяет понять, как технология преобразует не только методы и инструменты прокурорского надзора, но и онтологический статус самой фигуры прокурора, подвергая переосмыслению его роли как гаранта законности. Эта трансформация требует разработки институциональных и этических фильтров, ограничивающих власть алгоритма и возвращающих приоритет правовой рациональности над технической.

Рассмотрение цифровой деятельности органов прокуратуры сквозь **призму ее экономической результативности** позволяет отнести данный процесс к категории стратегических инструментов институционального развития государства. В рамках парадигмы «e-government» – системы, использующей информационные технологии для взаимодействия между правительством, гражданами и организациями как средства стимулирования экономического роста, информационные технологии рассматриваются не как вспомогательные элементы управления, а как катализаторы системных преобразований, способствующих укреплению макроэкономической устойчивости и рационализации бюджетных расходов.

Применительно к надзорной деятельности цифровые решения – от автоматизированных систем анализа и обработки обращений до интерактивных платформ мониторинга исполнения законов, выполняют двойную функцию. С одной стороны, они ускоряют регламентные процедуры, минимизируют дублирование функций и снижают транзакционные издержки, характерные для бумажного документооборота и ручного контроля. С другой стороны, они становятся ключевыми элементами экономической профилактики, позволяя в режиме реального времени отслеживать и пресекать нарушения, связанные с нецелевым использованием бюджетных средств, нарушениями налоговой дисциплины, а также коррупционными схемами в закупочной или социальной сферах.

Так, автоматизированные панели прокурорского мониторинга, интегрированные с финансовыми и фискальными реестрами, обеспечивают проактивный контроль за исполнением нормативов в сферах, имеющих критическую значимость для социально-экономического развития: здравоохранение, образование, инфраструктура. Своевременное обнаружение финансовых аномалий или отклонений в расходовании средств становится возможным за счет алгоритмического анализа больших данных, что снижает нагрузку на надзорный аппарат и одновременно увеличивает его охват.

Кроме того, цифровая трансформация прокуратуры в этом виде способствует повышению инвестиционной привлекательности юрисдикции за счет повышения правовой определенности и снижения уровня правового риска.

Прозрачность процессов прокурорского реагирования, открытость данных и возможность общественного контроля через цифровые каналы формируют более предсказуемую и рационально управляемую институциональную среду, что положительно сказывается на экономическом климате в целом.

Следовательно, с точки зрения подхода «технологии как средства экономического развития» цифровизация органов прокуратуры выступает не как изолированная административная инновация, а как часть более широкой стратегии устойчивого и подотчетного управления, включающей правовую, фискальную и управленческую модернизацию.

В современном научном дискурсе информационные технологии (ИТ) выходят далеко за рамки инструментального определения и приобретают статус социотехнического феномена, оказывающего влияние на антропологическую структуру познания, коммуникации и принятия решений в публичной сфере. С философско-правовой точки зрения, ИТ следует рассматривать как форму институционализированной рациональности, трансформирующую не только способы обработки и хранения данных, но и саму природу правового регулирования, юридической ответственности и взаимодействия человека с властью.

ИТ не являются нейтральным инструментом, а воплощают в себе определенные логики управления, нормативные посылки и культурные коды. Они создают новую парадигму юридической реальности, в которой информация и алгоритмы становятся не вспомогательным элементом, а структурообразующим фактором процессов правообеспечения и правоосуществления. Через призму философии технологии можно утверждать, что ИТ конституируют особый тип «техно-правового порядка», в котором юридическая практика все чаще опосредуется цифровыми формами познания, моделирования и контроля.

Особую значимость такое осмысление приобретает в деятельности органов прокуратуры. Интеграция ИТ в прокурорскую практику вызывает необходимость переосмысления самой категории юридического усмотрения, поскольку алгоритмизация надзорных функций влияет на пределы субъективной оценки, допустимость цифрового вмешательства и институциональную автономию человека в процессе принятия решений.

Таким образом, понимание ИТ с философско-правовых позиций позволяет выйти за рамки утилитарного подхода и задать более глубокие вопросы: какие формы юридической рациональности порождают цифровые технологии? Как изменяется структура правовых институтов в условиях алгоритмизации? Где пролегает граница между технологической эффективностью и правовой справедливостью?

Осмысление пределов и ограничений применения ИИ в правоохранительной деятельности обретает глубокую концептуальную основу в интеграции теоретико-методологических подходов, выработанных в рамках теории управления рисками, правового гуманизма и концепции прозрачности проведения процессуальных процедур. Указанные теоретические парадигмы,

будучи органично взаимосвязаны, позволяют не только обозначить, но и всесторонне обосновать внутренние нормативные и этические рубежи допустимости использования алгоритмических технологий в одной из наиболее чувствительных и социально значимых сфер государственного управления –сфере правоохранительной деятельности, где затрагиваются фундаментальные права, свободы и законные интересы личности. Применение ИИ в этом формате предстает как процесс, требующий не только технической безупречности и функциональной эффективности, но прежде всего соответствия базовым принципам справедливости, гуманности и правовой допустимости, без чего его интеграция в систему правоприменения может породить угрозу для самой сущности правопорядка, основанного на уважении человеческого достоинства.

Идеи правового гуманизма, истоки которых восходят к фундаментальным трудам Рудольфа Иеринга и Густава Радбруха, вносят в проблематику допустимости применения ИИ в правоохранительной деятельности ключевую концептуальную установку на приоритет человеческой личности над инструментальными аспектами права. Согласно этому направлению правовой мысли, право существует не ради собственной внутренней логики, не ради абстрактной эффективности функционирования государственных механизмов, а прежде всего ради защиты человеческого достоинства, обеспечения свободы личности и утверждения справедливости в ее социально-правовом измерении.

Е. Мохоря в своей статье подробно изучил философию Г. Радбруха и приводит его цитату о праве: «это воля, стремящаяся к справедливости. А справедливость заключается в том, чтобы судить без оглядки на авторитет и ко всем подходить с одинаковой меркой… Если законы сознательно попирают волю справедливости, например, предоставляя тому или иному лицу права человека или отказывая в них исключительно по произволу, то в этих случаях подобные законы недействительны, народ не обязан подчиняться им, а юристы должны найти в себе мужество не признавать их правовой характер»[20].

Р.Ф. Иеринг также высказывался о праве: «всякое право в мире является результатом борьбы, каждое важное правовое положение должно сначала победить, те, которые сопротивляются ему, и каждое право, – право народа, как и право отдельного человека, – предполагает постоянную готовность к его отстаиванию» и «право – не просто мысль, но живая сила. Поэтому правосудие, держащее в одной руке весы, которыми оно взвешивает право, в другой руке держит меч, которым утверждает право. Меч без весов есть голое насилие, весы без меча – бессилие права»[21].

Применительно к современным вызовам, связанным с внедрением ИИ в практику правоприменения, данная позиция требует жесткого ограничения технической автономии алгоритмов, поскольку ни одна, даже самая совершенная технологическая система, не способна заменить интуитивное, ценностное и

[20] Цит по: Мохоря Е. Проблема соотношения права и закона в философии И. Канта и Г. Радбруха // Traditie şi inovare în cercetarea ştiinţifică. – 2018. – С. 310-316.
[21] Иеринг Р. Борьба за право / пер. с нем. С.И. Ершова. – М.: Юридическая литература, 2007. – 176 с.

этическое измерение человеческого правосудия. ИИ в данном случае может быть признан допустимым исключительно в качестве вспомогательного средства, служащего достижению высших целей права – справедливости, гуманности, правовой определенности и защиты человеческой свободы.

Допущение ИИ в процессы, имеющие значение для правового статуса личности, возможно лишь при условии строгой нормативной подчиненности алгоритмических решений принципам правового гуманизма. Это означает, что ИИ не должен становиться автономным субъектом юридически значимых действий или решений: каждое его применение должно осознанно оставаться инструментальным, с обязательной верификацией его результатов человеческим субъектом, наделенным профессиональной, правовой и моральной ответственностью. В противном случае возникает опасность технологической подмены права – подчинения правоприменительной деятельности механистической эффективности в ущерб ее гуманитарному содержанию.

Таким образом, идеи правового гуманизма устанавливают непреодолимую границу между допустимым и недопустимым в использовании технологий в праве: право должно сохранять свое человекоцентрическое измерение даже в условиях цифровизации, а защита человеческого достоинства должна оставаться незыблемой ценностью, приоритетной по отношению к любым технологическим достижениям.

Положения теории процедурной справедливости акцентируют внимание на том, что восприятие институциональных решений как справедливых формируется не только и не столько на основе их конечного результата, сколько в зависимости от того, насколько сами процедуры их принятия соответствуют критериям открытости, беспристрастности и участия. В рамках этой теории, наиболее полно разработанной в трудах Дж. Ролза и Т. Тайлера, устанавливается приоритет формы над содержанием, процедуры над результатом, что особенно актуально при интеграции ИИ в сферы, где последствия решений затрагивают фундаментальные права личности[22]. Как отмечает Т. Тайлер: «Процедурная справедливость – это восприятие людьми справедливости процессов, с помощью которых принимаются решения и разрешаются споры»[23].

Применительно к правоохранительной системе это означает, что даже технически эффективная ИИ-модель, демонстрирующая высокие показатели точности, не может считаться допустимой, если она не обеспечивает процедурную транспарентность, возможность обоснования и правового обжалования своих решений. Именно параметризация как формализованный механизм фиксации и оценки ключевых характеристик алгоритма становится здесь инструментом обеспечения процедурной справедливости. Качественные параметры, такие как интерпретируемость, правовая релевантность, устойчивость к расовой и иной дискриминации и нормативная обоснованность, играют решающую роль в легитимации ИИ-систем, позволяя согласовать

[22] Ролз Дж. Теория справедливости. – М.: Новое издательство, 2020. – 592 с.
[23] Тайлер Т. Почему люди соблюдают закон. – М.: Издательство института Гайдара, 2019. – 342 с.

алгоритмическую рациональность с фундаментальными правовыми ценностями.

Теория управления рисками, развиваемая в работах Э. Гидденса, К. Худа, исходит из того, что в условиях комплексного общества, характеризующегося высокой степенью неопределенности, право должно выполнять не только функцию нормоустановления, но и функцию минимизации институциональных рисков[24]. Теория управления рисками является одной из ключевых методологических основ осмысления допустимости применения ИИ в правоохранительной сфере. Здесь же дополнительно упомянем монографию Ортвина Ренна, которая представляет собой одну из наиболее авторитетных и концептуально насыщенных работ, посвященных проблематике управления рисками в условиях экспоненциального технологического развития[25].

В сфере правоохранительной деятельности, где под угрозой оказываются такие базовые ценности, как личная свобода, безопасность, неприкосновенность частной жизни и презумпция невиновности, применение систем ИИ должно основываться на принципиально строгом разграничении сфер их допустимого использования в зависимости от уровня риска для правового статуса личности. Применение ИИ в зонах пониженного риска, к числу которых относятся криминологическая аналитика, мониторинг преступных тенденций, а также прогнозирование оперативной нагрузки на правоохранительные органы, допустимо при условии обеспечения эффективного внутреннего контроля и надлежащего процедурного аудита. Однако в тех сферах, где алгоритмические решения могут непосредственно затрагивать права и законные интересы граждан, например при вынесении решений об аресте, инициировании уголовного преследования, проведении следственных действий или оценке доказательственной базы, требуется установление особо строгих нормативных регламентаций, обязательное внедрение многоступенчатых процедур верификации результатов ИИ-анализа и безусловное сохранение приоритета профессионального человеческого суждения на всех критических этапах правоприменительного процесса.

Данный режим регламентации корреспондирует с принципом предосторожности, который требует минимизации вероятности причинения непоправимого вреда правам личности вследствие применения даже высокоточных, но все же ограниченных по своей природе алгоритмических решений. Игнорирование данного принципа и чрезмерная автоматизация процессов принятия решений в правоохранительной практике чреваты утратой гуманистического содержания правосудия и его подменой формально-технологическими процедурами, не способными адекватно учитывать многоаспектную природу человеческих правовых отношений. В этой связи теория управления рисками предоставляет концептуально обоснованный фундамент для построения многоуровневой системы контроля над функционированием ИИ в

[24] Giddens A. The Consequences of Modernity. – Stanford: Stanford University Press, 1990. – 186 p.; Hood C., Rothstein H., Baldwin R. The Government of Risk: Understanding Risk Regulation Regimes. – Oxford: Oxford University Press, 2001. – 256 p.

[25] Renn O. Risk Governance: Coping with Uncertainty in a Complex World. – London: Earthscan, 2008. – 368 p.

правоохранительной деятельности, в рамках которой интенсивность регулятивного вмешательства должна находиться в прямой зависимости от уровня потенциальной угрозы правам, свободам и законным интересам субъектов права.

О. Ренн подчеркивает, что процессы принятия решений в отношении внедрения таких технологий требуют не механистической оценки вероятности ущерба, а системной дифференциации рисков на основе их потенциального воздействия на критические общественные институты и базовые права личности[26]. В этой логике возникает необходимость выстраивания многоуровневых регулятивных режимов, адекватных различным уровням риска, что особенно актуально для алгоритмически опосредованных решений в правоохранительной деятельности, где ставка делается не только на эффективность, но и на сохранение легитимности институтов, гарантирующих справедливость и защиту прав человека.

Концепция процедурной справедливости, разработанная Томом Тайлером, находит свое органичное продолжение в исследовании допустимости и пределов применения систем ИИ в сфере правоохранительной деятельности. Восприятие легитимности решений, принимаемых органами государственной власти, в значительной степени определяется не столько их материально-правовым содержанием или объективной результативностью, сколько характером процедур, посредством которых такие решения формируются. Процедуры должны восприниматься как справедливые, прозрачные, беспристрастные и обеспечивающие субъектам процесса реальную возможность быть услышанными. Легитимность власти и добровольное соблюдение установленных ею норм зависят от того, насколько глубоко индивид ощущает участие, уважение и равноправие в процессах принятия решений, даже если результаты этих решений оказываются для него неблагоприятными.

Т. Тайлер утверждает, что «учитывая важность процессуального правосудия, на какие аспекты судебной практики следует обращать особое внимание судебным органам? Существует четыре ключевых принципа процессуального правосудия: право голоса, нейтральность, уважение и доверие»[27].

В условиях внедрения ИИ в процессы правоприменения требования процедурной справедливости приобретают еще большую актуальность. Алгоритмические системы, несмотря на их потенциальную способность к повышению эффективности и оптимизации анализа данных, не могут и не должны подменять собой основу правосудия – человеческое участие, ответственность и ценностно-нормативную осознанность. Применение ИИ в сферах, где принимаемые решения способны оказывать непосредственное влияние на такие фундаментальные права, как личная свобода, неприкосновенность частной жизни, достоинство личности и репутация гражданина, допустимо лишь при условии обязательного сохранения человеческого контроля и окончательной юридической верификации выводов,

[26] Там же.
[27] Tyler T.R. Procedural justice and the courts// Court Rev. – 2007. – Vol. 44, Issue 1-2. – P. 26-31.

полученных с помощью алгоритмических инструментов.

ИИ, даже будучи высокотехнологичным и функционально надежным, должен оставаться вспомогательным средством, предназначенным для повышения качества профессионального суждения, но не заменяющим его. Финальное решение должно приниматься уполномоченным лицом, несущим как юридическую, так и моральную ответственность за последствия своих действий, а не передаваться в ведение автономных систем, лишенных способности к оценке справедливости, соразмерности и уважения к человеческому достоинству.

Таким образом, пределы допустимости применения ИИ в правоохранительной деятельности выводятся не столько из уровня технологической зрелости или оперативной эффективности соответствующих алгоритмов, сколько из моральной и правовой оценки их воздействия на личность и общественное доверие к институтам правосудия. Интеграция ИИ в правоохранительную практику должна основываться на соблюдении принципов гуманности, справедливости и соразмерности риска, гарантируя с одной стороны повышение функциональной эффективности правоохранительных органов, а с другой – безусловное сохранение базовых гарантий прав, свобод и достоинства личности.

Принципиальное разграничение областей применения ИИ в зависимости от уровня риска воздействия на права человека приобретает не только прикладное организационное значение, но и отражает более фундаментальную нормативно-ценностную установку. В рамках данной парадигмы утверждается приоритет права над техникой и человека над алгоритмом как обязательное и непреодолимое требование к правовому регулированию цифровой трансформации публичной власти.

Рассматривая пределы применения ИИ в органах прокуратуры сквозь призму философии права и морально-этической рефлексии, следует подчеркнуть, что мы вступаем в сферу, находящуюся на пересечении технологического прогресса и глубоко укорененных оснований человеческой цивилизации, таких как достоинство личности, верховенство права, общественная мораль и универсальные ценности справедливости. Этот вопрос обостряет проблему допустимости алгоритмического вмешательства в процессы, традиционно требующие высшего уровня нормативного осмысления и моральной ответственности.

Данная проблематика может быть репрезентирована в нескольких взаимосвязанных плоскостях, требующих философско-правового рассмотрения. Одной из центральных является оппозиция: право и алгоритм – это замещение человеческого начала или его технологическое дополнение?

Не только прокуратура, но и вся правоохранительная деятельность по своей природе сопряжена с осуществлением решений, имеющих глубокие последствия для судеб людей. Однако право как социальный институт представляет собой не только совокупность предписаний, регулирующих поведение, но и живую интерпретацию этих норм в конкретных человеческих ситуациях. В этот момент

возникают принципиальные вопросы: способен ли алгоритм постичь дух закона, который в правовой теории традиционно понимается как воплощение идеи справедливости, а не просто буквальную логику текста? Может ли ИИ интерпретировать норму с учетом ее этического содержания, целей и ценностей, которые зачастую выходят за пределы формально-логического анализа?

Еще более остро встает вопрос о границах допустимости делегирования алгоритму моральной и правовой ответственности, которая в классическом понимании правосудия неразрывно связана с человеческим сознанием, способностью к сопереживанию и индивидуальной оценке последствий. Может ли человек отказаться от своего долга быть субъектом ответственности, передавая его системе, основанной исключительно на вероятностной обработке данных и оптимизации заданных параметров?

Ответ на эти вопросы очерчивает один из существенных пределов применения ИИ в правоохранительной практике. Алгоритм, как бы высоко ни была развита его способность к обработке информации, не способен заменить моральную интуицию, ценностное осмысление и способность к справедливой интерпретации уникальных жизненных ситуаций, которые являются сутью правоприменения. ИИ может и должен рассматриваться исключительно как вспомогательный инструмент, расширяющий когнитивные возможности человека, но не замещающий его нравственную и юридическую автономию.

Право, будучи неотъемлемой частью социальной сферы общества, воплощает в себе ожидания справедливости, моральные ориентиры и идеалы гуманности. Оно неизбежно требует субъекта, способного не только к техническому применению норм, но и к критическому осмыслению их высших ценностей. Следовательно, принципиальным ограничением применения ИИ в правоохранительной деятельности выступает недопустимость его полной автономизации в принятии решений, затрагивающих личные права, свободы и судьбы граждан. Сохранение приоритета человеческого разума, человеческой совести и человеческой ответственности над алгоритмической логикой является необходимым условием обеспечения легитимности и гуманистической направленности системы права в условиях цифровизации.

Проблематика ответственности в условиях внедрения ИИ не только в деятельность прокуроров, но и в правоохранительную в целом, приобретает качественно новые черты, порождая фундаментальные вызовы как для юридической доктрины, так и для философии права. Если в традиционных моделях правоприменения ошибки и злоупотребления могли быть прямо атрибутированы конкретному субъекту – следователю, прокурору, судье, то в условиях алгоритмически опосредованных процессов возникает феномен размытия ответственности между разработчиками программного обеспечения, операторами систем и конечными пользователями технологий[28].

[28] Садыков М.Б. Искусственный интеллект в правоохранительной деятельности: правовые и организационно-тактические аспекты: дис. …д-ра философии (PhD). – Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2025.

Как отмечает М.Б. Садыков: «Следует четко различать решения, принимаемые системой ИИ, в случае ее нормальной работы, от решений в результате неправильного обучения, сбоя или внешнего вмешательства. Есть несколько вариантов позиций для определения ответственности систем на основе систем ИИ. Это коллективная ответственность разработчиков с созданием специальных фондов компенсации вреда пострадавшим от действий (бездействий) подобных систем, безусловная и безвиновная ответственность как разработчика, когда исключены внешние факторы риска, так и оператора системы, когда исключены внутренние факторы риска или система выполнила прямые команды оператора. Также можно выделить солидарную ответственность оператора и разработчика и распределенную ответственность, где пропорции устанавливает государство. Вопрос о "личной" ответственности ИИ может быть поставлен лишь при наделении подобных систем правосубъектностью, что является вопросом отдаленного будущего. При определении ответственности за решения и выводы систем ИИ могут возникнуть проблемы из-за различий в юрисдикциях. К примеру, в одной стране ответственность несет разработчик, который скрывается в другой стране, где подобная ответственность либо не предусмотрена, либо ее несет оператор системы. В целом на данном этапе развития систем ИИ следует воспринимать данные системы как помощника в принятии решений, а не как замену человеку. Финальное решение всегда должен принимать человек»[29].

В данной ситуации мы сталкиваемся с тем, что можно назвать кризисом ответственности: алгоритмические системы, будучи по сути инструментами обработки данных, не обладают субъектностью в юридическом или моральном смысле и, следовательно, не могут выступать носителями ответственности за принятые решения или совершенные ошибки. Однако функциональное участие ИИ в процессах, имеющих юридически значимые последствия для прав и свобод личности, создает иллюзию распределенной, а в действительности – часто утраченной ответственности, скрытой в технологическом «черном ящике» процессов машинного обучения, обработки больших данных и автоматизированного анализа.

Философское осмысление данной проблемы неизбежно приводит к выводу о недопустимости размывания или делегирования ответственности вне сферы человеческого контроля. В правовом аспекте ответственность должна сохраняться за конкретным субъектом – человеком, осуществляющим разработку, настройку, внедрение или использование алгоритмической системы в правоохранительных целях. Любая попытка перенести ответственность на автономное функционирование алгоритма подрывает основу моральной легитимности правосудия, поскольку устраняет из процесса необходимую связку между действием и ответственностью, между решением и этическим осмыслением его

[29] Садыков М.Б. К вопросу о юридической ответственности за решения и действия искусственного интеллекта // Искусственный интеллект и право: опыт Республики Казахстан и зарубежных стран: Мат-лы международ. науч.-практ. конф. – Астана, 2024. – С. 70–76.

последствий.

Человеческая ответственность за действия ИИ должна пониматься как системная и неделимая категория, охватывающая все стадии жизненного цикла алгоритмической системы: от замысла и программирования до конкретного применения в ситуациях, затрагивающих судьбы граждан. Лишь при условии сохранения этой ответственности в руках конкретных субъектов может быть обеспечено соответствие принципам справедливости, гуманизма и правового государства, без чего само правосудие утратит свою моральную основу и общественную легитимность.

Следовательно, внедрение ИИ в правоохранительную деятельность требует не только технической регламентации и процедурных гарантий, но прежде всего философско-правового утверждения базового постулата: ответственность за последствия всегда остается на стороне человека. Только в этом случае возможно избежать трансформации права в безликий технологический механизм, лишенный ценностного содержания и подотчетности перед обществом.

Внедрение систем ИИ в процессы правоприменения ставит на повестку дня вопрос о природе и границах общественного доверия: может ли социум воспринимать как справедливые и законные решения, вынесенные не человеком, а алгоритмом? Способно ли правосудие, лишенное личностной основы, сохранять ту глубинную связь с моральными ожиданиями общества, без которой оно утрачивает свой социальный мандат?

Философское осмысление справедливости требует признания того, что справедливость – это не только и не столько результат решения, сколько справедливость самого процесса принятия этого решения. Обществу важно ощущать, что за правовым актом стоит человек, способный осмыслить страх, боль, раскаяние, мотивацию поступка, а не безличный, математически запрограммированный алгоритм. Это формирует принципиальные ограничения для применения ИИ: использование алгоритмических систем в правоохранительной практике не должно размывать фундаментальное доверие к правосудию как к человеческому институту, способному учитывать не только факты, но и ценностные аспекты человеческой жизни.

Переходя к организационному измерению данной проблемы, необходимо подчеркнуть, что массовая интеграция ИИ в деятельность правоохранительных органов трансформирует традиционные модели управленческой практики и институциональной культуры. Возникает новая форма власти — власть алгоритма, заключающаяся в перенесении центра принятия решений на уровень автоматизированных систем. Это угрожает автономии профессионального субъекта — следователя, оперативного работника, прокурора, судьи, превращая его из активного носителя юридической и нравственной ответственности в пассивного оператора, исполняющего предписания цифрового кода.

Встает принципиальный вопрос: кто в новой системе будет обладать верховной полномочностью принимать окончательное решение – человек или машина? Как будет трансформироваться правоохранительная организация, в

которой человеческое суждение окажется подчиненным механической логике алгоритмического анализа? Эти вопросы требуют институционального ответа, состоящего в установлении строгих организационных рамок, не допускающих дегуманизации правоохранительной деятельности и превращения носителей государственной власти в технических агентов без воли и ответственности.

Наконец, в гуманистическом измерении необходимо подчеркнуть, что правоохранительная деятельность по своей природе не сводится к механистическому исполнению норм, а является прежде всего моральным актом. Каждый акт применения права – это акт оценки, акцент на уважении достоинства личности, признание права на свободу, презумпцию невиновности, на возможность быть услышанным и понятым.

В этой связи возникает ряд важных вопросов: способен ли ИИ в полной мере учитывать ценностное измерение правоприменения, распознавать уникальные особенности человеческой судьбы, уважать право на ошибку и проявлять необходимое для правосудия сострадание и милосердие? Можем ли мы допустить, чтобы алгоритмические решения лишили человека права на гуманное рассмотрение его ситуации?

Эти соображения подводят нас к фундаментальному философскому пределу: интеграция ИИ в сферу правосудия не должна разрывать внутреннюю связь между юридическим процессом и гуманистическим содержанием права. Моральные качества, присущие человеку – милосердие, эмпатия, сострадание, чуткость к конкретным жизненным обстоятельствам, должны неизменно сохранять приоритет над технологическими возможностями. Без этого право рискует превратиться из инструмента социальной справедливости в бездушный механизм цифрового управления, утратив свое сущностное предназначение.

В свете проникновения ИИ в различные сферы жизнедеятельности руководители правоохранительных органов оказываются перед качественно новым вызовом: они должны не только интегрировать передовые технологические решения в оперативные процессы, но и выработать зрелое понимание принципиальных пределов их допустимого использования. Организационная зрелость правоохранительных органов определяется сегодня не столько формальным наличием современных технических средств и алгоритмических платформ, сколько способностью этих организаций выстраивать внутренние нормативные рамки, регламентирующие применение ИИ, а также разрабатывать методики оценки его эффективности, правомерности и социального воздействия в каждом конкретном случае.

Эффективное функционирование правоохранительных органов в новой технологической реальности требует формирования кадрового корпуса, обладающего уникальным синтезом компетенций: пониманием технических характеристик и архитектуры алгоритмических систем, глубоким осознанием операционных особенностей их внедрения в практическую деятельность, а также способностью адекватно оценивать неизбежные компромиссы, связанные с использованием ИИ в условиях уголовного правосудия. Подготовка таких

специалистов требует системного обучения, ориентированного на постоянное обновление знаний с учетом динамичного развития технологий.

Квалифицированный сотрудник в условиях алгоритмизированной правоохранительной деятельности должен быть способен анализировать источники данных, использованных для обучения моделей ИИ, осознавать возможные ограничения этих данных, распознавать потенциальные механизмы воспроизводства дискриминации и предвзятости, а также предлагать стратегии минимизации их негативных последствий. Он обязан понимать, каким образом скрытые искажения на стадии сбора, обработки или интерпретации данных могут влиять на результаты алгоритмической оценки риска, классификации подозреваемых или прогнозирования рецидивов и какие меры могут быть приняты для устранения или компенсации подобных системных изъянов.

Особое значение приобретает задача внедрения эффективных процедур мониторинга и аудита алгоритмических систем. Мониторинг должен включать регулярную проверку актуальности данных, оценку справедливости результатов работы ИИ, анализ побочных эффектов алгоритмических решений, а также своевременное выявление и устранение нарушений стандартов справедливости, прозрачности и законности.

Отдельным серьезным организационным вызовом становится обеспечение прозрачности и подотчетности алгоритмических процессов в правоохранительной деятельности. По мере усложнения архитектуры машинного обучения и увеличения числа уровней нейронных сетей алгоритмы становятся все более закрытыми и трудно поддающимися интерпретации даже для их разработчиков. Это усиливает риск утраты эффективного контроля над последствиями их применения и создания правовых ситуаций, в которых нарушаются права личности без четко установленных субъектов ответственности.

В этих условиях правоохранительные органы обязаны выстраивать новые институциональные механизмы внутреннего и внешнего контроля над применением ИИ. Необходимо создание специализированных подразделений аудита алгоритмов, формирование междисциплинарных экспертных комиссий, регулярное проведение независимой оценки социальной допустимости применения алгоритмических решений в правоохранительной практике. Только при наличии таких механизмов можно обеспечить не только соответствие применения ИИ формальным требованиям законности, но и сохранение материальной справедливости, доверия общества и моральной легитимности правоохранительных институтов в цифровую эпоху.

«Human in the loop», что по смыслу можно перевести как «человек в контуре» или «человек в цепи управления» - это подход, при котором человек остается частью процесса принятия решений. Человеческое суждение должно оставаться центральным элементом при разработке и использовании ИИ в правоохранительной деятельности. ИИ должен улучшать, а не заменять процесс принятия решений человеком. Человек может участвовать не только для перепроверки результатов работы ИИ, но непосредственно проводить надзор за

процессом обучения модели, в том числе проверяя Dataset для обучения.

Результаты работы интеллектуальных систем должны критически оцениваться соответствующими должностными лицами, а выходные данные ИИ не должны быть предрешающей основой для принятия процессуальных решений, затрагивающих права и свободы людей[30].

Особенно глубоким является тезис, что решения, принимаемые сейчас, определят, какими людьми мы станем в будущем. Действительно, повсеместное использование ИИ в правоохранительной деятельности напрямую влияет на общественное сознание. Если алгоритмы воспринимаются обществом как беспристрастные и объективные, это может привести к пассивному принятию любых решений, даже несправедливых, под видом технологической необходимости. Таким образом, мы рискуем перейти от общества сознательных граждан, которые понимают и ценят справедливость и ответственность, к обществу потребителей готовых решений, утративших способность к самостоятельному критическому мышлению.

Более того, система правопорядка, излишне полагающаяся на ИИ, рискует постепенно утратить человеческое лицо. Это связано с тем, что правоохранительная деятельность исторически ориентирована на человека и его права, а не на безличные технологические алгоритмы.

Развивая вышеуказанные вопросы, необходимо подчеркнуть, что эффективное и правомерное внедрение ИИ в правоохранительную деятельность предполагает обязательное разграничение сфер его применения в зависимости от уровня риска воздействия на права, свободы и законные интересы личности. Данная стратификация представляет собой не просто техническую меру процессуальной оптимизации, но является выражением принципиального требования соблюдения баланса между инновационной эффективностью и охраной фундаментальных правовых ценностей.

В области применения ИИ, сопряженной с низким уровнем риска, допустимо его использование для целей криминологического анализа, прогнозирования криминальных тенденций и общей оперативной аналитики. В этих случаях вмешательство ИИ ограничивается обработкой обезличенных данных и выполнением вспомогательных задач, что позволяет минимизировать угрозу индивидуальным правам и, соответственно, требует лишь базового уровня внутреннего контроля и обеспечения прозрачности процедур.

Средний уровень риска связан с применением ИИ для автоматизированной фильтрации обращений граждан, сортировки заявлений, а также поддержки правоохранительных органов в построении предварительных версий событий. Здесь алгоритмические выводы начинают оказывать влияние на юридическую судьбу конкретных лиц, пусть и в косвенной форме. В этой связи применение ИИ должно сопровождаться внутренними регламентами контроля, регулярным

[30] Artificial Intelligence and Criminal Justice. Final Report, December 3, 2024 //https://www.justice.gov/olp/media/1381796/dl. 10.01.2025.

аудитом алгоритмических процедур, а также необходимостью проведения промежуточной проверки со стороны уполномоченных сотрудников.

Наиболее чувствительная зона – это сферы, в которых ИИ начинает воздействовать на принятие решений, имеющих прямые юридические последствия для правового статуса личности. Речь идет о применении ИИ в оценке доказательств, поддержке решений об аресте, инициировании следственных действий и других действиях, непосредственно влияющих на свободу и честь гражданина. Здесь система ИИ может использоваться исключительно в рекомендательном режиме, с обязательной проверкой результатов человеком и с полным сохранением за человеком всей полноты юридической и моральной ответственности за итоговое решение. Принятие решений в этих сферах не может и не должно становиться автоматизированным, так как любое нарушение прав несет особо тяжелые социальные последствия.

Таким образом, ИИ в правоохранительной системе должен рассматриваться исключительно как инструмент поддержки принятия решений, но не как самостоятельный субъект правосудия. Его функции должны заключаться в усилении способности человека к более качественному, аргументированному и своевременному принятию решений, а не в замещении человеческого морального выбора и юридической ответственности. Применение ИИ должно способствовать реализации принципов законности, справедливости и уважения прав человека, усиливая гуманистическую природу правоохранительной деятельности, а не подрывая ее основы в стремлении к технологической эффективности.

Полагаем, что развитие систем ИИ требует совершенствования правовой инфраструктуры ИИ, внедрения этических стандартов, усиления механизмов подотчетности и, главное, сохранения человеческого измерения правосудия в эпоху цифровизации.

Цифровая трансформация органов прокуратуры предстает не как простая техническая модернизация или инструмент повышения управленческой эффективности, а как глубинный социально-философский сдвиг, затрагивающий основы правоприменительной деятельности, нормативной субъектности и институциональной идентичности. Применение информационных и интеллектуальных технологий в прокурорской сфере требует всестороннего теоретико-методологического осмысления, выходящего за рамки прагматического подхода и обращающегося к парадигмам социального и технического детерминизма, а также концепциям правового гуманизма и институциональной этики.

Проникновение алгоритмических систем в надзорную практику не только переопределяет функциональную структуру прокуратуры, но и трансформирует саму логику правового регулирования, смещая акцент с человеческого усмотрения на формализованную, машинную интерпретацию правовых норм. Это влечет за собой риски эрозии ценностных оснований права, отчуждения субъекта от функции и подмены юридической ответственности технико-функциональной рациональностью. В условиях роста технологической автономии особую

значимость приобретает философская рефлексия над пределами допустимости алгоритмического вмешательства в процессы, имеющие правовое и этическое значение.

Таким образом, цифровизация прокуратуры не может быть сведена к категории нейтральных инноваций: она предполагает переосмысление самих оснований правовой справедливости, легитимности и публичной ответственности. Интеграция ИИ и цифровых решений в эту сферу допустима лишь при соблюдении жестких нормативных и этических рамок, гарантирующих приоритет гуманистических ценностей над технологической эффективностью. Только при этом условии возможно гармоничное и легитимное сосуществование алгоритмических систем с принципами правового государства, в котором человек остается не объектом, а полноправным субъектом правоприменения.

Интеграция ИИ в сферу правоохранительной деятельности ставит перед обществом и государственными институтами сложнейшие философские, юридические и организационные вызовы, требующие не просто технологического решения, но и нормативной и ценностной рефлексии. Встает принципиальный вопрос: кто будет обладать полномочиями принимать окончательное решение – человек, наделенный моральной ответственностью, или машина, оперирующая статистической логикой?

В данной перспективе правоохранительная система предстает как пространство институциональной трансформации, где формируется новая модель взаимодействия человека и алгоритма. Однако критически важно, чтобы алгоритмические технологии не подменяли гуманистическую сущность правоприменения, а лишь усиливали способность человека к принятию обоснованных и справедливых решений. Применение ИИ должно быть строго регламентировано, с учетом стратификации по уровням риска, сохраняющей приоритет прав, свобод и достоинства личности.

Наиболее чувствительные зоны, сопряженные с юридическим статусом граждан, требуют неизменного присутствия человеческого суждения, правовой ответственности и моральной интуиции. В этих условиях концепция «human in the loop» приобретает статус не просто технической предосторожности, но этического императива. Правоохранительная деятельность по-прежнему должна основываться на способности к сочувствию, уважению к человеческой уникальности, признанию права на ошибку и обязательству слышать каждого.

Вызов цифровой эпохи состоит не только в технической интеграции ИИ, но и в сохранении человеческого измерения права. Без институционального и нормативного закрепления этой приоритетности существует риск утраты моральной легитимности и превращения системы правопорядка в обезличенный алгоритмический механизм. Только при соблюдении этих условий возможно формирование устойчивой, справедливой и этически приемлемой модели цифровой правоохранительной деятельности.

Таким образом, осмысление пределов и ограничений использования ИИ в правоохранительной деятельности ясно показывает, что граница применения ИИ

не столько техническая, сколько моральная и правовая. Использование ИИ не может превращаться в самоцель, а всегда должно оставаться средством достижения гуманного, справедливого и социально одобряемого правопорядка.

Именно по этим причинам целесообразно приступить к исследованию понятийных основ и особенностей нормативного регулирования информационных технологий, а также их конкретного применения в деятельности органов прокуратуры государств-участников СНГ.

§ 1.3 Международные стандарты, принципы и ограничения применения искусственного интеллекта в правоохранительной деятельности

Настоящий раздел посвящен анализу международных стандартов и принципов, регламентирующих применение ИИ в деятельности правоохранительных органов, а также ограничений, обеспечивающих баланс между эффективностью и соблюдением прав человека. Особое внимание уделяется сопоставлению различных подходов и выявлению тенденций в сфере глобального нормативного регулирования.

Стремительное развитие технологий ИИ коренным образом трансформирует все сферы общественной жизни, включая правоохранительную деятельность. Механизмы предикативной аналитики, биометрической идентификации, интеллектуального видеонаблюдения и алгоритмов принятия решений уже активно внедряются в практику, изменяя как методы оперативно-розыскной работы, так и принципы уголовного преследования.

Вместе с тем столь масштабное внедрение ИИ порождает целый ряд правовых, этических и социальных вызовов. Угроза нарушения прав человека, непрозрачность алгоритмических решений, риск дискриминации – все это требует не только технической экспертизы, но и выработки универсальных стандартов и принципов регулирования. Международное сообщество, включая ООН, Совет Европы, ЕС и другие организации, предпринимает значительные усилия по формированию нормативной основы, направленной на безопасное, справедливое и подотчетное использование ИИ в правоохранительной сфере.

Настоящий раздел посвящен анализу международных стандартов и принципов, регламентирующих применение ИИ в деятельности правоохранительных органов, а также ограничений, обеспечивающих баланс между эффективностью и соблюдением прав человека. Особое внимание уделяется сопоставлению различных подходов и выявлению тенденций в сфере глобального нормативного регулирования.

Для более глубокого понимания истоков и масштабов нормативного реагирования на вызовы, связанные с применением ИИ в сфере правопорядка, представляется необходимым рассмотреть хронологический контекст формирования ключевых технологических и правовых тенденций. Эволюция ИИ

неразрывно связана с этапами его внедрения в деятельность правоохранительных органов, что, в свою очередь, обусловило постепенное развитие международных механизмов регулирования.

Хронология мировых трендов в сфере ИИ и их применения в правоохранительной деятельности, представленная ниже в табличной форме, позволяет проследить, каким образом формировались технологические предпосылки, институциональные инициативы и нормативно-этические ориентиры с начала XXI века по настоящее время. Этот обзор закладывает аналитическую основу для изучения современных международных стандартов и принципов регулирования применения ИИ в правоохранительной сфере.

ХРОНОЛОГИЯ МИРОВЫХ ТРЕНДОВ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ИХ ПРИМЕНЕНИЕ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

до 2000-х годов

НАЧАЛО РАЗВИТИЯ ИИ

1950г. - Разработка концепции искусственного интеллекта А.Тьюрингом;
1990 г. - ФБР США разрабатывает систему CODIS, для сопоставления ДНК;
1995 г. - Запуск CompStat в США для статистического анализа преступлений;
1999 г. - ФБР и ЦРУ начало использование нейронных сетей для анализа больших массивов данных.

2000-е годы

НАЧАЛО ИНТЕГРАЦИИ ИИ В ПРАВООХРАНИТЕЛЬНУЮ СФЕРУ

2001 г. – Запуск проекта COPLINK в США, системы на основе ИИ, анализирующей полицейские базы данных для выявления связей между преступлениями;
2005 г. – Внедрение первых роботов-патрульных в Сингапуре для мониторинга общественных мест.

2010-е годы

АКТИВНОЕ РАЗВИТИЕ ИИ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

2012 г. – Полиция США начинает использовать систему PredPol для прогнозирования преступлений на основе машинного обучения;
2016 г. – В Великобритании запущен HART (Harm Assessment Risk Tool), применяющий ИИ для оценки вероятности повторных преступлений;
2017 г. – Китай внедряет системы распознавания ИИ для выявления подозреваемых;
2018 г. – В Китае разработан «робот-прокурор», использующий ИИ.

2020-е годы

МАССОВОЕ ВНЕДРЕНИЕ ИИ В ПРАВООХРАНИТЕЛЬНУЮ

2020 г. – Компания OpenAI представляет ИИ чат бот GPT-3;
2021 г. – Полиция Дубая вводит в эксплуатацию робота-полицейского, использующего ИИ для распознавания лиц и взаимодействия с гражданами;
2023 г. –Китай внедряет интеллектуальные суды;
2024 г. – В США прокуроры начинают использовать ИИ-ассистентов для подготовки судебных исков и анализа прецедентного права.

