АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

Садыков М.Б.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Косшы, 2025

АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

Садыков М.Б.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Монография

Косшы, 2025

УДК 343.9:004.8
ББК 67.7:32.813
С14

Рецензенты:
Бертовский Лев Владимирович – директор Института высокотехнологичного права, социальных и гуманитарных наук Национального исследовательского университета «Московский институт электронной техники», профессор кафедры криминалистики Московского государственного университета имени М.В. Ломоносова, доктор юридических наук, профессор;
Гагарина Лариса Геннадьевна – директор Института системной и программной инженерии и информационных технологий Национального исследовательского университета «Московский институт электронной техники», доктор технических наук, профессор;
Сейтенов Калиолла Кабаевич – Первый проректор Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, доктор юридических наук, профессор, почетный академик Национальной академии наук Республики Казахстан.

Садыков М.Б.
Концептуальные основы интеграции искусственного интеллекта в деятельность правоохранительных органов: монография / М.Б. Садыков. – Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2025. – 200 с.

В монографии исследуются концептуальные основы применения искусственного интеллекта в деятельности правоохранительных органов Республики Казахстан. Рассмотрены ключевые направления использования интеллектуальных технологий в судебной, следственной, прокурорской и экспертной практике, выявлены актуальные проблемы регулирования, риски и условия, влияющие на эффективность и законность внедрения ИИ в сферу обеспечения правопорядка.

Издание предназначено для сотрудников правоохранительных и государственных органов, научных и педагогических работников, обучающихся юридических и управленческих специальностей, а также для широкого круга читателей, интересующихся вопросами цифровизации, права и безопасности.

УДК 343.9:004.8
ББК 67.7:32.813

Рекомендовано к публикации Ученым советом
Академии правоохранительных органов при Генеральной прокуратуре
Республики Казахстан (протокол № 5 от 24 декабря 2025 г.).

ISBN 978-601-82428-2-3

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

в т.ч.	- в том числе
г.	- год
ЕС	- Европейский союз
ИИ	- Искусственный интеллект
КНР	- Китайская Народная Республика
МИИЦР РК РК	- Министерство искусственного интеллекта и цифрового развития Республики Казахстан
ООН	- Организация Объединенных Наций
ОЭСР	- Организация экономического сотрудничества и развития
РК	- Республика Казахстан
РФ	- Российская Федерация
ст.	- статья
США	- Соединенные Штаты Америки
т.е.	- то есть
т.к.	- так как
ФБР США	- Федеральное бюро расследований Соединенных Штатов Америки
УК РК	- Уголовный кодекс Республики Казахстан
УПК РК	- Уголовно-процессуальный кодекс Республики Казахстан

ВВЕДЕНИЕ

Монография предлагает концептуальный анализ правовых и организационных оснований применения искусственного интеллекта в правоохранительной деятельности.

Технологии искусственного интеллекта (ИИ) становятся важным элементом трансформации государственного управления, включая сферу обеспечения общественного порядка. Внедрение интеллектуальных цифровых решений в практику правоохранительных органов открывает новые возможности для оперативного анализа, обработки больших данных, распознавания лиц и предиктивной оценки угроз. Вместе с тем активное использование ИИ в деятельности, напрямую затрагивающей права и свободы граждан, требует осмысления с точки зрения правового регулирования и тактического применения.

Глава государства Касым-Жомарт Токаев на протяжении последних лет неоднократно подчеркивал важность технологий ИИ и их применения для экономического роста страны, а вершиной уделяемого Главой государства внимания данной теме стало Послание народу Казахстана от 8 сентября 2025 года. Как отметил Глава государства: «Стремительное развитие искусственного интеллекта уже влияет на мировоззрение и поведение людей, особенно молодежи. Иной альтернативы нет, поскольку данный процесс кардинально меняет миропорядок и образ жизни всего человечества. Мы должны быть готовы к этому. Нужно действовать решительно, промедление чревато самыми тяжелыми последствиями. Поэтому мною поставлена стратегическая по своей важности задача превращения Казахстана в течение трех лет в полноценную цифровую страну» [1].

Поддержка на высшем государственном уровне указывает на приоритетность создания правовой и институциональной базы, способной обеспечить безопасное и этически выверенное применение ИИ, в том числе в правоохранительном блоке.

В соответствии с указом Главы государства от 17 сентября 2025 года было создано Министерство ИИ и цифрового развития Республики Казахстан, которое возглавляет министр в статусе заместителя Премьер-министра [2], [3].

Первым государством, в состав Кабинета министров которого вошел министр на основе ИИ, контролирующий сферу государственных закупок, стала Албания [4].

С июля 2025 года Министерство внутренних дел Республики Казахстан реализует в городе Косшы Акмолинской области пилотный проект «Помощник следователя» на базе ИИ [5].

В отчете Департамента юстиции США ставится вопрос, что для построения устойчивой и целостной системы управления ИИ органам уголовной юстиции следует четко определить решаемую задачу и обосновать, почему применение ИИ предпочтительнее иных инструментов [6].

Консалтинговая компания McKinsey провела исследование экономического влияния ИИ [7]. Исследовано несколько интеллектуальных

систем: ИИ для наблюдения, понимания и автоматизации, когнитивные технологии и технологии автоматизации, а также ИИ для более умного и автоматизированного будущего. Прогнозируется, что к 2030 году ожидается широкое внедрение ИИ (70% компаний используют по крайней мере один тип технологий), полное использование всех категорий может оказаться сложной задачей. В отличие от других технологий, интеграция ИИ может происходить более быстрыми темпами, но полное внедрение остается под вопросом.

По состоянию на декабрь 2025 года во многих странах по-прежнему отсутствует комплексное национальное регулирование ИИ, особенно применительно к правоохранительной деятельности, однако ожидается новая волна специальных актов и стандартов. В Европейском союзе действует Регламент об искусственном интеллекте с прямыми запретами и особыми правилами для правоохранительной сферы, в Китае введены обязательные меры по обозначению синтетического контента, которые закрепляют прозрачность результатов и