2025 год

УСИЛЕНИЕ КОНКУРЕНЦИИ МЕЖДУ ИИ-СИСТЕМАМИ

Январь 2025 г. – Китай запускает ИИ чат бот DeepSeek V3;
Февраль 2025 г. – Франция запускает ИИ чат бот Mistral AI;
Февраль 2025 г. – Илон Маск представляет ИИ Grok 3.

Ранние межправительственные инициативы

В парадигме развития международных регуляторных механизмов в сфере ИИ особое внимание заслуживает вклад межгосударственных организаций, формирующих универсальные и этически обоснованные подходы к использованию ИИ. Одним из первых официальных документов, отражающих попытку институционализировать принципы ответственного обращения с ИИ на международном уровне, стала **Рекомендация по ИИ Организации экономического сотрудничества и развития (ОЭСР) от 22 мая 2019 года №165**[31].

Данный документ, признанный важной вехой в правовом дискурсе, предлагает пять универсальных принципов и пять прикладных рекомендаций для национальных правительств, нацеленных на обеспечение прозрачности, подотчетности и этической устойчивости ИИ-систем. В совокупности данные положения призваны создать нормативную среду, способную уравновесить интересы технологического прогресса и защиты прав человека. Существенным подтверждением значимости этих рекомендаций стало их одобрение на уровне G20 9 июня 2019 года (документ №166), включая такие государства, как США, Китай, Россия, Германия, Франция, Италия, Великобритания, Япония и др., что расширяет легитимность подхода ОЭСР на глобальном уровне и особенно актуализирует его в правоприменительной практике, включая деятельность органов охраны правопорядка.

8 ноября 2023 года в Рекомендацию ОЭСР 2019 года были внесены изменения, включая уточнение определения ИИ-систем. Повторный пересмотр Рекомендации состоялся 3 мая 2024 года с учетом технологических и политических изменений, включая развитие генеративного ИИ.

В ноябре 2024 года ОЭСР представила аналитический отчет, в котором определены 10 приоритетных направлений политики, включая установление ответственности за вред, раскрытие информации о ИИ-системах, управление рисками, борьбу с гонкой разработок, инвестиции в безопасность и обучение.

В марте и июле 2024 года Генеральная Ассамблея ООН приняла первые две резолюции по ИИ:

- A/RES/78/265 (21.03.2024 г.) – о безопасном и надежном ИИ для устойчивого развития;
- A/RES/78/311 (01.07.2024 г.) – об укреплении международного сотрудничества в области развития ИИ.

19 сентября 2024 года Консультативный орган ООН по ИИ представил доклад с рядом институциональных предложений: от создания международной научной группы до учреждения глобального офиса по ИИ при Генеральном секретаре ООН.

31 OECD. Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, № OECD/LEGAL/0449 [Электронный ресурс]. – Режим доступа: https://www.oecd-ilibrary.org/science-and-technology/oecd-principles-on-artificial-intelligence_d62f618a-en – (дата обращения: 01.07.2025).

Принципы ОЭСР включают следующие положения:

- ИИ должен способствовать благу человека и планеты, поддерживая устойчивое развитие и общее благосостояние;

- ИИ-системы должны проектироваться с учетом верховенства права, прав человека, демократических ценностей и культурного разнообразия, включая механизмы контроля и возможности вмешательства человека;

- прозрачность и информированность о принципах работы ИИ необходимы для понимания и возможности обжалования решений, принимаемых ИИ-системами;

- ИИ-системы должны функционировать надежно и безопасно на протяжении всего жизненного цикла, включая постоянную оценку и управление рисками;

- юридические и физические лица, участвующие в разработке и применении ИИ, несут ответственность за соблюдение вышеуказанных принципов.

Рекомендации ОЭСР по ИИ представляют собой важный шаг к формированию глобальной нормативной архитектуры в условиях стремительного технологического прогресса. Принятие документа авторитетной организацией и наличие институциональной поддержки (создана сеть экспертов ОЭСР по ИИ (ONE AI)) подчеркивают его международную легитимность, с фокусом на права человека, поддержку инноваций.

При этом Рекомендация имеет необязательный (неформальный) характер, она выполняет функцию «мягкого права» (soft law), способствуя гармонизации подходов и формированию правовой культуры ответственного использования ИИ. Для правоохранительной сферы эти принципы особенно актуальны, поскольку позволяют выстраивать механизмы подотчетности, предотвращать дискриминацию и обеспечивать соблюдение прав человека в условиях цифровизации правосудия.

Вместе с тем такие категории в документе, как доверие и справедливость. требуют конкретизации в национальных правовых нормах. Также документ имеет свои ограничения для применения в силовых структурах, ввиду того что правоохранительные органы часто действуют в условиях, где баланс между эффективностью и правами человека особенно уязвим.

В контексте формирования глобальных этических рамок использования ИИ ключевым рубежом стало принятие **Рекомендации ЮНЕСКО по этике ИИ от 23 ноября 2021 года**[32]. Документ был разработан в результате двухлетней деятельности международной экспертной группы, учрежденной по решению Генеральной конференции ЮНЕСКО в 2019 году, и стал одним из первых универсальных межгосударственных актов, охватывающим все 193 государства-члена организации.

[32] ЮНЕСКО. Рекомендация об этике искусственного интеллекта. Принята 41-й сессией Генеральной конференции 23 ноября 2021 года [Электронный ресурс]. – Режим доступа: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus – (дата обращения: 01.07.2025).

Основная цель Рекомендации – создание универсальной этической базы, обеспечивающей справедливое, инклюзивное и безопасное применение ИИ. В основу положены десять принципов, охватывающих ключевые аспекты прав человека, устойчивости, технологической подотчетности и культурного многообразия.

К числу основополагающих принципов относятся: принцип соразмерности и непричинения вреда, конфиденциальность и защита данных, справедливость, недискриминация и инклюзивность, цифровая грамотность и повышение осведомленности, безопасность, объяснимость и прозрачность, человеческий контроль и ответственность разработчиков, устойчивое развитие, глобальное, инклюзивное управление.

Важным последствием Рекомендации стало расширение документа, а именно: принятие на ее основе принципов этичного использования ИИ в системе ООН (20.09.2022 г.), что свидетельствует о признании документа в рамках международного публичного управления, и разработка **Руководства ЮНЕСКО по генеративному ИИ в образовании и науке** (07.09.2023 г.), содержащего практические рекомендации по защите данных учащихся, возрастным ограничениям и созданию регулятивной базы для образовательных учреждений.

Документ имеет международную легитимность, так как охватывает 193 государства, включая страны с различными уровнями технологического и правового развития.

Сочетание гуманистических и технологических принципов делает Рекомендацию пригодной для широкого круга отраслей – от образования до обороны, что подчеркивает ее универсальность и глубину.

Акцент на предупреждение вреда и защите прав человека на ранних стадиях разработки ИИ дает превентивный характер, а механизм локальной имплементации с учетом культурного контекста – гибкость и адаптивность.

Вместе с тем Рекомендации ЮНЕСКО по этике ИИ имеют ограничения и вызовы реализации.

Несмотря на масштабность охвата и прогрессивный характер положений, Рекомендация ЮНЕСКО по этике ИИ сталкивается с рядом структурных и методологических ограничений, препятствующих ее повсеместной имплементации и институционализации:

- непридание обязательного юридического статуса: документ носит рекомендательный характер и не обладает правовой обязательностью (binding force). Это означает, что государства-члены сами определяют степень и форму внедрения его положений, что снижает уровень ответственности за их неисполнение;

- неравномерность национальных подходов к внедрению: учитывая различия в правовых системах, уровне технологического развития, политических приоритетах и ресурсной обеспеченности стран, имплементация принципов Рекомендации происходит неравномерно и фрагментарно. Это затрудняет формирование единых этических стандартов в глобальном масштабе;

- отсутствие четких механизмов мониторинга и оценки эффективности: несмотря на провозглашенные цели, Рекомендация не содержит процедурных инструментов для регулярной верификации исполнения – таких как контрольные индикаторы, механизмы отчетности или санкционные меры. В результате реальное соответствие принципам остается на совести государств и организаций;

- вероятность столкновения с суверенными цифровыми политиками: ряд государств может воспринять универсальные этические нормы как угрозу вмешательства во внутреннюю политику и самостоятельную разработку стандартов цифрового управления. Это особенно актуально в условиях усиливающейся конкуренции в сфере высоких технологий;

- размытость отдельных понятий и ценностей: такие концепты, как «устойчивость», «справедливость» или «глобальное инклюзивное управление», требуют дополнительной конкретизации и нормативного закрепления, что затрудняет их практическое применение в сложных регуляторных или конфликтных ситуациях.

Рекомендация ЮНЕСКО по этике ИИ является значимым ориентиром на пути глобального гуманистического регулирования технологий. Ее значение не столько в создании юридически обязывающих норм, сколько в формировании концептуального и ценностного базиса для последующей кодификации, адаптированной к нуждам конкретных отраслей, включая правоохранительную деятельность. Тем не менее, дальнейшее развитие механизмов оценки, мониторинга и практического применения остается необходимым условием для перехода от декларативного уровня к институциональной эффективности.

Усилия ООН по формированию глобального регулирования.

В июле 2023 года Совет Безопасности ООН впервые провел заседание, посвященное ИИ. В результате была учреждена **Консультативная группа высокого уровня по ИИ**, первое заседание которой состоялось 27 октября 2023 года.

Информация о действиях ООН в 2023 году свидетельствует о переходе от фрагментарных инициатив к попытке выработки глобальной архитектуры управления ИИ.

Отдельное заседание по вопросам ИИ стало символическим признанием ИИ как фактора, способного влиять на международную безопасность, устойчивое развитие и права человека.

Создание Консультативной группы высокого уровня отражает стремление ООН к институционализации глобального диалога по вопросам регулирования ИИ. В состав группы вошли представители научного сообщества, технологических компаний, гражданского общества и международных организаций. В 2024 году группа представила итоговый доклад, в котором предложены меры по устранению пробелов в международной системе управления ИИ, включая создание глобальной архитектуры регулирования, основанной на международном сотрудничестве; учреждение Международной научной группы экспертов по ИИ; формирование Глобального фонда ИИ и Глобальной сети по

развитию потенциала; обеспечение технической совместимости ИИ-систем через обмен стандартами; устранение информационного и технологического неравенства между странами.

ООН подчеркивает необходимость перехода от этических принципов к конкретным правовым нормам. В докладе 2024 года отмечаются «дефицит управления» и отсутствие подотчетности в глобальной системе. При этом ИИ-технологии с двойным (гражданским и военным) назначением требуют особого внимания международного сообщества и координации усилий в целях предотвращения угроз безопасности и нарушения прав человека.

Несмотря на амбициозность, инициатива сталкивается с рядом таких вызовов, как отсутствие обязательной юридической силы у доклада; ограниченное участие стран Глобального Юга в процессах регулирования (по данным ООН, только 7 из 193 государств активно вовлечены в инициативы по управлению ИИ); доминирование транснациональных корпораций в разработке ИИ, что затрудняет демократизацию регулирования; необходимость согласования интересов государств с различными политико-экономическими системами.

Таким образом, инициатива ООН по созданию Консультативной группы высокого уровня по ИИ представляет собой важный шаг к формированию инклюзивной, транспарентной и многоуровневой модели глобального управления ИИ. Хотя документ группы аналогично не носит обязательного характера, он выполняет функцию «нормативного компаса», задающего вектор для будущих международных соглашений. В условиях отсутствия единой правовой архитектуры в сфере ИИ усилия ООН могут стать основой для выработки универсальных стандартов, особенно в таких чувствительных сферах, как безопасность, права человека и цифровое неравенство.

На сегодня одним из первых международных стандартов в сфере ИИ является стандарт ISO/IEC 42001-2023 «Информационные технологии. Искусственный интеллект. Система менеджмента», разработанный **Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC)**[33].

Международная организация по стандартизации (ISO, ИСО) – это независимая, неправительственная международная организация, основанная в 1947 г. по инициативе 25 национальных организаций по стандартизации на конференции в Лондоне, обладает консультативным статусом при ООН, но не входит в ее структуру.

Организация является частью Всемирного союза стандартизации (WSC) вместе с Международной электротехнической комиссией (IEC) и Международным союзом электросвязи (ITU). Членами организации являются 167 стран. Примеры полноправных членов ISO – ANSI (США), DIN (Германия), BSI (Великобритания), ГОСТ Р/Росстандарт (Россия), KAZMEMST (Казахстан).

[33] Стандарт ISO / Технический комитет ISO/IEC JTC 1/SC 42 / [Электронный ресурс] – Режим доступа: https://www.iso.org/ru/committee/6794475.html// _(дата обращения: 23.09.2024).

ISO создана с целью разработки и публикации международных стандартов, охватывающих практически все отрасли экономики и технологий, за исключением электротехники и телекоммуникаций (которые регулируются IEC и ITU соответственно).

Международная организация по стандартизации (ISO) в партнерстве с Международной электротехнической комиссией (IEC) осуществляет разработку стандартов в области ИИ через совместный технический комитет ISO/IEC JTC 1/SC 42 «Artificial Intelligence». Основной задачей комитета является формирование универсальных технических и управленческих рамок, обеспечивающих этичное, надежное и подотчетное применение ИИ в различных отраслях.

Принципы, лежащие в основе стандартов ISO в сфере ИИ, включают: обеспечение прозрачности и объяснимости алгоритмов; соблюдение принципов справедливости и недискриминации; управление рисками и устойчивостью ИИ-систем; обеспечение совместимости и интероперабельности; поддержание человеческого контроля и подотчетности.

Стандарт ISO/IEC 42001-2023 «Artificial Intelligence Management System (AIMS)» («Информационные технологии. Искусственный интеллект. Система менеджмента») призван помочь организациям в разработке, предоставлении и применении системы искусственного интеллекта, определяя руководящие положения по его созданию, внедрению, поддержанию и совершенствованию.

Наряду с указанными, среди основных международных стандартов в сфере ИИ выделяют следующие[34]:

- ISO/IEC 4213 – Информационные технологии, ИИ, оценки классификации машинного обучения;
- ISO/IEC 5338 – Информационные технологии, ИИ, процессы жизненного цикла системы ИИ;
- ISO/IEC 23894-2 – Информационные технологии, ИИ, управление рисками;
- ISO/IEC 24027 – Информационные технологии, предвзятость в системах искусственного интеллекта и с использованием ИИ;
- ISO/IEC 38507 – Информационные технологии, управление ИИ, последствия использования систем ИИ.

Преимуществами стандартов ISO в сфере ИИ являются:

- глобальная применимость: стандарты разрабатываются с учетом многообразия правовых и культурных контекстов;
- техническая нейтральность: акцент на функциональность, а не на конкретные технологии;
- поддержка правового регулирования: стандарты могут использоваться как основа для национальных законов и сертификационных процедур;

[34] ISO/IEC. Artificial Intelligence – Risk Management: ISO/IEC 23894:2023 [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/77608.html – (дата обращения: 01.07.2025).

- интеграция с другими инициативами: согласуются с подходами ОЭСР, ЮНЕСКО, ЕС и ООН.

Вместе с тем в стандартах ISO можно отметить и определенные вызовы, к примеру, потенциальное отставание от технологических реалий, а именно длительный цикл разработки стандартов, который может не успевать за быстрым развитием ИИ.

Помимо этого, ограниченная транспарентность разработки – участие в рабочих группах требует членства и ресурсов, что может ограничивать доступ стран с низким уровнем вовлеченности.

Недостаточная адаптация к правовым системам является еще одним аспектом по реализации, так как стандарты требуют трансформации в национальные нормативные акты для эффективного применения. При этом стандарты имеют добровольный характер и не являются юридически обязательными.

Таким образом международные стандарты ISO в области ИИ представляют собой фундаментальный элемент глобальной нормативной инфраструктуры, обеспечивающий техническую совместимость, управляемость и этическую устойчивость ИИ-систем. Несмотря на их необязательный характер, они выполняют функцию опосредованного регулирования, способствуя гармонизации подходов и снижению рисков, связанных с внедрением ИИ в чувствительные сферы, включая правоохранительную деятельность. В условиях отсутствия универсального международного договора по ИИ стандарты ISO становятся важным инструментом «мягкого права», способствующим формированию доверия, прозрачности и ответственности в цифровую эпоху.

В **Совете Европы** в мае 2024 года была принята **Рамочная конвенция об искусственном интеллекте, правах человека, демократии и верховенстве права**[35] – первый в Европе международный договор, содержащий обязательства государств. Конвенция предусматривает три всеобъемлющих гарантии: защиту прав человека, демократии и верховенства закона, включая регулирование рисков на всех стадиях жизненного цикла ИИ-систем.

Конвенция была открыта для подписания 5 сентября 2024 года на Конференции министров юстиции в Вильнюсе. Среди первых подписантов – государства-члены Совета Европы (например, Великобритания, Норвегия, Грузия, Молдова), а также страны-наблюдатели и партнеры (США, Израиль, Япония, ЕС и др.). Документ разработан в рамках работы Комитета по искусственному интеллекту (CAI), созданного в 2022 году на базе Специального комитета CAHAI, действовавшего с 2019 года.

Конвенция охватывает весь жизненный цикл ИИ-систем – от проектирования и разработки до внедрения, эксплуатации и вывода из эксплуатации. Ее положения распространяются как на государственный, так и на

[35] Совет Европы. Рамочная конвенция об искусственном интеллекте, правах человека, демократии и верховенстве права (CETS № 225) [Электронный ресурс]. – Страсбург: Совет Европы, 2024. – Режим доступа: https://www.coe.int/en/web/artificial-intelligence/convention – (дата обращения: 01.07.2025).

частный сектор, при этом государства могут самостоятельно определить объем обязательств в отношении последнего.

Ключевыми элементами Конвенции являются три универсальные гарантии:

- защита прав человека, включая право на неприкосновенность частной жизни, свободу выражения мнений, защиту от дискриминации;

- сохранение демократических институтов, включая прозрачность, участие и подотчетность;

- соблюдение принципа верховенства права, включая доступ к правосудию, правовую определенность и эффективные средства правовой защиты.

Наряду с указанным, Конвенция закрепляет принцип технологической нейтральности, что обеспечивает ее устойчивость к будущим технологическим изменениям; допускает вариативность имплементации, позволяя государствам адаптировать положения к национальным правовым системам; не распространяется на сферы национальной безопасности, обороны и фундаментальных научных исследований.

Документ является юридически обязательным к исполнению сторонами ратификации. В отличие от soft law-документов, Рекомендаций ОЭСР или ЮНЕСКО, Конвенция обладает статусом международного договора, подлежащего ратификации и исполнению.

Конвенция согласуется с Регламентом ЕС об ИИ (AI Act), усиливая правовую архитектуру в Европе и имеет системный подход к рискам: охватываются все стадии жизненного цикла ИИ, включая оценку воздействия, аудит и механизмы правовой защиты.

При этом рисковой стороной документа видится гибкость формулировок, которая может привести к различной интерпретации и фрагментарной имплементации.

Отсутствие перечня запрещенных ИИ-систем указывает на самостоятельность их определения государствами самостоятельно, что может ослабить единообразие регулирования ИИ.

На территории Европейского Союза поэтапно (с 2025 по 2027 гг.) вступает в силу **Закон Европейского Союза «Об искусственном интеллекте», или Регламент (ЕС) 2024/1689 – «Об искусственном интеллекте» (AI Act)**.

Регламент, известный как AI Act, представляет собой единую нормативно-правовую основу, регулирующую разработку, внедрение и применение ИИ-систем на едином рынке Европейского Союза. Его ключевая цель – обеспечить достоверность, безопасность, защиту фундаментальных прав и этических стандартов при использовании ИИ.

Закон был предложен Европейской Комиссией в апреле 2021 г., утвержден Европарламентом 13 марта 2024 г. и одобрен Советом ЕС 21 мая 2024 г.

Его юрисдикционное поле охватывает все государства-члены ЕС (27 стран). Также закон имеет экстерриториальный эффект: распространяется на любые организации, вне зависимости от места регистрации, если их деятельность затрагивает граждан ЕС или связана с ЕС рынками.

Основные принципы:

- риск-ориентированный подход: четыре категории ИИ – от «неприемлемого» до «минимального» риска;

- запрет недопустимых практик: социальный рейтинг, манипуляция, предиктивная полиция, распознавание лиц и эмоций запрещены, за исключением строго ограниченных случаев правоохранения;

- ограничения на системы высокого риска: обязательны оценка воздействия, обеспечение прозрачности, надзор, сертификация и соответствие стандартам;

- прозрачность и маркировка: пользователи должны быть проинформированы о взаимодействии с ИИ, агенты генеративного ИИ – маркироваться;

- гарантия человеческого контроля: при принятии решений – обязательно участие человека; в случае ИИ-ошибок – возможность обжалования;

- многоуровневая система надзора: включает Европейское AI Office, национальные органы надзора, ЕАИБ, панель экспертов и консультативный форум.

Преимуществами закона являются унификация правовых подходов и повышение правовой определенности для разработчиков и поставщиков услуг; усиление защиты фундаментальных прав, включая неприкосновенность частной жизни и борьбу с дискриминацией; поощрение инноваций через «регуляторные песочницы» и поддержку стартапов при соблюдении требований; создание глобального стимула к стандартизации: EU-феномен («Brussels Effect»).

Вместе с тем имеются недостатки и ограничения. К таким аспектам можно отнести высокую административную нагрузку и расходы на соответствие нормативам, особенно для малых и средних предприятий, неоднозначность элементов регулирования, таких как объяснимость, киберустойчивость и масштабируемость, требующие вынесения дополнительных регуляторных актов; фрагментарность исполнения на уровне стран-членов – риск разного применения норм членами союза.

На сегодняшний день имеются риски ограничения инновационной деятельности, так как некоторые компании призывают отложить применение закона.

Например, как сообщает агентство Reuters, многие технологические гиганты, включая Alphabet, Meta, Mistral AI и ASML, обращались в Европейскую комиссию с просьбой отложить вступление в силу AI Act, утверждая, что это нанесет ущерб конкурентоспособности Европы в быстро развивающейся сфере ИИ. Однако представители Европейской комиссии против паузы по вступлению в силу закона[36].

Закон об ИИ представляет собой регулирование, основанное на оценке рисков применения искусственного интеллекта. Он полностью запрещает ряд «неприемлемых» сценариев использования, таких как манипулирование

[36]https://www.ixbt.com/news/2025/07/05/es-ne-drognul-zakon-ob-ii-vstupit-v-silu-nesmotrja-na-protesty-tehnogigantov.html – (дата обращения: 01.07.2025).

поведением или социальный рейтинг. Также AI Act определяет категории «высокого риска», включая биометрию и распознавание лиц, а также применение ИИ в сферах образования и занятости. Разработчики приложений будут обязаны регистрировать свои системы и соблюдать требования к управлению рисками и качеством для получения доступа к рынку ЕС.

Отдельную категорию составляют приложения ИИ с «ограниченным риском», такие как чат-боты, к которым применяются менее строгие требования к прозрачности.

Европейский Союз начал поэтапное внедрение AI Act в прошлом году, при этом полное вступление в силу всех положений запланировано на середину 2026 года. Это решение, безусловно, повлияет на стратегии компаний, работающих с ИИ в Европе и планирующих выход на европейский рынок.

Полагаем, высокие требования коснутся и разработчиков систем ИИ для правоохранительного блока. Так, системы распознавания лиц, анализ доказательств, предиктивный полицейский контроль и др. требуют соблюдения строгих стандартов, они теперь относятся к «высокорисковой классификации».

Строгих запретов и исключений коснется реальное время распознавания лиц и оценка эмоций, они теперь запрещены без особых обстоятельств (угроза терроризма, поиск пропавших).

В судебном/административном разрешении будет действовать ограниченный масштаб применения и обязательный надзор при использовании RBI (автоматическое распознавание биометрических параметров).

К отдельным ограничительным аспектам можно отнести нехватку временных ресурсов для правоохранительной и судебных сфер, так как сертификация ИИ требует времени, компетенций и финансирования, требование объяснимости и возможности обжалования судебных решений на базе ИИ, они должны быть прозрачны и основаны на человеческой оценке.

Регламент AI Act – это значительный шаг вперед, направленный на гарантированную безопасность, уважение прав и этические стандарты в применении ИИ. Однако его комплексность, адаптация национальных механизмов и вопросы исполнении могут стать препятствиями. Особенно это актуально для правоохранительной области, где необходимо найти баланс между эффективностью и соблюдением прав человека, обеспечивая достаточное финансирование и экспертную поддержку при внедрении ИИ.

Таким образом, наблюдается отчетливая региональная тенденция перехода «мягкого права» (рекомендаций, этических норм и стандартов) к выработке обязательных правовых механизмов «жесткого права».

Основными направлениями развития остаются: уточнение понятийного аппарата – защита прав человека, управление трансграничными рисками, формирование глобальных институтов регулирования.

Анализ основополагающих международных инициатив – Рекомендаций ОЭСР и ЮНЕСКО, мер, принятых в рамках ООН, международных стандартов ISO/IEC, а также Регламента Европейского Союза AI Act, позволяет

констатировать, что к настоящему моменту сложилось ядро многоуровневой нормативной архитектуры, регулирующей сферу ИИ. Эти инициативы представляют собой различные формы нормативного воздействия: от soft law до binding regulation, обеспечивающие как концептуальную, так и операционную легитимность технологий ИИ.

Рекомендации ОЭСР и ЮНЕСКО формируют универсальную этическую основу, ориентированную на обеспечение транспарентности, прав человека и устойчивого развития. Они способствуют выстраиванию нормативной культуры ответственного обращения с ИИ и служат фундаментом для национальных и региональных стратегий. Особое значение приобретают положения, связанные с человеческим контролем, недискриминацией, объяснимостью и безопасностью, что особенно актуально в сфере правоохранительной деятельности, подверженной высоким регуляторным и гуманистическим рискам.

В свою очередь, деятельность ООН отражает институциональное стремление к координации глобального цифрового управления, включая формирование архитектуры подотчетности, снижение технологического неравенства и профилактику угроз международной безопасности. Предложенные ООН меры по созданию международных структур, научных групп и обмену стандартами представляют собой начало институционализации диалога и перехода от этических рамок к правовым формам международного регулирования.

Международные стандарты ISO/IEC обеспечивают техническую нейтральность, управляемость и совместимость ИИ-систем, содействуя формализации практик и поддержке национального правового регулирования. Они особенно важны для правоохранительных органов как база для построения процедур аудита, контроля качества данных, минимизации предвзятости и оценки рисков.

Регламент Европейского Союза AI Act воплощает нормативную конкретизацию, отражая переход к юридически обязательным механизмам регулирования. Его риск-ориентированная модель, запрет недопустимых практик и система многоуровневого надзора являются образцом правового подхода к цифровым технологиям. Особо значимы положения, касающиеся ИИ высокого риска в правоохранительной сфере, что обеспечивает соблюдение фундаментальных прав личности и институциональную устойчивость.

Таким образом, в условиях становления цифрового правопорядка международные инициативы по ИИ представляют собой комплексный нормативный ландшафт, сочетающий этические принципы, технические стандарты и правовые механизмы. Для правоохранительной практики это означает необходимость внедрения ИИ в рамках четко определенных организационно-правовых и ценностных ограничений. Только соблюдение этих условий позволяет обеспечить легитимность, справедливость и доверие общества к институтам цифрового правосудия.

Вместе с тем, рассматривая вопрос об имплементации норм международных рекомендаций, необходимо учитывать национальные интересы каждой страны в отдельности, региональные аспекты и технологическую зрелость.

Выводы главы 1

Анализ понятийного аппарата и правовой природы ИИ-технологий показал, что несмотря на наличие общих функциональных характеристик (восприятие, обработка данных, обучение и принятие решений), существующие международные определения остаются фрагментарными и недостаточно универсальными для эффективного правового регулирования. Различия в подходах национальных и международных правовых систем затрудняют выработку единых стандартов, особенно в условиях правовой инерции на постсоветском пространстве. В этой связи предлагаются скомпилированные универсальные определения ИИ, направленные на устранение понятийной неопределенности и обеспечение нормативной применимости в различных юрисдикциях.

Функциональный анализ внедрения ИИ в сферу деятельности органов прокуратуры демонстрирует, что цифровизация в данном контексте представляет собой не просто технологическое нововведение, а фундаментальный институциональный и философский вызов, затрагивающий основы правоприменения, нормативной субъектности и этики государственной власти. Интеграция алгоритмических решений трансформирует логику правового регулирования, смещая акценты с индивидуального правосознания на формализованную машинную интерпретацию, что порождает риски отчуждения субъекта, эрозии правовых ценностей и подмены юридической ответственности функциональной рациональностью.

В этих условиях особенно актуальной становится необходимость строгой нормативно-этической регламентации применения ИИ, обеспечивающей приоритет гуманистических принципов и соблюдение пределов допустимости алгоритмического вмешательства в процессы, имеющие правовое и моральное значение. Центральной задачей становится сохранение человеческого измерения права, где ключевая роль в принятии окончательных решений остается за человеком, наделенным моральной ответственностью, правовой чувствительностью и способностью к справедливому суждению. Концепция «human in the loop» выступает не просто технической мерой, а этическим императивом, обеспечивающим легитимность и доверие к системе правоприменения в условиях цифровой трансформации.

Тем самым, устойчивое и этически оправданное включение ИИ в деятельность органов прокуратуры возможно лишь при условии целенаправленного нормативного осмысления, философской рефлексии и институционального переустройства, ориентированного на укрепление правовой справедливости, публичной ответственности и защиты человеческого достоинства. Перспективное исследование в этом направлении требует детального анализа понятийных и регулятивных основ использования информационных

технологий в прокурорской практике, особенно в контексте правовых систем государств-участников СНГ.

Исследование международных стандартов применения ИИ в правоохранительной деятельности выявило устойчивую тенденцию перехода от этико-рекомендательных подходов к формированию юридически обязательных норм. В условиях становления цифрового правопорядка складывается многоуровневая нормативная архитектура, включающая soft law, технические стандарты ISO/IEC и документы «жесткого права», такие как AI Act ЕС. Эти инициативы обеспечивают легитимность и управляемость ИИ-систем, особенно в чувствительных сферах, включая правоохранительную. Внедрение ИИ требует строгого соблюдения правовых и этических ограничений, с учетом национальных интересов, региональной специфики и уровня технологической зрелости.

В условиях становления цифрового правопорядка международные инициативы по ИИ представляют собой комплексный нормативный ландшафт, сочетающий этические принципы, технические стандарты и правовые механизмы. Для правоохранительной практики это означает необходимость внедрения ИИ в рамках четко определенных организационно-правовых и ценностных ограничений. Только соблюдение этих условий позволяет обеспечить легитимность, справедливость и доверие общества к институтам цифрового правосудия.

Вместе с тем, рассматривая вопрос об имплементации норм международных рекомендаций, необходимо учитывать национальные интересы каждой страны в отдельности, региональные аспекты, степень технологической и практической зрелости.

ГЛАВА 2. СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОКУРОРСКОЙ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВ СНГ

§ 2.1 Анализ действующего законодательства и правоприменительной практики в сфере искусственного интеллекта

В государствах-участниках СНГ предпринимаются шаги по созданию нормативно-правовой базы для регулирования технологий ИИ.

Одной из ключевых инициатив и документов, направленных на регулирование ИИ в государствах-участниках СНГ, является **Модельный закон СНГ** об искусственном интеллекте, принятый на 58 пленарном заседании Межпарламентской Ассамблеи СНГ 18 апреля 2025 года[37].

Целью модельного закона является содействие формированию единых подходов к системе правового регулирования общественных отношений, возникающих в связи с использованием технологий ИИ, которые ориентированы на приоритет человека и направлены на улучшение качества его жизни, безопасности, а также повышение эффективности национальных экономик государств-участников СНГ за счет стимулирования разработки, внедрения и использования ИИ.

Действие модельного закона распространяется на технологии ИИ и системы с их использованием, кроме технологий и систем для военных и оборонных целей. Закон направлен в парламенты государств-участников МПА СНГ для имплементации в национальном законодательстве.

Принятие закона стало важным шагом к формированию единого подхода к правовому регулированию ИИ на пространстве СНГ.

Основной целью закона является также унификация законодательства государств-участников в сфере ИИ. Он устанавливает правила управления рисками использования ИИ, обработки данных, защиты прав потребителей и ответственности за нарушения. Разработка закона осуществлялась Объединенным институтом проблем информатики Национальной академии наук Беларуси.

9 декабря 2024 года постановлением № 17-7.5 **Парламентской ассамблеи Организации Договора о коллективной безопасности (ОДКБ)** приняты Рекомендации для государств-членов ОДКБ по выработке общих принципов развития национального законодательства в области создания ИИ и робототехники в целях обеспечения национальной безопасности.

В основу регулирования ИИ в целях обеспечения национальной безопасности в государствах-членах ОДКБ рекомендовано заложить принципы законности, уважения и защиты прав и свобод человека, баланса развития и безопасности, государственного контроля, обмена информацией, прозрачности и

[37]Модельный закон «О технологиях искусственного интеллекта», принят Межпарламентской Ассамблеей СНГ/ [Электронный ресурс] – Режим доступа: https://uiip.basnet.by/rus/news/438/_(дата обращения: 02.07.2025).

понятности, человеческого контроля, непрерывности, технологического суверенитета, доступности.

Как уже было отмечено, в странах СНГ внедрение технологий ИИ в деятельность органов прокуратуры рассматривается как одно из перспективных и быстроразвивающихся направлений цифровой трансформации.

Вместе с тем ИИ в странах СНГ еще не внедрен в деятельность органов прокуратуры и наблюдаются лишь попытки его интегрирования, а также тестирования отдельных элементов «слабого» ИИ. При этом страны СНГ уже принимают стратегические и программные документы, предусматривающие внедрение и применение систем ИИ, в том числе и в органах прокуратуры.

Среди стран СНГ в части правового регулирования ИИ значительных успехов достигла **Российская Федерация**. В стране принято несколько комплексных правовых документов, определивших концептуальные основы внедрения и развития ИИ.

Так, в 2019 году утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года[38]. Она направлена на создание благоприятных условий для внедрения и развития технологий искусственного интеллекта в различных секторах экономики и государственного управления. Ключевыми целями стратегии являются стимулирование инноваций, развитие научных исследований в сфере ИИ, создание благоприятных условий для подготовки квалифицированных специалистов, укрепление нормативно-правовой базы для регулирования ИИ, а также повышение международной конкурентоспособности страны.

Одновременно в 2020 году принят Федеральный закон по проведению эксперимента и внедрению технологий искусственного интеллекта[39]. В данном законе впервые на постсоветском пространстве было выработано понятие искусственного интеллекта.

Значительно серьезнее в РФ продвинулось нормативно-техническое регулирование в сфере ИИ. В настоящее время принят ряд ГОСТов, посвященных искусственному интеллекту. К примеру, «ГОСТ Р 59276-2020. Национальный стандарт Российской Федерации. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» и другие. Подобные стандарты разрабатываются специальным комитетом «ТК-164» при Росстандарте[40]. В **Кыргызской Республике** в 2024 году принята Концепция цифровой

[38] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») / [Электронный ресурс] – Режим доступа: https://base.garant.ru/72838946/_(дата обращения: 23.09.2024).

[39] Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"» от 24 апреля 2020 г. № 123-ФЗ принятый Государственной Думой 14 апреля 2020 г. и одобрен Советом Федерации 17 апреля 2020 г. / [Электронный ресурс] – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW _351127/_(дата обращения: 23.09.2024).

[40] Приказ Росстандарта № 1732 от 25 июля 2019 г. О создании технического комитета по стандартизации «Искусственный интеллект» / [Электронный ресурс] – Режим доступа: https://disk.yandex.ru/i/43so MCH64SAFbQ _(дата обращения: 23.09.2024).

трансформации Кыргызской Республики на 2024-2028 годы[41]. В плане по ее реализации среди ключевых мер предусмотрено развитие ИИ.

Кроме того, в целях комплексного внедрения технологий ИИ в Кыргызской Республике ведется разработка единого Цифрового кодекса. При создании этого акта были учтены многочисленные международные стандарты и документы, которые на протяжении нескольких лет успешно используются на практике в странах Запада.

Проект Цифрового кодекса вобрал в себя положения ряда законов Кыргызской Республики, в частности, законов «Об электронном управлении», «Об электронной подписи», «О биометрической регистрации граждан», «Об информации персонального характера» и «Об электрической связи», а также иные инструкции и положения, затрагивающие вопросы цифровизации.

Особо важным моментом названного Кодекса является то, что в нем подробно регулируются вопросы, связанные с ИИ. Отдельная глава Кодекса подробно рассматривает базовые аспекты создания, разработки и использования систем ИИ, включая принципы, регулирующие эти процессы, а также определяет ограничения и меры ответственности, связанные с их разработкой и эксплуатацией.

На сегодня проект Кодекса получил положительную оценку со стороны Рабочей группы ЮНСИТРАЛ (Комиссия ООН по праву международной торговли).

Ряд концептуальных стратегических документов принят и в **Республике Узбекистан**.

В 2020 году Президент Узбекистана утвердил Стратегию «Цифровой Узбекистан – 2030»[42], которая направлена на продвижение информационно-коммуникационных технологий и внедрение современных цифровых инноваций, включая системы ИИ. В целях ее реализации 17 февраля 2022 года было издано специальное Постановление Президента Республики Узбекистан.

В рамках этого Постановления заложены следующие меры:

- в первую очередь создание правовой основы, которая будет регулировать единые требования, ответственность, безопасность и прозрачность в процессе создания и использования технологий ИИ;

- создание списка проектов и сфер для внедрения технологий ИИ;

- создание НИИ по вопросам ИИ при Министерстве по развитию информационных технологий и коммуникаций;

- создание в структуре вышеуказанного Министерства нового подразделения – департамента по внедрению и развитию технологий ИИ;

---

[41] Указ Президента Кыргызской Республики от 5 апреля 2024 г. УП №90 «Об утверждении Концепции цифровой трансформации Кыргызской Республики на 2024-2028 годы» / [Электронный ресурс] – Режим доступа: https://cbd.minjust.gov.kg/5-10577/edition/6413/ru_(дата обращения: 23.09.2024).

[42] Указ Президента Республики Узбекистан от 5 октября 2020 г. № УП-6079 «Об утверждении Стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации» / [Электронный ресурс] – Режим доступа: https://lex.uz/docs/5031048?ONDATE=02.04.2021&ONDATE2=12.08.2021&action=compare_(дата обращения: 23.09.2024).

- внедрение международных стандартов в области ИИ в национальную систему.

В Республике Казахстан принято значительное количество законодательных и стратегических документов, которые составляют прочную основу для развития информатизации и технологий ИИ.

По состоянию на июль 2025 года в Казахстане действуют следующие правовые акты, регламентирующие данную сферу:

- Закон РК от 24 ноября 2015 года «Об информатизации», включает нормы, касающиеся использования «открытых данных» и «персональных данных», а также содержит положения, регулирующие объекты информатизации, связанные с критически важной инфраструктурой и другими аспектами;

- Закон РК от 5 июля 2004 года «О связи», включает положения, которые регулируют вопросы создания инфраструктуры для обеспечения доступа к телекоммуникационным услугам;

- Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства РК от 20 декабря 2016 года, устанавливают критерии обеспечения информационной безопасности;

- Требования по управлению данными, утвержденные приказом МЦРИАП РК от 14 октября 2022 года, закрепляют положения, касающиеся дифференцированного подхода к управлению данными с учетом особенностей различных отраслей;

- Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы, определяет ключевые меры, необходимые для продвижения ИИ.

- Концепция развития искусственного интеллекта на 2024-2029 годы, определяет ключевые принципы, подходы и направления его развития в стране, а также представляет План действий для ее реализации.

Для достижения поставленных задач по развитию данной области в стране был создан Комитет по искусственному интеллекту и инновациям при МЦРИАП РК. Основные функции данного ведомства включают формирование и реализацию государственной политики, а также создание условий для продвижения ИИ.

Мажилис Парламента Республики Казахстан в мае 2025 г. в первом чтении принял Закон Республики Казахстан «Об искусственном интеллекте», в работе Цифровой кодекс Республики Казахстан[43].

Целью закона являются обеспечение развития ИИ и стимулирование его внедрения в различных областях для улучшения качества жизни человека и повышения эффективности экономики.

Основными положениями являются правовое и организационное регулирование использования ИИ, обеспечение прозрачности и безопасности,

[43] https://orda.kz/v-kazahstane-prinjali-zakon-ob-iskusstvennom-intellekte-401685/ (дата обращения: 08.07.2024).

нормы для работы с ИИ в государственных органах и квазисекторе, уточнение прав и обязанностей всех участников ИИ-среды, расширение полномочий Правительства Республики Казахстан по формированию государственной политики в этой сфере.

Закон определяет роль государства в вопросах внедрения ИИ в разных отраслях экономики, а также устанавливает базовые принципы регулирования общественных отношений в сфере ИИ.

Важным аспектом закона является введение правового режима систем ИИ. В зависимости от степени воздействия на безопасность пользователей, общество и государство, они подразделяются на системы:

1) минимального риска – нарушение или прекращение функционирования которых окажет минимальное влияние на их пользователей;

2) среднего риска – нарушение или прекращение функционирования, которых может привести к снижению эффективности и результативности деятельности пользователей, и может нанести материальный ущерб;

3) высокого риска – нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, пользователей, инфраструктуры Республики Казахстан, жизнедеятельности физических лиц.

Системы ИИ высокого риска подлежат включению в перечень критически важных объектов информационно-коммуникационной инфраструктуры в соответствии правилами и критериями отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры, утвержденными уполномоченным органом в сфере обеспечения информационной безопасности.

Принципами закона являются в первую очередь – законность, справедливость и равенство, прозрачность и объяснимость, ответственность и подконтрольность, приоритет благополучия человека, свободы воли в принятии им решений, защита конфиденциальности и данных, безопасность и защищенность.

Важной частью законопроекта является Национальная платформа ИИ-единая инфраструктура для разработки и использования продуктов с ИИ. Платформа будет обеспечивать и формировать доступ разработчиков к библиотекам данных для обучения моделей ИИ.

Несмотря на наличие значительного количества правовых актов в Казахстане существует ряд вопросов внедрения ИИ, которые требуют своего разрешения:

Во-первых, в Казахстане только вводится понятие искусственного интеллекта. Это не только препятствует внедрению проектов с применением ИИ, но и создает в обществе сложности восприятия функций и возможностей применения ИИ-систем. Многие государственные структуры в погоне за

цифровизацией любые информационные системы, содержащие автоматизированные алгоритмы, выдают за систему с ИИ.

Во-вторых, **наряду с отсутствием понятийного аппарата, в стране не** регламентированы **этические вопросы** применения ИИ. К примеру, на сегодня в Казахстане, как и в большинстве стран мира, остается открытым вопрос относительно института интеллектуальной собственности.

В-третьих, **в стране еще не сформулировано четкое понимание сферы** регулирования ИИ. Недостаток регулирования отношений между участниками сферы ИИ включает неопределенность в компетенциях государственных органов, а также в правах, обязанностях и ответственности всех субъектов в данной области.

В-четвертых, **в Казахстане еще не разработан технический регламент** или государственный **стандарт,** который бы регулировал сферу технологий ИИ.

На территории СНГ, как и во всем мире, существуют определенные сложности при внедрении ИИ как в работу прокурора в частности, так и в правоохранительную и судебную сферы в целом.

Внедрение ИИ в сферы государственного управления и правоохранительной деятельности сопровождается как потенциалом значительного повышения эффективности, так и серьезными рисками трансформации основополагающих принципов демократического правопорядка. Возникает концепт так называемого государства машинного обучения (Machine-Learning State), в котором аналитические и прогностические возможности ИИ радикально изменяют характер взаимоотношений между государством и гражданином.

Современные ИИ-системы позволяют государству в реальном времени собирать, интерпретировать и использовать поведенческие данные граждан. Такие возможности могут укрепить управленческий потенциал, однако одновременно несут угрозу чрезмерной концентрации власти и потери индивидуальной автономии. При отсутствии нормативных и институциональных сдержек это может привести к смещению акцентов от конституционно закрепленного приоритета прав и свобод личности в сторону тоталитарной рациональности, основанной на алгоритмическом контроле.

Исследователи в сфере ИИ опасаются дегуманизации принятия решений, утраты прозрачности и подотчетности публичной власти, формирования «черных ящиков» алгоритмического управления, не поддающихся общественному контролю.

В условиях активного внедрения ИИ-систем в деятельность публичной власти требуется институционализация норм конституционного и отраслевого права, закрепляющих принцип верховенства права и прав человека при использовании ИИ, прозрачности алгоритмических решений, разработки механизмов юридической и этической подотчетности ИИ, введение обязанности государства обеспечивать научную экспертизу и независимый контроль.

Актуальной становится идея «публичного конституционного ИИ», который на этапе проектирования должен включать алгоритмическое уважение к основополагающим правам и принципам – праву на личную автономию, защиту личной жизни, неприкосновенность частной информации.

Сложность правового регулирования усиливается при рассмотрении длительности существования ИИ-систем. Их способность к самообновлению и накоплению знаний порождает этическую дилемму «права на уничтожение», особенно в случае, если ИИ будет выполнять социально значимые функции в течение неопределенного времени.

Некоторые исследователи предлагают ограничить жизненный цикл ИИ юридически (например, закреплением физической оболочки, ограничением сроков функционирования), тогда как другие указывают на моральную неоднозначность подобных мер, особенно если ИИ приобретет черты автономности, близкие к человеческой.

Развитие нейротехнологий, нейроимплантов и систем когнитивного улучшения предопределяет будущую юридическую и социальную трансформацию. Предполагается возникновение категории граждан с «усиленными» возможностями — так называемых киборгов, обладающих физическими и когнитивными преимуществами.

Это влечет необходимость закрепления равного доступа к технологиям, повышающим человеческий потенциал, определение права на отказ от интеграции с ИИ, разработки конституционных гарантий сохранения биологической природы человека и базовых прав традиционных субъектов права.

Без нормативной проработки этих аспектов возрастает риск усиления социальной стратификации и дискриминации на основе нейротехнологического статуса.

Наиболее активное внедрение ИИ фиксируется в уголовно-правовой сфере. Среди направлений его использования выделяются поиск и систематизация судебной практики, юридическое консультирование и составление типовых процессуальных документов, предиктивная юриспруденция и прогнозирование судебных решений, автоматизация статистической отчетности, помощь следователям и дознавателям в оценке и моделировании криминальной ситуации.

Однако это требует пересмотра принципов уголовно-процессуального права, поскольку автоматизация рискует подорвать гарантии состязательности и гуманистичности, заложенные в современном правосудии.

Имеют место технологические ограничения и методологические барьеры. Так, ИИ по-прежнему ограничен отсутствием семантического и социального интеллекта, необходимого для комплексной юридической интерпретации, недоступностью качественно размеченных репрезентативных данных, невозможностью креативного решения нетипичных задач, выходящих за рамки обучающих выборок, сложностью в правовом представительстве, где коммуникация требует эмпатии и эмоционального интеллекта.

Кроме того, высокие затраты на разработку и обучение ИИ ограничивают его использование кругом финансово состоятельных субъектов, что также может усилить неравенство в доступе к правосудию.

Анализ действующего законодательства и правоприменительной практики в сфере ИИ показывает, что его внедрение в публичное управление и уголовное судопроизводство представляет собой двойственный процесс: с одной стороны, это шаг к цифровой трансформации и эффективности, с другой – вызов гуманистическому и правовому основанию государства. Требуется комплексное нормативное, этическое и научное сопровождение, ориентированное на защиту человека, правовую стабильность и технологическую подотчетность.

Без своевременной адаптации правовой системы риск перехода к государству машинного обучения может дать сложные последствия.

На основе изучения вопросов правового регулирования технологий ИИ полагаем необходимым учесть следующее:

1. Требуется разработка универсального понятия «искусственный интеллект» с учетом технологических аспектов и правовых особенностей национального и международного законодательства.

На сегодня имеются следующие официальные определения ИИ, которые могут быть взяты за основу и учтены в проекте разрабатываемого в Казахстане Закона «Об искусственном интеллекте» (скомпилированные определения, указанные в главе 1.1 – выработаны с учетом нижеприведенных вариантов):

1) «искусственный интеллект – *комплекс технологических решений, позволяющих имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека»*[44];

2) «система искусственного интеллекта – *система на основе машины, предназначенная для работы с различными уровнями автономности, которая может проявлять адаптивность после ее внедрения. Для достижения явных и не явных целей эта система может делать выводы о том, как генерировать выходные данные, такие как прогнозирование, рекомендации и решения, которые могут влиять на физическую и виртуальную среду»*[45];

3) «искусственный интеллект – *означает машинную систему, которая может для заданного набора определенных человеком целей делать прогнозы, рекомендации»*[46];

4) «система искусственного интеллекта – *это система, которая используя модель, делает выводы для получения результатов, включая прогнозы, рекомендации или решения»*[47].

---

[44] Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статью 6 и 10 Федерального закона "О персональных данных"» от 24.04.2020 г. №123-ФЗ.

[45] Закон Европейского союза «Об искусственном интеллекте» (EU Artificial Intelligence Act) принятый Европейским парламентом 13 марта 2024 г. и одобрен Советом ЕС 21 мая 2024 г.

[46] Национальный закон США «Об искусственном интеллекте» 2020 г. (National Artificial Intelligence Act of 2020).

[47] Закон Канады «Об искусственном интеллекте и данных» 2024 г. (Artificial Intelligence and Data Act).

2. При разработке национальных законов, правил и иных правовых актов в сфере ИИ следует руководствоваться основополагающими принципами (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Конвенции ООН и др.), и рассмотреть вопрос о необходимости имплементации значимых норм международных документов (Закон ЕС «Об искусственном интеллекте» 2024 года, Общий регламент по защите персональных данных GDPR и др.), направленных на развитие новых технологий в странах СНГ.

В основе национальных правовых актов должны лежать фундаментальные принципы, гарантирующие право человека на неприкосновенность частной жизни и обеспечивающие гарантию сохранности персональных данных при сборе и обработке информации системами ИИ.

3. Законодательное регулирование систем ИИ должно одновременно сопровождаться мероприятиями, направленными на повышение цифровой грамотности как населения, так и сотрудников правоохранительной и судебной системы. Мероприятия могут включать следующее:

- проведение курсов по основам ИИ, кибергигиене, киберэтике и защите персональной информации в образовательных учреждениях и государственных органах;
- организация вебинаров и семинаров, посвященных вопросам ИИ и кибербезопасности;
- запуск информационных кампаний в СМИ и социальных сетях, направленных на повышение осведомленности о значимости цифровой грамотности;
- создание платформ для онлайн-обучения с доступом к разнообразным учебным материалам и инструментам;
- открытие центров цифрового обучения и консультирования в каждом регионе, обеспеченных необходимыми ресурсами и специалистами;
- организация ежегодных олимпиад и конкурсов по цифровым технологиям как в образовательных учреждениях, так и в государственных организациях;
- проведение исследований и опросов для оценки уровня цифровой грамотности среди населения.

§ 2.2 Сравнительное исследование институциональных моделей внедрения искусственного интеллекта в прокуратурах СНГ

Страны СНГ имеют схожие исторические, правовые и политические предпосылки для развития технологий, что обусловлено общей правовой системой и интеграционными процессами. Однако с точки зрения развития информационных технологий и внедрения ИИ в деятельность органов прокуратуры ситуация значительно отличается.

Если в России уже сформирована нормативная база, включающая федеральный закон, определяющая понятие и принципы использования ИИ, закреплены государственные стандарты в области ИИ, а также проводятся практические эксперименты по его внедрению в правоохранительные органы, то в других странах СНГ ситуация менее однозначна.

В одних государствах разработаны стратегические документы, предусматривающие направления развития ИИ, в других – ИИ остается на стадии обсуждений, без закрепления в нормативных актах или программных документах. Это говорит о том, что развитие технологий в сфере прокурорской деятельности в СНГ идет неравномерно: от активного тестирования и нормативного закрепления в одной стране до концептуального осмысления в другой.

Следующим логическим шагом в нашем исследовании стало изучение информационных технологий, лежащих в основе ИИ, а также практики их внедрения в органах прокуратуры стран СНГ. Здесь мы сосредоточимся на анализе современных информационных технологий и систем ИИ, применяемых в прокурорской деятельности, рассмотрим их функциональные возможности, области использования и перспективы развития в странах СНГ.

Однако прежде чем перейти к анализу конкретных информационных технологий, используемых в органах прокуратуры, необходимо рассмотреть само понятие «информационные технологии» и особенности их правового регулирования в странах СНГ, поскольку именно это определяет рамки их применения и направления развития ИИ.

С точки зрения законодательного понимания, информационные технологии определяются следующим образом.

В **Беларуси** Закон «Об информации, информатизации и защите информации» трактует информационные технологии как совокупность процессов, методов и инструментов, используемых для работы с информацией.

В **России,** согласно Федеральному закону «Об информации, информационных технологиях и о защите информации», информационные технологии – это процессы, методы и средства, применяемые для сбора, обработки, хранения, распространения и использования информации.

В **Казахстане** в Законе «Об информатизации» информационные технологии понимаются как совокупность методов, процессов, программных и технических средств, обеспечивающих выполнение информационных процессов.

В **Кыргызстане** Закон «Об электронном управлении» определяет информационные технологии как технологии, обеспечивающие автоматизированный сбор, обработку, хранение и передачу данных в цифровой форме.

Эти определения формируют правовую основу для использования информационных технологий в различных сферах, включая деятельность органов прокуратуры и позволяют понять, какие подходы применяются в разных странах СНГ.

С научной точки зрения информационные технологии рассматриваются как совокупность методов, программных и аппаратных средств, обеспечивающих обработку и передачу информации. Различные авторы дают свои определения.

Так, В.М. Глушков определяет информационные технологии как совокупность процессов, методов и технических средств, используемых для сбора, хранения, обработки и передачи информации с целью удовлетворения информационных потребностей общества[48].

Г.А. Титоренко подчеркивает, что информационные технологии – это не просто средства обработки данных, а важнейший элемент цифровой трансформации, изменяющий структуру управления, взаимодействия и принятия решений в государственных и частных структурах[49].

Научные подходы показывают, что информационные технологии охватывают не только технические, но и управленческие, социальные и правовые аспекты. Их внедрение в деятельность государственных органов, включая органы прокуратуры, требует комплексного подхода, учитывающего нормативные, организационные и технологические факторы.

Остановимся на примерах использования информационных технологий в органах прокуратуры Республики Казахстан, Российской Федерации, Республики Беларусь и Кыргызской Республики.

Республика Казахстан. В соответствии со статьей 83 Конституции Республики Казахстан и статьей 1 Конституционного закона Республики Казахстан «О прокуратуре» прокуратура от имени государства в установленных законом пределах и формах осуществляет высший надзор за соблюдением законности на территории Республики Казахстан, представляет интересы государства в суде и от имени государства осуществляет уголовное преследование.

Для эффективной реализации поставленных целей и задач в надзорной деятельности органами прокуратуры активно внедряются и используются различные информационные технологии, в том числе с элементами ИИ.

Генеральной прокуратурой в рамках Государственной программы «Цифровой Казахстан» было создано и внедрено 4 цифровых проекта по автоматизации уголовного и административного процессов, назначения проверок, работы с обращениями, что позволяет внедрять новые модели взаимоотношений с гражданами, обеспечить общественную безопасность и законность в стране.

Так, с 2015 года реализована автоматизированная база данных «Единый реестр досудебных расследований» (ЕРДР), предназначенная для регистрации уголовных правонарушений, расследования уголовных дел (в том числе в электронном формате), прокурорского надзора за ходом досудебного расследования и направления уголовных дел в суд.

---

[48] Глушко В.М. Информационные технологии в практике современного управления // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент» / [Электронный ресурс]: Режим доступа: https://cyberleninka.ru/article/n/teoriya-akademika-v-m-glushkova-i-informatsionnye-tehnologii-v-praktike-sovremennogo-upravleniya_(дата обращения 18.02.2025).

[49] Титоренко Г.А. Информационные технологии управления: Учебное пособие / [Электронный ресурс] – Режим доступа: http://library.lgaki.info: pdf _(дата обращения: 20.01.2025).

ЕРДР интегрирован с 13 информационными системами и базами данных, в том числе других госорганов, такиими как ИС Верховного Суда РК «Төрелік», базы данных государственных органов через СИО ПСО, ИС «ЕРАП», ИС «ЕРСОП», система «Е-Экспертиза» и «Е-Заң көмегі» Министерства юстиции и т.д.

На его базе создан функционал «Е-уголовное дело» (Е-УД), который позволяет расследовать и рассматривать дела в суде в электронном формате.

Внедрение ЕРДР позволило:

- исключить случайные ошибки, связанные с определением категории тяжести, квалификацией, анкетными данными, форматом документа и др. (ФЛК, шаблоны);

- обеспечить прозрачность уголовного процесса, то есть принятое процессуальное решение после подписания сразу сохраняется в ЕРДР и доступно для online-просмотра надзирающему прокурору, а также посредством публичного сектора для адвокатов и участников процесса, где имеется возможность подачи ходатайств и жалоб в электронном виде, мониторинга процесса ведения расследования;

- минимизировать риски фальсификации материалов дел, утери уголовных дел, так как все действия «логируются» (фиксируются в системе) в ИС и сохраняются в истории изменений, все электронные документы хранятся на серверах ГП, в том числе резервных, с соблюдением требований информационной безопасности;

- сократить сроки расследования и получения электронных санкций за счет возможности доступа к конкретному уголовному делу в режиме online и обеспечения системного ведомственного контроля и прокурорского надзора, а также автоматизации следственных действий.

В 2020 году отмечена необходимость законодательного возложения на прокурора обязанности согласования ключевых процессуальных решений, затрагивающих права и свободы человека[50]. В этой связи Генеральной прокуратурой совместно со всеми органами досудебного расследования был начат поэтапный переход к полноценной трехзвенной модели уголовного процесса.

С 2021 года все органы следствия и прокуратуры страны перешли на электронное согласование основных решений по уголовному делу. Теперь решения о признании подозреваемым, определении квалификации деяния подозреваемого, квалификации уголовного правонарушения, прерывании сроков досудебного расследования, прекращении, а также обвинительный акт будут считаться незаконными без согласования прокурором.

Законодательными нормами четко определены сроки согласования важных решений прокурором. Более того, электронное согласование позволяет руководству органов следствия и надзирающему прокурору в режиме онлайн контролировать ход расследования уголовных дел. Прокурор, который должен

[50] Послание Президента Республики Казахстан народу Казахстана от 1 сентября 2020 г. «Казахстан в новой реальности: время действий» / [Электронный ресурс] – Режим доступа: https://akorda.kz/ru/addresses/addresses_of_president/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-1-sentyabrya-2020-g_(дата обращения: 19.12.2024).

следить за законностью, включается в процесс не перед поступлением дела к нему, а с самого начала участвует в его расследовании. При электронном согласовании минимизированы манипуляции, что также исключает возможность фальсификации.

В 2019 году разработана информационная система «Единый реестр административных производств» (ЕРАП), в которой автоматизирован весь процесс административного производства, начиная от возбуждения дела и заканчивая исполнением взыскания со снятием ограничений.

ЕРАП интегрирован с 12 информационными системами Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан (КПСиСУ) и других государственных органов.

В настоящее время все субъекты административной практики (67 государственных органов) имеют возможность вести административное производство в электронном формате, в том числе в минимальные сроки составлять административные протокола на планшетах посредством мобильного приложения с вынесением постановления о наложении взыскания.

Внедрение ЕРАП позволило:

- обеспечить неотвратимость наказания за совершение административного правонарушения путем получения SMS-отчета о доставке сообщения о наложенном взыскании правонарушителю через SMS-шлюз портала «Электронного правительства». Такое уведомление о привлечении к административной ответственности признается надлежащим образом доставленным;

- автоматизировать рассылку предписаний о необходимости уплаты штрафа;

- повысить взыскиваемость наложенных штрафов.

Сейчас каждый пользователь смартфона может оплатить штраф на месте совершения правонарушения через мобильные предложения 19 банков второго уровня, банковской картой через терминал или другим удобным способом, при этом штраф автоматически будет погашен.

Кроме того, проектом обеспечено исключение коррупционных рисков и контактов, а также оперативность и прозрачность административного производства.

В целях обеспечения неотвратимости наказания за правонарушения расширяется охват системами фото-, видеофиксации и проводятся интеграции с другими источниками информации об административных правонарушениях.

В рамках модернизации экономики страны Генеральной прокуратурой постоянно принимается комплекс мер по защите бизнеса от незаконных проверок. С этой целью в 2019 году разработана и внедрена система «Единый реестр субъектов и объектов проверок» (ЕРСОП), предназначенная исключать необоснованные, незаконные проверки.

ЕРСОП интегрирован с 6 информационными системами КПСиСУ и других государственных органов. Благодаря системе государственные органы перешли на электронную регистрацию актов о назначении проверок.

Так, с момента запуска системы зарегистрировано более 400 тысяч электронных актов с QR-кодом, с которыми бизнес может ознакомиться онлайн и проверить их подлинность при помощи мобильного приложения «Qamqor».

Заложенные критерии оценки рисков позволяют отбирать недобросовестных предпринимателей без участия «человеческого» фактора в полугодовые графики и списки проверок. Всего автоматизировано в ЕРСОП более 20 тысяч субъективных критериев и 17 тысяч требований проверочных листов.

На платформе «Smart Bridge» размещен универсальный сервис по передаче информации о проверках и их результатах в сфере государственного контроля и надзора.

Составной частью ЕРСОП являются 2 мобильных приложения: «Qamqor» – для предпринимателей и «Teksery» – для проверяющих.

Внедрение ЕРСОП позволило:

- обеспечить прозрачность государственного контроля и надзора;
- оптимизировать процесс планирования проверок;
- сократить коррупционные риски и субъективный подход при назначении проверок;
- обеспечить защиту предпринимателей от необоснованных проверок.

Наряду с вышеуказанными ключевыми цифровыми проектами сотрудники органов прокуратуры Республики Казахстан имеют доступ к следующим информационным системам.

Система информационного обмена для правоохранительных, специальных государственных органов (СИОПСО) – информационная система, позволяющая в автоматическом режиме получать информацию для уголовного, административного, гражданского, исполнительного производства и иной деятельности.

Согласно требованиям статьи 6 Закона Республики Казахстан «О государственной правовой статистике и специальных учетах» КПСиСУ является оператором данной системы.

СИОПСО охватывает 26 государственных органов и организаций и содержит 89 сервисов (сведений баз данных).

Внедрение СИОПСО позволило:

- автоматизировать процессы обмена информацией;
- гарантировать сохранность и безопасность конфиденциальной информации;
- обеспечить легитимность получаемой электронной информации;
- сократить время получения информации;
- повысить эффективность борьбы с преступностью.

Следующая информационная система «Аналитический центр» (АЦ) – является многофункциональным инструментом аналитики и прогнозирования для решения задач органов прокуратуры и государственных органов.

АЦ интегрирована с базами данных других государственных органов.

Реализована возможность публиковать данные на портале Qamqor.gov.kz в виде аналитики для мониторинга правонарушений РК по территориальности, по виду преступления и объекту анализа за определенный промежуток времени, в том числе в виде географической визуализации пространственных данных и форм статистических отчетов путем указания различных критериев (год, месяц, регион, район и др.).

В целом, внедрение АЦ позволило:

- обеспечить доступ к системам КПСиСУ и сведениям из систем государственных органов по принципу «одного окна»;

- аккумулировать разрозненную информацию, формировать специальные учеты и отчеты для анализа и мониторинга соблюдения законности в стране;

- обеспечить визуализацию аналитической информации в формате таблиц, графиков, географических карт, списков с возможностью просмотра источников данных (скачивания процессуальных документов);

- автоматизировать процесс получения аналитической информации.

Заинтересованным государственным органам доступ к информационным базам КПСиСУ для обеспечения своевременной, полной и достоверной информацией, находящейся в ведении правовой статистики и специальных учетов, предоставляется посредством автоматизированной информационной системы «Информационный сервис» (АИС ИС).

АИС ИС интегрирована с 5 информационными системами КПСиСУ (АИС СУ, ЕУСС, ЕУОЛ, ЕРДР, СИОПСО).

Внедрение АИС ИС позволило обеспечить оперативное получение правоохранительными и государственными органами своевременной, полной и достоверной правовой, статистической, аналитической и другой интересующей их информации, находящейся в ведении КПСиСУ, в режиме «онлайн», в том числе сведения о лицах, состоящих на специальных учетах Комитета, лицах, имеющих задолженность перед государством, запросы требования на госслужащих, статистические отчеты и другие данные.

Открытая информация, в том числе сведения о преступности, показателях работы правоохранительных органов, доступна на интернет-портале КПиСУ «Информационный сервис» (Qamqor.gov.kz), где любой желающий при наличии доступа к сети Интернет может получить необходимую ему информацию как об общих тенденциях в сфере правовой статистики, так и касающуюся лично этого человека, а также подать заявление о совершенном уголовном правонарушении или обжаловать какие-то незаконные действия правоохранительного органа.

В 2016 году внедрена электронная «Карта уголовных правонарушений» (http://qamqor.gov.kz). На карте отображается информация о совершенных правонарушениях. Сведения поступают после заполнения сотрудниками полиции

реквизита «Место совершения правонарушения» информационного учетного документа формы Е-1 при регистрации в ЕРДР. Карта преступности находится в свободном доступе для всех интернет-пользователей.

Нажав на любую область, можно увидеть общее количество преступлений. Также имеется возможность более детального изучения сведений по месту совершения, времени или видам преступлений.

Отдельно выделен раздел статистики, где отражена динамика преступности региона. Она позволяет сравнивать области, города, районы по уровню преступности.

Кроме того, указанные сведения используются ситуационными и мониторинговыми центрами акиматов городов и областей для анализа состояния правопорядка.

По аналогии карты уголовных правонарушений внедрено 5 геоинформационных карт:

1) аварийности (ДТП);

2) уголовных правонарушений, совершенных несовершеннолетними;

3) проверок предпринимателей;

4) обращений физических и юридических лиц в государственные органы;

5) лиц, привлеченных к уголовной ответственности за совершение преступлений против половой неприкосновенности несовершеннолетних.

Внедрение геоинформационных карт позволило:

- общественности – контролировать эффективность работы органов внутренних дел;

- сотрудникам полиции – анализировать состояние криминогенности по местоположению;

- гражданам – выбирать наиболее безопасные места проживания, учебы и отдыха;

- местным исполнительным органам – более эффективно планировать и устанавливать уличное освещение, камеры наблюдения, домофоны.

Таким образом, органы прокуратуры Республики Казахстан обладают достаточно обширными базами цифровых платформ, позволяющими оперативно и качественно решать поставленные задачи при осуществлении надзорной деятельности.

Применение ИИ в информационных технологиях органов прокуратуры Республики Казахстан.

Планом действий по реализации Концепции правовой политики, утвержденным постановлением Правительства Республики Казахстан от 29 апреля 2022 года №264, предусмотрено внедрение цифровых и информационных технологий в уголовный процесс. Внедрение подобных цифровых технологий включает и применение элементов ИИ в надзорной деятельности прокуроров.

Так, в рамках электронного уголовного дела внедряется интеллектуальный помощник следователя, который будет подсказывать, какую статью Уголовного кодекса выбрать, какое провести следственное действие, какое решение принять и

т.д. Вместе с тем окончательное процессуальное решение всегда будет оставаться за следователем и прокурором.

Планируется совершенствование функционала «Заңдылық», подсказывающего прокурорам, какую меру наказания, по какой статье необходимо назначить с учетом всех процессуальных моментов, формирует обвинительную речь гособвинителя.

Элементы ИИ внедряются при создании и использовании геоинформационных карт. Все уголовные правонарушения отображаются на карте, с разбивкой по видам, времени совершения и другим параметрам. Этот массив данных позволяет прогнозировать вероятность совершения преступления в том или ином месте, соответственно система позволит строить маршруты патрулирования, расстановку средств и сил полиции.

Аналогично и в профилактике аварийности на дорогах. В режиме реального времени на карте можно установить наиболее аварийные участки дорог, количество и виды ДТП, причины и условия, которые им способствовали. При правильном анализе система будет подсказывать принятие мер для снижения смертности и травматизма на дорогах.

В 2023 году Генеральной прокуратурой начата работа по созданию информационной системы «Мемлекеттік айыптаушы» («Государственный обвинитель») на основе элементов ИИ. Целью этой системы является повышение качества гособвинения при помощи современных информационных технологий.

К преимуществам новой системы также относится: составление проектов документов с использованием ИИ, автоматический расчет наказаний, ведение календаря судебных процессов, уведомление о сроках подачи ходатайств и протестов. Кроме повышения качества гособвинения, внедрение этой системы позволит снизить бумажный документооборот, повысить оперативность принятия решений и обеспечить единообразие судебной практики.

Разработана информационная система «Цифровой надзор».

На первом этапе реализован модуль «Розыск», в котором сформирована единая база разыскиваемых лиц, произведена интеграция с объектами информатизации отдельных государственных органов, транспортных организаций и систем видеонаблюдения, имеющих элементы ИИ по распознаванию лиц.

Продолжается интеграция с базами других государственных органов и организаций, а также системами видеоаналитики.

По цифровым следам и системам видеонаблюдения устанавливаются разыскиваемые преступники, должники, лица, без вести пропавшие и утратившие связь с родственниками.

Теперь правоохранительным органам не нужно искать цифровые следы разыскиваемых лиц по различным базам, это делает система, а прокуроры с помощью системы осуществляют надзор за решениями и действиями инициаторов розыска.

Ведутся доработки технической спецификации по оцифровке надзора за законностью во всех сферах, включая образование, транспорт, жилищно-коммунальное хозяйство, здравоохранение, безопасность, социально-экономическую сферу, строительство, защиту бизнеса.

Система может функционировать с компонентом «Умный город» и базами центральных государственных органов для осуществления надзора за управлением государственным имуществом, повышением эффективности обслуживания населения, профилактики правонарушений, а также функционирования государственных органов. При правильной расстановке задач система будет предупреждать о возможных рисках.

Разработано и введено в работу приложение «Мобильный прокурор» с элементами ИИ для прокуроров, государственных органов и населения. Приложение обеспечивает удаленный доступ прокурора к цифровому рабочему месту, тесный и постоянный контакт с населением, а также оперативное взаимодействие с государственными органами для решения вопросов общества.

По поручению Президента страны МВД и Генеральная прокуратура запустили новый ИИ-проект для ускорения расследований, который: переводит речь в текст; находит противоречия в показаниях; предлагает вопросы для допроса; автоматически готовит документы. Встроены 4 модуля: планирование, анализ показаний, подготовка документов, аналитика.

Таким образом, анализ применения ИИ в органах прокуратуры РК показывает, что в стране создана достаточно широкая технологическая база для развития и внедрения ИИ, ведутся перспективные проекты по его внедрению, которые позволят повысить эффективность надзорной деятельности. Вместе с тем говорить о полноценном внедрении ИИ в деятельность прокуратуры говорить еще преждевременно.

Российская Федерация. Анализ развития и применения информационных технологий, включая ИИ, в Российской Федерации показал, что данному вопросу в стране уделяется особое внимание, в том числе в органах прокуратуры.

Указом Президента Российской Федерации от 21 июля 2020 года № 474 определены основные национальные цели развития Российской Федерации на период до 2030 года, одной из которых является цифровая трансформация.

В органах прокуратуры проект цифровой трансформации реализуется с 2017 года в рамках национальной программы «Цифровая экономика Российской Федерации»[51].

Основными задачами цифровизации органов прокуратуры являются внедрение высокотехнологичного надзора в практическую деятельность органов прокуратуры, создание прозрачной среды взаимодействия органов прокуратуры и граждан, повышение оперативности прокурорского реагирования на нарушения

[51] «Цифровизация деятельности органов прокуратуры». Сборник материалов семинара (круглого стола) / Москва, 30 сентября 2020г. // [Электронный ресурс] – Режим доступа: https://agprf.org/userfiles/ufiles/nii/2021/9.pdf__(дата обращения19.12.2024).

закона, а также координация деятельности правоохранительных органов с использованием цифровых технологий.

В целях реализации указанных задач приказом Генерального прокурора Российской Федерации от 14 сентября 2017 года № 627 утверждена Концепция цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года.

В рамках данной Концепции планируется к 2025 году внедрить ряд инструментов «мягкого искусственного интеллекта» (soft AI), который подходит для выполнения узкоспециальных задач, а также обработки больших массивов данных (big data). ИИ облегчит деятельность прокуратуры, а именно: сократит время в области работы с документами, а также в сфере аналитики и сбора статистических данных.

Технологической основой для внедрения ИИ в органах прокуратуры является расширение возможностей применения различных информационно-аналитических систем. В настоящее время в Генеральной прокуратуре функционирует 12 информационных систем, две из которых государственные.

В ходе масштабной работы по интеграции органов прокуратуры в создаваемую систему цифровой экономики России все органы прокуратуры объединены в единую защищенную сеть передачи данных (ЕЗСПД). В сети созданы два сегмента с разными классами защиты информации – закрытый контур (используемый при работе с информационными системами органов прокуратуры) и открытый контур (используемый при взаимодействии органов прокуратуры с иными государственными органами, а также органами местного самоуправления, юридическими лицами и гражданами).

На сегодня в органах прокуратуры РФ используются различные информационные системы и комплексы, среди которых:

- информационная система межведомственного электронного взаимодействия Генеральной прокуратуры Российской Федерации (ИС МЭВ);

- государственная автоматизированная система правовой статистики (ГАС ПС – использование приостановлено);

- единый портал прокуратуры Российской Федерации (ЕПП);

- портал правовой статистики (crimestat.ru – внесение данных приостановлено);

- федеральная информационная система, предназначенная для организации взаимодействия систем электронного документооборота (СЭД) участников межведомственного электронного документооборота (система межведомственного электронного документооборота – МЭДО);

- федеральная государственная информационная система «Единый реестр контрольных (надзорных) мероприятий» (ЕРКМН);

- федеральная государственная информационная система «Единый реестр проверок» (ЕРП) и др.

Так, с помощью информационной системы межведомственного электронного взаимодействия осуществляется информационное взаимодействие с

Федеральной налоговой службой, Росреестром, МВД России, МЧС России, Минцифры России, Федеральным казначейством, Пенсионным фондом России, Росфинмониторингом, Федеральным агентством лесного хозяйства и другими органами. Это позволяет прокурорским работникам оперативно получать необходимые сведения, содержащиеся в информационных системах других ведомств.

Функциональные возможности федеральной государственной информационной системы «Единый реестр контрольных (надзорных) мероприятий» позволяют своевременно выявлять нарушения порядка проведения органами государственного контроля проверок субъектов предпринимательской деятельности. Ее подсистемный ресурс – федеральная государственная информационная система «Единый реестр проверок», содержит сведения о проводимых контролирующими органами плановых и внеплановых проверках, контрольных закупках, их основаниях и результатах, принятых мерах. Содержащаяся в ЕРКНМ и ЕРП информация используется прокурорскими работниками при оценке законности действий контролеров, даче согласия на проведение проверок, анализе правомерности и своевременности внесения информации в реестр.

Единый портал прокуратуры Российской Федерации является единой точкой доступа к информации и функциям органов прокуратуры для граждан, юридических лиц, индивидуальных предпринимателей и органов государственной власти. В органах прокуратуры созданы условия для направления обращений, а также записи на личный прием в прокуратуру посредством форм Единого портала государственных услуг (ЕПГУ), встроенных в Единый портал прокуратуры.

В органах прокуратуры Российской Федерации используются автоматизированные рабочие места по сервисной модели (АРМ), сервер контроллер домена, сервер резервного копирования, АРМ удаленного пользователя для закрытого и открытого сегментов ЕЗСПД, IP-телефоны, видео-конференц-связи (ВКС), модули медиаресурсов ВКС, голосовые шлюзы, поточные сканеры по сервисной модели, многофункциональные устройства, комплекты сканирующего оборудования, которые повышают эффективность деятельности во всех сферах, в том числе функционирование в цифровой среде.

В 2009 году создана и эксплуатируется автоматизированная информационная система «Архивное дело ОП», которая предназначена для автоматизации ведения номенклатуры дел, их приема в архивное хранение, ведения сводных описей дел.

Для организации единого кадрового учета в органах прокуратуры разработан автоматизированный информационный комплекс «Кадры-ОП», предназначенный для автоматизации деятельности кадровых подразделений, учета, хранения, анализа и выдачи данных об организационно-штатной структуре и работниках органов прокуратуры, формирования отчетов и справок.

Одновременно в Генеральной прокуратуре создается единая база нормативно-правовой информации органов прокуратуры с использованием Системы ведения баз данных Консультант-Плюс.

Для реализации поставленных целей и задач в области цифровизации и внедрения систем ИИ в органах прокуратуры создаются специальные подразделения.

По приказу Генерального прокурора Российской Федерации в структуре Главного управления по надзору за исполнением федерального законодательства Генеральной прокуратуры создано и успешно функционирует спецподразделение по защите информации – отдел по надзору за исполнением законов в сфере информационных технологий и защиты информации. Под его надзором находятся все крупные государственные проекты, связанные с цифровизацией.

Также Генеральная прокуратура Российской Федерации внедряет систему ИИ, разработанную в рамках цифровой трансформации прокуратуры, для оценки коррупциогенных факторов в ведомственных нормативных актах[52].

Для повышения эффективности этой деятельности сейчас тестируется специальная программа с элементами ИИ, разработанная в рамках продолжающихся мероприятий по цифровой трансформации ведомства.

В июне 2023 года Генеральный прокурор Российской Федерации И.В. Краснов сообщил, что в Генеральной прокуратуре организовано специализированное подразделение для прогнозирования перспективных направлений в деятельности органов прокуратуры на длительный срок, а также состояния преступности, в том числе в связи с использованием ИИ, но эта работа охватывает перспективу на 20-30 лет вперед[53].

В апреле 2024 года Генеральным прокурором Российской Федерации подписан План по внедрению и использованию технического искусственного интеллекта, нейронных сетей для работы прокурора. Согласно указанному Плану, нейросети будут использоваться для аналитической работы, прогнозирования роста преступности в отдельных регионах, анализа законопроектов и других документов[54].

Несмотря на значительные проекты и инициативы, в настоящее время непосредственно в деятельности органов прокуратуры Российский Федерации ИИ не применяется при осуществлении надзора и принятии решений. Решение всегда принимается в конечном счете сотрудником прокуратуры при осуществлении анализа состояния законности, надзора за исполнением законов, мониторинге и межведомственном взаимодействии.

В органах прокуратуры **Республики Беларусь** и Государственном учреждении «Научно-практический центр проблем укрепления законности и

---

[52] ГП тестирует искусственный интеллект для оценки коррупционных факторов в нормативных актах / [Электронный ресурс] – Режим доступа: https://tass.ru/obschestvo/12936661_ (дата обращения 20.12.2024).

[53] ГП стала применять искусственный интеллект для прогнозирования ситуации с преступностью / [Электронный ресурс] – Режим доступа: https://tass.ru/obschestvo/18042003_ (дата обращения 11.01.2025).

[54] Генпрокуратура начала внедрять в свою работу искусственный интеллект / [Электронный ресурс] – Режим доступа: https://tass.ru/politika/20634537_ (дата обращения 15.01.2025).

правопорядка Генеральной прокуратуры Республики Беларусь» для выполнения возложенных задач и функций используется ряд автоматизированных информационных (информационно-аналитических) систем, систем обмена документами в электронном виде, а также имеется удаленный доступ к электронным информационным ресурсам иных государственных органов и организаций.

1. **Система ведения статистической отчетности и осуществления аналитической деятельности «Аналитика»** предназначена для сбора и обработки статистических данных, анализа преступности и деятельности правоохранительных органов. Она содержит сведения как о преступности, так и о ряде социально-экономических показателей развития всех регионов государства. Позволяет на их основе оперативно проводить ряд аналитических исследований, в том числе отслеживать динамику и структуру преступности, выявлять тенденции и прогнозировать ее изменения. При этом передача данных закодирована.

2. **Автоматизированная информационная система, обеспечивающая формирование Национального реестра правовых актов Республики Беларусь** (АИС НРПА). Основной функцией АИС НРПА является обеспечение автоматизации электронного информационного взаимодействия государственных органов (организаций) в рамках определенных этапов нормотворческого процесса, к которым относится и обязательная криминологическая экспертиза нормативных правовых актов и их проектов, проводимая специалистами НПЦ Генеральной прокуратуры.

Использование АИС НРПА существенным образом повлияло на сокращение документооборота, позитивно отразилось на внутриведомственном планировании, улучшило механизмы контроля, формирования отчетности.

В рамках дальнейшего процесса цифровизации нормотворческой деятельности в настоящее время осуществляется разработка и тестирование автоматизированной информационной системы по обеспечению нормотворческого процесса (АИС «Нормотворчество»), которая обеспечит полную цифровизацию процессов взаимодействия государственных органов и организаций на всех стадиях нормотворческой деятельности.

3. **Система DIRECTUM Standart** предназначена для обмена документами в электронном виде как в системе органов прокуратуры, так и с другими государственными органами – абонентами системы межведомственного документооборота (СМДО), а также для регистрации входящей и исходящей корреспонденции.

Что касается информационных ресурсов иных государственных органов и организаций, в органах прокуратуры имеется удаленный доступ к информационным ресурсам Министерства внутренних дел Республики Беларусь, таким как Единая государственная база данных о правонарушениях, информационные системы «Паспорт» и «ГАИ», а также к информации в электронном виде о платежах в автоматизированной информационной системе

единого расчетного и информационного пространства Республики Беларусь (АИС «Расчет»).

Анализ внедрения информационных технологий в том числе ИИ в Республике Беларусь показал, что данный процесс реализуются согласно положению Декрета Президента Республики Беларусь от 21 декабря 2017 года «О развитии цифровой экономики», который предполагает также цифровую трансформацию органов прокуратуры республики. Документ создает благоприятные условия для развития ИТ-отрасли и дает серьезные конкурентные преимущества стране в создании цифровой экономики.

Декрет разработан в соответствии с поручением Президента Администрацией Парка высоких технологий совместно с резидентами ПВТ, ИТ-сообществом, ведущими юридическими и консалтинговыми фирмами Республики Беларусь, а также зарубежными экспертами. В процессе обсуждения и согласования проекта с государственными органами были сохранены и одобрены все его существенные положения.

Новый Декрет продлил действие специального налогово-правового режима Парка высоких технологий до 2049 года.

Сохранен экстерриториальный принцип регистрации, также остались неизменными базовые условия хозяйствования для резидентов ПВТ.

Декрет легализует ICO, криптовалюты и смарт-контракты. Благодаря принятию этого документа Республика Беларусь становится первой в мире юрисдикцией с комплексным правовым регулированием бизнесов на основе технологии блокчейн.

Декрет не предполагает никаких ограничений и специальных требований к операциям по созданию, размещению, хранению, отчуждению, обмену токенов, а также деятельности криптобирж и криптоплатформ. Деятельность по майнингу, приобретению, отчуждению токенов, осуществляемая физическими лицами, не является предпринимательской деятельностью, а токены не подлежат декларированию. При этом до 2023 года деятельность по майнингу, созданию, приобретению и отчуждению токенов не облагается налогами.

Введя в правовое поле белорусского законодательства смарт-контракт и предоставив право осуществлять посредством его совершение и (или) исполнение сделок, Беларусь становится первой страной в мире, легализовавшей смарт-контракты на государственном уровне.

Попытки внедрения ИИ в Беларуси находят применение в сфере судебной экспертизы. Научно-практический центр Государственного комитета судебных экспертиз Беларуси разрабатывает новые средства и методы экспертной работы, включая новейшие разработки и проекты, где задействован ИИ. Центр выполняет экспертизы для правоохранительных органов, судов и граждан.

Перспективным видится внедрение ИИ при проведении криминологической экспертизы проектов нормативных правовых актов.

Реализация этой актуальной задачи осуществляется Национальным центром правовой информации Республики Беларусь (далее – НЦПИ) в тесном взаимодействии с НПЦ.

Основной функцией данной системы является обеспечение автоматизации электронного информационного взаимодействия государственных органов (организаций) в рамках определенных этапов нормотворческого процесса, к которым относится и проведение криминологической экспертизы. В связи с этим с 2019 года с привлечением специалистов НПЦ велась разработка указанного блока.

В частности, происходило создание алгоритмов информационного взаимодействия между государственными органами (организациями) и НПЦ по обмену данными (информацией, необходимой для проведения криминологической экспертизы, документами о результатах ее проведения, иной сопроводительной документацией), выстраивались схемы от начала до завершения производства криминологической экспертизы, в том числе маршруты внутреннего движения документов в НПЦ, подготовки заключения криминологической экспертизы, его визирования, подписи и направления субъекту, представившему проект нормативного правового акта, и многое другое.

К моменту завершения данной работы в силу вступили нормы законодательства в сфере регулирования электронного нормотворчества. В соответствии с подпунктом 4.1 пункта 4 Указа Президента Республики Беларусь от 17 ноября 2020 года №415 «О повышении оперативности и качества нормотворческой деятельности» с 1 апреля 2021 года проекты правовых актов Главы государства, законов и постановлений Совета Министров Республики Беларусь направляются на криминологическую экспертизу только посредством АИС НРПА.

Следует отметить, что проекты ведомственных актов государственных органов не направляются для проведения криминологической экспертизы посредством АИС НРПА. Также электронное информационное взаимодействие государственных органов (организаций) не осуществляется в АИС НРПА в отношении проектов нормативных правовых актов (нормативных правовых актов), содержащих служебную информацию ограниченного распространения.

С момента начала использования возможностей АИС НРПА в НПЦ обеспечивается полный цикл производства криминологической экспертизы. На стадии регистрации поступившего для проведения криминологической экспертизы проекта нормативного правового акта осуществляется присвоение номера производства (согласно правилам внутреннего делопроизводства организации), равно как и присваивается номер документу, который завершает проведение экспертизы, параллельно с наличием в АИС НРПА идентификатора – номера регистрационно-контрольной карты, присваиваемого с момента ее создания и сохраняющегося на всех стадиях нормотворческого процесса.

Вход в АИС НРПА доступен только для тех работников НПЦ, которые в соответствии с должностными обязанностями осуществляют проведение

криминологической экспертизы. Указанные работники имеют учетную запись в системе и реквизиты для авторизации (логин и пароль, который генерируется случайным способом без участия человека и сообщается непосредственно пользователю). В настоящее время вход в систему доступен с любого устройства, имеющего выход в Интернет.

Следует отметить, что институт криминологической экспертизы служит действенным инструментом, позволяющим одновременно влиять на детерминанты преступности и формировать эффективное правовое регулирование, повышать уровень законности и правопорядка в стране, обеспечивать развитие позитивного права во взаимосвязи с устоявшимися и прогрессивными научными методами и подходами. Дальнейшая цифровизация, в том числе путем внедрения ИИ, экспертно-криминологических исследований законодательства будет способствовать эффективности данных направлений, своевременности и повышению качества реализации принимаемых на государственном уровне правовых решений.

Таким образом, с учетом представленной белорусской стороной информации на текущем этапе мы видим начальные признаки готовности к применению систем ИИ для органов прокуратуры Беларуси, при этом требуется дальнейшее институциональное, техническое и нормативное развитие в данном направлении. Эти шаги подкрепляются принятием Модельного закона СНГ «О технологиях искусственного интеллекта», разработанного учеными Объединенного института проблем информатики Национальной академии наук совместно с заинтересованными организациями Беларуси. При этом необходимы национальные нормы, регулирующие применение ИИ, институциональных механизмов контроля, кадровую подготовку.

Анализ применения ИИ в **Кыргызской Республике** показал, что в стране для внедрения данной инновации подготовлена достаточно прочная технологическая база.

Во всех государственных структурах внедряются инновационные технологии, которые, с одной стороны, сокращают бумажную волокиту, бюрократию и автоматизируют алгоритм действий государственных и муниципальных служащих и, с другой стороны, ускоряют получение гражданами качественных государственных услуг и обеспечивают им оперативный доступ к данным, находящимся в ведении государственных органов.

Вопрос цифровой трансформации органов прокуратуры Кыргызской Республики не является исключением и на данном этапе продолжает наращивать свой потенциал, тем самым улучшая уровень цифровизации электронного государственного управления в стране.

В 2019 году Советом безопасности Кыргызской Республики была одобрена Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023», в этом же году Правительством Кыргызской Республики утверждена «дорожная карта» по ее реализации.

Далее, в 2022 году было издано распоряжение Кабинета Министров Кыргызской Республики о дальнейшем развитии цифровизации государственного управления и цифровой инфраструктуры в республике на 2022-2023 годы.

При этом Генеральной прокуратуре Кыргызской Республики была отведена роль по модернизации технологической инфраструктуры всех правоохранительных органов республики по внедрению единой платформы автоматизированной информационной системы «Единый реестр преступлений» (далее – АИС «ЕРП»).

В целях исполнения Концепции цифровой трансформации «Цифровой Кыргызстан 2019-2023» и Национальной программы развития Кыргызской Республики до 2026 года, утвержденной Указом Президента Кыргызской Республики от 12 октября 2021 года УП №435, а также в свете приоритетности внедрения электронного управления в законодательной, исполнительной и судебной ветвях власти Генеральной прокуратурой с 1 января 2019 года разработана и внедрена во всех правоохранительных органах автоматизированная информационная система «Единый реестр преступлений» наряду с новыми Уголовным, Уголовно-процессуальным и другими кодексами Кыргызской Республики, и соответствующей инфраструктурой (компьютерное и серверное оборудование).

Единый реестр преступлений (АИС «ЕРП») – это электронная база данных, в которую вносятся сведения о начале досудебного производства, процессуальных действиях и решениях, движении дела, заявителях и участниках уголовного судопроизводства.

Впервые система внедрена в 2019 году (Единый реестр преступлений и проступков), в декабре 2021 года система полностью переработана в связи с кардинальными изменениями в законодательстве (УК, УПК).

В настоящее время в системе работают 5 государственных органов (прокуратура, МВД, органы национальной безопасности, служба исполнения наказания и таможня), количество активных пользователей насчитывает более 3,5 тысячи лиц.

На сегодняшний день полностью реализована регистрационная часть системы, досудебная часть системы продолжает наращиваться. Полностью автоматизирована статистическая отчетность о состоянии преступности, разработана автоматизированная следственная справка о движении уголовных дел и материалов об отказе в возбуждении уголовных дел, являющаяся основой для автоматизации отчета о следственной работе.

Внедрена ежесуточная сводка о происшествиях с применением технологии репликации базы данных и выгрузки информации в соответствии с установленным порядком. Автоматизирована алфавитная карточка на лицо, привлеченное к уголовной ответственности. Расширены возможности поиска информации в системе, в том числе по сгенерированным процессуальным документам. Проведена интеграция АИС «ЕРП» с АИС «Единый портал по производству судебных экспертиз», разрабатываемой судебно-экспертной службой

при Министерстве юстиции Кыргызской Республики. С момента создания АИС «ЕРП» реализована интеграция с базами данных ГРС, посредством которых пользователи получают данные на заявителя, потерпевшего, обвиняемого и других лиц, участвующих в уголовном процессе, по сервису «Персональный идентификационный номер». Также на стадии тестирования находится сервис служебных запросов, по которым следователи могут получить данные об имеющемся имуществе обвиняемого и другие данные.

В АИС «ЕРП» реализованы требования УПК в части генерации документов. На сегодняшний день разработаны и внедрены более 30 форм генерации процессуальных документов. На стадии внедрения более 30 дополнительных форм генерируемых документов, которые являются неотъемлемым компонентом «Электронного уголовного дела» (далее – «ЭУД»).

В части дальнейших планов по АИС «ЕРП» – в ближайшее время планируется реализовать еще один шаг по внедрению проекта «ЭУД», а именно: внесение в систему сканированных документов, где по результатам слияния данных по генерируем и сканируемым документам, составлению следователем описи материалов уголовного дела с возможностью выставления хронологического или логического порядка появится возможность увидеть полную копию бумажного уголовного дела в электронном формате.

Внедрение АИС «ЕРП» обеспечило полный учет преступлений, открытость уголовного процесса, экономию процессуального времени, актуальную правовую статистику, снизило риски фальсификации и укрытия преступлений, повысило качество прокурорского надзора и ведомственного контроля, оптимизировало работу следователей и прокуроров.

Необходимо отметить, что Генеральной прокуратурой и региональными звеньями уделяется большое внимание обучению пользователей АИС «ЕРП». При каждом новом назначении сотрудника правоохранительного органа или его передвижении с новым объемом функциональных обязанностей обязательно проводится первичное обучение.

Кроме этого, Генеральной прокуратурой ежегодно проводятся массовые обучения с охватом каждого региона и каждого органа.

Расширение возможностей АИС «ЕРП» и его постоянная модернизация являются одной из приоритетных задач органов прокуратуры Кыргызской Республики. Работа в этом направлении ведется постоянно и совместно с государственным учреждением «Укук» при Генеральной прокуратуре, являющегося техническим оператором информационных систем правоохранительных, судебных органов, органов прокуратуры, а также информационных ведомственных систем государственных органов, работающих на основе данных Единого реестра преступлений, Единого реестра правонарушений, уголовного и уголовно-процессуального законодательства.

Единый реестр правонарушений (АИС «ЕРПн») – это автоматизированная информационная система, в которой ведется производство по делам о правонарушениях в электронной форме.

Ранее эта система велась со стороны МВД. После передачи ее в ведение Генеральной прокуратуры она была полностью переработана.

Произведена интеграция с проектом «Безопасный город», который также был полностью переработан силами Генеральной прокуратуры.

В настоящее время в АИС «ЕРПн» работают порядка 60 государственных органов (министерств, ведомств, подразделений) и более 20 тыс. пользователей.

Принятыми Генеральной прокуратурой Кыргызской Республики стратегическими мерами удалось поднять процент оплачиваемости наложенных штрафов с 30 до 75%.

Внедрение АИС «ЕРПн» обеспечило полный и оперативный учет правонарушений, усилило прокурорский надзор и ведомственный контроль, а заложенные алгоритмы в системе дали толчок для реальной работы уполномоченных государственных органов и повышению эффективности их деятельности (т.е. система начала контролировать их деятельность путем выставления счетчиков времени, заполнения обязательных реквизитов и соблюдения других требований).

Произведена интеграция АИС «ЕРПн» с системой медицинского освидетельствования Министерства здравоохранения Кыргызской Республики, которая масштабирована по всей республике. Кроме этого, ранее по результатам проверки Генеральной прокуратуры и рассмотрения представления Министерством здравоохранения разработан новый акт медицинского освидетельствования по алкогольному опьянению. Все это позволило минимизировать коррупционные риски и факты фальсификации результатов освидетельствований.

Также Генеральной прокуратурой проведена работа по стандартизации мобильных аппаратно-программных комплексов «Трехножка», что также позволило увеличить эффективность по выявляемым правонарушениям и увеличило наполняемость государственного бюджета.

В рамках модернизации АИС «ЕРПн» разработана двухконтурная система – **правовой портал «Төлөм»**.

Служебная часть предназначена для сотрудников правоохранительных органов, которые посредством служебных планшетов могут на местах получить оперативную информацию по госномеру автотранспортного средства или паспорту гражданина об имеющихся штрафах, действительности водительского удостоверения, нахождении в розыске авто или его владельца, разрешении на тонировку и т.д. Необходимо отметить, что в целях эффективного использования портала «Төлөм» по инициативе Генеральной прокуратуры сотрудникам автоинспекции выдано 195 планшетов. За время работы служебного портала произведено более 120 000 запросов.

Публичная часть портала предназначена для граждан, которые могут в любое время получить информацию обо всех имеющихся у них штрафах и их статусе на текущий момент (www.tolom.kg). Если ранее граждане по другим сервисам могли видеть только нарушения, зафиксированные камерами

«Безопасного города», на портале «Төлөм» они получают полную информацию обо всех зарегистрированных правонарушениях (как выписанных вручную, так и зафиксированных мобильными и стационарными аппаратно-программными комплексами), что также положительно влияет на повышения уровня правосознания. За второе полугодие 2023 года работы гражданского портала пользователями произведено более 5 млн запросов.

В служебной части портала «Төлөм» также имеются данные о топ-100 правонарушителях, в отношении которых проводится усиленная работа по установлению их местонахождения и взысканию штрафов. Тем самым ужесточаются меры к злостным правонарушителям и предупреждаются другие правонарушения.

Система электронного документооборота (АИС «СЭД») – это автоматизированная информационная система, обеспечивающая сбор документов, их обработку, управление документом и доступ к ним в электронном формате.

АИС «СЭД» позволила оптимизировать работу с документами путем сокращения их на бумажных носителях, повышения оперативности доставки адресатам, формирования единого информационного пространства.

Указанная система работает в полном объеме во всех органах прокуратуры Кыргызской Республики. На сегодняшний день реализован проект «Шлюза электронного документооборота», что также повысило в разы оперативность обмена информацией между государственными органами.

В начале текущего года платформа «СЭД» органов прокуратуры обновлена, в новой версии реализованы подсистемы/модули актов прокурорского реагирования, в т.ч. автоматизированный отчет о работе прокурора в направлении надзора за исполнением законов и противодействию коррупции, база правовых актов Генерального прокурора и организационно-распорядительных актов органов прокуратуры, а также кадровая система. Кроме этого, обновлен и оптимизирован интерфейс «СЭД», время отклика работы с системой увеличено в разы.

Необходимо отметить, что платформа «СЭД» органов прокуратуры используется (внедрена или на стадии внедрения) в МВД, Конституционном суде, судебно-экспертной службе и службе исполнения наказаний при Министерстве юстиции, а также в пограничной службе.

Автоматизированная информационная система «Регистрация проверок субъектов предпринимательства» (АИС «РПСП») – это информационная система, обеспечивающая автоматизацию основных процессов регистрации проверок, проводимых проверяющими органами в отношении субъектов предпринимательства. Держателем данной информационной системы и вышеупомянутых систем является Генеральная прокуратура Кыргызской Республики. Использование информационной системы является обязательным для сотрудников органов прокуратуры, правоохранительных органов и органов налоговой службы при осуществлении проверок.

В целях полноценной и бесперебойной работы всех вышеуказанных автоматизированных информационных систем органов прокуратуры на базе отдела приема граждан и документирования Генеральной прокуратуры Кыргызской Республики организован «Call Center». По предложениям, поступившим от пользователей и регистраторов систем, «Call Center» осуществляет мониторинг и анализ эффективного функционирования электронной системы, что способствует устранению недостатков в системе и продвижению программы.

Таким образом, в целом выбранная стратегия и дальнейшие действия Генеральной прокуратуры Кыргызской Республики по цифровой трансформации органов прокуратуры показали свою высокую эффективность. Благодаря инновационным решениям и техническим возможностям таких систем, как АИС «ЕРП», АИС «ЕРПн», АИС «СЭД» и АИС «РПСП» у органов прокуратуры, правоохранительных и контролирующих органов Кыргызской Республики появились реальные возможности видеть все данные о преступлениях, правонарушениях, электронного документооборота, служебных проверок и отслеживать весь алгоритм процессуальной деятельности вышеуказанных органов.

В настоящее время разрабатывается и планируется внедрить первый прототип электронного уголовного дела путем гибридизации функций генерации процессуальных документов АИС «ЕРП» и сканирования материалов уголовного дела. В последующем, при появлении надлежащих технических условий и отработанной юридической среды, будет внедрена графическая подпись на планшетах и электронная цифровая подпись.

Также будут продолжены работы по дальнейшей интеграции АИС «ЕРП» с информационными системами и базами данных других государственных органов.

В части АИС «ЕРПн» будет продолжена работа по наращиванию ее функционала и интеграции. В АИС «СЭД» будет продолжена разработка модулей по другим направлениям прокурорской деятельности в целях оптимизации работы и полной автоматизации статистической отчетности о работе прокурора.

Генеральная прокуратура Кыргызской Республики совместно с ГУ «Укук», ежедневно работает в направлении цифровизации как своего ведомства, так и других правоохранительных и государственных органов.

Необходимо отметить, что ГУ «Укук» при Генеральной прокуратуре Кыргызской Республики, являясь техническим оператором государственных органов, параллельно ведет разработку и внедрение порядка 40 проектов.

При этом применение ИИ в деятельности органов прокуратуры Кыргызской Республики наряду с вышеуказанными автоматизированными системами поможет повысить качество и уровень работы органов прокуратуры, что будет способствовать укреплению законности.

В рамках изучения представленной кыргызской стороной информации, мы видим схожесть моделей развития автоматизации, цифровизации, интеграции, разработки нормативной базы с казахстанской моделью совершенствования деятельности правоохранительной деятельности, стремления к применению в

надзорных функциях новых технологических решений. Полагаем для применения ИИ в работе прокурора необходимы институциональные изменения, принятие нормативно-правовых и технических решений, подготовка универсальных специалистов.

Анализ опыта указанных стран-участников СНГ в развитии ИИ и его внедрении в деятельность органов прокуратурыпоказывает, что ими заложены правовые и технологические основы для развития и внедрения ИИ, что выразилось главным образом в подготовке и принятии ряда нормативных правовых актов концептуального характера и реализации цифровых платформ в системе органов прокуратуры.

Органы прокуратуры перечисленных стран СНГ для выполнения основных целей и задач активно внедряют и использует различные информационно-аналитические системы. Эти системы позволяют улучшить анализ данных, автоматизировать процессы, обеспечивать прозрачность и контроль, а также обрабатывать большие объемы информации.

Среди используемых информационных технологий можно выделить системы для электронного документооборота, базы данных правовой статистики, системы мониторинга и прогнозирования, а также системы с элементами ИИ. Вместе с тем ИИ в органах прокуратуры стран СНГ в буквальном его понимании **не используется**. На сегодня отдельными странами СНГ ведутся лишь пилотные проекты и разработки в виде **«мягкого ИИ»** (soft AI) в различных направлениях надзорной и следственной деятельности. Подобные системы представлены в виде:

- интеллектуальных поисковых систем и помощников для следователей и прокуроров;

- информационных систем по выявлению и прогнозированию преступности;

- информационных систем по розыску лиц по камерам видеонаблюдения;

- систем для анализа проектов нормативных правовых актов, помощников и др.

Как показал анализ, органы прокуратуры стран СНГ (представивших информацию) обладают достаточно широким набором цифровых платформ, перспективных для внедрения элементов ИИ.

Однако **отсутствие достаточного правового регулирования**, **технического оснащения** (суперкомпьютеры, машиночитаемые метаданные и т.д.), **нехватка квалифицированных IT-специалистов** по разработке и дальнейшему обслуживанию систем ИИ, а также **потребность в постоянном обучении** прокуроров основам нейронных сетей на сегодняшний день являются **основными барьерами** для дальнейшего развития и внедрения ИИ в деятельность органов прокуратуры.

Необходимость подготовки специалистов и обучение прокуроров работе с новыми технологиями подтверждается проведением электронного анкетирования более 1,5 тысячи сотрудников прокуратуры Беларуси, Казахстана, Кыргызстана и России.

Анализ разработок и применения систем ИИ в информационных технологиях органов прокуратуры стран СНГ позволил выделить преимущества, риски и перспективные направления для их внедрения.

Основные преимущества внедрения ИИ в деятельность прокуроров заключаются в следующем:

- *ускорение процессов:* ИИ может значительно ускорить обработку и анализ данных, что позволяет быстрее продвигать расследования и судебные процессы;

- *снижение нагрузки на сотрудников:* автоматизация рутинных задач освобождает сотрудников от монотонной работы, позволяя им сосредоточиться на более сложных и требующих аналитики задачах;

- *улучшение прогнозирования:* прогнозирование исходов дел и выявление закономерностей помогает в планировании и стратегии расследования;

- *поддержка принятия решений:* ИИ может предоставлять рекомендации и аналитическую информацию, помогая прокурорам в принятии обоснованных и законных решений.

§ 2.3 Выявление проблем правового регулирования и практические вызовы цифровизации

На сегодняшний день развитие и внедрение ИИ в деятельность органов прокуратуры государств-участников СНГ сопровождается рядом комплексных и системных вызовов, которые касаются как недостатков правового регулирования, так и институциональной неподготовленности к полноценной цифровой трансформации. Несмотря на наличие отдельных нормативных актов концептуального характера и пилотных разработок «мягкого ИИ» (soft AI), правовая система большинства стран СНГ остается фрагментарной и не обеспечивает полноценной регуляторной среды для безопасного и этически обоснованного использования технологий ИИ.

Одной из ключевых проблем выступает отсутствие комплексного правового акта, регулирующего использование ИИ, его правовой статус, классификацию систем, базовые принципы разработки и ответственности за результаты и его функционирования. Это порождает правовую неопределенность в части распределения юридической ответственности между разработчиками, операторами и государственными органами в случае технических сбоев, предвзятых решений или нарушений прав граждан.

Классические действующие институты гражданского и уголовного права, к примеру в части установления вины, умысла, деликта, к ИИ неприменимы.

Существенным препятствием остается и отсутствие правовых механизмов обеспечения прозрачности алгоритмов. Деятельность сотрудника прокуратуры требует полной обоснованности и воспроизводимости принятых решений, тогда как «черные ящики» алгоритмов машинного обучения затрудняют контроль за обоснованностью результатов. Кроме того, риск алгоритмической предвзятости,

обусловленный обучением на искаженных данных, может привести к нарушению принципов справедливости и равенства перед законом.

Особую тревогу вызывает угроза нарушения прав человека, в частности, права на защиту персональных данных, неприкосновенность частной жизни и презумпцию невиновности. В ряде государств СНГ с учетом стремительной цифровизации правовые и технические механизмы по обеспечению контроля за обработкой данных, включая биометрические и поведенческие данные, защиты конфиденциальной информации при внедрении ИИ в процессуальные и надзорные процедуры требуют нормативного правового мониторинга. Уязвимость же ИИ-систем к кибератакам лишь усиливает указанные риски, особенно при использовании облачных технологий и иностранных программных решений.

Прогрессирующая цифровизация также порождает конфликт между автоматизацией и принципами справедливости и процессуальных гарантий. Возникают вопросы правоприменения ИИ в правосудии, прокурорском надзоре или следственной деятельности, так как это может нарушать презумпцию невиновности, право на защиту, право на объективное судебное разбирательство; сложности с обоснованием решений, принятых с использованием алгоритмов, в рамках судебных и прокурорских процедур.

Также проблемным остается вопрос институциональной готовности органов прокуратуры к использованию ИИ. В числе острых вызовов — дефицит квалифицированных IT-специалистов, низкий уровень цифровой грамотности сотрудников, отсутствие профильного образования и курсов по правовой аналитике в контексте работы с ИИ. Кроме того, высокая стоимость внедрения и эксплуатации систем ИИ, зависимость от импортного оборудования и отсутствие «регуляторных песочниц» (sandbox regulation) существенно сдерживают масштабирование технологических решений.

Так, в большинстве стран СНГ не созданы правовые режимы «тестирования» ИИ в условиях ограниченной ответственности и правового надзора. Это может ограничивать внедрение инноваций и мешать апробации технологий в контролируемой среде.

Нерешенными остаются вопросы с правами интеллектуальной собственности. Здесь не урегулирован вопрос авторства и прав на результаты, созданные ИИ, к примеру, кто является правообладателем при генерации текста, кода, решений, а также вопрос возможности использования ИИ без согласия его автора.

Одной из значительных проблем является угроза суверенитету и цифровой безопасности страны, так как использование ИИ, основанного на иностранном ПО и «облачных» технологиях, создает угрозу утечки конфиденциальных данных. Зависимость от зарубежных поставщиков делает невозможным контроль за процессами принятия решений и обработкой информации.

Недостаточная нормативная правовая адаптивность стоит отдельным вопросом. Ввиду стремительного прогресса в разработке новых технологий

законодательство не только стран СНГ, но и других мировых держав не успевает выработать правовые нормы и в условиях быстрого технического развития они устаревают до их принятия.

Таким образом, для стран СНГ приоритетными направлениями правовой политики в сфере ИИ в органах прокуратуры должны стать:

- формирование комплексной нормативно-правовой базы, включающей международные стандарты и этические ориентиры;
- создание института правовой ответственности при использовании ИИ в надзорной деятельности;
- внедрение механизмов алгоритмической прозрачности и контроля решений, принятых ИИ;
- нормативное закрепление прав граждан в условиях цифровизации уголовного судопроизводства;
- системная цифровая трансформация и профессиональная переподготовка кадров прокуратуры;
- стимулирование научных исследований, правовой экспертизы и разработки национальных технологий в сфере ИИ.

Только при условии преодоления указанных барьеров возможно формирование устойчивой, законной и этически выверенной модели применения ИИ в органах прокуратуры государств СНГ, ориентированной на защиту прав человека, соблюдение верховенства права и укрепление доверия общества к цифровым правоприменительным механизмам.

Правовые базы большинства государств, в том числе стран СНГ, не успевают адаптироваться к стремительному развитию технологий, что порождает целый ряд вопросов, связанных с правовым регулированием ИИ.

В условиях недостатка четких юридических норм, определяющих статус, ответственность и допустимые границы применения ИИ, возникают риски нарушения прав и свобод граждан, в том числе злоупотреблений технологиями.

Как было отмечено в 1 главе, в международной правовой науке и практике отсутствует единое определение ИИ. Отсутствие единой, универсальной и юридически закрепленной дефиниции создает правовую неопределенность и препятствует развитию целостной регуляторной системы.

В свою очередь, отсутствие четких, универсальных и юридически закрепленных понятий приводит к различиям в толковании и применении норм. Это влечет за собой сложность классификации ИИ-систем, определения субъектов ответственности и последующего правоприменения.

Аналогичной позиции придерживается юрист и правовед М. Бибер, отмечая, что «правовая неопределенность в отношении ИИ создает риски не только для пользователей и разработчиков, но и для судов, которые вынуждены принимать решения в условиях отсутствия нормативного регулирования»[55].

Правовой статус ИИ – одна из наиболее сложных проблем современной юридической науки. Традиционно ИИ рассматривается как «инструмент»,

[55] Bibér M. Legal Frameworks for AI Regulation. AI & Law Journal, 2022_(дата обращения: 23.06.2025).

ответственность за действия которого лежит на пользователях и разработчиках. Однако с ростом уровня автономности и способности к самообучению таких систем появляются аргументы в пользу признания ограниченной правосубъектности ИИ.

Как отмечает профессор А.В. Пискарев[56], «технологический прогресс требует переосмысления традиционных моделей ответственности. Современные ИИ-системы часто функционируют автономно и способны принимать решения, что требует введения гибридной модели ответственности, сочетающей ответственность человека и системы».

Схематично можно выделить три модели ответственности:

1. Модель традиционного инструмента – ответственность несут операторы и создатели. Это наиболее распространенный подход в СНГ.

2. Модель «цифрового агента» – ИИ рассматривается как особый субъект, несущий ограниченную ответственность. Этот подход обсуждается в законодательстве ЕС и в некоторых проектах СНГ, включая Казахстан.

3. Коллективная ответственность – ответственность распределяется между всеми участниками жизненного цикла ИИ: разработчиками, операторами, пользователями, регуляторами.

Индивидуальное законодательное видение к пониманию ИИ стран СНГ ведет к фрагментарности и неоднородности подходов.

Так, в Российской Федерации на уровне федерального законодательства отсутствует отдельный закон об ИИ. Регулирование осуществляется через нормы принятого в 2020 году Федерального закона «По проведению эксперимента и внедрению технологий искусственного интеллекта»[57] и правовые акты по установлению государственных стандартов.

Значительно серьезнее в РФ продвинулись в нормативно-техническом регулировании ИИ.

В Республике Казахстан один из наиболее продвинутых проектов – законопроект «Об искусственном интеллекте», в котором предусмотрены понятия уровней автономности ИИ, требования к прозрачности и безопасности, а также ответственность операторов.

В Республике Беларусь законодательство по регулированию сферы ИИ находится на стадии разработки, хотя в национальной стратегии развития цифровой экономики (до 2025 г.) отражены ключевые направления регулирования ИИ. Правовые нормы пока представлены общими правилами о персональных данных и защите информации.

---

[56] Пискарёв А.В. Правовые аспекты ответственности за искусственный интеллект. – М., 2023_(дата обращения: 23.06.2025).

[57] Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"» от 24 апреля 2020 г. № 123-ФЗ, принят Государственной Думой 14 апреля 2020 г. и одобрен Советом Федерации 17 апреля 2020 г. / [Электронный ресурс] – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW _351127/_(дата обращения: 23.09.2024).

Наряду с этим, как указывалось ранее, в Беларуси 18 апреля 2025 г. на 58 пленарном заседании Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств принят Модельный закон СНГ «О технологиях искусственного интеллекта», направленный на регулирование ИИ в государствах-участниках СНГ[58].

В настоящее время правоприменительная практика СНГ сталкивается с затруднениями в привлечении к ответственности за вред, причиненный ИИ. Отсутствие конкретных правил приводит к спорам и вопросам об ответственности — разработчик или владелец системы, либо конечный пользователь?

Например, в Российской Федерации Московским городским судом в деле № 12-2513/2021 рассмотрен вопрос использования данных, собранных автоматической системой фиксации нарушений ПДД. Суд признал такие доказательства допустимыми, однако подчеркнул необходимость сертификации и прозрачности алгоритмов.

В Республике Беларусь Минский экономический суд подтвердил законность налоговой проверки, основанной на аналитике ИИ, однако отметил, что процесс должен сопровождаться прозрачностью и контролем (дело № 3-15/2020).

В Республике Казахстан в 2023 г. Алматинский городской суд в деле по спору о страховой выплате отказал в признании решения ИИ единственным доказательством, указав на необходимость участия человека в окончательном решении.

Эти дела отражают общий тренд: отсутствие детальных правил приводит к неоднозначным судебным решениям и рискам правовой неопределенности.

ИИ несет риски дискриминации, нарушения конфиденциальности, утраты контроля над процессами принятия решений. Отсутствие нормативов по этике ИИ приводит к возможным злоупотреблениям.

Не только ИИ в отдельности, сам процесс цифровизации сопровождается сложными вызовами. Это не только технические вопросы, но и инфраструктурные, кадровые, правовые и социальные проблемы, которые взаимосвязаны и требуют комплексного подхода.

Цифровая трансформация в СНГ – одновременно технологический и институциональный вызов. При этом различие стратегий и инфраструктурные разрывы приводят к неравномерному развитию регионов.

В мегаполисах инфраструктура развивается динамично, но сельские и удаленные территории испытывают дефицит интернета и современных технологий, что соответственно усиливает миграцию в крупные мегаполисы.

Общеизвестные факты о меньшей технологической развитости регионов, наличии региональных цифровых разрывов, в особенности в отдаленных от мегаполисов населенных пунктов, приводят к обоснованному выводу о неравномерном проникновении инновационных инструментов, в том числе с применением ИИ, что может ограничивать эффективное использование ИИ-

[58] Модельный закон «О технологиях искусственного интеллекта», принят Межпарламентской Ассамблеей СНГ/ [Электронный ресурс] – Режим доступа: https://uiip.basnet.by/rus/news/438/_(дата обращения: 02.07.2025).

платформ в работе прокуроров в контексте географической проекции на отдаленные регионы.

Данный аспект создает цифровой разрыв между крупным городом и отдаленным населенным пунктом, который с учетом стремительного прогресса цифровизации будет только усиливаться и создаст техно-логистический коллапс. Соответственно прокуроры здесь могут отставать в использовании ИИ-решений для анализа, данных, автоматизации процессов и взаимодействия с другими органами, с которыми в городах системы интегрированы. Это приведет к снижению оперативности, неравенству по доступу к цифровым технологиям на периферии.

Немаловажным фактором является вопрос разницы между требованиями навыков работы с новыми технологиями и уровнем подготовки сотрудников органов прокуратуры в СНГ. Компетенция действующих работников с учетом опроса сотрудников органов прокуратуры СНГ оставляет желать лучшего, в то же время необходимость работы с прогрессирующими новыми технологиями, требующая знаний IT-сферы, уже назрела.

При этом низкий уровень цифровой грамотности населения, особенно среди пожилых и социально уязвимых, также тормозит внедрение цифровых сервисов.

Законодательство в сфере цифровых технологий в СНГ часто не соответствует текущим реалиям. Отсутствие комплексного и гибкого регулирования порождает неопределенность и риски, а увеличение числа кибератак и утечек данных ставит под угрозу доверие к цифровым платформам без системной киберзащиты.

Отдельным требованием для работы электронных систем в органах прокуратуры стран СНГ является стабильное финансирование технического обслуживания. Ограниченность бюджетных ресурсов создаст проблемы с финансированием цифровых проектов.

Помимо указанного, в СНГ имплементация этических норм в законодательство находится на стадии развития, что создает риски для пользователей и общества. Отсутствие на сегодняшний день согласованной политики и правовых норм в странах СНГ ведет к сложности в регулировании трансграничных ИИ-систем, ограничивает возможность обмена опытом и судебной практики, а также создает угрозу технологического отставания.

Необходимо рассмотреть вопрос по закреплению в законодательстве стран СНГ единого понятия ИИ с учетом международных стандартов. Это позволит унифицировать подходы и облегчить правоприменение.

С учетом изложенного основными рисками внедрения ИИ в деятельность прокуроров можно назвать следующее:

- *социальное недоверие.* Общество может проявлять недоверие к решениям, принятым ИИ, особенно в таких чувствительных областях, как правосудие;

- *отсутствие прозрачности.* Алгоритмы ИИ непрозрачны, что затрудняет понимание и объяснение принятых ими решений;

- *риск предвзятости.* ИИ может унаследовать предвзятость данных, на которых он обучался, что может привести к несправедливым или дискриминационным решениям;

- *зависимость от качества данных.* Качество работы ИИ сильно зависит от качества загружаемых в программу данных. Ошибочные или неполные данные могут привести к неверным выводам и решениям.

- *вопросы безопасности и конфиденциальности.* Системы ИИ могут быть уязвимы для кибератак, что ставит под угрозу конфиденциальность персональных данных и безопасность системы;

- *этические и правовые проблемы.* Использование ИИ поднимает вопросы этики, защиты данных и прав человека, которые необходимо тщательно учитывать и регулировать.

Наряду с этим, внедрение ИИ несет в себе риски нехватки квалифицированных специалистов, зависимости от импортной компьютерной техники и программных обеспечений, высокой стоимости внедрения и обслуживания, сложности определения субъекта юридической ответственности.

Основные перспективные направления для внедрения ИИ.

С учетом задач органов прокуратуры, результатов анкетирования сотрудников прокуратур государств-участников СНГ выделены наиболее востребованные и перспективные направления для внедрения ИИ:

- анализ и обработка обращений граждан;
- подготовка проектов процессуальных и иных документов (протоколы, постановления, речь государственного обвинителя и т.д.);
- анализ и обработка материалов уголовных, гражданских и административных дел;
- анализ и обработка судебных актов;
- прогнозирование преступности;
- мониторинг СМИ и социальных сетей на предмет нарушений прав физических и юридических лиц;
- поиск и установление местонахождения имущества, добытого преступным путем.

Выводы главы 2

Анализ современных тенденций в сфере законодательного регулирования и практического внедрения ИИ в публичное управление и уголовное судопроизводство выявляет необходимость баланса между технологическим прогрессом и фундаментальными правовыми и гуманистическими ценностями. Использование ИИ в этих сферах представляет собой не только шаг к повышению эффективности управления и правосудия, но и порождает риски для прав человека, включая угрозу частной жизни, персональных данных и правовой предсказуемости.

Для предотвращения негативных последствий и обеспечения технологической подотчетности требуется создание комплексной нормативной

базы, основанной на универсальных международных принципах и документах, таких как Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, а также правовые акты, регулирующие ИИ в зарубежных юрисдикциях (например, Закон ЕС «Об искусственном интеллекте» 2024 года и GDPR). Имплементация соответствующих норм на национальном уровне позволит обеспечить правовую определенность, защиту личности и повышение доверия к технологиям ИИ.

Кроме того, законодательные инициативы в сфере ИИ должны быть неразрывно связаны с мероприятиями, направленными на повышение цифровой грамотности, прежде всего среди сотрудников правоохранительных и судебных органов, а также среди широких слоев населения. Это обеспечит не только техническую подготовленность, но и устойчивость правовой и этической среды в условиях стремительной цифровой трансформации. Таким образом, устойчивое и правомерное развитие ИИ возможно только при условии междисциплинарного подхода, сочетающего правовое регулирование, этические ориентиры, образовательные инициативы и научное сопровождение.

Проведенный анализ опыта стран СНГ по внедрению технологий ИИ в деятельность органов прокуратуры демонстрирует наличие правовых и организационно-технологических предпосылок для постепенной цифровизации надзорной и следственной функций. В настоящее время в указанных государствах реализуются пилотные проекты и применяются элементы так называемого «мягкого ИИ», включающие интеллектуальные поисковые системы, аналитические платформы для мониторинга преступности, технологии распознавания лиц и инструменты правовой аналитики. Эти решения позволяют автоматизировать рутинные процессы, повысить точность анализа информации, а также улучшить контроль и прозрачность прокурорской деятельности.

Однако, несмотря на положительную динамику, полноценное использование ИИ в прямом смысле этого понятия пока не достигнуто. Ключевыми барьерами остаются: ограниченность нормативно-правового регулирования, недостаточный уровень технической инфраструктуры, нехватка квалифицированных специалистов в сфере ИИ и информационных технологий, а также потребность в целенаправленном обучении сотрудников прокуратуры основам цифровой грамотности и работе с новыми технологиями. Массовое внедрение ИИ требует не только адаптации правовых механизмов, но и формирования устойчивой профессиональной среды, способной эффективно взаимодействовать с высокотехнологичными инструментами.

Таким образом, перспективное развитие ИИ в органах прокуратуры стран СНГ возможно при условии комплексного подхода, включающего развитие нормативной базы, инвестиции в инфраструктуру, подготовку кадров и научно-методическое сопровождение. При наличии этих условий можно ожидать устойчивую интеграцию ИИ в практику прокурорской деятельности, с сохранением законности, профессиональной ответственности и соблюдением прав человека.

Анализ современного состояния и перспектив использования ИИ в деятельности органов прокуратуры стран СНГ также позволяет сделать вывод о наличии объективной потребности в цифровой трансформации правоохранительной сферы. ИИ способен существенно повысить эффективность надзорной и следственной деятельности за счет автоматизации рутинных операций, ускорения обработки информации, повышения точности анализа и возможности прогнозирования преступной активности. Наиболее перспективными направлениями его внедрения, исходя из задач прокуратуры и мнений самих сотрудников, выступают: обработка обращений граждан, подготовка процессуальных документов, анализ судебных актов и материалов дел, мониторинг медиа-пространства, а также розыск преступного имущества.

Вместе с тем цифровизация органов прокуратуры сопряжена с рядом системных проблем правового и практического характера. Среди них следует выделить:

- социальное недоверие к решениям, принятым с участием ИИ, особенно в сферах, затрагивающих права и свободы личности;
- отсутствие алгоритмической прозрачности, что затрудняет проверку обоснованности и законности принимаемых решений;
- риск алгоритмической предвзятости, обусловленный низким качеством исходных данных;
- угрозы кибербезопасности и конфиденциальности персональной информации;
- отсутствие четких юридических механизмов определения ответственности при ошибках, допущенных ИИ-системами;
- дефицит правового регулирования, касающегося как самих технологий, так и этических стандартов их применения в уголовно-правовой сфере.

К дополнительным практическим вызовам можно отнести нехватку квалифицированных специалистов в области цифровых технологий, зависимость от иностранных программных решений и аппаратного обеспечения, высокие затраты на внедрение и сопровождение ИИ-систем, а также слабую готовность институциональной среды к восприятию технологических изменений.

Успешное и безопасное внедрение ИИ в органы прокуратуры стран СНГ требует не только технологического прогресса, но и комплексного междисциплинарного подхода, включающего разработку специализированного законодательства, инвестиции в подготовку кадров, повышение цифровой грамотности и создание условий для институциональной адаптации к новым формам цифровой правоприменительной практики. При обеспечении указанных требований ИИ сможет эффективно выполнять вспомогательную роль в осуществлении прокурорского надзора, не нарушая при этом принципов законности, справедливости и правовой ответственности.

ГЛАВА 3. ПРАВОВЫЕ ГАРАНТИИ И МЕХАНИЗМЫ КОНТРОЛЯ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОКУРОРСКОЙ ДЕЯТЕЛЬНОСТИ И ПЕРСПЕКТИВЫ

§ 3.1 Защита персональных данных и обеспечение конфиденциальности при работе с системами искусственного интеллекта

Проблема защиты персональных данных физических лиц остро встала перед обществом в связи с широким использованием автоматизированных средств их обработки, в том числе с применением систем ИИ.

Современная мировая правовая система о персональных данных (ПДн) основана на нескольких международных документах, таких как Всеобщая декларация прав человека, Конвенция о защите прав человека и основных свобод и ряде других. Эти документы тесно связаны между собой общим подходом, определяющим право физического лица на уважение личной и семейной жизни. Суть этого права заключается в том, что сам человек, владеющий некими сведениями о себе, вправе решать, подлежат они разглашению или нет.

Тем не менее, законодательством большинства стран мира установлен также перечень субъектов, способных ограничить право человека на неприкосновенность его персональных данных. В случае неправомерного разглашения таких сведений их владелец имеет право на защиту своих нарушенных интересов, при этом меры ответственности нарушителя носят не только гражданско-правовой характер. В ряде стран, в том числе в СНГ, неправомерное разглашение персональных данных является уголовно наказуемым деянием.

Институт защиты персональных данных неразрывно связан с одним из фундаментальных конституционных прав человека – правом на неприкосновенность частной жизни.

В казахстанской юридической науке учеными выработано собственное теоретически обоснованное понятие неприкосновенности частной жизни, под которым следует понимать «гарантированное государством неотчуждаемое и непередаваемое иным способом, за исключением случаев, установленных законодательными актами, право человека на невмешательство, неиспользование и неразглашение охраняемых законом любых, не являющихся общедоступными на равных условиях для неограниченного круга лиц, сведений о личных и семейных нематериальных благах и правах»[59].

Право на неприкосновенность частной жизни, тайну частной жизни, обозначаемое в мире термином **«прайвеси»**, стало фундаментальным правом человека и в концепции прав человека понимается как граница, через которую государство либо третьи лица не должны переступать.

[59] Неприкосновенность частной жизни: Монография / Под общ. ред. проректора-директора МНИИ Академии Г.К. Шушиковой. – Косшы: Академия правоохранительных органов при ГП РК, 2020. – 196 с.

Во Всеобщей декларации прав человека[60], Европейской конвенции о защите прав и основных свобод[61], Международном пакте о гражданских и политических правах[62] и других международных актах закреплено право каждого на неприкосновенность и уважение личной и семейной жизни.

Нормы международных актов в области неприкосновенности частной жизни и защиты персональных данных основаны на следующих ключевых положениях:

Международный акт	Норма
Всеобщая декларация прав человека (1948 г.)	Статья 12: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или посягательств»
Международный пакт о гражданских и политических правах (1966 г.)	Статья 17: «Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на его честь и репутацию»
Европейская Конвенция о защите прав человека и основных свобод (1950 г.)	Статья 8: «Каждый имеет право на уважение его частной и семейной жизни, его жилища и его корреспонденции»
Конвенция СНГ о правах и основных свободах человека (1995 г.)	Статья 9: «Каждый человек имеет право на уважение его личной и семейной жизни, на неприкосновенность жилища и тайну переписки»
Общий регламент по защите данных (GDPR, 2018 г.)	Преамбула: «Защита физических лиц в отношении обработки персональных данных является фундаментальным правом. Принципы и правила защиты физических лиц в отношении обработки их персональных данных должны, независимо от гражданства или места жительства лиц, уважать их фундаментальные права и свободы, в частности их право на защиту персональных данных»

Начиная с 1970 года в Германии, а затем и в других европейских государствах были приняты национальные законы, касающиеся защиты данных (Франция, Швеция)[63]. В 1978 году в Австрии право на защиту данных закреплено в качестве конституционного положения[64]. В дальнейшем таким же путем пошли Венгрия, Словакия, Чехия, Норвегия и другие европейские государства.

[60] Всеобщая декларация прав человека: Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года / [Электронный ресурс] – Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml _(дата обращения: 02.05.2024).

[61] Европейская конвенция по правам человека. – 63 с. / [Электронный ресурс] – Режим доступа: https://www.echr.coe.int/documents/d/echr/Convention_RUS_(дата обращения: 03.05.2024).

[62] Международный пакт о гражданских и политических правах: Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года / [Электронный ресурс] – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 03.05.2024).

[63] Privacy, Data Protection and Cybersecurity: Germany – Lexology [Electronic resource] – Access mode: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany_(Access data: 02.04.2024).

[64] Data Protection in Austria – GDPRhub [Electronic resource] – Access mode: https://gdprhub.eu/Data_Protection_in_Austria_(Access data: 04.04.2024).

Первым международным документом по защите данных стала принятая Советом Европы в 1981 году Конвенция о защите физических лиц при обработке персональных данных, которая регулировала вопросы автоматизированной обработки данных[65].

В 2001 году был принят «Дополнительный протокол» к данной Конвенции №181, в 2018 году – «Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных» (CETS № 223). Изменения внесены вместе с «Элементами регламента Конвенционного комитета».

Данная Конвенция касается только автоматизированной обработки персональных данных. В Конвенции дано определение понятия «персональные данные». Персональные данные означают любую информацию об определенном или поддающемся определению физическом лице («субъект данных»).

При этом есть определенные категории персональных данных, которые в принципе не могут подвергаться автоматизированной обработке, если внутреннее законодательство не устанавливает соответствующих гарантий. Это персональные данные, которые касаются расовой принадлежности, политических взглядов или религиозных и других убеждений, здоровья или половой жизни, судимости физического лица.

Меры безопасности, применяемые для защиты персональных данных, хранящихся в автоматизированных базах данных, должны быть направлены на предотвращение их случайного или несанкционированного уничтожения, или случайной потери, а также на предотвращение несанкционированного доступа, изменения или распространения таких данных.

В 1995 году Европейский Парламент и Совет Европейского Союза разработали и приняли совместную директиву. Она касалась защиты и свободного обращения персональных данных физических лиц[66].

В 2000 году права на уважение частной и семейной жизни, а также на защиту персональных данных нашли свое отражение в Хартии Европейского Союза об основных правах[67]. В 2016 году Советом Европейского Союза и Европейским парламентом принят Генеральный регламент о защите персональных данных (General Data Protection Regulation, далее – GDPR)[68].

Данные правовые акты зачастую выступают основой и ориентиром при разработке различными государствами национального законодательства.

---

[65] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Electronic resource] – Access mode: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108_(Access data: 24.03.2024).

[66] Директива Европейского парламента и Совета Европейского Союза от 24 октября 1995 года № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31067635_(дата обращения: 04.04.2024).

[67] Четвериков А.О. Хартия Европейского союза об Основных правах [Электронный ресурс] – Режим доступа: https://eulaw.ru/treaties/charter/_(дата обращения: 24.03.2024).

[68] General Data Protection Regulation [Electronic resource] – Access mode: https://ogdpr.eu/ru (Access data: 18.05.2024).

Согласно отчету ООН относительно электронного правительства по состоянию на 2021 год, в 145 государствах были приняты законы о конфиденциальности данных. В отдельных случаях особенности использования персональных данных являются достаточно кардинальными.

К примеру, в 2018 году Бразилия внедрила законодательные изменения, направленные на обеспечение безопасности и целостности информации, принадлежащей владельцу. Эти нововведения были представлены в форме нового закона, который создает основу для защиты персональных данных и регулирования их обработки в стране. Закон обеспечивает обязательное соблюдение определенных стандартов и мер безопасности, которые направлены на защиту прав и интересов владельцев данных. Он предусматривает строгие требования к организациям и учреждениям, осуществляющим сбор и обработку персональных данных, и предусматривает санкции за нарушение этих правил.

С 2020 года граждане Бразилии стали владельцами своих персональных данных и обладают правами на эту информацию, имея возможность требовать прозрачности со стороны компаний относительно сбора, хранения и использования данных. Также законодательно закреплено обязательство об информировании относительно случаев утечки персональных данных, чтобы вызвать осознание важности обеспечения интересов интернет-пользователей и преимуществ для всего бразильского общества.

В то же время другие государства обычно проявляют большую снисходительность, предоставляя компаниям и ассоциациям значительную степень саморегулирования, например, США.

В США действует система саморегулирования в отношении персональных данных, где компании и ассоциации принимают собственные меры по защите конфиденциальности. Эта система сочетается с федеральными законами, такими как Закон «О конфиденциальности» 1974 года и положением о конфиденциальности Закона «Об электронном правительстве» 2002 года.

При этом одним из принципов данных законов является принцип минимизации данных, т.е. обработка данных должна быть ограничена тем, что необходимо для достижения цели самой обработки.

В частности, согласно Закону «О конфиденциальности», компании обязаны соблюдать требования Федерального закона «О защите личной информации» (HIPAA), Закона «О личной информации» в Калифорнии (CCPA), Закона «О защите данных потребителей Вирджинии» (VCDPA) и другие регулирующие акты на уровне штатов[69].

Однако стоит отметить, что позднее США вынуждены были ужесточить некоторые аспекты своего регулирования.

Международное и европейское право предусматривает значимые превентивные меры в рамках регулятивных отношений для предотвращения нарушений прав субъектов персональных данных в будущем. В связи с широким

[69] Закон «О конфиденциальности» /[Электронный ресурс] – Режим доступа: https://ybcase.com/company-services/corporate-services/zakony-ssa-o-konfidencialnosti-dannyh_(дата обращения: 14.01.2025).

сбором и увеличивающейся угрозой безопасности персональных данных в некоторых государствах принимаются законы, предоставляющие контрольные функции определенным лицам в отношении сбора, обработки и передачи персональных данных государственным и частным организациям.

Целесообразно затронуть практику Европейского суда по правам человека (далее – ЕСПЧ), поскольку на ее основании формировались требования по защите персональных данных.

Практика ЕСПЧ разработала критерии для правомерного ограничения прав на персональные данные, которые соответствуют общим принципам законного вмешательства в частную жизнь. Эти критерии включают следующее: вмешательство должно соответствовать закону, быть обусловленным легитимной целью и необходимым в демократическом обществе.

Принцип законности обработки персональных данных получает дополнительное разъяснение благодаря практике ЕСПЧ. В этой практике понятие «согласно закону» трактуется не только как требование, чтобы соответствующие меры имели определенное основание в законе, но и как требование к качеству этого закона. Это означает, что закон должен быть доступным и должен предсказуемо влиять на последствия его применения. Доступность закона подразумевает, что нормативно-правовой акт должен быть обнародован. Предсказуемость означает, что норма должна быть ясной, чтобы лицо могло при необходимости регулировать свое поведение с помощью соответствующей поддержки[70].

Легитимность преследуемой цели и необходимость вмешательства в контексте демократического общества должны оцениваться с учетом их соответствия насущным общественным потребностям и принципу пропорциональности по отношению к законной цели. В частности, в случае проверки кандидата на значимую государственную должность, имеющую отношение к вопросам национальной безопасности, интересы безопасности государства могут иметь приоритет над личными интересами субъекта персональных данных, при условии соблюдения принципа минимизации вмешательства в частную жизнь[71].

Таким образом, практика ЕСПЧ определяет критерии и ограничения, которые должны соблюдаться для правомерной обработки персональных данных и защиты прав и свобод граждан.

Понятие «персональные данные», по мнению ЕСПЧ, включает не только информацию о «частной жизни», которая не должна трактоваться узко, поскольку уважение частной жизни включает право устанавливать и развивать отношения с другими людьми, но и информацию о профессиональной и деловой деятельности. Кроме того, публичная информация может рассматриваться как

[70] Case of Amann v. Switzerland, App. No.27798/95. (1992, march) [Electronic resource] / – Access mode: http://hudoc.echr.coe.int/eng?i=001-58497 (Access data: 21.11.2023).
[71] Case of Leander v. Sweden, App. No.9248/81. (1987, march) [Electronic resource] / – Access mode: http://hudoc.echr.coe.int/eng?i=001-57519 (Access data: 28.11.2023).

«частная жизнь», если она систематически собирается и хранится в базах данных, принадлежащих публичным органам власти[72].

ЕСПЧ устанавливает широкий спектр персональных данных, на которые распространяются его решения и примеры, что иллюстрирует разнообразие ситуаций, в рамках которых происходит обработка персональных данных. Это помогает определить границы и защиту прав субъектов данных в соответствии с национальным законодательством.

Среди прав субъекта персональных данных, выделенных в практике ЕСПЧ, можно отметить следующие:

1. Право на доступ к своим персональным данным, которое включает обязанность государства не вмешиваться произвольно в частную жизнь, ограничивая возможность лица получать доступ к информации о себе, которая собирается, хранится, используется и передается государственными органами.

2. Обеспечение защиты персональных данных предполагает положительную обязанность государства по обеспечению уважения к частной жизни путем введения системы правил и гарантий, направленных на защиту данных. Это включает практический и эффективный механизм защиты, который исключает возможность несанкционированного доступа к персональным данным.

3. Право на изменение или уничтожение своих персональных данных является одним из прав, признанных ЕСПЧ. Согласно судебной практике, отказ в предоставлении возможности опровергнуть неправильные персональные данные является нарушением права на уважение частной жизни. Кроме того, положительная обязанность государства в обеспечении уважения к частной жизни включает создание процедур, позволяющих вносить изменения в персональные данные, включая информацию об этническом происхождении. ЕСПЧ также признает так называемое право на забвение, которое предусматривает, что длительное хранение персональных данных без достаточных оснований может составлять несоразмерное вмешательство в право на уважение частной жизни.

В 2021 году в Китае вступил в силу новый закон, который впервые предусматривает всестороннее урегулирование вопросов хранения, передачи и обработки персональных данных. «Закон о защите персональной информации» содержит принцип согласия на использование и передачу персональных данных; анализ влияния на личную жизнь; положения о безопасности и использовании, а также борьбе с утечкой данных.

Статья 2 Закона гласит: «Персональные данные физических лиц защищены законом; организациям, как и частным лицам, не разрешается нарушать права и интересы физических лиц, касающиеся персональных данных».

До этого времени в Китае не существовало комплексной защиты персональных данных. Новый закон восполнил этот пробел и так же, как Общий регламент защиты персональных данных ЕС от 2018 года, стал важным шагом к

[72] Case of Rotaru v. Romania, App. No.28341/95. (1995, february) [Electronic resource] – Access mode: http://hudoc.echr.coe.int/eng?i=001-58586 (Access data: 11.11.2023).

унификации, актуализации и конкретизации принципов защиты персональных данных.

«Этот закон действительно несет на себе четкий отпечаток европейского регламента», – считает профессор права и член комитета по кибербезопасности университета связи Китая Хань Синьхуа. – «Его нормы, например, определение понятия персональных данных, правила обработки конфиденциальной информации, обязательства по мерам безопасности, определение сроков хранения данных, введение должности уполномоченного по защите персональных данных и т.д., во многих отношениях похожи».

Отказ самой густонаселенной страны в мире с самым большим внутренним рынком для цифровых технологий от американской модели и обращение большей частью к европейскому регламенту свидетельствует о значительном успехе Европы в области цифровой экономики.

Новый закон необходимо рассматривать через призму ряда других законов, в которых в течение последних лет сделана попытка дать новое определение правовому цифровому пространству в Китае.

Во-первых, это «Закон о кибербезопасности», вступивший в силу в Китае в июне 2017 года. Далее следует упомянуть «Закон о защите данных», который начал действовать с 1 сентября 2021 года и содержит положения, регулирующие использование, сбор и защиту данных в КНР.

Эксперт по китайскому праву Кембриджского университета Женьбинь Цзуо рассматривает и закон о кибербезопасности, и закон о безопасности данных в рамках международного законодательства по безопасности. Си Цзиньпин также подчеркнул эту связь: «Без кибербезопасности невозможна и национальная безопасность»[73].

В рамках масштабных правовых реформ, приуроченных к 50-летию образования Объединенных Арабских Эмиратов, правительство страны приняло Федеральный закон №45 от 2021 года (далее – Закон) о защите персональных данных (Personal Data Protection Law, PDPL).

Закон отражает стремление ОАЭ к гармонизации национального законодательства с международными стандартами, включая Общий регламент по защите данных Европейского союза (GDPR). При этом, несмотря на общую концептуальную близость к европейской модели, Закон содержит ряд национально-ориентированных особенностей, продиктованных специфическими социально-правовыми условиями Эмиратов.

Закон регулирует вопросы сбора, обработки, хранения и передачи персональных данных, устанавливая юридические обязанности для всех участников обработки – контролеров и обработчиков данных. Контролер – это лицо (физическое или юридическое), определяющее цели и способы обработки персональных данных. Обработчик – лицо или организация, обрабатывающая данные от имени и по поручению Контролера.

[73] [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-kitae-zakonodatelstvo-v-tsifrovuyu-epohu_(дата обращения: 05.03.2025).

Закон закрепляет базовые принципы обработки данных, среди которых:

- законность, справедливость и прозрачность обработки;
- ограничение цели (обработка только в заранее определенных рамках);
- точность и актуальность данных;
- ограниченное по времени хранение;
- обеспечение технической и организационной безопасности.

Особое внимание уделяется обязательности удаления персональных данных после достижения цели их обработки, что соотносится с принципом «**право на забвение**».

Законом закреплены права физических лиц, включая:

- право на доступ к персональным данным;
- право на исправление или удаление неточной информации;
- право на ограничение или возражение против обработки;
- право на переносимость данных;
- право не быть объектом исключительно автоматизированных решений.

Данные положения подчеркивают приоритет субъекта данных в управлении личной информацией и формируют основу для правосубъектности в цифровом пространстве.

Закон распространяется на:

- всех контролеров и обработчиков, находящихся в ОАЭ;
- субъектов, осуществляющих обработку данных резидентов ОАЭ, независимо от юрисдикции;
- трансграничную обработку, если она затрагивает данные лиц, находящихся на территории ОАЭ.

В то же время из-под действия Закона выведены:

- государственные органы;
- компании, зарегистрированные в свободных экономических зонах (например, ADGM и DIFC), действующие по своим локальным законам о защите данных;
- чувствительная информация, уже регулируемая специализированными законами (например, в области здравоохранения и финансов).

Хотя согласие субъекта данных является ключевым условием для законной обработки, Закон допускает обработку и в безсогласных случаях, в том числе:

- при необходимости заключения, исполнения или расторжения договора;
- в случае явного обнародования информации самим субъектом;
- при защите жизни и интересов субъекта;
- при участии в судебных процессах или обеспечении общественной безопасности;
- при осуществлении государственной политики в сфере здравоохранения.

Одновременно с Законом был принят Федеральный закон № 44 от 2021 года «Об управлении данными», которым учрежден Офис по защите данных ОАЭ (UAE Data Office) – уполномоченный орган по контролю за соблюдением PDPL. В его функции входят:

- разработка методических рекомендаций и регламентов;
- создание систем подачи жалоб и обращений;
- мониторинг соблюдения закона;
- применение административных санкций[74].

В целом следует отметить, что странами с развивающейся индустрией ИТ-технологий и ИИ проводится кропотливая работа по разработке законодательства в сфере защиты персональных данных. В свою очередь законодательство, регламентирующее порядок применения систем ИИ, находится на начальной стадии своего развития.

Вместе с тем развивающаяся и быстро меняющаяся технологическая среда создает новые угрозы и риски в сфере защиты персональных данных. В этой связи индивидуальная ответственность пользователей в области безопасности данных также играет важную роль.

Для повышения уровня безопасности необходимо, чтобы все участники процессов хорошо знали основополагающие принципы защиты персональных данных и могли эффективно их применять. Именно принципы защиты персональных данных устанавливают рамки применения законодательной базы, регулируя сбор и обработку персональных данных.

Вопрос о необходимости защиты персональных данных в органах прокуратуры не вызывает сомнений. Кроме этого, данная задача актуализируется в связи с проходящей цифровой трансформацией прокуратур стран СНГ, а также с внедрением в их деятельность технологий и систем ИИ, которые используются в том числе и для обработки персональных данных.

Республика Казахстан

Казахстан при вступлении в ООН принял обязательства по выполнению положений Всеобщей декларации прав человека, а затем ратифицировал и Международный Пакт о гражданских и политических правах.

Последовательное закрепление права на неприкосновенность частной жизни в Пакте о гражданских и политических правах, Конвенции о защите прав человека и основных свобод, Конвенции СНГ о правах и основных свободах человека и других международных актах стало ключевым моментом в признании его со стороны международного сообщества.

В Республике Казахстан вопросы правового регулирования защиты персональных данных в деятельности органов прокуратуры играют важную роль в обеспечении прав и свобод граждан, а также правопорядка и законности.

Правовое регулирование защиты персональных данных в Казахстане строится на основе Конституции Республики Казахстан, законов и подзаконных актов, включая Закон «О персональных данных», принятый в 2013 году.

[74] [Электронный ресурс] – Режим доступа: https://www.damacproperties.com/ru/blog/uae-data-protection-law-compliance-steps-businesses/_(дата обращения: 05.03.2025).

Основные нормативные правовые акты Республики Казахстан, регулирующие отношения в сфере защиты персональных данных и деятельности органов прокуратуры Республики Казахстан		
1	Конституция РК от 30 августа 1995 года	Содержит основные нормы и принципы, касающиеся прав и свобод граждан, включая право на конфиденциальность и защиту персональных данных
2	Конституционный закон РК «О прокуратуре» от 5 ноября 2022 года № 155-VII ЗРК	Определяет компетенцию, организацию и порядок деятельности прокуратуры Республики Казахстан
3	Закон РК «О персональных данных и их защите» от 21 мая 2013 года № 94-V	Устанавливает правовые принципы сбора, обработки и хранения персональных данных, а также определяет права и обязанности субъектов персональных данных и операторов
4	Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V	Регулирует общественные отношения в сфере информатизации в Казахстане между госорганами, физ- и юрлицами при создании, развитии и эксплуатации объектов информатизации, а также при господдержке развития отрасли ИКТ
5	Закон РК «О связи» от 5 июля 2004 года № 567-II	Включает в себя нормы, регулирующие обмен информацией через сети связи, в том числе о персональных данных
6	Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства РК от 20 декабря 2016 года №832	Устанавливают единые требования в области ИКТ и обеспечения информационной безопасности
7	Правила сбора, обработки персональных данных, утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 21 октября 2020 года № 395/НҚ	Устанавливают правила сбора, обработки персональных данных
8	Ряд других нормативных актов, принятых органами исполнительной власти, включающих в себя приказы, инструкции, правила и т.д.	Устанавливают конкретные процедуры и требования к обработке и защите персональных данных в различных сферах деятельности

Согласно Закону «О персональных данных и их защите» от 21 мая 2013 года № 94-V (далее – Закон), **персональные данные** – это сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе. Закон определяет основные принципы сбора, обработки и хранения персональных данных, устанавливает ответственность за их нарушение, а также

предусматривает механизмы контроля со стороны государственных органов, включая прокуратуру.

Регулирование обработки и защиты персональных данных императивно вынесено за пределы действия Закона в части отношений, касающихся: личных и семейных нужд; формирования, хранения и использования архивных документов; защиты государственных секретов; разведывательной, контрразведывательной, оперативно-розыскной деятельности; осуществления охранных мероприятий по обеспечению безопасности охраняемых лиц и объектов.

11 декабря 2023 года Президентом Республики Казахстан подписан Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» № 44-VIII, который вносит изменения и дополнения в 14 нормативных правовых актов, в т.ч. в 4 кодекса и 10 законов: Кодекс РК «Об административных правонарушениях» от 5 июля 2014 года; Предпринимательский кодекс РК от 29 октября 2015 года; Трудовой кодекс РК от 23 ноября 2015 года; Кодекс РК «О здоровье народа и системе здравоохранения» от 7 июля 2020 года; Закон РК «О банках и банковской деятельности в Республике Казахстан» от 31 августа 1995 года; Закон РК «О страховой деятельности» от 18 декабря 2000 года; Закон РК «О рынке ценных бумаг» от 2 июля 2003 года; Закон РК «О кредитных бюро и формировании кредитных историй в Республике Казахстан» от 6 июля 2004 года; Закон РК «О миграции населения» от 22 июля 2011 года; Закон РК «О микрофинансовой деятельности» от 26 ноября 2012 года; Закон РК «О персональных данных и их защите» от 21 мая 2013 года; Закон РК «Об информатизации» от 24 ноября 2015 года; Закон РК «О платежах и платежных системах» от 26 июля 2016 года; Закон РК «О цифровых активах в Республике Казахстан» от 6 февраля 2023 года.

В соответствии с законом собственник и (или) оператор с 1 июля 2024 года обязаны в течение одного рабочего дня с момента обнаружения нарушения безопасности персональных данных уведомить уполномоченный орган о таком нарушении с указанием контактных данных лица, ответственного за организацию обработки персональных данных (при наличии).

Деятельность органов прокуратуры в Республике Казахстан включает надзор за соблюдением законов, в том числе и в области защиты персональных данных. Прокуратура имеет право проводить проверки и расследования в случае нарушений законодательства о персональных данных, а также предпринимать меры по пресечению таких нарушений.

Согласно Конституционному закону Республики Казахстан «О прокуратуре» от 5 ноября 2022 года № 155-VII ЗРК, прокурор в соответствии со своей компетенцией вправе в установленном законодательством Республики Казахстан порядке получать доступ к информационным системам и ресурсам правоохранительных и иных государственных органов и организаций с соблюдением требований по защите персональных данных и иной охраняемой законом тайны.

Одним из ключевых аспектов правового регулирования защиты персональных данных и деятельности органов прокуратуры в Казахстане является обеспечение баланса между защитой прав граждан на конфиденциальность и безопасность персональных данных и обеспечением безопасности общества и государства. Прокуратура играет важную роль в этом процессе, обеспечивая соблюдение законов и защиту прав граждан.

Законодательство Казахстана опирается на базовый принцип предоставления субъектом персональных данных своего согласия на их сбор и обработку. При этом отсутствует указание на такие условия правомерности обработки персональных данных, как конклюдентные действия субъекта и договорные отношения между субъектом и собственником (оператором). Законодатель также фиксирует возможность обработки персональных данных в иных установленных законодательством случаях. Особенностью является правомерность обработки персональных данных в случае неисполнения субъектом своих обязанностей по представлению персональных данных в соответствии с действующими НПА.

В ноябре 2020 года вступили в силу Правила сбора, обработки персональных данных, утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

Правила распространяются на отношения, возникающие между собственниками, операторами, субъектами, а также третьими лицами в процессе сбора и обработки персональных данных. Согласно документу, сбор и обработка собственником или оператором персональных данных допускается в объеме, определенном перечнем персональных данных, необходимом и достаточном для выполнения осуществляемых задач.

При этом перечень персональных данных определяется и утверждается в соответствии с правилами определения собственником или оператором перечня персональных данных.

Отдельно говорится об обработке персональных данных в деятельности судов. Так, тексты судебных актов Верховного суда Республики Казахстан, местных и других судов, за исключением текстов судебных актов, предусматривающих положения, которые содержат сведения, составляющие государственную или иную охраняемую законом тайну, а также судебные акты по делам, рассмотренным в закрытом судебном разбирательстве, размещаются на сервисах «Судебный кабинет», «Банк судебных актов» интернет-ресурса Верховного Суда в полном объеме. Для обеспечения безопасности участников судебного процесса и защиты охраняемой законом тайны при сборе и использовании либо распространении третьими лицами судебных актов из них исключаются (обезличиваются) персональные данные. При этом третьи лица принимают на себя обязательства по обеспечению выполнения требований закона.

Что касается вопросов безопасности персональных данных при их обработке, то следует отметить, что в действующем на сегодняшний день законодательстве Казахстана присутствует только лишь частичная регламентация

необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий.

Тем не менее, существуют отдельные императивные нормы о предотвращении несанкционированного доступа к персональным данным, о своевременном обнаружении фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить, и о минимизации неблагоприятных последствий несанкционированного доступа к персональным данным.

Трансграничная передача персональных данных определена как передача персональных данных на территорию иностранных государств безотносительно статуса получающей стороны. Иначе говоря, трансграничной будет признана передача персональных данных с территории Казахстана на территорию другого государства, даже в том случае, если такая передача производится внутри одной базы данных, собственником либо оператором которой является резидент Республики Казахстан. Особенностью является отсутствие института получения предварительного разрешения уполномоченного органа для передачи персональных данных на территорию иностранного государства, если оно не обеспечивает удовлетворительный уровень защиты персональных данных. Кроме того, существует норма о «локализации» персональных данных, а именно: «хранение персональных данных осуществляется собственником и (или) оператором, а также третьим лицом в базе, которая хранится на территории Республики Казахстан».

Вместе с тем, следует отметить, что Республика Казахстан не является участником Конвенции о защите физических лиц при автоматизированной обработке персональных данных ETS от 28 января 1981 года № 108. Однако подходы к регулированию рассматриваемой сферы близки к принципам и положениям данного документа. Общая структура регулирования является компактной и содержит минимально необходимый набор нормативных актов, включая основной закон о персональных данных и их защите и подзаконные акты в виде постановлений Правительства Республики Казахстан и приказов Министерства цифрового развития, инноваций и аэрокосмической промышленности республики.

Законом Республики Казахстан от 11 декабря 2023 года введено понятие **«нарушение безопасности персональных данных»**, понимаемое как *«нарушение защиты персональных данных, повлекшее незаконное распространение, изменение и уничтожение, несанкционированное распространение передаваемых, хранимых, обрабатываемых персональных данных или несанкционированный доступ к ним»*[75].

[75] Закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет»

Уполномоченный государственный орган в сфере защиты персональных данных компетентен **осуществлять государственный контроль за соблюдением законодательства о персональных данных и их защите**. Ранее для возбуждения административного дела требовалась жалоба лица, то теперь основанием могут быть и выявленные нарушения в ходе проверки.

В случае утечки или нарушения безопасности персональных данных операторы обязаны немедленно уведомлять уполномоченный орган и предпринимать меры по устранению последствий таких нарушений.

Национальное законодательство предусматривает ответственность по статье 508 КРКоАП за разглашение участниками национального превентивного механизма сведений о частной жизни лица. Если это сопряжено с нарушением персональных данных, то ответственность наступает по части 4 статьи 451 КРКоАП.

Уголовная ответственность наступает по статьям 138, 147, 148, 149, 321, 151 УК за разглашение тайны усыновления (удочерения), нарушение неприкосновенности частной жизни и законодательства о персональных данных, тайны переписки, неприкосновенности жилища, врачебной тайны, тайны голосования.

За нарушение законодательства о персональных данных предусмотрена административная ответственность по статье 79 КРКоАП («Нарушение законодательства о персональных данных»), части 4 статьи 451 («Распространение персональных и биометрических данных, иной информации»), пункту 1 части 1 статьи 641 («Нарушение законодательства об информатизации»).

В случаях совершения деяний, связанных с нарушением законодательства о персональных данных и их неправомерным использованием, уголовная ответственность наступает по части 1 статьи 147 УК «Нарушение неприкосновенности частной жизни и законодательства о персональных данных и их защите» и по статьям 205, 206, 208, 209, 211 УК главы 7 «Уголовные правонарушения в сфере информатизации и связи».

Случаи прекращения в связи с отсутствием состава правонарушения начатых административных или уголовных производств могут быть обжалованы в предусмотренном законом порядке.

Невозможность привлечения к административной либо уголовной ответственности также не лишает право лица обратиться в суд в порядке гражданского судопроизводства за защитой нарушенных прав.

Одним из важнейших институтов, при помощи которого обеспечивается нормативность Конституции, является **Конституционный Суд РК**.

К примеру, в Конституционный Суд поступило обращение физического лица, о том, что подпункт 3 пункта 1-1 статьи 14 Закона «О средствах массовой информации» (далее – СМИ), в соответствии с которым не требуется согласие отображаемого в СМИ лица, если его использование осуществляется в целях

[Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z2300000044/history_ (дата обращения: 02.10.2024).

защиты конституционного строя и охраняемых законов прав, не соответствует пункту 2 статьи 4 и пункту 1 статьи 18 Конституции РК.

Норма нарушает **право на неприкосновенность частной жизни**, личную и семейную тайну, защиту чести и достоинства, в связи с чем лицо просило признать ее неконституционной.

Ранее судами в иске о возложении обязанности удалить фотоизображение заявителя, опубликованное без его согласия в СМИ, а также в апелляционной жалобе указанному лицу было отказано.

Конституционный Суд не усмотрел нарушений неприкосновенности частной жизни и постановил признать подпункт 3 пункта 1-1 статьи 14 Закона «О средствах массовой информации» соответствующим Конституции РК.

По выводу суда право на изображение не должно создавать необоснованные затруднения гражданам в реализации других прав, а также препятствия СМИ в информировании о событиях, вызывающих общественный интерес, и об участвующих в них лицах (Нормативное постановление Конституционного Суда РК от 21 апреля 2023 года № 11).

В Конституционный Суд также поступило обращение кандидата в депутаты городского маслихата о рассмотрении на соответствие пункту 3 статьи 33 Конституции РК нормы подпункта 2 пункта 4 статьи 4 Конституционного закона «О выборах в Республике Казахстан». Регистрация заявителя в качестве кандидата в депутаты была аннулирована ввиду указания недостоверных сведений в декларации о привлечении к уголовной ответственности.

Решениями всех судебных инстанций заявителю было отказано в удовлетворении иска к избирательной комиссии.

Из материалов следует, что ранее заявитель был осужден и приговорен к лишению свободы с лишением права занимать государственную должность сроком на два года.

Конституционный Суд указал, что международные стандарты допускают установление ограничений пассивного избирательного права граждан во внутреннем законодательстве страны с соблюдением принципа пропорциональности и соразмерности. Законодатель вправе установить повышенные требования к репутации лиц, занимающих публичные должности. В этой связи подпункт 2 пункта 4 статьи 4 Конституционного закона РК «О выборах в Республике Казахстан» признан соответствующим Конституции.

Таким образом, изучение правового регулирования института защиты персональных данных в Республике Казахстан показало, что для применения систем ИИ необходимы четкие стандарты, определяющие гарантию правовой защищенности личности, которые могут быть законодательно закреплены в виде принципов сбора, обработки и защиты персональных данных (законности и справедливости, целесообразности; распределенности персональных данных; достаточности и точности обработки).

Необходимо установление в законе понятия «конфиденциальность» как требования, предъявляемого в отношении ответственных лиц, осуществляющих работу с персональными данными.

Ученые в сфере правоохранительной деятельности Республики Казахстан полагают, что в целом действующее национальное законодательство в сфере защиты тайны частной жизни, законодательство о персональных данных и их защите необходимо совершенствовать с учетом подходов, сформулированных общепризнанными международными институтами, организационной готовности среды его применения и степени востребованности общества[76].

Российская Федерация[77]

Понятие персональных данных в Российской Федерации было введено Указом Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера» и получило дальнейшее развитие в связи с принятием нового Трудового кодекса Российской Федерации в 2001 году.

Основным нормативным правовым актом, регулирующим правоотношения в области использования персональных данных в Российской Федерации, является Федеральный закон «О персональных данных».

Закон регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами и др., с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Основной целью указного Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, затрагивающей его право на неприкосновенность частной жизни, личную и семейную тайну. Персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

По смыслу федерального законодательства, персональные данные представляются в качестве информации, неразрывно связанной с личностью ее обладателя. Персональные данные можно представить в виде открытого перечня сведений, независимо от формы их представления. Законодатель сохраняет возможность расширения этого перечня по мере того, как будет меняться социальный статус и иной статус их обладателя. В основу такого перечня положены: фамилия, имя, отчество, дата и место рождения, адрес, семейное,

---

[76] [Электронный ресурс] – Режим доступа: https://academy-rep.kz/item.php?id=770/Монография «Неприкосновенность частной жизни»_(дата обращения: 10.10.2024).

[77] Информация авторского коллектива Генеральной прокуратуры и Университета прокуратуры Российской Федерации/ исх.№1-11-2024/578-24/ 04.04.2024 г.

социальное, имущественное положение, образование, профессия, доходы физического лица и т.д.

Обеспечивая защиту персональных данных, государство тем самым укрепляет правовую защищенность и безопасность человека и гражданина, реализуя на практике положения Конституции Российской Федерации о защите прав и свобод человека и гражданина, создает благоприятную обстановку для всестороннего развития гражданского общества.

Защита персональных данных граждан предполагает, прежде всего, обеспечение их защиты) от несанкционированного доступа к ним со стороны криминальных структур, других граждан, представителей государственных органов и служб, не имеющих на то соответствующих полномочий, а также обеспечение сохранности, целостности и доступности персональных данных.

Закон «О персональных данных» (ст.7) устанавливает обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать их третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. То есть персональные данные относятся к категории сведений конфиденциального характера, что обуславливает отсутствие свободного доступа к ней (т.е. обеспечение ее конфиденциальности).

Обеспечение конфиденциальности персональных данных в процессе их обработки наряду с установленными принципами работы с ними и получением согласия на обработку является обязательным условием, определяющим дальнейшую деятельность оператора. Требование конфиденциальности связано с ограничением на распространение персональных данных без согласия субъекта персональных данных или наличия иного законного основания. Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться их конфиденциальность.

Требование конфиденциальности не распространяется на персональные данные, разрешенные субъектом персональных данных для распространения, обезличенные персональные данные. Федеральным законом предусмотрено исключение из режима конфиденциальности для общедоступных массивов персональных данных (справочники, телефонные книги, адресные книги и т.п.), которые создаются в целях информационного обеспечения общества.

Помимо требования обеспечения конфиденциальности персональных данных при их обработке, оператор обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В контексте статьи 16 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ можно говорить о необходимости защиты персональных данных, т.е.

организации деятельности, направленной на предотвращение утечки персональных данных, несанкционированных и непреднамеренных воздействий на персональные данные, то есть обеспечения их безопасности. Основные меры по обеспечению безопасности персональных данных определены в статье 19 Федерального закона Российской Федерации «О персональных данных».

К органам, участвующим в правоотношениях, связанных с обработкой персональных данных в соответствии с законодательством, относится Правительство Российской Федерации, основными задачами которого в части защиты персональных данных являются: определение перечня мер, направленных на выполнение требований нормативных правовых актов операторами персональных данных[78]; установление уровней защищенности персональных данных при их обработке в информационных системах ПДн (далее – ИСПДн) и требований к защите персональных данных при их обработке в указанных системах, а также требований к материальным носителям биометрических персональных данных; определение особенностей обработки персональных данных, осуществляемой без использования средств автоматизации.

Состав и содержание требований к защите персональных данных, организационным и техническим мерам по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) устанавливаются ФСБ России и ФСТЭК России в пределах их полномочий. Данное право и одновременно обязанность установлена частью 4 статьи 19 Федерального закона «О персональных данных».

Одновременно с этим частью 8 указанной статьи контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в государственных ИСПДн также осуществляются ФСБ России и ФСТЭК России в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн.

Кроме указанных органов контроля и регулирования правоотношений в области обработки и обеспечения безопасности персональных данных в статье 23 Федерального закона «О персональных данных» определен уполномоченный орган по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

Таким органом является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

[78] Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» / [Электронный ресурс]: Режим доступа: http://government.ru/docs/all/81438/_(дата обращения: 05.03.2024).

Из всех видов конфиденциальной информации, обрабатываемой органами прокуратуры, пожалуй, наибольший объем составляют персональные данные граждан.

Как отмечено в Национальной стратегии развития искусственного интеллекта на период до 2030 года, в Российской Федерации в связи с изменением экономической ситуации, введением отдельных, по своему масштабу односторонних ограничительных мер, возникли новые вызовы для Российской Федерации в сфере развития ИИ, к которым в том числе относится необходимость обеспечения защиты персональных данных и иной информации ограниченного доступа.

В целях обеспечения реализации требований законодательства Российской Федерации в области защиты персональных данных при их обработке в органах прокуратуры необходимо дальнейшее развитие и совершенствование соответствующей системы, т.е. системы защиты персональных данных. Данная система призвана обеспечивать конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных органов прокуратуры.

Правовое регулирование обработки и защиты персональных данных в органах прокуратуры Российской Федерации осуществляется по двум направлениям. Первое связано с осуществлением прокурорского надзора, второе – с прохождением службы (работой) в органах и организациях прокуратуры Российской Федерации.

Органы прокуратуры Российской Федерации имеют право осуществлять обработку персональных данных физических лиц, в том числе специальных категорий персональных данных в соответствии с требованиями Конституции Российской Федерации, положениями федеральных законов «О прокуратуре Российской Федерации», «О персональных данных», «О противодействии коррупции», «Об основах охраны здоровья граждан в Российской Федерации». Обработка в органах прокуратуры персональных данных, полученных в связи с реализацией прокурорского надзора, осуществляется в целях обеспечения защиты прав и свобод человека и гражданина, укрепления законности и правопорядка.

Необходимо обратить внимание на тот факт, что в последнее время процесс обработки и защиты персональных данных в органах прокуратуры при осуществлении прокурорского надзора все более тесно связан с процессом цифровой трансформации органов и организаций прокуратуры Российской Федерации.

В рамках цифровой трансформации в органах прокуратуры создаются условия для совершенствования надзорной функции в связи с цифровизацией объектов надзора. Это обуславливает необходимость дальнейшего развития прокуратуры в рамках такого приоритетного направления цифровой трансформации, как высокотехнологичный надзор. Он в первую очередь связан с формированием на основе комплексной оптимизации выполнения надзорной функции единой безопасной цифровой платформы для обеспечения

электронного взаимодействия органов прокуратуры всех уровней между собой и с другими государственными органами.

Повышение эффективности надзора предполагается осуществить путем внедрения современных и перспективных информационных технологий обработки первичной информации во всех видах надзорной деятельности. Как представляется, наиболее современными и перспективными являются технологии, основанные на ИИ, внедрение которых в прокурорскую деятельность и происходит в настоящее время.

Таким образом, совершенствование правого регулирования защиты персональных данных в органах прокуратуры должно осуществляться с учетом всех особенностей функционирования и развития информационных систем, в которых реализованы алгоритмы ИИ.

В ходе реализации надзорной деятельности прокуроры используют целый комплекс автоматизированных информационных систем, цифровых сервисов, систем мониторинга и анализа больших данных, информационно-аналитических комплексов и систем, систем дистанционного контроля и надзора и др., решающих узкоспециализированные задачи, то есть использующих алгоритмы «слабого» ИИ.

Обеспечение безопасности персональных данных в органах прокуратуры Российской Федерации является неотъемлемой частью процесса обработки персональных данных. Как отмечено выше, вопросы организации работ по обеспечению их безопасности регулируются «Инструкцией о порядке обработки в органах прокуратуры Российской Федерации персональных данных, полученных в связи с осуществлением прокурорского надзора», утвержденной приказом Генерального прокурора Российской Федерации.

Так, одним из основных мероприятий по обеспечению безопасности персональных данных является назначение лица, ответственного за организацию обработки персональных данных, полученных в связи с осуществлением прокурорского надзора. Данное лицо обязано осуществлять внутренний контроль за соблюдением требований законодательства Российской Федерации к защите персональных данных.

Кроме этого на работников прокуратуры возложена обязанность принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, представления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Также на работников прокуратуры возложена обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

Помимо обработки персональных данных физических лиц, осуществляемой в рамках прокурорского надзора, в органах прокуратуры осуществляется обработка ПДн работников прокуратуры в связи с прохождением службы (работой) в органах

и организациях прокуратуры Российской Федерации, а также пенсионеров и ветеранов органов и организаций прокуратуры.

Так, в пункте 4 статьи 41.2 Федерального закона Российской Федерации «О прокуратуре Российской Федерации» установлено, что обработка персональных данных, включенных в состав личного дела прокурорского работника, реализация прав прокурорских работников как субъектов персональных данных осуществляются в соответствии с положениями законодательства Российской Федерации в области персональных данных. Помимо вышеназванного закона, обработка и защита персональных данных в органах и организациях прокуратуры Российской Федерации осуществляется с учетом требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации и иными законодательными и нормативными правовыми актами Российской Федерации, регламентирующими порядок обработки персональных данных.

Генеральным прокурором Российской Федерации утверждены «Правила обработки персональных данных в связи с прохождением службы (работой) в органах и организациях прокуратуры Российской федерации» в соответствии с которыми осуществляется обработка персональных данных и их защита.

Установлено обязательное требование обеспечения защиты персональных данных от неправомерного их использования или уничтожения в порядке, установленном нормативными правовыми актами Российской Федерации, а также требование обеспечения их конфиденциальности. Данные требования в первую очередь касаются работников, ответственных за обработку персональных данных в органах прокуратуры.

В органах и организациях прокуратуры страны обеспечение безопасности персональных данных, обрабатываемых в автоматизированных информационных системах, достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным.

Вместе с тем в целях выявления и предотвращения нарушений законодательства Российской Федерации в области персональных данных в органах, организациях прокуратуры осуществляется внутренний контроль соответствия обработки персональных данных нормам законодательства Российской Федерации в области персональных данных, в том числе требований к их защите от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

В настоящее время для обработки персональных данных работников и пенсионеров органов прокуратуры России используются специализированный автоматизированный информационный комплекс. Комплекс предназначен для автоматизированного управления кадрами, распределенного учета сотрудников органов прокуратуры и их персональных данных, процессов дополнений и изменений в штатном расписании, а также для учета и сопровождения

пенсионного обеспечения бывших работников органов прокуратуры и членов их семей.

Разграничение прав доступа пользователей осуществляется на основе реализованной ролевой модели. Для хранения данных выделена отдельная система хранения данных. Взаимодействие со смежными информационными системами отсутствует. **Кыргызская Республика**

Анализ законодательного регулирования защиты персональных данных в Кыргызской Республике показывает, что Конституцией страны закреплено право каждого человека на неприкосновенность личной жизни, а именно: запрет сбора, хранения, использования и распространения конфиденциальной информации и информации о частной жизни человека без его согласия.

В 2008 году был принят Закон «Об информации персонального характера», направленный на правовое регулирование работы с персональными данными на основе общепринятых международных принципов и норм в соответствии с Конституцией и законами Кыргызской Республики.

Персональные данные – это любая информация, используя которую, можно прямо или косвенно узнать (идентифицировать) человека. Например, ФИО, персональный идентификационный номер (ПИН/ИНН), биометрические данные, семейное положение, онлайн-идентификатор (имя пользователя в социальных сетях, IP-адрес), кадры камеры видеонаблюдения, позволяющие идентифицировать физическое лицо и другая информация.

В 2021 году в соответствии с Указом Президента Кыргызской Республики учреждено Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики, разрабатывающее и реализующее единую государственную политику в сфере информации персонального характера, осуществляющее функции по обеспечению защиты прав субъектов персональных данных (субъектов), регистрации держателей (обладателей) массивов персональных данных, ведению Реестра держателей массивов персональных данных.

Целью деятельности Агентства является обеспечение защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных, независимо от применяемых средств обработки этой информации, включая использование информационных технологий.

Вместе с тем в соответствии с требованиями пункта 10 Положения Государственного агентства по защите персональных данных функции в сфере регулирования, координации, надзора и контроля не распространяются на персональные данные, полученные в результате деятельности органов прокуратуры Кыргызской Республики, правоохранительных органов и органов, осуществляющих оперативно-розыскную, разведывательную и контрразведывательную деятельность, производство официальной статистики, правовой режим которых устанавливается в соответствии с законами Кыргызской Республики «Об оперативно-розыскной деятельности» и «О защите государственных секретов Кыргызской Республики».

Таким образом, прокуратура Кыргызской Республики как высший надзорный орган за исполнением законов на территории страны самостоятельно устанавливает политику защиты персональных данных, в соответствии с Законом «Об информации персонального характера».

Генеральная прокуратура Кыргызской Республики как держатель стратегических, государственных автоматизированных информационных систем (Единые реестры преступлений, правонарушений, система электронного документооборота, пробация, база данных осужденных и другие) обеспечивает охрану персональных данных, режим их конфиденциальности, во избежание несанкционированного доступа, блокирования, передачи, а равно их случайного или несанкционированного уничтожения, изменения или утраты. Также прокуратура как держатель и разработчик информационных систем, содержащих в себе массивы персональных данных, обеспечивает сохранность и достоверность персональных данных, а также определяет режим доступа к ним.

С технической стороны, государством поставлен заслон самовольной записи персональных данных и изменению или уничтожению записанных персональных данных и обеспечена возможность установления, когда, кем и какие персональные данные были изменены (логирование действий в системах). Также обеспечена безопасность систем обработки данных, ранжированный доступ к информации, т.е. каждый пользователь систем имеет доступ только к тем персональным данным, к обработке которых он имеет допуск[79].

Внедрение искусственного интеллекта в работу прокуроров в контексте защиты персональных данных.

С точки зрения деятельности органов прокуратуры перспективными для внедрения и использования являются такие виды ИИ, как **машинное обучение** (machine learning – ML) и **обработка естественного языка** (Natural Language Processing – NLP), наиболее отвечающие характеру деятельности прокуроров. Безусловно, они могут использоваться и **для обработки персональных данных,** а следовательно, обеспечение их защиты должно учитывать особенности обработки информации данными видами ИИ.

Применение систем ИИ для обработки персональных данных неизбежно ставит вопрос об адекватности существующих правил их защиты и о необходимости развития и совершенствования всего спектра средств и методов обеспечения безопасности персональных данных.

Развитие правовых норм, регулирующих вопросы использования технологий и систем ИИ в деятельности органов прокуратуры для обработки персональных данных и вопросы их защиты, является важной задачей. Как представляется, такая работа должна проводиться в органах прокуратуры с учетом ряда особенностей, на которые необходимо обратить внимание.

Ограничение на использование искусственного интеллекта при обработке персональных данных.

[79] Информация авторского коллектива Генеральной прокуратуры Кыргызской Республики по п.10. Рабочей программы/ 24/150-16-16-05-04805/29.08.2024 г.

Автоматизированные системы, использующие ИИ, привлекательны тем, что, на первый взгляд, обладают «математической объективностью», т.е. абсолютной беспристрастностью при принятии решений. Такая беспристрастность, основанная на математических алгоритмах, может создать соблазн принимать решения, основываясь только на результатах, предложенных ИИ. Однако такой подход представляется не вполне оправданным, а в ряде случаев и опасным.

Прокурор, принимающий решения, должен иметь правовую основу принятия решений, руководствоваться внутренними убеждениями и совестью, которые не доступны и отличаются от тех, которые принимаются/предлагаются системой ИИ, он должен обладать реальной свободой в процессе принятия решения.

В случаях, когда лица, принимающие решения, не имеют по каким-либо причинам возможности контролировать решения, принимаемые системой ИИ, необходимо на основе анализа рисков и мнения экспертов определить целесообразность применения систем ИИ.

Обеспечение прозрачности принятия решений системами ИИ при обработке ПДн в органах прокуратуры.

Прозрачность применения ИИ может относится к алгоритмам или логике работы ИИ, а также к наборам данных, используемым для обучения алгоритмов. Обеспечение прозрачности направлено на снижение риска противоправного использования ПДн, обеспечение их безопасности.

Что касается доступа к алгоритмам работы ИИ, то здесь может возникнуть ряд проблем, связанных как с обеспечением защиты прав интеллектуальной собственности, так и с трудностью восприятия человеком сложных математических формул.

Тем не менее, прозрачность важна для обеспечения контроля за автоматизированными моделями принятия решений ИИ, так как одно лишь заявление об использовании систем ИИ не дает гарантий защиты от незаконного использования ПДн. Сложные процессы обработки ПДн с использованием систем ИИ также не способствуют обеспечению прозрачности.

Наличие только доступа к алгоритмам ИИ недостаточно для обнаружения потенциальных угроз безопасности ПДн. Для проведения полного анализа работы систем ИИ потребуются еще время и навыки интерпретации результатов деятельности систем ИИ.

Алгоритмы являются лишь одним из компонентов приложения ИИ, другим являются наборы ПДн, используемые для обучения или обработки. Нерепрезентативные наборы данных автоматически дают необъективные результаты. Кроме этого, обеспечение прозрачности ПДн сталкивается с требованием законодательства, связанным с обеспечением их конфиденциальности.

Несмотря на это, обеспечение прозрачности функционирования систем ИИ играет важную роль в обеспечении защиты ПДн, особенно в правоохранительной деятельности.

Например, в недавно принятом европейском законе об ИИ установлены требования к прозрачности систем ИИ общего назначения. Такие системы должны соответствовать определенным требованиям прозрачности в соответствии с законодательством ЕС об авторском праве, а также публиковать подробные резюме набора данных, используемого для обучения систем ИИ.

К более мощным моделям систем ИИ общего назначения, которые могут представлять системные риски, предъявляются дополнительные требования, включая проведение оценки моделей, оценку и смягчение системных рисков, а также отчетность об инцидентах. Кроме того, искусственные или поддельные изображения, аудио- или видеоконтент (дипфейки) должны быть четко обозначены как таковые.

Ответственность в отношении систем ИИ.

Вопрос ответственности за действия, совершаемые системами ИИ вызывает споры и активное обсуждение.

Одним из предлагаемых решений данной проблемы является возложение всей полноты ответственности за работу систем ИИ на производителя систем, реализующих алгоритмы.

Некоторые считают такой вариант ответственности более работоспособным, чем возложение ответственности на работников подразделения по защите информации, которые отвечают за работу алгоритма ИИ в тот момент, когда он обрабатывает ПДн.

Установление ответственности, в том числе за нарушение правил по защите ПДн, необходимо как «последний рубеж» защиты ПДн в случаях, когда иные правовые, организационные и технические средства ее защиты не сработали.

Не можем не упомянуть европейский закон об ИИ как первый пример установления ответственности в виде штрафов и других принудительных мер (которые также могут включать предупреждение и неденежные меры), применимых к нарушителям данного закона. Установлены штрафы в отношении поставщика, производителя продукта, разработчика, уполномоченного представителя, импортера или дистрибьютора систем ИИ.

Кроме этого европейский закон об ИИ устанавливает обязательства поставщиков, обязательства импортеров, дистрибьюторов, обязанности разработчиков, требования и обязанности нотифицированных органов.

Вопросы ответственности за нарушения требований по защите ПДн в органах и организациях прокуратуры при использовании технологий и систем ИИ также требует своего решения. Как представляется, правовое регулирование такой ответственности должно основываться на национальном законодательстве.

Анализ правовых и институциональных механизмов, направленных на защиту персональных данных и чувствительной информации при использовании систем ИИ в прокурорской деятельности России, Казахстана и Кыргызстана,

свидетельствует о формировании устойчивых, но в ряде аспектов фрагментарных подходов к обеспечению информационной безопасности в условиях цифровизации правосудия.

В Российской Федерации реализуется модель нормативного регулирования, основанная на Федеральном законе № 152-ФЗ «О персональных данных», дополненная специальными актами, регулирующими экспериментальные правовые режимы в сфере ИИ. Отмечается совершенствование правовой системы, направленной на системность ее правоприменения в практике.

Казахстан демонстрирует стремление к институционализации ИИ через разработку специального закона «Об искусственном интеллекте» и усилению защиты персональных данных. Важным шагом стало внедрение государственного и негосударственного сервисов контроля доступа к персональным данным. Тем не менее, практическая реализация норм требует дальнейшего укрепления технической инфраструктуры и повышения цифровой грамотности сотрудников прокуратуры.

В Кыргызской Республике наблюдаются активные законодательные реформы, направленные на гармонизацию национального регулирования с международными стандартами, включая Закон «Об информации персонального характера», создание Государственного агентства по защите персональных данных, что отражает институциональную готовность к внедрению ИИ в публичный сектор. Вместе с тем отсутствие специализированных норм, регулирующих применение ИИ в правоохранительной деятельности, остается основным вызовом для правоприменения.

Таким образом, перспективы внедрения ИИ в прокурорскую деятельность напрямую зависят от зрелости национальных моделей защиты персональных данных. В условиях трансграничного обмена информацией и роста объемов чувствительных данных особую значимость приобретает обеспечение принципов законности, пропорциональности и прозрачности обработки данных. Для устойчивого развития ИИ в прокуратуре необходимо не только совершенствование нормативной базы, но и внедрение механизмов алгоритмической подотчетности, независимого аудита ИИ-систем.

§ 3.2 Участие прокурора в электронном судопроизводстве: применение технологий искусственного интеллекта

В зарубежных странах внедрение электронных систем уголовного делопроизводства уже дало заметные результаты в плане эффективности и доступности судебных услуг. Например, в США на федеральном уровне действуют две системы «Управление делами/электронный архив дел» (Case Management / Electronic Case Files - CM/ECF) и «Открытый электронный доступ к судебным материалам» (Public Access to Court Electronic Records – PACER).

Автоматизированная система управления делами электронного дела (CM/ECF) начала действовать в федеральных округах США в 2004 году. Система

является самой крупной, непрерывной, интегрированной системой управления делами и электронной подачи судебных обращений в мире. Она была разработана силами специализированной группы высококвалифицированных и опытных программистов, системных аналитиков, компьютерных, а также других IT-специалистов, работающих в Административном управлении судов США (AOUSC), Агентстве по обеспечению судебной власти в США, отвечающих за всю административную и управленческую поддержку федеральных судов.

Системы электронного уголовного дела используются и в других странах, включая Канаду, Великобританию, Германию, Швейцарию, Австралию, Японию и др. Эти системы не только упрощают доступ к судебным материалам, но и значительно ускоряют процесс рассмотрения дел, минимизируя время и ресурсы, затрачиваемые на бумажную работу.

Так, в Сингапуре для облегчения принятия судебных решений все судьи имеют доступ к комплексному набору онлайн правовых информационных систем, таких как:

- LawNetLegalWorkbench, которая обеспечивает интеллектуальный поиск по юридическим базам данных;

- база данных сотрудников судебных органов (JODB), которая содержит судебные рабочие документы и сборники;

- система правил вынесения приговоров (SINGS), которая обеспечивает критерии вынесения приговора и информацию;

- система управления приоритетами ресурсов (IMPRESS), которая фиксирует все прошлые решения по делам, рассмотренным как в Верховном суде, так и подчиненными судами.

В национальном экономическом плане Сингапура в XXI веке информационные технологии были определены в качестве основного двигателя для поддержания непрерывного экономического роста страны в глобализированной экономике знаний[80].

С 1997 года в судах Сингапура применяется электронная система подачи документов (Electronic Filing System) и, что не менее интересно, кроме электронной подачи документов, система позволяет получать судебные акты в электронном виде. Первоначально использование данной системы носило добровольный характер, но спустя всего три года применение этой формы обращения в суд было признано успешным, и электронная форма взаимодействия с судебной системой стала носить императивный характер[81].

Электронное правосудие в Сингапуре в части организационно-правового обеспечения реализуется посредством:

– предоставления услуг и приложений для виртуальных судов;

– компьютеризации процессов управления делами;

– совместной разработки межведомственных систем;

---

[80] Ai Tee Koh. Singapore's national economic plan for the 21st century: Issues and Strategies// McGraw-Hill, 2002. P 387.

[81] Слабоспицкий А. С. Судебная система Сингапура (опыт работы в пандемию 2020 года) // Вестник Казахского национального университета. Серия юридическая. – 2021. – Т. 97, № 1. – С. 81.

– компьютеризации судебной администрации и корпоративных услуг[82].

Сингапур является одним из первых государств, которое стало предоставлять развернутые виртуальные судебные услуги для населения через мультимедийные приложения. В судах Сингапура впервые была применена процедура видеоконференции, являющаяся в настоящее время наиболее универсальной и продуктивной технологией современности[83].

Системы электронного управления делами нашли свое отражение в первой волне компьютеризации страны и представлены следующими системами:

– система регистрации и информации по уголовным делам;

– система повесток по нормативным правонарушениям;

– система электронного оборота по гражданским делам.

Для управления делами в июне 1999 года внедрена система «TICKS 2000», которая предоставляет онлайн-интерфейсы для правоохранительных органов для электронного обмена данными. Пользователям, которые не имеют своих собственных систем управления делами, суды предоставляют удаленный доступ к TICKS 2000, чтобы они могли регистрироваться и получать информацию о своих делах в онлайн-режиме. Система «TICKS 2000» позволяет отправлять судебные документы в электронном виде, то есть электронные документы вместо бумажных[84].

Использование ИИ в кибербезопасности Сингапура освещает в своей статье Ф.А. Касенов. Так, государство активно внедряет инновации и технологические решения для укрепления кибербезопасности, используя передовые технологии, включая ИИ, машинное обучение и блокчейн, чтобы обеспечить более эффективную защиту от киберугроз.

ИИ и машинное обучение играют ключевую роль в современных системах кибербезопасности, обеспечивая возможность обнаружения и анализа сложных угроз в реальном времени. Эти технологии способны анализировать большие данные, выявляя аномалии и потенциальные угрозы, что позволяет предотвратить кибератаки до того, как они нанесут ущерб. Кроме того, ИИ может обучаться на основе новых данных о киберугрозах, постоянно улучшая свою эффективность.

Сингапур разработал системы, которые используют ИИ для мониторинга и анализа сетевого трафика в реальном времени, чтобы обнаружить и предупреждать о потенциальных угрозах[85].

Положительный опыт Сингапура ориентирует мировое сообщество к цели и формам создания по-настоящему безбумажного электронного правосудия.

---

[82] Shapiro C., Hal, R. Varian, Information Rules: A Strategic Guide to the Networked Economy (1999), Harvard Business School Press / [Electronic resource] – Access mode: http://yunus.hacettepe.edu.tr/~tonta/yayinlar/hal-varian-information-rules-chapter-1.pdf_(Access data: 14.05.2024).

[83] Шульгин Е.П. Зарубежный опыт деятельности органов, осуществляющих производство по уголовным делам в электронном формате // Академическая мысль: сетевое издание. – 2019. – № 4. – С. 86.

[84] PS-Online Action Plan: Delivery of Electronic Public Services, jointly prepared by the Prime Minister's Office, the Ministry of Finance and the National Computer Board / [Electronic resource] – Access mode: URL: http://npan1.un.org/intradoc/groups/public/documents/apcity/unpan012807.pdf_(Access data: 19.05.2024).

[85] Касенов Ф.А. Роль Сингапура в укреплении кибербезопасности в ASEAN // Юго-Восточная Азия: актуальные проблемы развития – 2024. – Том 2. №63. – С. 208-220. DOI: 10.31696/2072-8271-2024-2-2-63-208-220.

В 2024 году Аргентина объявила о создании при Министерстве безопасности специального подразделения по прогнозированию преступлений с помощью ИИ. Будущие преступления планируется прогнозировать и выявлять посредством анализа социальных сетей, путем отслеживания перемещения преступных группировок, предугадывая начало массовых беспорядков при подозрительной активности, в том числе с использованием камер видеонаблюдения. Отслеживать планируется и подозрительные финансовые операции путем создания профилей подозреваемых лиц, выявления связей различных дел, исторических данных о преступлениях[86].

Прочно вошло в практику представление материалов уголовного дела в электронном виде в суд и в США. Подача документов в электронном формате посредством интернет-ресурсов в США зародилась еще в 1980 году и нашла свое продолжение благодаря применяемым в то время пилотным проектам, что впоследствии позволило укрепить и набрать должный потенциал внедрения электронного документооборота в федеральных судах (2003 г.).

Электронное правосудие в США берет свое начало с создания многопрофильной функциональной системы «Public Accessto Court Electronic Records» (далее – PACER).

PACER – система публичного доступа к данным окружных судов и апелляционных судов США. Немаловажной особенностью систем PACER является ее коммерческая составляющая, то есть пользователи могут запросить интересующую их информацию за определенную плату[87]. Совместно с системой PACER начала свое функционирование система «Case Management/Electronic Case Files» (далее – CM/ECF). CM/ECF – система, позволяющая осуществлять электронное регистрирование и управление уголовными делами.

Таким образом, в США расследование в электронном формате осуществляется посредством функционирования двух самостоятельных систем: PACER и CM/ECF. Первая используется для публичного доступа к электронным судебным записям, а вторая – для ведения дел и электронной подачи судебных документов[88].

Как следует из названия, система CM/ECF является результатом комбинации инструментов, обеспечивающих две функции: «Управление делами» (CM) и «Электронный файл дел» (ECF). Затем два элемента системы образуют интегрированную систему, дополненную PACER, системой, предоставляющей доступ к электронным файлам посредством сети Интернет.

Список функций, предоставляемых этой системой, можно обобщить следующим образом: ведение документации (отслеживание запросов, ответов, сроков и слушаний); управление электронными документами, их хранение,

---

[86] Передаем прогноз нарушений закона /Алексей Алексеев 17.08.2024 г. / [Электронный ресурс] – Режим доступа: https://www.kommersant.ru/doc/6894036_(дата обращения: 04.09.2024).

[87] Официальный сайт правительства США – публичный доступ к записям суда / [Электронный ресурс] – Режим доступа: https://pacer.uscourts.gov/_(дата обращения: 04.06.2024).

[88] Официальный сайт федеральной судебной системы США / [Электронный ресурс] – Режим доступа: https://www.uscourts.gov/court-records/electronic-filing-cmecf_(дата обращения: 04.06.2024).

безопасность и архивирование; доставка документов в суд, из него и в его пределах; дополнительная информация от других сторон при подаче документов. Доступ к указанным системам осуществляется посредством использования логина пользователя и пароля, присваиваемого соответствующим федеральным судом. В отдельных судах указанные данные формально приравниваются к индивидуальной электронно-цифровой подписи. Использование систем электронного судопроизводства функционирует круглосуточно, направление материалов уголовного дела в электронном формате в компетентные органы (суд, прокуратура и т.д.) не требует от пользователей каких-либо дополнительных затрат по сравнению с направлением документов на бумажных носителях.

В начале 2000-х годов правила по ведению судопроизводства в электронном виде содержались только в виде рекомендаций окружных судов о предоставлении файлов и записей по уголовным делам. Однако, начиная с 1 ноября 2006 года в соответствии с Судебным регламентом № 5503[89], Окружной суд США по Южному округу штата Калифорния требует от сторон и других лиц подавать документы в суд в электронном виде через Интернет не только по уголовным, но и по гражданским делам. Суд обязывает стороны прямо подавать все документы в электронной форме (must be electronically filed).

Система электронного документооборота нового поколения заключается в том, что регистрация в электронной системе управления электронным делопроизводством является обязательной для адвокатов и всех должностных лиц, осуществляющих судопроизводство. Каждый участник уголовного процесса несет ответственность за поддержание электронного почтового адреса, своей учетной записи, необходимой для получения электронного уведомления о движении дела и принимаемых решениях[90].

Полагаем, что на сегодняшний день лидером среди передовых стран по многим параметрам, в том числе в электронном уголовном судопроизводстве, является Китай.

Общеизвестно, что китайские ученые еще в 2015 году разработали ИИ, который в помощь прокурорам выдвигает свои версии обвинений. Прокуроры Китая уже применяют нейросети в оценке доказательств.

По результатам встречи представителей Генеральной прокуратуры Республики Казахстан, Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан с представителями Государственной академии прокуроров Китайской Народной Республики, состоявшейся в конце 2023 года, стало известно, что типичные сценарии применения ИИ прокурорами включают следующее: ИИ помогает в записи в реальном времени и транскрипции текста в судебных заседаниях и допросах; при обработке файлов он предоставляет инструменты для исправления ошибок, автоматической проверки, подготовки

---

[89] Официальный сайт федеральной судебной системы США / [Электронный ресурс] – Режим доступа: https://www.uscourts.gov/court-records/electronic-filing-cmecf_(дата обращения: 04.06.2024).
CASDPolicies_09-24-2018. Pdf.

[90] Электронное правосудие: Монография / Е.В. Бурдина [и др.]; под ред. Е.В. Бурдиной, С.В. Зуева. — М.: РГУП, 2021. –С. 258.

документов и вынесения приговоров; при запросе он рекомендует соответствующие знания о законах, правилах, делах и мнениях экспертов; предлагает такие функции, как автоматический ввод информации.

Система ИИ используется для повышения качества и эффективности правосудия.

Во-первых, это помогает стандартизировать производительность и улучшить качество; во-вторых, обеспечивает умную помощь для повышения эффективности.

При внедрении систем ИИ в прокурорскую работу учитываются инновационность, разумность, безопасность и практичность.

Согласно информации китайской стороны, ИИ в настоящее время используется не только для принятия решений, но и в повседневных процессах. При принятии решений ИИ обеспечивает технологическую поддержку для принятия продуманных решений и бережливого управления путем проведения интеллектуального анализа различных данных и показателей обработки дел для выявления аномалий данных и рисков отклонения индикатора.

В повседневной работе ИИ способствует автоматическому заполнению информации о деле, подготовке документов, оказывает помощь в чтении файлов и дает рекомендации при вынесении приговоров. В то же время гостями сделан акцент, что технологии не заменят прокуроров.

При использовании ИИ соблюдаются национальные законы и правила, включая Закон о кибербезопасности КНР (2017), Закон о безопасности данных КНР (2021 г.), Закон КНР о защите персональных данных (2021 г.), Закон КНР против недобросовестной конкуренции (изменен в 1993 г.), а также руководящие документы, такие как «Произведено в Китае» 2025 года и План развития ИИ нового поколения 2017 года.

Как пояснили представители китайской делегации, базы данных прокуратур включают в себя следующие данные: данные, собранные или приобретенные прокурорами в ходе рассмотрения ими дел; данные, переданные органами общественной безопасности и другими правоохранительными органами; и те, что получены за счет совместного использования другими органами власти.

В настоящее время прокуроры расследуют преступления как с помощью бумажных документов, так и с помощью электронных файлов, таких как видеодоказательства и записи телефонных звонков. Электронные файлы обычно хранятся в системе обработки дел, а после завершения дела они передаются в систему управления файлами для сохранения и архивирования. Срок хранения определяется особенностями дела, а срок хранения электронных документов, как правило, такой же, как и у бумажных.

При разработке соответствующих прикладных систем часто используемые алгоритмы ИИ включают: сверхточные нейронные сети, машинное обучение и случайные настройки. На практике системы ИИ не предъявляют прямых обвинений в преступлениях, но они предоставляют улики и юридические руководящие принципы для прокуроров для обвинения в преступлении. Конечно,

существуют угроза безопасности данных, технической надежности, риски алгоритмического черного ящика и технических злоупотреблений при использовании ИИ в конкретных случаях.

С точки зрения оценки доказательств ИИ, его основная цель в настоящее время заключается в оказании прокурорам помощи при рассмотрении дел во избежание недостатков и упущений доказательств и в обеспечении целостности системы доказательств путем проверки соответствия стандартам доказательств.

Судебные органы Китая при этом сосредотачивают свои исследования на оценке результатов технологического применения при оценке рисков использования ИИ.

В первые интернет-суды были использованы в городах Ханчжоу, Пекин и Гуанчжоу. Суды здесь работают на основе больших данных, технологии блокчейн и ИИ выполняет значительный объем судейской работы, автоматически создавая юридические документы для судей.

Еще в июле 2019 года в таком суде в г.Пекин была внедрена система с искусственным судьей, действующим с применением ИИ и отвечавшим на 82 консультационных вопроса. Такие суды могут рассматривать споры, связанные с онлайн-продажей товаров и услуг, кредитованием, владением и нарушением авторских и смежных прав, и некоторые другие виды споров.

Исследователи из Китая утверждают, что они разработали первый в мире ИИ, способный анализировать дела и предъявлять людям обвинения в преступлениях[91].

Как утверждает команда Китайской академии наук, разработавшая систему, программа может предъявить обвинение на основании словесного описания дела с точностью до 97 %.

Система была создана и протестирована в Народной прокуратуре Шанхая Пудун, крупнейшей и самой загруженной окружной прокуратуре страны. Команда исследователей планировала расширить ее возможности, включив в нее больше составов преступлений и увеличив нагрузку.

Алгоритм – уникальная математическая формула, из которой состоит ИИ, может работать на стандартном настольном компьютере и выдвигать обвинения на основе 1000 незаконных или противоречивых характеристик, взятых из описания случая, созданного человеком.

По словам профессора Ши Юна, директора лаборатории управления большими данными и знаниями Китайской академии наук, который является ведущим ученым проекта, эта технология может снизить ежедневную рабочую нагрузку прокуроров, позволяя им сосредоточиться на более сложных задачах. «Эта система может в определенной степени заменить прокуроров в процессе принятия решений».

[91] Научный обзор «Применение ИИ в деятельности органов прокуратуры государств-участников СНГ: реалии и перспективы» // Материалы для межгосударственного научного исследования «Информационные технологии (ИИ) в органах прокуратуры государств-участников СНГ». Университет прокуратуры РФ. 2024.

Инженеры тестировали программу, исследуя более 17 000 дел с 2015 по 2020 год. Китайские исследователи заявили, что им удалось выявить и выдвинуть обвинения по обычным преступлениям. В настоящее время программа может выявлять и выдвигать обвинения по восьми наиболее часто совершаемым преступлениям, таким как мошенничество с кредитными картами, азартные игры, опасное вождение, кража, мошенничество, умышленное причинение вреда, воспрепятствование выполнению служебных обязанностей, а также по политическим, по выявлению «инакомыслия» против государства – «подрыв политической власти государства» и «саботаж национального единства». Но на данный момент система не играет никакой роли в процессе принятия решений и не предлагает вид наказания.

Прокуроры Китая были одними из первых, кто с 2016 года использует ИИ, в частности инструмент, известный как Система 206, для оценки доказательств, условий ареста и того, представляет ли подозреваемый какую-либо опасность для общества.

Продвигаясь вперед в глобальной гонке за ИИ, китайские власти в 2017 году запустили первый в стране киберсуд, позволяющий сторонам, участвующим в исках, связанных с киберпространством, таких как электронная коммерция, выступать через видео перед судьями, основанными на ИИ. Хотя идея состоит в том, чтобы помочь системе справиться с большим количеством дел, судьи-люди по-прежнему контролируют каждый шаг, прежде чем вынести решение.

Потому что для принятия таких решений потребуется, чтобы машина идентифицировала и переводила сложный человеческий язык в формат, понятный компьютеру. Технология машинного обучения, которая дает компьютерам возможность интерпретировать, манипулировать и понимать человеческий язык (Natural Language Processing – NLP), необходима для анализа текста, записей или изображений, созданных или загруженных людьми, и требует суперкомпьютеров, к которым прокуроры не имеют доступа.

В рамках перехода к технологии NLP на базовом компьютере команда разработчиков планирует модернизировать ее так, чтобы она могла распознавать менее распространенные преступления и выдвигать несколько обвинений против одного подозреваемого.

Между тем некоторые прокуроры выражают обеспокоенность по поводу нового компьютеризированного судьи и присяжных: «Точность в 97 % может быть высокой с технологической точки зрения, но всегда будет вероятность ошибки. Кто возьмет на себя ответственность, когда это произойдет? Прокурор, машина или разработчик алгоритма?». Многие прокуроры не хотят, чтобы компьютеры вмешивались в их работу, ИИ может помочь обнаружить ошибку, но он не может заменить людей в принятии решения[92].

[92] Китайские ученые разрабатывают ИИ-«прокурора», который может выдвигать собственные обвинения / 26.12.2021 Стивен Чен / [Электронный ресурс] – Режим доступа: https://www.zmescience.com/science/china-has-created-the-worlds-first-ai-prosecutor/https://www.scmp.com/news/ china/science /article/3160997/chinese-scientists-develop-ai-prosecutor-can-press-its-own_(дата обращения 16.10.2024).

Эстония взяла курс на создание электронного государства с начала 2000-х годов. Строительство этой системы началось с базового законодательного фундамента. Уже в 2000 году был принят Закон о цифровой подписи (Digital Signatures Act, 2000), который приравнял электронную подпись к обычной рукописной. Благодаря этому шагу прокуроры и население страны получили возможность подписывать процессуальные документы онлайн. Через несколько лет, в 2004 году был принят Закон об электронном обмене данными (Electronic Data Exchange Act, 2004), обеспечивший безопасную инфраструктуру обмена документами между государственными органами.

Но самой настоящей цифровой революцией стали изменения, внесенные в Гражданский процессуальный и Уголовно-процессуальный кодексы в период с 2008 по 2020 год. Эти поправки легализовали подачу исков прокуроров, адвокатов и других авторов обращений в электронном виде, проведение судебных заседаний через видеосвязь и использование электронных доказательств.

Так появились системы e-File и e-Court. Первая охватывает весь жизненный цикл дела – от подачи заявления до исполнения решения, вторая – делает возможным проведение судебного заседания онлайн. К 2023 году 94% гражданских исков в Эстонии подаются в электронном виде, до 89% процессов проходят дистанционно.

В основе всей системы – технологическая платформа X-Road, разработанная в 2001 году. Она соединяет суды с государственными регистрами – от кадастра до реестра населения и обеспечивает надежный, шифрованный обмен данными. Это не просто техническое решение, а основа доверия в цифровой юрисдикции.

Опыт Эстонии стал основой для регламента eIDAS, принятого в ЕС в 2014 году. Этот документ унифицировал электронную идентификацию и юридическую силу цифровых подписей в Европе. Кроме того, идеи Эстонии легли в основу европейского портала e-Justice, позволяющего гражданам ЕС получать правовые услуги онлайн.

Этим Эстония показала, что цифровизация правосудия не только возможна, но и эффективна. Судебные процессы стали быстрее (сроки рассмотрения дел сократились на 30-40%), доступнее (возможность участвовать удаленно), прозрачнее (все решения хранятся в цифровом архиве)[93].

Таким образом, системы ИИ уже существуют в правоохранительных органах по всему миру, но ограничиваются оценкой доказательств или судебной экспертизой, а обвинения выдвигаются впервые.

Возвращаясь к результатам встречи казахстанской и китайской сторон, необходимо обратить особое внимание на следующее.

По мнению китайской стороны, существует угроза технологической надежности. Рискованно быть чрезмерно зависимым от принятия решений ИИ.

Наряду с этим, некоторые системы ИИ, такие как глубокие нейронные сети, настолько сложны, что его внутренний принцип работы и логика принятия

[93] https://cyberleninka.ru/article/n/tsifrovoe-pravosudie-v-estonii (дата обращения 22.07.2025).

решений не могут быть полностью поняты, что приводит к неинтерпретируемости и неконтролируемости. Кроме того, алгоритмический черный ящик может также вызывать разную степень дискриминации, что уже наблюдалось в разной степени в развитии интернет-экономики Китая (например, ценовая дискриминация на основе больших данных в отношении существующих клиентов).

Также было указано на наличие риска злоупотреблений. Так, ИИ имеет свои ограничения, и он не подходит для применения во всех сценариях. Например, в некоторых важных областях принятия решений ИИ не является «панацеей». Требуется тщательный анализ того, когда и как его применять.

Опыт государств-участников СНГ в развитии электронного судопроизводства

Республика Казахстан

Расследование уголовных дел на территории Республики Казахстан, как и в других государствах-участниках СНГ, длительное время велось на бумажных носителях и в период СССР имело общую концепцию.

Последние два десятилетия электронное судопроизводство в Казахстане активно развивается, охватывая не только уголовное, но гражданское и административное судопроизводство.

При этом органы прокуратуры республики начали работу по цифровизации надзора еще в 2004 году.

В суде данная работа началась с 2012 года с проекта «Электронный суд». Концептуально это подкреплено еще в 2000 году с введением Конституционного закона РК «О судебной системе и статусе судей», где описано электронное уголовное судопроизводство, внедрение систем для проведения видеоконференций и электронного обмена.

В 2014 году был принят новый Уголовно-процессуальный кодекс, в рамках которого с внедрением ЕРДР стадия регистрации всех уголовных правонарушений была полностью переведена **в электронный формат**.

В 2016 году Верховный Суд завершил автоматизацию процедуры рассмотрения дел судом и внедрил информационную систему «Төрелік».

В последующем Указами Президента Республики Казахстан утверждены государственные программы «Цифровой Казахстан» (2017 г.) и «Информационный Казахстан – 2020» (2018 г.), которые обеспечили внедрение «цифрового суда».

Поэтапный переход уголовного судопроизводства на электронный формат осуществлялся также в рамках государственной программы «Цифровой Казахстан» и Стратегического плана развития Республики Казахстан до 2025 года, утвержденного Указом Президента Республики Казахстан от 15 февраля 2018 года № 636.

С учетом опыта перехода на электронный формат расследования таких стран, как Грузия, Литва, Саудовская Аравия, Сингапур, Турция, Финляндия и Эстония, Генеральная прокуратура Республики Казахстан в 2017 году на базе

ЕРДР **разработала подсистему, позволяющую в электронном формате осуществлять расследование по уголовным делам и обеспечивать прокурорский надзор**.

Посредством автоматизации все стадии уголовного процесса в стране в конце 2017 года были интегрированы между собой, обеспечив переход с «бумажного» уголовного судопроизводства на электронный формат.

С переходом на электронный формат были минимизированы риски фальсификации и утери уголовных дел, сэкономлено время уголовного процесса, внедрено получение электронных санкций, достигнута прозрачность уголовного процесса, обеспечен доступ к уголовному делу в режиме онлайн, достигнута экономия финансовых затрат, введена электронная правовая статистика и аналитика.

Параллельно были внесены изменения в уголовно-процессуальное законодательство, что позволило приступить к расследованию дел в электронном формате уже с 1 января 2018 года; усовершенствована техническая часть обеспечения нововведений; улучшена информационная безопасность; проведено обучение сотрудников работе с новыми системами.

Сегодня все материалы уголовных дел направляются в суд в электронном формате. Разработаны шаблоны основных процессуальных документов, которые заполняются системой автоматически по имеющимся данным, следователь лишь дополняет его необходимыми следствию сведениями.

Внедрена технология внесения рукописной подписи посредством графического планшета, который фиксирует индивидуальные параметры нанесения подписи – скорость, силу нажатия, угол наклона и другие особенности, что дает возможность идентифицировать подлинность подписи. Одновременно уполномоченным государственным органом утверждена методика проведения экспертиз цифровой подписи.

В целях оперативности проведения уголовного процесса автоматизирован процесс получения сведений из государственных баз данных в отношении подозреваемых лиц. Реализован функционал вызова участников уголовного процесса через СМС-повестки.

До 2021 года в стране правоохранительными органами в электронном формате расследовались дела лишь по уголовным проступкам и преступлениям небольшой, средней тяжести, а с 2021 года начаты расследования также по тяжким и особо тяжким преступлениям.

С октября 2020 года автоматизирован процесс назначения адвокатов, в том числе оплата гарантированной государственной юридической помощи.

Адвокатам и участникам уголовного процесса предоставлен портал «Публичный сектор», через который можно направить заявление, ходатайство, жалобу, получить электронный ответ, участникам ознакомиться с материалами дела, получить копии документов. Цифровизирован процесс назначения и получения заключения по криминалистическим исследованиям и судебным экспертизам.

Санкционирование содержания лиц под стражу также допускается в дистанционном формате, для чего все изоляторы временного содержания полиции подключены к судам.

С ведением в 2021 году трехзвенной модели уголовного процесса **в системе ЕРДР ключевые решения следователь согласовывает и утверждает с прокурором в электронной форме**. Начальник следователя и прокурор осуществляют ведомственный контроль и надзор над процессом расследования также через электронные системы, с возможностью дачи указания по делу или отмены незаконно принятого решения.

Планируется реализовать и внедрить новую программу «Интеллектуальный помощник следователя», которая будет полезна для молодых сотрудников, ориентировать их на проведение необходимых следственных действий и принятие законных решений. Внедрена опция «Оффлайн-приложение», с помощью которой можно производить осмотр, составлять схемы, фиксировать следы преступлений, проводить допросы и другие следственные действия непосредственно на месте преступления.

Особое внимание уделяется вопросам информационной безопасности. Так, доступ к системе ЕРДР предоставляется исключительно по защищенному каналу связи, с применением трехфакторной авторизации пользователя, т.е. следователь, прокурор заходят в систему посредством ЭЦП, логина и отпечатка пальца.

Наряду с этим для защиты от несанкционированных воздействий имеется журнал событий, предназначенный для контроля действий должностных лиц по конкретному уголовному делу, то есть в системе фиксируется, кто и когда имел доступ к уголовному делу, что просматривал, какие вносил корректировки и предпринимал другие действия.

Описанный прогресс в судопроизводстве несомненно дал определенные преимущества – это повышение эффективности и скорости процесса за счет его автоматизации и цифровизации, улучшение доступа к информации для всех участников процесса, снижение административных затрат на бумажные носители и физическое хранение дел.

Одновременно существуют такие риски и внешние вызовы для электронного судопроизводства, как технические сбои в системе и внешнее несанкционированное воздействие. В связи с этим необходимо обеспечение системы защиты и безопасности информационных систем, с постоянным ее совершенствованием. Наряду с указанным необходимы обучение и адаптация участников процесса к новым технологиям.

Вместе с тем веяния времени требуют постоянного развития и совершенствования уже самих нововведений, включая дальнейшее изменение законодательной базы для поддержки и расширения использования электронного судопроизводства, интеграцию новых технологий, таких как ИИ и блокчейн, для повышения прозрачности и эффективности процесса, а также разработку и внедрение стандартов и протоколов для обеспечения совместимости различных электронных систем и платформ.

Данные аспекты являются ключевыми для понимания текущего состояния и перспектив развития электронного судопроизводства в Казахстане.

Для нормативного правового регулирования ведения уголовного производства в электронном формате в УПК РК введена новая статья 42-1 (о формате уголовного судопроизводства). Указанная норма предусматривает возможность ведения уголовного судопроизводства в бумажном и/или электронном форматах. Решение о выборе формата принимается лицом, ведущим уголовный процесс, с учетом мнения участников и технических возможностей.

Реализация вышеназванной нормы о формате уголовного дела (статья 42-1 УПК РК) осуществлена Приказом Генерального Прокурора от 3 января 2018 года №2 путем утверждения Инструкции о ведении уголовного судопроизводства в электронном формате.

Согласно этой норме, нормативные правовые акты, принятые Генеральным Прокурором Республики Казахстан в пределах своей компетенции, обязательны для исполнения органами уголовного преследования.

Инструкция о ведении уголовного судопроизводства в электронном формате представляет собой значимый шаг в развитии электронного правосудия в стране. Нормативно-правовая база, описанная в ней, структурирует процессы досудебного расследования и правореализует использование современных технологий для повышения эффективности и прозрачности уголовного процесса.

Заключительным этапом производства электронного уголовного дела на досудебной стадии уголовного судопроизводства является направление прокурором или лицом, ведущим уголовный процесс, электронного уголовного дела в суд. Оно производится посредством интеграции ИС ЕРДР с автоматизированной информационно-аналитической системой судебных органов «Төрелік».

Согласно общим условиям главного судебного разбирательства, Уголовно-процессуальным кодексом предусмотрена непосредственность и устность судебного разбирательства (статья 331). Вместе с тем в главном судебном разбирательстве также применяются информационные технологии.

В рамках цифровизации судопроизводства и в целях установления гармонии между обеспечением безопасности участников процесса и доступом к правосудию в судах Республики Казахстан расширены IT-мощности: установлены дополнительные серверы для мобильной видео-конференцсвязи, увеличена пропускная способность каналов связи. Это позволило судам полностью перейти на удаленный формат работы.

Внедрено единое электронное окно для доступа ко всем судебным услугам. С любого устройства и из любой точки, используя мобильное приложение, можно подать в суд более 100 видов электронных обращений. Удаленно можно отслеживать регистрацию обращения, узнавать его статус и в итоге получить судебный акт.

Все залы судебных заседаний оборудованы современными системами аудио- и видеофиксации. Тем самым IT-сервисы изменили взаимодействие людей с судами и позволили системе развиваться дальше.

Законом Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам судебной системы и статусу судей» еще в 2016 году закреплено проведение судебных заседаний с использованием видео-конференцсвязи.

Более того, с 2022 года Верховным Судом Республики Казахстан активно внедряются и элементы ИИ.

ИС «Судебная практика». В данной системе ИИ минимизирует ошибки при применении уголовного и уголовно-процессуального законодательства, автоматически высчитывая возможные наказания, виды исправительных учреждений и рецидивы.

Ранее ИИ выполнял расчеты, когда необходимо было определить максимальный срок наказания, допустимый по закону, выбрать подходящее исправительное учреждение для подсудимого, установить вид рецидива в действиях виновного и другие аспекты. С внедрением этого модуля случаи неправильного применения наказаний, назначения исправительных учреждений и других подобных ошибок значительно сократились. Сегодня этот модуль активно используется судьями первой инстанции при рассмотрении уголовных дел.

«Цифровая аналитика судебной практики». Система предоставляет два раздела поисковой системы: по ключевым словам и интеллектуальный поиск. Она обучена понимать суть судебных решений, анализирует и сравнивает судебные акты, выделяя аномалии, определяет категории дел и процент удовлетворения исков. Система демонстрирует, какое количество найденных по запросу решений обжаловалось, и их результаты, позволяя судьям видеть судебную практику по схожим делам.

Применение ИИ в судопроизводстве обладает значительным потенциалом для повышения оперативности принятия решений, разгрузки судов от рутинной работы и минимизации судебных ошибок. Для успешной интеграции ИИ необходимо соответствующее правовое регулирование и учет международных норм и стандартов. Основной целью должно оставаться обеспечение защиты прав и свобод граждан, что возможно при грамотном и ответственном применении ИИ в судебной деятельности.

Таким образом, период введения электронного судопроизводства в Казахстане выпал в среднем на второй десяток 2000-х годов, и стал важным этапом модернизации уголовного судопроизводства, направленным на повышение эффективности и прозрачности судебных процессов.

Необходимо учитывать, что внедрение новых технологий и систем требует не только технических изменений, но и значительных усилий по обновлению законодательной базы, обучению кадров и обеспечению безопасности данных.

Кыргызская Республика

Генеральная прокуратура Кыргызской Республики, являющаяся держателем (владельцем) автоматизированных информационных систем государственного, стратегического значения, проводит политику цифровизации органов прокуратуры, правоохранительных и других государственных органов, задействованных в орбите уголовного, процессуального законодательства и законодательства о правонарушениях.

В рамках разработки и внедрения автоматизированной информационной системы «Единый реестр преступлений» (АИС «ЕРП»), содержащей в себе полный цикл движения заявления или сообщения о преступлении (досудебная стадия), Генеральная прокуратура Кыргызской Республики в настоящее время проводит пилотный проект «Электронное уголовное дело» в ряде регионов страны.

Электронное дело представляет собой один из конечных продуктов АИС «ЕРП» (помимо актуальной уголовно-правовой статистики), включает в себя более 70 шаблонов, форм процессуальных документов, которые генерируются в системе с присвоением уникального идентификатора и QR-кода.

В АИС «ЕРП» заложено множество форматно-логических контролей, позволяющих минимизировать ошибки следователей при работе с системой и максимально наполнить ее информацией, содержащей необходимые статистические реквизиты, в том числе определен процессуальный порядок взаимодействия следователя, прокурора и следственного судьи, являющихся основными пользователями (регистраторами) системы.

В рамках пилотного проекта «Электронное уголовное дело» следователи производят в системе процессуальные действия, которые оформляются практически полным спектром процессуальных документов, в числе которых допросы, очные ставки участников уголовного процесса, производство выемки, обыска, назначение экспертиз, привлечение специалистов, экспертов, переводчиков, признание вещественным доказательством, следственные поручения и запросы, применение мер процессуального принуждения, избрание, изменение и прекращение мер пресечения в отношении обвиняемых, выведение ребенка из системы уголовного судопроизводства, регистрация потерпевших, регистрация формы на наркотические средства, передача материалов доследственных проверок и уголовных дел по территориальности и подследственности, соединение материалов или уголовных дел, изменение квалификации деяния, а также приостановление или окончание производства следствия (прекращение, создание обвинительного акта и направление в суд или применение принудительных мер медицинского характера), и ряд других.

Проведена интеграция АИС «ЕРП» с рядом государственных органов, что позволяет следователям получать достоверные данные о лицах (анкетные данные, дата рождения, прописка) по их персональному номеру в паспорте или свидетельстве о рождении (база данных регистрации населения), а также с судебно-экспертной службой, что позволяет в режиме онлайн направлять постановления о назначении экспертиз и получать в электронном виде

заверенные заключения по их результатам (что не отменяет необходимости доставки нарочно в орган экспертизы исследуемые объекты).

В части процессуальных документов, вынесенных в полевых условиях или которые невозможно реализовать в АИС «ЕРП», применяется вложение отсканированных документов (протокол осмотра места происшествия, допросы вне рабочих кабинетов, ответы государственных и других органов и т.д.).

Надзирающие за следствием прокуроры имеют полный доступ к материалам доследственной проверки или уголовных дел, в рамках «Электронного уголовного дела» имеют функционал согласования отдельных следственных действий (согласование мер пресечения, изменения квалификации, прекращения или приостановления дела, обвинительного акта, продление сроков проверки и расследования и т.д.), в том числе временно исполняют в АИС «ЕРП» роль следственного судьи ввиду отсутствия полноценной интеграции с информационной системой судебных органов Кыргызской Республики.

Таким образом, при полноценном внедрении «Электронного уголовного дела» появится возможность осуществления прокурорского надзора за следствием в режиме онлайн, то есть удаленное ознакомление с ходом доследственной проверки или расследованием, без отрыва от производства следователей, в том числе у руководителей правоохранительных органов в разы повысится качество ведомственного контроля за деятельностью подчиненных следователей.

Внедрение «Электронного уголовного дела» позволит минимизировать и возможно исключить факты фальсификации материалов доследственной проверки и уголовных дел, в связи с использованием инструмента автоматического формирования описи, невозможностью удаления, изменения или дополнения сгенерированных процессуальных документов. Все манипуляции со сгенерированными документами подлежат согласованию с прокурором, в части его касающейся (отмена необоснованных или неправильных решений следователя), изменения и дополнения возможны при установлении новых обстоятельств только путем проведения дополнительных следственных действий (дополнительные допросы, очные ставки, экспертизы, новое обвинение и т.д.).

Генеральная прокуратура Кыргызской Республики, являющаяся разработчиком ряда масштабных автоматизированных информационных систем, пользователями которых являются множество государственных органов и десятки тысяч сотрудников, стремится оптимизировать и облегчить работу государственных служащих в рамках внедрения цифровых продуктов.

При разработке информационных систем закладываются алгоритмы, обеспечивающие дисциплинированность сотрудников государственных органов (таймеры, счетчики, предупреждение об истекающих сроках), так и минимизирующие количество ошибок, допускаемых при работе с ними.

Вместе с тем в эпоху развития ИИ Генеральной прокуратурой Кыргызской Республики рассматривается возможность применения некоторых систем ИИ, таких как, например, нейроскоринг.

Данная технология позволит производить различные расчеты и прогнозирование. К примеру, в АИС «ЕРП» аккумулируются все данные по досудебному уголовному судопроизводству, в том числе фиксируется деятельность каждого прокурора и следователя. Технология нейроскоринга позволит высчитать эффективность деятельности того или иного следователя на основании показателей расследования, то есть количества находящихся в производстве уголовных дел, процента их раскрываемости (прекращения по нереабилитирующим основаниям и направления дел в суд), категории преступлений, которые им раскрываются с определенной периодичностью, а также категории нераскрытых преступлений, сроков расследования уголовных дел, количества принятых решений, отмененных прокурором.

Аналогично данную технологию можно применить и в отношении деятельности прокурора, взяв в расчеты количество отмененных процессуальных решений следователя и последующие принятые по ним решения, количество указаний прокурора и последующие раскрытия уголовных дел, количество рассмотренных жалоб прокурором и последующую их повторность и т.д.

Определив эффективность деятельности следователя или прокурора, можно скорректировать направление их деятельности для достижения больших результатов или минимизации негативных последствий.

Также технологию нейроскоринга возможно применить для прогнозирования преступности, опять же, с использованием данных АИС «ЕРП», где следователями вносится ряд статистических реквизитов, таких как само преступление, место, дата и время, способ его совершения, кем оно совершено, род его деятельности, должность и т.д.

Взяв в расчеты определенные критерии и применив методы аналитики данных, возможно спрогнозировать динамику преступности за определенный период, то есть в какое время года совершаются чаще те или иные преступления, в каком месте они совершаются, а также в какие часы или периоды суток.

Таким образом, при эффективном применении технологии нейроскоринга можно скорректировать работу служб общественной безопасности, направить патрули в определенные дислокации и в определенное время в целях профилактики правонарушений и снижения уровня криминогенной обстановки[94].

Анализ вопроса участия прокурора в электронном судопроизводстве, в том числе с применением и перспективой применения технологий ИИ показывает, что трансформация правосудия в условиях цифровизации, включая развитие электронного судопроизводства и интеграцию технологий ИИ, оказывает существенное влияние на деятельность прокурора как участника судебного процесса. Зарубежный опыт (в частности, практика Китая, Сингапура, Эстонии и США) демонстрирует, что ИИ уже активно применяется в процессах предварительного анализа доказательств, автоматизации рутинных процедур, прогнозирования решений и оптимизации документооборота.

[94] Информация авторского коллектива Генеральной прокуратуры Кыргызской Республики по п.11. Рабочей программы/ 24/150-16-16-05-04805/29.08.2024 г.

Вместе с тем, в силу различных аспектов, связанных с техническими возможностями, внутренними регламентами страны и другими составляющими, развитие электронного судопроизводства имеет место не во всех странах СНГ. В некоторых государствах-членах такие технологии находятся преимущественно на этапе апробации и нормативного осмысления, хотя отдельные проекты указывают на наличие потенциала для дальнейшего развития.

Перспективы развития электронного судопроизводства напрямую зависят от технологических достижений, наличия и квалификации специалистов в сфере IT-технологий, финансовых возможностей технического обеспечения и соответствующего обучения представителей органов уголовного преследования и судебного блока для введения электронного судопроизводства, стремления к прозрачности уголовного процесса.

При этом немаловажное значение имеет разумность подхода к применению высоких технологий. Стремление «не терять позиций и идти в ногу» по внедрению ИИ в правоохранительную и судебную деятельность может играть как положительную роль в совершенствовании судопроизводства, так и нанести непоправимый ущерб в виде нарушений законных прав участников процесса, а также государства.

Несомненно, как при внедрении, так и при применении ИИ необходимо обеспечивать информационно-техническую безопасность от технических сбоев, несанкционированного преступного воздействия, учитывать все возможные риски при внедрении высоких технологий в уголовный процесс.

Для органов прокуратуры перспективным представляется использование ИИ в сферах надзора за соблюдением законодательства, аналитической обработки больших массивов данных, к примеру статистики, судебной практики, при подготовке заключений по делам. Применение интеллектуальных систем может способствовать снижению нагрузки на сотрудников, повышению оперативности реагирования.

Вместе с тем широкое внедрение ИИ в прокурорскую деятельность сопряжено с рядом рисков. В их числе – угроза подмены человеческого правосознания алгоритмическими решениями, снижение уровня индивидуализации подхода к делам, вопросы правовой ответственности за действия автоматизированных систем, а также риски нарушения конфиденциальности и утечки чувствительной информации. Кроме того, сохраняются значительные правовые и этические неопределенности, связанные с допустимостью использования ИИ в процессуальной деятельности, особенно в контексте принципов справедливости, состязательности и равенства сторон.

Учитывая указанные обстоятельства, эффективное включение ИИ в электронное судопроизводство возможно лишь при условии комплексного правового регулирования, разработки четких стандартов подотчетности ИИ-систем, а также обеспечения прозрачности алгоритмов и сохранения ведущей роли прокурора как носителя правовой воли государства. Цифровая трансформация не должна нивелировать ценность человеческого участия, но

обязана служить его усилению на основе современных технологических инструментов.

§ 3.3 Стратегические направления перспективного развития применения искусственного интеллекта в органах прокуратуры государств СНГ

Прокурорский надзор, являясь одной из ключевых функций государства, направленных на обеспечение верховенства закона, защиту прав и свобод граждан, а также поддержание единства правоприменительной практики, в современных условиях претерпевает качественные изменения под воздействием цифровых технологий.

В условиях роста информационной нагрузки, усложнения правоприменительных процессов и усиления требований к оперативности реагирования системы ИИ начинают рассматриваться в качестве вспомогательного механизма, способствующего укреплению аналитической и прогностической составляющей надзорной деятельности. Интеграция ИИ позволяет повысить эффективность мониторинга исполнения законодательства, осуществлять углубленный анализ правоприменительной практики, своевременно выявлять скрытые закономерности правонарушений и прогнозировать потенциальные риски отклонения от установленных правовых стандартов. Вместе с тем использование интеллектуальных технологий должно основываться на четком соблюдении принципов законности, процессуальной самостоятельности органов надзора и уважении к фундаментальным гарантиям прав человека, исключая возможность подмены профессиональной оценки прокурора алгоритмическими рекомендациями. Таким образом, ИИ в прокурорском надзоре выступает не заменой традиционных институтов правоприменения, а их технологическим усилением, требующим одновременно тщательной нормативной регламентации и этической рефлексии.

Одним из наиболее перспективных направлений внедрения систем ИИ в сферу деятельности органов прокуратуры выступает автоматизация составления актов прокурорского надзора и реагирования. В условиях возрастающей сложности управленческих и правовых задач, а также увеличения объемов обрабатываемой информации применение ИИ становится не просто технологической инновацией, а необходимым элементом институционального укрепления надзорной функции государства.

Автоматизация составления актов прокурорского реагирования охватывает широкий спектр документов: от представлений и протестов до официальных предостережений и требований устранения нарушений законодательства. Современные интеллектуальные системы позволяют формировать проекты этих актов на основе анализа правонарушений, зафиксированных в ходе надзорной деятельности, с учетом юридической квалификации выявленных фактов, нормативной базы, судебной практики и иных правовых источников. В частности,

алгоритмы могут автоматически сопоставлять обстоятельства конкретного дела с типовыми ситуациями, извлеченными из обширного корпуса архивных прокурорских актов, а также включать соответствующие правовые формулировки и ссылки на нормативные документы.

Благодаря обучению на больших массивах текстов, ИИ способен выявлять устойчивые правовые конструкции, повторяющиеся аргументативные шаблоны и формальные признаки, характерные для тех или иных сфер правонарушений: в сфере трудового, экологического, бюджетного, административного, уголовного или антикоррупционного законодательства. Например, в случаях, связанных с нарушением сроков выплаты заработной платы, система может автоматически предложить текст представления с обоснованием в рамках Трудового кодекса и практики Верховного Суда, включающим данные о количестве пострадавших лиц, размере задолженности и предложением конкретных мер реагирования.

Интеллектуальные инструменты могут быть интегрированы с базами данных государственных органов, суда, правоохранительных органов и других субъектов взаимодействия, что обеспечивает полноту сведений для подготовки акта. Кроме того, такие системы позволяют избежать дублирования усилий, формализовать процесс предварительной правовой экспертизы и унифицировать подходы к оформлению надзорных актов, что особенно важно при оценке правомерности действий областных и горрайпрокуроров.

Не менее значимым является аспект повышения скорости реагирования на правонарушения. Использование интеллектуальных систем позволяет значительно сократить сроки подготовки правовых документов, оперативно подготавливая черновики актов, пригодных к последующей доработке прокурором. В условиях жестких временных рамок, связанных, например, с защитой прав социально уязвимых категорий граждан, обеспечение быстрого и качественного реагирования приобретает принципиальное значение.

Важно подчеркнуть, что даже при высоком уровне автоматизации окончательное решение о содержании и подписании акта остается за уполномоченным прокурором. Интеллектуальная система должна рассматриваться исключительно как вспомогательный инструмент, обеспечивающий информационно-аналитическую поддержку, но не замещающий профессионального юридического суждения. Такой подход соответствует принципам правовой определенности и индивидуального подхода, лежащим в основе прокурорской деятельности.

Автоматизация также открывает новые возможности для внутриорганизационного контроля качества. Все проекты актов, сформированные с использованием ИИ, могут автоматически индексироваться, сопоставляться с ранее изданными документами по аналогичным поводам, анализироваться на предмет корректности ссылок, полноты аргументации и соответствия действующим требованиям. Это позволяет не только повысить качество выходной правовой продукции, но и сформировать массив репрезентативной статистики для анализа эффективности прокурорского надзора в той или иной сфере.

Применение систем ИИ в автоматизации подготовки актов прокурорского надзора позволяет существенно повысить качество, обоснованность и единообразие документов, а также сократить временные затраты на их составление.

Например, в случаях выявления нарушений сроков выплаты заработной платы интеллектуальная система на основе анализа норм **трудового законодательства** и практики Верховного Суда может автоматически сформировать проект представления с обоснованием, указанием на количество пострадавших работников, размер задолженности, период просрочки и конкретные предложения по устранению выявленных нарушений, включая меры дисциплинарного и административного воздействия. При этом система способна учитывать региональные особенности правоприменения и уточнять ссылки на применимые нормативные акты.

В области экологического надзора ИИ может генерировать проекты актов реагирования при обнаружении фактов загрязнения окружающей среды: например, при фиксации сброса сточных вод без разрешительных документов. Система автоматически включит в текст нормативные основания (Экологический кодекс, санитарные правила), параметры превышения допустимых концентраций вредных веществ, описание причиненного ущерба окружающей среде и рекомендации по устранению нарушений и компенсации вреда.

При осуществлении надзора за соблюдением бюджетного законодательства интеллектуальные алгоритмы способны формировать проекты протестов или представлений по фактам нецелевого расходования бюджетных средств. В тексте автоматически будет обосновано наличие финансовых нарушений, приведены ссылки на положения Бюджетного кодекса и акты государственных аудиторов, а также предложены меры по возмещению ущерба и привлечению виновных должностных лиц к ответственности.

В сфере административного надзора ИИ может поддерживать прокурора при подготовке актов реагирования на факты нарушения прав граждан, например, в части неправомерного отказа в предоставлении социальных пособий. Система выявит несоответствие действий органов социальной защиты установленным требованиям законодательства, сформулирует соответствующие доводы, приведет статистические данные по аналогичным случаям, а также предложит конкретные формулировки для устранения нарушений.

В уголовно-правовой сфере автоматизированные решения могут использоваться для подготовки представлений по выявленным фактам нарушений при расследовании преступлений, например, в случае необоснованного затягивания сроков расследования или необоснованного прекращения уголовных дел. Интеллектуальные системы способны оперативно сопоставить действия (или бездействие) следственных органов с процессуальными требованиями уголовно-процессуального законодательства, выявить отклонения от сроков расследования, отсутствие надлежащего уведомления потерпевших, неполноту следственных

действий и сформировать мотивированное представление о необходимости устранения выявленных нарушений.

Аналогичным образом **в рамках антикоррупционного надзора** ИИ может помогать выявлять признаки конфликта интересов у государственных служащих или нарушения требований к декларированию доходов и имущества. В случае установления фактов сокрытия сведений интеллектуальная система способна сгенерировать проект представления с юридическим обоснованием выявленного нарушения, перечнем недекларированного имущества, ссылками на применимое законодательство и рекомендациями по применению мер дисциплинарного или иного воздействия.

Важным преимуществом внедрения ИИ в процесс подготовки актов прокурорского надзора является способность систем учитывать не только текстуальные закономерности, но и такие нюансы, как социальная значимость выявленного нарушения, характер и степень причиненного вреда, особенности правового регулирования конкретной сферы. Это позволяет автоматизированно подстраивать структуру и содержание актов в зависимости от тяжести правонарушения, статуса субъекта проверки и целей надзорного вмешательства.

Более того, интеллектуальные системы могут накапливать базы данных типовых актов реагирования, сформированных ранее по аналогичным случаям, с их последующей адаптацией к новым ситуациям. Это особенно актуально для прокуроров, работающих в отдаленных районах или при высокой нагрузке, когда необходимо оперативно формировать качественные документы, соответствующие современным требованиям юридической техники.

Таким образом, автоматизация подготовки актов прокурорского надзора с использованием ИИ открывает новые перспективы для повышения эффективности надзорной деятельности, обеспечения единообразия правоприменительной практики и укрепления законности. Вместе с тем развитие данных технологий требует тщательной правовой регламентации, обеспечения прозрачности алгоритмических процедур и сохранения пространства для профессиональной юридической оценки, без которой невозможно осуществление полноценного надзора за соблюдением закона в условиях цифровизации.

Автоматизация составления актов прокурорского надзора и реагирования посредством применения систем ИИ является ключевым направлением институциональной цифровизации прокуратуры. Она способствует повышению правовой точности, ускоряет процедуры реагирования, обеспечивает единообразие правоприменения, снижает административную нагрузку на сотрудников прокуратуры и одновременно служит гарантией более высокого уровня защиты общественных интересов и прав граждан. Эффективная реализация данного направления требует нормативного закрепления процедур использования ИИ, прозрачности алгоритмических решений, а также организационных мер по обучению персонала работе с новыми интеллектуальными инструментами.

Несмотря на очевидные преимущества, широкомасштабное внедрение ИИ в сферу прокурорского надзора сопряжено с рядом существенных рисков и ограничений, игнорирование которых может негативно повлиять на легитимность и качество надзорной деятельности. Один из острых вызовов заключается в угрозе стандартизации юридической аргументации, при которой акты прокурорского реагирования теряют индивидуализированный подход и становятся результатом машинной компиляции. Такая тенденция чревата снижением гибкости правоприменения, ослаблением предметного анализа и искажением принципа соразмерности реагирования по отношению к конкретным правонарушениям.

Вторым немаловажным ограничением является недостаточная адаптивность ИИ к динамике законодательства и правоприменительной практики. Даже при регулярном обновлении алгоритмических баз, интеллектуальные системы могут опираться на устаревшие или неоднозначные правовые положения, что повышает риск ошибок в формулировке правовой позиции или выводов о нарушении. Кроме того, алгоритмизация актов надзора зачастую затрудняет их апелляционную защиту в случае последующего судебного обжалования, поскольку прокурору необходимо будет не только отстаивать правовую позицию, но и объяснять основания, на которых ее сформировал алгоритм, что связано с проблемой «черного ящика» в ИИ.

Особую обеспокоенность вызывает и угроза подмены прокурорского усмотрения алгоритмической репликацией шаблонов, при которой автоматизированная система может без должной юридической чувствительности воспроизводить формальные конструкты, не учитывая деликатные социальные, этические или межведомственные обстоятельства. Это особенно критично при надзоре в сферах, где необходима не просто юридическая корректность, но и гуманистический подход.

Также необходимо учитывать возможность алгоритмической предвзятости – как следствие ошибок, заложенных на этапе обучения модели. Например, если система формировалась на основе выборки актов, содержащих устойчиво негативные суждения о деятельности конкретных органов или категорий субъектов, она может воспроизводить такую предвзятость в будущем, закрепляя необоснованные обвинения или перекосы в оценке одних и тех же ситуаций.

Не менее существенной является проблема юридической ответственности. Вопрос о том, кто несет ответственность за юридическую ошибку в акте прокурорского надзора, сформированном с участием ИИ – разработчик, оператор, прокурор или ведомство в целом – до сих пор остается без нормативного разрешения. Это создает неопределенность, снижает предсказуемость правовых последствий и может повлечь затруднения в привлечении к дисциплинарной ответственности за недобросовестную надзорную практику.

Наконец, нельзя исключать риски утечки персональных данных, поскольку составление актов нередко связано с обработкой чувствительной информации, касающейся частной жизни граждан, служебной деятельности должностных лиц,

внутренней документации государственных органов. В этой связи автоматизированные системы должны соответствовать высоким стандартам информационной безопасности и иметь многоуровневую архитектуру защиты от несанкционированного доступа.

Проведение анализа состояния законности с использованием ИИ представляет собой одно из наиболее перспективных направлений модернизации надзорной функции государства. Интеграция ИИ в аналитическую деятельность органов прокуратуры обеспечивает принципиально новый уровень обработки правоприменительной информации, позволяет систематизировать, обобщать и интерпретировать данные в масштабах, ранее недоступных при использовании исключительно традиционных методов. Такой подход не только расширяет возможности надзора за соблюдением законности, но и формирует основу для выработки научно обоснованных, обобщенных и адресных мер прокурорского реагирования.

ИИ-системы, обученные на репрезентативных выборках нормативных правовых актов, судебных решений, статистических данных, материалов прокурорских проверок и обращений граждан, способны формировать комплексные аналитические отчеты по состоянию законности в конкретной сфере или территории. Например, в сфере соблюдения трудовых прав система может выявить устойчивую корреляцию между количеством обращений о задержке заработной платы и неблагоприятной динамикой банкротства предприятий в определенном регионе. На этой основе формируются обоснованные выводы, подлежащие прокурорскому осмыслению и использованию в дальнейших мерах реагирования.

Применение ИИ позволяет существенно сократить временные затраты на первичную обработку больших массивов данных и выявить ранее скрытые закономерности. Так, анализ динамики правонарушений в сфере охраны окружающей среды может быть дополнен сопоставлением с погодными условиями, индексом загрязненности, количеством жалоб граждан и результатами проверок контролирующих органов. Это позволяет установить глубинные причины нарушений и разрабатывать профилактические меры с опорой на фактические взаимосвязи.

Кроме того, интеллектуальные системы могут выполнять мониторинг изменений законодательства и правоприменительной практики, предсказывать вероятные последствия законодательных новаций и моделировать риски недобросовестного применения новых норм. Например, **при анализе правоприменения в сфере государственных закупок** ИИ способен выявить частоту и причины признания торгов несостоявшимися, динамику количества жалоб в антимонопольные органы, повторяемость конкретных нарушений у одних и тех же заказчиков.

Важным преимуществом ИИ в надзорной деятельности является его способность анализировать межведомственные данные и строить межсистемные связи. Это позволяет прокуратуре выходить за пределы локальных инцидентов и

формировать представление о системных нарушениях. Так, при рассмотрении вопросов незаконного оборота лекарственных препаратов ИИ может обрабатывать данные из регистра лекарственных средств, системы электронных рецептов, протоколов проверок аптек и актов санитарно-эпидемиологического надзора, выявляя не только отдельные нарушения, но и криминогенные схемы, требующие координации с правоохранительными органами.

Однако столь широкомасштабное использование ИИ в прокурорском надзоре сопряжено и с рядом существенных рисков. Прежде всего, это угроза алгоритмической предвзятости, возникающей в случае, если обучающие выборки содержат искаженные или нерепрезентативные данные. Такие алгоритмы могут некорректно интерпретировать информацию, акцентируя внимание на второстепенных признаках или упуская из виду важные нюансы. В результате возможна подмена объективного анализа стереотипными выводами, особенно в социально чувствительных сферах, таких как миграционное право, права инвалидов, доступ к медицинской помощи.

Также вызывает опасения проблема так называемого «черного ящика» – неспособности объяснить логику принятого ИИ решения. В надзорной деятельности, где каждое действие должно быть юридически обосновано и документально подтверждено, недопустимо использование выводов, не поддающихся верификации и воспроизведению. Это требует внедрения только тех ИИ-систем, которые соответствуют критерию explainability (объяснимости), то есть позволяют пользователю проследить логические шаги, приведшие к тому или иному результату анализа.

Еще одним немаловажным аспектом является защита персональных данных. Поскольку анализ законности зачастую требует работы с конфиденциальной информацией, в том числе в сфере уголовного преследования, социального обеспечения, трудовых отношений, необходимо обеспечить строгий режим обработки, хранения и передачи данных, задействованных в работе ИИ. Без соблюдения этих условий использование интеллектуальных технологий не только теряет правовую легитимность, но и может повлечь репутационные риски для прокуратуры.

Кроме того, необходимо учитывать риск избыточной зависимости от технических решений. Интеллектуальные алгоритмы могут эффективно выполнять вспомогательные аналитические функции, но не способны заменить экспертное правовое суждение. Решения о наличии или отсутствии нарушений, выборе формы прокурорского реагирования и оценке последствий должны оставаться в исключительной компетенции прокурора, обладающего необходимым профессиональным опытом, концептуальным пониманием ситуации и правовой ответственностью.

В современных условиях транснациональной экономики и высокой подвижности капиталов незаконное приобретение, вывод и последующее сокрытие активов стали одним из приоритетных объектов прокурорского надзора и антикоррупционной политики. Эффективное противодействие этим формам

правонарушений требует внедрения новых подходов к мониторингу финансовых потоков, анализу транзакционных цепочек и выявлению скрытых схем аффилированности и обналичивания. На этом фоне интеграция ИИ в деятельность органов прокуратуры и правоохранительной системы в целом приобретает особую значимость. Интеллектуальные системы, опирающиеся на обработку больших данных (Big Data), машинное обучение и алгоритмы предиктивной аналитики, способны значительно повысить оперативность и точность выявления аномалий в финансовом обороте, что затруднительно при использовании традиционных методов анализа.

Применение ИИ в указанной сфере может реализовываться в нескольких направлениях. Во-первых, это автоматизированный мониторинг открытых и закрытых источников информации, включая банковские транзакции, государственные закупки, отчеты юридических лиц, международные базы по движению капитала и активов. Такие системы способны в реальном времени отслеживать подозрительные перемещения средств, не соответствующие обычной экономической логике или значительно отклоняющиеся от среднестатистических поведенческих паттернов субъектов предпринимательства. Например, алгоритмы могут идентифицировать дробление платежей, их нерациональную маршрутизацию через офшорные зоны, либо установление деловых связей с компаниями, фигурирующими в санкционных списках или имеющими признаки фиктивности.

Во-вторых, ИИ может быть использован для выявления взаимосвязей между лицами и структурами, участвующими в незаконных операциях, путем построения графов взаимодействия, выявления перекрестного владения и номинальных структур. Это особенно актуально при расследовании дел, связанных с коррупцией, отмыванием доходов, а также с активами, полученными путем хищения бюджетных средств или злоупотреблений при исполнении государственных функций. Алгоритмы, обученные на судебной и прокурорской практике, способны распознавать схемы скрытого контроля и косвенного участия в управлении, позволяя значительно ускорить процесс аналитической проверки и выстраивания логической цепочки правонарушения.

Третьим направлением является **интеграция ИИ в процедуры международного сотрудничества по вопросам возврата активов**. В рамках таких процессов интеллектуальные системы могут сопоставлять данные о декларированных доходах, имуществе, регистрационных записях, судебных и корпоративных базах данных различных юрисдикций, выявляя расхождения, фиктивные транзакции или сокрытие имущества. Например, в делах, где подозреваемые лица перевели значительные суммы за рубеж через сложные цепочки компаний-«прокладок», ИИ может выстроить трассировку активов, основываясь на данных из международных реестров, реестров конечных бенефициаров и цифровых следов трансграничных операций.

Однако, вновь возвращаясь к вопросам надежности систем, отметим, что столь мощные инструменты неизбежно сопряжены с рядом рисков и требуют

тщательного нормативного оформления. На первом плане стоит вопрос допустимости автоматизированного анализа персональных и финансовых данных в сфере соблюдения прав на частную жизнь, защиту персональной информации и соблюдение стандартов законности. Использование ИИ не должно подменять собой надлежащие процессуальные процедуры проверки, а результаты автоматического анализа не могут выступать в качестве единственного доказательства. Необходим строгий судебный или прокурорский контроль за использованием таких систем, включая обязательную верификацию выводов человека-аналитика.

Необходимо еще раз напомнить об алгоритмической непрозрачности, когда даже квалифицированные специалисты не могут проследить, на основании каких параметров ИИ сделал тот или иной вывод. Это особенно критично при принятии решений, затрагивающих права субъектов, таких как возбуждение уголовного дела, наложение ареста на имущество или направление запроса о возврате активов из-за рубежа. Следовательно, используемые алгоритмы должны быть подотчетны, интерпретируемы и подлежащими аудиту, а механизмы их применения – четко регламентированы.

Важным является и вопрос национального суверенитета в информационной сфере: использование ИИ, созданного зарубежными компаниями, в сфере анализа чувствительных данных может привести к утечке информации или несанкционированному доступу третьих сторон. В данном аспекте развитие отечественных решений и платформ становится ключевым условием обеспечения информационной безопасности в сфере мониторинга активов.

Интеллектуальные технологии обладают значительным потенциалом в сфере анализа информации, связанной с незаконным приобретением и трансграничным перемещением активов, но их применение должно быть встроено в четкую нормативную архитектуру. Необходима разработка специальных методических рекомендаций для органов прокуратуры, регламентирующих использование ИИ в надзорной и аналитической работе, включая вопросы правовой ответственности, процедурного контроля и защиты прав граждан. Только в условиях нормативной определенности, этической допустимости и технической прозрачности можно обеспечить эффективное и одновременно правомерное использование ИИ в целях борьбы с преступным обогащением и восстановления социальной справедливости.

Определение оснований для отмены мер запретительного либо ограничительного характера, а также приостановления действия нормативных или индивидуальных правовых актов, признанных незаконными, представляет собой важнейшее направление надзорной деятельности, в том числе с учетом возможностей, предоставляемых технологиями ИИ. В рамках прокурорского анализа такие меры интерпретируются как временные инструменты правового воздействия, направленные на пресечение или недопущение дальнейших нарушений законности, в том числе в сфере государственного управления,

финансового контроля, соблюдения экологических норм, трудовых и социальных гарантий.

Однако по мере устранения обстоятельств, послуживших основанием для введения ограничительных или запретительных мер, перед правоприменительными органами, в том числе прокуратурой, встает задача осуществления повторной правовой оценки их обоснованности и актуальности. Такая переоценка должна учитывать как фактические изменения в ситуации, так и трансформации нормативного поля, включая вступление в силу новых актов, отмену ранее действовавших положений или изменение судебной практики. В данном случае ключевым становится вопрос о правомерности продолжения действия ограничений, особенно если они затрагивают имущественные права, свободу передвижения или экономическую деятельность физических и юридических лиц.

Применение интеллектуальных систем в подобных ситуациях позволяет повысить точность и оперативность анализа. ИИ, задействованный в процессах мониторинга и правовой аналитики, может быть обучен на базе прецедентов, судебных решений, заключений органов правового надзора и текущего законодательства. Такая система способна выявлять закономерности, указывать на устаревшие основания, сопоставлять временные рамки действия акта с текущими обстоятельствами и тем самым формировать аргументированные выводы о необходимости его отмены или пересмотра.

Например, при введении ранее мер по ограничению деятельности предприятия по экологическим основаниям интеллектуальная система, анализируя обновленные заключения уполномоченных органов (например, уполномоченного органа в сфере экологии) и судебные решения, вынесенные по аналогичным делам, может сигнализировать о том, что предприятие устранило выявленные нарушения, а значит – дальнейшее действие ограничений утрачивает законную основу. Кроме того, система может автоматически отследить, были ли внесены в законодательство изменения, которые исключают необходимость таких ограничений в принципе – например, отмена ранее обязательного разрешительного порядка или пересмотр санитарных норм.

В случае приостановления действия акта государственного органа ИИ может проанализировать динамику нормативных актов по смежной тематике, выявить наличие новых разъяснений Генеральной прокуратуры, решений высших судебных инстанций или измененной практики применения норм, на которых основывался приостановленный акт. Все это позволяет органам надзора объективно оценить, сохраняются ли основания для поддержания ограничительных мер или требуется их отмена.

Важно подчеркнуть, что в таких случаях ИИ не подменяет правовую оценку прокурора или судьи, но предоставляет инструментарий, позволяющий более быстро и обоснованно выявить обстоятельства, при которых мера становится юридически избыточной. Это особенно значимо в сфере защиты предпринимательской деятельности, для соблюдения баланса между частными

интересами и публичными мерами воздействия, а также в ситуациях, затрагивающих права и свободы человека и гражданина.

Таким образом, использование интеллектуальных аналитических инструментов в процессе установления обоснованности продолжения действия ограничительных или запретительных мер формирует основу для более эффективного, правомерного и своевременного реагирования со стороны органов надзора, обеспечивает соблюдение принципов правовой определенности, соразмерности и справедливости в динамично изменяющихся правовых условиях.

Еще одной из важнейших форм надзорной деятельности, направленной на обеспечение законности в уголовном судопроизводстве, является **проверка материалов уголовных дел прокурором.** При этом особое внимание уделяется оценке законности получения первичных доказательств, наличию оснований для ограничения прав и свобод лица, а также полноте проверки сообщения о преступлении.

В рамках стадий составления обвинительного акта и направления дела в суд прокурор осуществляет более детальную проверку всех материалов, оценивая законность процессуальных действий, достаточность доказательственной базы, правильность квалификации содеянного и соблюдение прав участников процесса.

Интеграция систем ИИ в процессы прокурорской проверки материалов уголовных дел позволяет существенно повысить эффективность аналитической деятельности на данном этапе. Применение интеллектуальных систем может реализовываться в нескольких направлениях.

Во-первых, ИИ способен автоматизировать проверку полноты досудебного расследования, анализируя наличие всех необходимых процессуальных документов, касающихся уведомления о правах подозреваемого, проведения следственных действий с участием понятых, соблюдения сроков процессуальных решений. Например, в деле о хищении государственного имущества интеллектуальная система может выявить отсутствие заключения финансово-экономической экспертизы.

Также отсутствие протокола допроса лиц, выполняющих функции финансового контроля в организации, свидетельствует о неполной реализации принципа всесторонности при сборе доказательственной базы.

Во-вторых, интеллектуальные алгоритмы позволяют оперативно обнаруживать процессуальные ошибки, которые в дальнейшем могут повлечь признание доказательств недопустимыми. Система может идентифицировать, например, протокол допроса, оформленный при отсутствии защитника в случаях, когда его участие является обязательным, либо зафиксировать факт отсутствия подписей понятых в протоколе обыска, что влечет необходимость соответствующего прокурорского реагирования в рамках надзора за соблюдением процессуального законодательства.

В-третьих, ИИ может служить инструментом проверки соблюдения процессуальных прав участников процесса. Путем анализа текстов протоколов, постановлений и жалоб, интеллектуальные системы способны сигнализировать о

потенциальных нарушениях права на защиту либо выявлять случаи задержания без вынесения соответствующего процессуального акта в срок.

Кроме того, ИИ позволяет применять методы предиктивной аналитики для оценки судебной перспективы дела. Обрабатывая массив данных о предыдущих судебных решениях по аналогичным делам, система может формировать прогноз вероятности вынесения обвинительного приговора, применения сокращенного порядка судебного разбирательства или заключения соглашения о признании вины. Такая информация может использоваться прокурором исключительно как вспомогательный ориентир при выработке позиции по делу, сохраняя при этом приоритет самостоятельной юридической оценки.

Интеллектуальные технологии также могут способствовать выявлению связей между различными уголовными производствами, что особенно важно при расследовании организованных форм преступности и коррупционных схем. На основе анализа данных о фигурантах, компаниях, номерах телефонов, электронных адресах ИИ способен строить графы связей, выявляя скрытые структуры преступных группировок, что дает основание для объединения производств или возбуждения новых уголовных дел по выявленным эпизодам.

Дополнительно интеллектуальные системы могут предлагать проекты процессуальных решений: постановлений о возврате дела для дополнительного расследования, об изменении меры пресечения, о прекращении уголовного дела за отсутствием состава уголовного правонарушения. При этом необходимым условием является обязательная правовая экспертиза и утверждение подготовленных решений со стороны прокурора, поскольку ни одна автоматизированная рекомендация не может заменить профессиональное юридическое суждение, основанное на принципах законности, справедливости и оценке конкретных обстоятельств дела.

Например, в практике может возникнуть ситуация, когда дело о мошенничестве в сфере страхования поступает в прокуратуру для составления обвинительного акта. ИИ-система, анализируя материалы дела, выявляет, что все допросы потерпевших проведеных без соблюдения положений о разъяснении их прав и обязанностей. В этом случае прокурору будет предложено обратить внимание на данные нарушения для принятия соответствующего решения.

Другой пример, в производстве находится дело о легализации доходов, полученных преступным путем. Интеллектуальная система, анализируя движение денежных средств по счетам фигуранта и сопоставляя данные с международными базами подозрительных операций, выявляет факты перевода средств на счета компаний, зарегистрированных в юрисдикциях с высоким уровнем банковской тайны. Эта информация позволяет прокурору инициировать дополнительные международные запросы в рамках исполнения конвенционных обязательств.

Несомненно, интеграция ИИ в процессы прокурорской проверки требует строгого соблюдения стандартов процессуальной законности и защиты прав участников уголовного процесса. Результаты работы интеллектуальных систем могут использоваться исключительно в качестве аналитических ориентиров, но не

в качестве самостоятельных доказательств или оснований для принятия процессуальных решений без их верификации прокурором. Особое внимание должно уделяться вопросам защиты персональных данных, конфиденциальности сведений предварительного расследования и прозрачности алгоритмов анализа.

Таким образом, использование систем ИИ в проверке материалов уголовных дел открывает широкие возможности для повышения качества прокурорского надзора, однако требует одновременно соблюдения строгих правовых рамок, исключающих риски автоматизации правосудия без должного контроля со стороны органов прокуратуры.

Одним из центральных этапов досудебного производства, определяющим структуру и качество последующего судебного разбирательства, является **формирование линии обвинения**. После изучения материалов уголовного дела, поступившего с отчетом о завершении досудебного расследования, прокурор принимает решение о составлении обвинительного акта. При этом он обязан убедиться в наличии достаточной совокупности допустимых доказательств, подтверждающих обоснованность предъявленного обвинения, а также в соблюдении прав обвиняемого. Линия обвинения должна основываться на внутренне непротиворечивом, логически выстроенном и доказательно обеспеченном изложении событий, охватывающем квалификацию деяния, установление субъекта преступления, мотивацию и механизм совершения противоправного деяния.

Формирование обвинения требует последовательного выполнения ряда задач: квалификационной оценки фактических обстоятельств дела, отбора релевантных доказательств, устранения процессуальных ошибок в материалах дела, прогнозирования возможных линий защиты и заблаговременной подготовки к их опровержению.

Интеграция систем ИИ в процессы формирования линии обвинения открывает новые возможности для аналитического сопровождения деятельности прокурора. Интеллектуальные системы способны осуществлять предварительную структуризацию доказательственного материала, группируя его по элементам состава преступления: объекту, объективной стороне, субъекту и субъективной стороне.

Например, в делах о коррупционных преступлениях интеллектуальные системы могут автоматически выделить блоки доказательств, подтверждающих наличие признаков служебного положения обвиняемого, фактов получения имущественных выгод и причинно-следственной связи между действиями субъекта и наступившими последствиями. Это позволяет прокурору не только структурировать обвинение в соответствии с процессуальными стандартами, но и заранее выявить потенциально слабые места в доказательственной базе.

ИИ также может использоваться для автоматизированного построения логических моделей событийной цепочки, позволяющих визуализировать последовательность противоправных действий обвиняемого, этапы подготовки, совершения и сокрытия преступления. Такие инструменты особенно полезны при

расследовании сложных многоэпизодных дел, например, связанных с экономическими преступлениями, где требуется восстановление сложных схем хищений или махинаций с финансовыми активами.

Интеллектуальные системы способны анализировать содержание допросов свидетелей, потерпевших и подозреваемых, выявлять противоречия в показаниях, а также формировать перечень вопросов, требующих дополнительной проверки или уточнения. Например, в деле о мошенничестве, где свидетельские показания противоречат друг другу в части размера причиненного ущерба, ИИ может рекомендовать проведение дополнительного допроса либо экономической экспертизы, что способствует своевременному устранению пробелов в доказательственной базе.

Помимо подготовки проектов процессуальных документов, обвинительных актов, отдельного внимания заслуживает возможность применения ИИ для составления ходатайств о применении мер пресечения, представлений о привлечении дополнительных доказательств. В этих проектах автоматически учитываются требования уголовно-процессуального законодательства о структуре обвинительного акта, включая описание инкриминируемых действий, правовую квалификацию, характеристику личности обвиняемого и обоснование необходимости применения конкретных процессуальных мер.

Тем не менее, следует подчеркнуть, что использование интеллектуальных систем при формировании линии обвинения носит вспомогательный характер и не освобождает прокурора от обязанностей самостоятельной юридической оценки материалов дела, критического анализа доказательств и профессиональной выработки позиции обвинения. Все выводы, предложенные интеллектуальной системой, должны быть верифицированы и оценены в свете принципов состязательности сторон, презумпции невиновности и недопустимости осуждения без достаточных доказательств.

Гипотетический пример практического применения ИИ можно представить следующим образом: в деле о взяточничестве система на основе анализа аудиозаписей, данных об электронных переводах и переписки в мессенджерах формирует график встреч подозреваемого с предполагаемым посредником. Далее алгоритм предлагает прокурору проект фабулы обвинительного акта, где подробно описываются обстоятельства передачи денежных средств, ссылки на конкретные доказательства и положения законодательства, устанавливающие ответственность за содеянное.

В другом примере, при расследовании масштабной схемы вывода бюджетных средств через подставные тендеры ИИ, анализируя финансовые потоки и корпоративные связи, выделяет ключевых участников схемы и последовательность их действий, что позволяет прокурору сформировать обвинение против организованной группы по соответствующим квалифицирующим признакам.

Особое внимание при применении ИИ должно уделяться защите прав обвиняемого и обеспечению процедурной справедливости. Применение

интеллектуальных систем не должно вести к автоматизированному обвинению без всестороннего исследования всех обстоятельств дела, в том числе оправдывающих подозреваемого. Каждый элемент обвинения обязан быть обоснованным, проверенным и подкрепленным допустимыми доказательствами, соответствующими требованиям процессуального закона.

Таким образом, формирование линии обвинения с использованием систем ИИ открывает новые горизонты для повышения качества прокурорской деятельности, однако требует строгого соблюдения правовых стандартов, приоритета человеческого профессионального суждения и уважения к фундаментальным принципам уголовного процесса[95].

Выводы главы 3

В государствах-участниках СНГ идет активная, с переломным успехом в отдельных государствах, трансформация судопроизводства в модель электронного ведения делопроизводства.

Перспектива внедрения и дальнейшего развития электронного судопроизводства зависит от ряда аспектов, связанных с технологическими достижениями и возможностями, бюджета, наличия квалифицированных специалистов, возможности обучения действующего состава правоохранительного и судебного блока, внутренних регламентов страны, стремления к прозрачности судопроизводства.

Эффективное использование ИИ в электронном делопроизводстве, уголовной и других сферах прокурорского надзора, помимо необходимого уровня технического обеспечения, требует соблюдения целого комплекса организационных и правовых условий.

Прежде всего, это разработка нормативных регламентов, определяющих сферы допустимого применения ИИ, процедуры верификации результатов и порядок применения алгоритмов, в особенности при постановке задач по вынесению решений.

Во-вторых, обеспечение профессиональной подготовки прокуроров к взаимодействию с интеллектуальными аналитическими платформами, включая навыки критического восприятия и интерпретации данных.

В-третьих, формирование механизмов внешнего и внутреннего контроля за использованием ИИ в надзорной практике, включая аудит алгоритмов, независимую экспертизу и участие общественных институтов в оценке последствий цифровизации прокурорской деятельности.

Только в условиях сбалансированного подхода, основанного на приоритете законности, прозрачности и соблюдении прав человека, интеграция ИИ в функции анализа состояния законности может стать устойчивым инструментом повышения эффективности и обоснованности прокурорского надзора. ИИ не

[95] Садыков М.Б. Искусственный интеллект в правоохранительной деятельности:правовые и организационно-тактические аспекты: дис. ...д-ра философии (PhD). – Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2025.

должен заменять человека, но обязан усиливать его способность видеть картину в целом, ориентироваться в сложных массивах информации и принимать решения, соответствующие принципам правового государства.

Принятие решение о подписании акта должно оставаться за уполномоченным прокурором. Интеллектуальная система должна рассматриваться исключительно как вспомогательный инструмент, обеспечивающий информационно-аналитическую поддержку, но не замещающий профессионального юридического суждения.

Анализ международной практики и перспектив применения ИИ в деятельности правоохранительных органов, в том числе ряде государств-участников СНГ, показывает следующие перспективные направления возможностей применения ИИ в надзорной деятельности:

- осуществление углубленного анализа правоприменительной практики, выявление скрытых закономерностей правонарушений и прогноз потенциальных рисков отклонения от установленных правовых стандартов;

- автоматизация составления актов прокурорского надзора и реагирования на основе анализа ИИ правонарушений, зафиксированных в ходе надзорной деятельности, с учетом юридической квалификации выявленных фактов, нормативной базы, судебной практики и иных правовых источников;

- автоматическая индексация проектов актов, сформированных с использованием ИИ, сопоставление с ранее изданными документами по аналогичным поводам, анализ на предмет корректности ссылок, полноты аргументации и соответствия действующим требованиям;

- выявление устойчивых правовых конструкций, повторяющихся аргументативных шаблонов и формальных признаков, характерных для тех или иных сфер правонарушений;

- способность систем ИИ учитывать не только текстуальные закономерности, но и такие нюансы, как социальная значимость выявленного нарушения, характер и степень причиненного вреда, особенности правового регулирования конкретной сферы;

- обнаружение процессуальных ошибок, которые в дальнейшем могут повлечь признание доказательств недопустимыми;

- осуществление проверки соблюдения процессуальных прав участников процесса;

- оценка судебной перспективы дела;

- выявление связей между уголовными производствами;

- проверка полноты досудебного расследования;

- составление проектов процессуальных решений;

- построение логических моделей событийной цепочки, позволяющих визуализировать последовательность противоправных действий обвиняемого, этапы подготовки, совершения и сокрытия преступления;

- принятие решение о составлении обвинительного акта;

- анализ содержания допросов свидетелей, потерпевших и подозреваемых, выявление противоречия в показаниях, формирование перечня вопросов, требующих дополнительной проверки или уточнения;

- формирование комплексных аналитических отчетов по состоянию законности в конкретной сфере или территории;

- проведение мониторинга законодательства и правоприменительной практики, прогнозирование вероятных последствий законодательных новаций и моделирование рисков недобросовестного применения новых норм;

- автоматическое формирование проектов представлений по устранению выявленных нарушений трудового законодательства (в случаях выявления нарушений сроков выплаты заработной платы) с указанием размера задолженности, периода просрочки и конкретных предложений, включая меры дисциплинарного и административного воздействия, с учетом региональных особенностей правоприменения;

- генерирование проектов актов реагирования в **области экологического надзора** при обнаружении фактов загрязнения окружающей среды;

- формирование проектов протестов или представлений по фактам нецелевого расходования бюджетных средств **при осуществлении надзора за соблюдением бюджетного законодательства;**

- выявление частоты и причин признания торгов несостоявшимися, динамики количества жалоб в антимонопольные органы, повторяемости конкретных нарушений у одних и тех же заказчиков **при анализе правоприменения в сфере государственных закупок;**

- помощь прокурору при подготовке актов реагирования на факты нарушения прав граждан **в сфере административного надзора;**

- подготовка представлений по выявленным фактам нарушений **при расследовании преступлений** (выявление необоснованного затягивания сроков расследования, незаконного прекращения уголовных дел, бездействия следственных органов, отсутствия надлежащего уведомления потерпевших, неполноты следственных действий);

- выявление признаков конфликта интересов у государственных служащих, нарушения требований к декларированию доходов и имущества **в рамках антикоррупционного надзора;**

- выявление присопоставлении расхождений данных о декларированных доходах, имуществе, регистрационных записях, судебных и корпоративных базах данных различных юрисдикций, фиктивных транзакциях, сокрытии имущества, в процедурах международного сотрудничества по вопросам возврата активов.

ЗАКЛЮЧЕНИЕ

Основные выводы и предложения

1. Текущее состояние цифровизации органов прокуратуры стран СНГ свидетельствует о целенаправленном внедрении информационно-аналитических систем, сосредоточенных на решении приоритетных задач в рамках надзорной деятельности. На национальном уровне активно реализуются проекты цифровизации, предусматривающие автоматизацию деятельности, в частности в сфере документооборота, аналитических функций, взаимодействия с иными государственными органами и населением по обработке обращений.

Несмотря на различие в количестве и функциональности используемых систем (от 4 до 25), прослеживается общая тенденция к построению комплексной цифровой среды прокурорской деятельности. Вместе с тем просматривается потребность в системном обучении персонала эффективному использованию новых технологий, особенно в государствах с наибольшим количеством ИТ-решений.

Уровень применения технологий ИИ в деятельности органов прокуратуры стран СНГ находится преимущественно на этапе апробации и разработки. В Российской Федерации и Республике Казахстан инициировано использование «мягкого ИИ» (soft AI) для решения узкоспециализированных задач, таких как обработка обращений, распознавание изображений с видеокамер, автоматизация документооборота, ИИ-помощник прокурора. В Кыргызской Республике и Республике Узбекистан ИИ-системы в органах прокуратуры на стадии разработки. Вместе с тем полноценное применение ИИ в органах прокуратуры государств-участников СНГ, в юридическом смысле, отсутствует.

Как показало исследование, существенными барьерами к его внедрению являются: несовершенство правового регулирования применения ИИ, недостаточное техническое оснащение (суперкомпьютеры, машиночитаемые метаданные и т.д.), нехватка квалифицированных IT-специалистов по разработке и дальнейшему обслуживанию систем ИИ, а также потребность в постоянном обучении прокуроров основам IT-технологий ввиду слабой цифровой компетентности работников прокуратуры и постоянным развитием ИИ-систем.

Вышеперечисленные аспекты также подтверждаются результатами проведенного опроса сотрудников органов прокуратуры стран СНГ (1500 человек).

Отсутствие единого юридического определения понятия «искусственный интеллект» на международном и национальном уровнях порождает проблемы классификации и правовой квалификации отдельных информационных систем. Наблюдается подмена понятий, когда автоматизированные системы ошибочно отождествляются с ИИ.

В целях унификации понятийного аппарата авторским коллективом составлен глоссарий терминов и определений в сфере ИИ, на основе международных и межгосударственных (Модельный закон об ИИ в СНГ)

стандартов скомпилированы собственные варианты определения термина ИИ, с фокусом на его практическое применение, позволяющие одновременно формировать научно обоснованный и единообразный подход к понятийному аппарату в данной области.

Отдельное внимание уделено критериям, отличающим ИИ от обычной автоматизации: использование машинного обучения, обработка естественного языка, генеративные алгоритмы и применение специализированного аппаратного обеспечения.

Для систематизации актов, регламентирующих сферу ИИ, составлены реестры международных и национальных актов.

2. Изучение материалов, предоставленных органами прокуратуры стран СНГ, показало, что формирование нормативной базы и проектов с ИИ осуществляется на основе принятых документов стратегического планирования и существующих профильных законодательных актов в области цифровизации.

В Республике Беларусь вопросы внедрения ИИ реализуются, согласно положению Декрета Президента Республики Беларусь от 21 декабря 2017 года «О развитии цифровой экономики», который предполагает также цифровую трансформацию органов прокуратуры. Вместе с тем информации о внедренных технологиях либо проектах с ИИ на основе предоставленных материалов не имеется.

В Республике Казахстан Генеральной прокуратурой разработана информационная система «Цифровой надзор», в 2024 году начата работа по подключению ИИ к камерам видеонаблюдения для автоматического распознавания разыскиваемых преступников, должников и пропавших без вести.

Также ведется разработка системы «Гособвинитель» на основе элементов ИИ. Ее внедрение позволит составлять проекты документов, производить автоматический расчет наказаний, вести календарь судебных процессов, уведомлять о сроках подачи ходатайств и протестов, реализовать другие задачи.

Продолжается интеграция с базами других государственных органов и организаций, а также системами видеоаналитики.

Ведутся доработки технической спецификации по оцифровке надзора за законностью во всех сферах, включая образование, транспорт, жилищно-коммунальное хозяйство, здравоохранение, безопасность, социально-экономическую сферу, строительство, защиту бизнеса.

Система может функционировать с компонентом «Умный город» и базами центральных государственных органов для осуществления надзора за управлением государственным имуществом, повышением эффективности обслуживания населения, профилактикой правонарушений, а также функционированием государственных органов.

При правильной расстановке задач система будет предупреждать о возможных рисках.

Разработано и введено в работу приложение «Мобильный прокурор» с элементами ИИ для прокуроров, государственных органов и населения.

Приложение обеспечивает удаленный доступ прокурора к цифровому рабочему месту, тесный и постоянный контакт с населением, а также оперативное взаимодействие с государственными органами для решения вопросов общества.

МВД и Генеральная прокуратура запустили новый ИИ-проект для ускорения расследований, который: переводит речь в текст; находит противоречия в показаниях; предлагает вопросы для допроса; автоматически готовит документы. Встроены 4 модуля: планирование, анализ показаний, подготовка документов, аналитика.

Таким образом, анализ применения ИИ в органах прокуратуры РК показывает, что в стране создана достаточно широкая технологическая база для развития и внедрения ИИ, ведутся перспективные проекты по внедрению ИИ, которые позволят повысить эффективность надзорной деятельности. Вместе с тем говорить о полноценном внедрении ИИ в деятельность прокуратуры говорить еще преждевременно.

В Кыргызской Республике с 2019 года реализуется Концепция цифровой трансформации «Цифровой Кыргызстан». В рамках цифровизации органов прокуратуры Кыргызстана Генеральной прокуратурой рассматривается возможность применения некоторых технологий ИИ, таких как нейроскоринг. Данная технология позволит производить различные расчеты и прогнозирование.

В Российской Федерации внедрение ИИ осуществляется в рамках Концепции цифровой трансформации органов и организаций прокуратуры РФ до 2025 года. Ряд инструментов «мягкого искусственного интеллекта» (soft AI) для выполнения узкоспециальных задач и обработки больших массивов данных (big data) планируется внедрить в 2025 году.

В Республике Узбекистан внедрение ИИ в информационные системы правоохранительных органов определено одним из приоритетных направлений стратегии «Цифровой прокурор – 2030». В рамках информационной системы «E-Murojaat» планируется использовать ИИ при распознавании лиц, классификации и распределении обращений среди правоохранительных органов.

Анализ текущего состояния и уровня развития ИИ позволяет сделать вывод, что на сегодня ИИ в буквальном его понимании еще не применяется в деятельности органов прокуратуры стран СНГ, охваченных исследованием.

Вышеприведенные примеры являются лишь отдельными элементами слабого (мягкого) ИИ.

3. Анализ международных и национальных норм, зарубежной и отечественной литературы свидетельствует об отсутствии единого понимания правовой природы термина «искусственный интеллект».

Подобный правовой пробел не позволяет разграничить применение ИИ от автоматизированных и запрограммированных информационно-аналитических систем.

Как следствие, на практике некоторые информационные системы ошибочно классифицируются как системы с применением ИИ.

Указанные выводы подтверждаются результатами проводимых международных встреч, выводами научных трудов и результатами настоящего исследования.

В этой связи необходимо учитывать, что использование ИИ характеризуется применением машинного обучения на данных без явного программирования; возможностью обработки естественного языка (распознавание текста, речи, голоса); наличием генеративных алгоритмов (создание контента включая изображения, текст, музыку или видео); применением современных «суперкомпьютеров» для машинного обучения и обработки данных.

Как показал анализ зарубежного опыта, имеются примеры применения ИИ в судебной деятельности и работе полиции.

Наибольший прогресс в данном направлении достигли Китай, США, ОАЭ, Эстония и ряд других государств. Вместе с тем ИИ с осторожностью внедряется в чувствительные для человека сферы, включая правоохранительную деятельность и отправление правосудия.

Исследование показало, что развитие информационных технологий, в том числе с применением элементов ИИ, является одним из приоритетных направлений цифровизации органов прокуратуры. Тем не менее здесь отсутствует четкое понимание возможностей ИИ и видение дальнейшего его применения, что создает риски фрагментарного и неэффективного внедрения инновационных решений.

В этой связи, с учетом задач органов прокуратуры, а также результатов анкетирования выделены наиболее востребованные и перспективные направления для внедрения ИИ:

- анализ и обработка обращений граждан и юридических лиц, а именно: автоматическое распознавание, сортировка и классификация обращений; маршрутизация по компетенции и приоритетам; выявление повторных или анонимных обращений;

- автоматизированная подготовка проектов процессуальных и иных документов: составление проектов протестов, заключений, представлений и других юридически значимых актов; проверка юридической корректности и логики документов; адаптация шаблонов под специфику дел и регионов;

- прогнозирование преступности: выявление закономерностей и трендов на основе больших массивов статистических данных; геоаналитика и моделирование зон риска; разработка рекомендаций по превентивным мерам;

- мониторинг и анализ СМИ на предмет правонарушений: выявление признаков публичных нарушений закона, призывов к экстремизму, клеветы, дискредитации госорганов и др.; оперативная фиксация и автоматизированная оценка рисков правонарушений;

- поиск и установление преступного имущества и теневых активов: сопоставление данных из различных источников для установления связи между субъектами; анализ транзакций, юридических лиц и реестров имущества; выявление попыток сокрытия доходов и активов;

- анализ и обработка материалов уголовных, административных и гражданских дел, исполнительного производства: выявление процессуальных ошибок, повторяющихся нарушений; построение моделей судебной и следственной практики; прогнозирование исходов по аналогичным делам;

- оценка эффективности прокурорского надзора, а именно: мониторинг выполнения предписаний и представлений; анализ статистики, временных показателей и эффективности реагирования; выявление слабых звеньев в системе надзора;

- проведение криминологической экспертизы проектов нормативных актов, а именно: анализ потенциальных последствий законодательных инициатив; выявление рисков роста криминогенной нагрузки или правовых пробелов.

Эти направления обладают значительным потенциалом для повышения эффективности прокурорского надзора и оптимизации процессов принятия решений.

Успешная интеграция ИИ в деятельность органов прокуратуры стран СНГ требует не только технологической готовности, но и разработки концептуальной, нормативной и методологической базы, обеспечивающей целенаправленное и безопасное внедрение интеллектуальных решений.

4. На основе зарубежного и национального опыта стран СНГ, опроса сотрудников и результатов исследования можно выделить следующие основные риски внедрения ИИ в деятельность органов прокуратуры стран СНГ:

- юридические риски: отсутствие четкой правовой регламентации применения ИИ в надзорной деятельности; сложности в определении ответственности за ущерб, причиненный ИИ-системами; возможные коллизии между решениями ИИ и принципами уголовного и административного процесса;

- технологические и эксплуатационные риски: программные сбои, технические ошибки, невозможность верификации и интерпретации решений ИИ; недостоверность исходных данных, повлекшая искажение аналитических выводов и управленческих решений; «черный ящик» ИИ – трудности в объяснении алгоритмических выводов или отсутствие прозрачности алгоритмов;

- киберриски и угрозы безопасности: несанкционированный доступ к данным, утечка или компрометация информации, включая персональные и служебные сведения; зависимость от зарубежных поставщиков программного обеспечения и оборудования; возможность вредоносного внедрения или манипуляции обучающими выборками (data poisoning);

- этические и социальные риски: предвзятость алгоритмов (algorithmic bias), основанная на неравномерном распределении данных; дегуманизация надзорной деятельности и утрата индивидуального подхода к делам; риск нарушения прав человека при автоматизированной классификации, прогнозировании или контроле;

- организационно-управленческие риски: снижение уровня доверия к решениям прокуратуры со стороны общества; возможное сокращение персонала

без должной адаптации и переквалификации; фрагментарность и дублирование функций ИИ-систем при отсутствии единой координации внедрения.

5. Потенциально интеграция ИИ в прокурорский надзор способна существенно повысить аналитическую составляющую надзорных процедур, обеспечив своевременное выявление нарушений законности, прогноз и тенденции правонарушений.

В эпоху цифровых преобразований стремительное развитие ИИ знаменует глубокую трансформацию – сдвиг в парадигме взаимодействия между человеком и машиной в процессе осуществления своих функций. ИИ перестает быть лишь техническим ресурсом, а становится частью когнитивного пространства прокурора, оказывая влияние на распознавание юридически значимых аномалий или закономерностей, на принятие решений в рамках надзорных функций и на интерпретацию правовой действительности.

Вместе с тем ключевым является вспомогательный характер алгоритмов, которые не должны подменять институционально закрепленную роль и ответственность сотрудника органов прокуратуры, а напротив, должны служить средством повышения обоснованности решений. Это особенно актуально в условиях неопределенности, наличия огромного массива, в том числе и противоречащей друг другу информации, а также ограниченного временного ресурса.

Такое понимание ИИ направлено на соблюдение баланса между неизбежной инновационной адаптацией и сохранением фундаментальной роли органов прокуратуры в структуре государственного управления. С философской точки зрения данный вывод базируется на принципе дополнительности, когда интеллектуальные системы должны усиливать, но не вытеснять человеческое суждение, сохраняя центральную роль прокурора как субъекта правовой оценки.

Рекомендации

В целях успешного внедрения ИИ в органах прокуратуры, снижения рисков и угроз как для органов прокуратуры, так и для правоохранительной системы в целом предлагается:

1) обеспечить подготовку квалифицированных кадров, предусмотрев обучение их основам функционирования и возможностей применения ИИ в практической деятельности и повышение квалификации действующих сотрудников с целью улучшения цифровой грамотности и навыков владения информационными системами.

В этих целях необходимо рассмотреть вопрос о разработке специализированных программ профессиональной переподготовки и повышения квалификации для сотрудников прокуратуры по направлениям цифровой грамотности, кибербезопасности, основам ИИ и машинного обучения; интегрировать модули по правовому регулированию ИИ в образовательные программы юридических и ИТ-специальностей; создать центры компетенций и учебно-научные кластеры при профильных вузах и научных учреждениях;

2) разработать четкие унифицированные национальные и межгосударственные стандарты и регламенты для применения ИИ в целях обеспечения безопасности данных и стабильности в правовой сфере. Предусмотреть правовые гарантии прозрачности алгоритмов, объяснимости решений и наличия механизма ответственности за действия систем ИИ.

Рассмотреть вопрос о возможности взять за основу стандарты международных организаций, таких как Европейская организация по стандартизации (ESO), Международная организация по разработке стандартов (SDO), Международный институт электросвязи (ITU), Международная организация по стандартизации (ISO), Международная электротехническая комиссия (IEC), Институт инженеров электротехники и электроники (IEEE).

При разработке стандартов руководствоваться основополагающими (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Конвенции ООН и др.) и специальными международными актами (Закон ЕС «Об искусственном интеллекте» 2024 г., «Общий регламент по защите персональных данных GDPR», Модельный закон СНГ «О технологиях искусственного интеллекта», направленный на регулирование ИИ в государствах-участниках СНГ).

В их основе должны лежать фундаментальные принципы, гарантирующие право человека на неприкосновенность частной жизни и обеспечивающие гарантию сохранности персональных данных при сборе и обработке информации системами ИИ;

3) обеспечить соответствующую инфраструктуру, включающую адекватные электромощности. Технологии ИИ, работающие на базе суперкомпьютеров, требуют значительных вычислительных ресурсов, что приводит к повышенным требованиям к электроснабжению;

4) обеспечить безопасную информационную инфраструктуру, включающую в себя внедрение надежных и современных технологий кибербезопасности, расширение штата IT-специалистов подразделений информационной безопасности; обеспечить доступ органов прокуратуры к высокопроизводительным вычислительным ресурсам, включая дата-центры, суперкомпьютеры и защищенные облачные платформы; развивать отечественные аппаратно-программные решения с учетом принципов цифрового суверенитета; внедрить современные технологии защиты персональных данных, криптографические протоколы, распределенные реестры (blockchain) и системы реагирования на киберинциденты.

5) обеспечить цифровой суверенитет, исключить внешнее вмешательство в цифровые системы, утечку чувствительной информации.

Для минимизации внешних угроз суверенитету отдельной страны необходимо формирование полного цикла создания отечественных ИИ-решений, включающих как разработку собственных алгоритмов, так и производство аппаратной базы: серверов, суперкомпьютеров, микропроцессоров, систем хранения данных, а также сборочных и расходных компонентов.

АВТОРСКИЙ КОЛЛЕКТИВ

Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан
Ерліханов Ә.С. – главный научный сотрудник;
Сагымбеков Б.Ж. – главный научный сотрудник, магистр права (LLM);
Мукатаев Т.М. – старший научный сотрудник;
Утепов Д.П. – доцент кафедры, магистр права;
Садыков М.Б. – ст.преподаватель кафедры, доктор философии (PhD)

Научно-практический центр укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь
Русецкий О.В. – заместитель директора, кандидат юридических наук;
Никитин Ю. А. – начальник отдела, кандидат юридических наук, доцент.

Генеральная прокуратура Кыргызской Республики
Чамбаев Э.Д. – заместитель начальника Главного управления информационных технологий;
Ногоева М.Ш. – старший прокурор Управления.

Университет прокуратуры Российской Федерации
Горошко И.В. – заведующий отделом, доктор технических наук;
Смирнов П.А. – заведующий отделом, кандидат юридических наук;
Камчатов К.В. – заведующий отделом;
Петров Л.Е. – заведующий отделом;
Соколов Д.А. – заместитель заведующего лаборатории;
Аристархов А.Л. – ведущий научный сотрудник, кандидат юридических наук;
Чащина И.В. – ведущий научный сотрудник, кандидат юридических наук;
Архипова Е.А. – старший научный сотрудник, кандидат юридических наук;
Литвинов А.А. – старший научный сотрудник;
Романова М.В. – старший научный сотрудник;
Рогачев Д.Е. – научный сотрудник.

Генеральная прокуратура Республики Узбекистан
Шаримов Х.У. – начальник Управления;
Исламов М.Р. – старший прокурор Управления.
Правоохранительная академия Республики Узбекистан
Тургунов А.А. – старший преподаватель кафедры оперативно-розыскной деятельности и киберправа.

ПРИЛОЖЕНИЕ

Реестр норм, инициатив, рекомендаций и других стандартов, регулирующих разработку и применение искусственного интеллекта

№	**Авторство (страны, организации, сообщества)**	**Разработанные документы (проекты), регулирующие сферу ИИ (международный стандарт, инициатива, норма (фреймворк), рекомендации)**	**Дата принятия акта (решения)/проект**
МЕЖДУНАРОДНЫЕ АКТЫ			
1	Документ разработан по результатам конференции Beneficial в Калифорнии, США.	«Азиломарские принципы»	2017 год
2	Группа ученых Монреальского и других университетов	Монреальская декларация об ответственном развитии ИИ	2017 год
3	Совет Европы	Руководство по этике для надежного ИИ Специальной группы экспертов высокого уровня Совета Европы	2018 год
4	Всемирная комиссия по этике научных знаний и технологий ЮНЕСКО	1) Доклад по этике ИИ (Рекомендации), 2) Рекомендация ЮНЕСКО об этических аспектах искусственного интеллекта от 23.11.2021	2019 год; 2021 год
5	Совет Европы	Европейская этическая хартия Совета Европы по использованию ИИ в	2019 год

		судебных системах (Страны Европы)	
6	Российская Федерация	Модельная Конвенция робототехники и искусственного интеллекта	2018 год
7	Совет Европы	Руководство по защите данных при использовании ИИ	2019 год
8	Совет Европы	Декларация Комитета Министров о манипулятивных возможностях алгоритмов	13.02.2019 года
9	Комиссар СЕ по правам человека при использовании ИИ	Рекомендации Комиссара СЕ по правам человека при использовании ИИ	2019 год
10	Экспертная группа по ИИ ОСЭР	Принципы ИИ и рекомендации по национальной политике Экспертной группы по ИИ (ОЭСР)	2019 год
11	Совет министров Совета Европы	Рекомендации Совета министров о влиянии алгоритмов на права человека (Совет Европы)	2019 год
НАЦИОНАЛЬНЫЕ ДОКУМЕНТЫ СТРАТЕГИЧЕСКОГО РАЗВИТИЯ ИИ			
12	Правительство США	Национальная стратегия правительства США по стандартизации критически важных и новых технологий	Май 2023 года
13	Франция	Национальная стратегия развития ИИ France IA 2018 год	Ноябрь 2018 года
14	Канада	Общеканадская стратегия ИИ	2018 год
15	Дания	Национальная стратегия по ИИ	2019 год
16	Российская Федерация	1) Национальная стратегия развития ИИ (утверждена Указом Президента РФ № 490); 2) Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г., (утв. распоряжением Правительства РФ № 2129-р).	10.10.2019 года 19.08.2020 года

17	Республика Беларусь	1) Концепция информационной безопасности утверждена постановлением Совета Безопасности № 1; 2) Государственная программа "Цифровое развитие Беларуси" на 2021-2025 годы, утверждена постановлением Совета Министров № 66; 3) Государственная программа инновационного развития на 2021-2025 годы, утверждена указом Президента № 348;	18.03.2019 года 02.02.2021 года 15.09.2021 года
18	Республика Казахстан	1) Концепция развития отрасли информационно-коммуникационных технологий и цифровой сферы. Утверждена Постановлением Правительства № 961 /https://adilet.zan.kz/rus/docs/P2100000961/history. 2) Концепции правовой политики Республики Казахстан до 2030 года. Утверждена Указом Президента № 674 // https://adilet.zan.kz/rus/docs/U2100000674	30.12.2021 года 15.10.2021 года
19	Кыргызская Республика	1) Концепция цифровой трансформации "Цифровой Кыргызстан 2019-2023" одобрена Решением совета безопасности года № 2; 2) План мероприятий по цифровизации управления и развития цифровой инфраструктуры в Кыргызской Республике на 2022-2023 годы, утвержден распоряжением Кабинета Министров КР № 2-р	14.12.2018 года 12.01.2022 года
20	Республика Таджикистан	Концепция цифровой экономики в Республике Таджикистан, утверждена постановлением Правительства Республики Таджикистан № 642	30.12.2019 года
ЗАКОНЫ И ПОДЗАКОННЫЕ АКТЫ			
21	Европейский союз	Закон Европейского союза «Об искусственном интеллекте»	2021 год
22	Российская Федерация	1) Федеральные законы № 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных" и от 31.07.2020 № 258-ФЗ "Об	24.04.2020 года

		экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации"; 2) "ГОСТ Р 60.0.0.1-2016. Национальный стандарт Российской Федерации. Роботы и робототехнические устройства. Общие положения" (утв. и введен в действие Приказом Росстандарта № 1373-ст) (ред. от 04.12.2020); "ГОСТ Р 59276-2020. Национальный стандарт Российской Федерации. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения" (утв. и введен в действие Приказом Росстандарта № 1371-ст); "ГОСТ Р 59277-2020. Национальный стандарт Российской Федерации. Системы искусственного интеллекта. Классификация систем искусственного интеллекта" (утв. и введен в действие Приказом Росстандарта № 1372-ст); "ГОСТ Р 59278-2020. Национальный стандарт Российской Федерации. Информационная поддержка жизненного цикла изделий. Интерактивные электронные технические руководства с применением технологий искусственного интеллекта и дополненной реальности. Общие требования" (утв. и введен в действие Приказом Росстандарта № 1373-ст); "ГОСТ Р 60.6.0.1-2021. Национальный стандарт Российской Федерации. Роботы и робототехнические устройства. Сервисные мобильные роботы. Уровни автономности. Термины и определения" (утв. и введен в действие Приказом Росстандарта № 407-ст); 3) Проект федерального закона № 512628-8 "О внесении изменений в Федеральный закон "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации" (внесен в Государственную Думу в декабре 2023 г.).	11.10.2016 года 23.12.2020 года 23.12.2020 года 23.12.2020 года 20.05.2021 года Проект 2023 год
23	Республика Казахстан	1) Закон Республики Казахстан № 418-V ЗРК «Об информатизации» // https://adilet.zan.kz/rus/docs/Z1500000418 2) Уголовный кодекс (гл.7 «Уголовные правонарушения в сфере	24.11.2015 года 03.07.2014 года

		информатизации и связи»); 3) Проект Цифрового кодекса	 2023 год
24	Кыргызская Республика	1) Закон № 127 "Об электронном управлении"; 2) Указ Президента № 64 «О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики»; 3) Проект Цифрового кодекса, [http://koomtalkuu.gov.kg/ru/view-npa/2927].	19.07.2017 года 17.12.2020 года Проект август 2023 года
25	Республика Таджикистан	1) Закон № 40 "Об информатизации" (действует в ред. 2022 г.); 2) Закон. № 1537 "О защите персональных данных".	06.08.2001 года 03.08.2018 года
26	Национальный институт стандартов и технологий (NIST) Министерства торговли США NIST возглавляет и участвует в разработке технических стандартов, включая международные стандарты, которые способствуют инновациям и общественному доверию системам, использующим ИИ	Система управления рисками ИИ NIST (AI RMF версия 1.0)	Стандарт, 2022 год
27	Международная организация по	1) Стандарты ISO/IES по регулированию работы с большими данными; 2) Стандарты ISO/IES по регулированию работы с ИИ	Стандарт, 2020 год Стандарт, 2020 год

	стандартизации (ISO) В ИСО есть специальный комитет, ISO/IEC/ JTC1/SC 42. Занимающийся стандартизацией в области ИИ. Этот комитет предоставляет рекомендации различным комитетам ИСО, разрабатывающим приложения для ИИ		
28	Республика Беларусь	Декрет Президента № 12 "О Парке высоких технологий" (ред. 2023 г.) предусматривает особый правовой режим (т.н. "регуляторную песочницу") для резидентов Парка, наделяет их правом вести деятельность "в сфере ИИ, создания систем беспилотного управления транспортными средствами".	22.09.2005 года

*** Содержание Реестра не является окончательным и может дополняться новыми данными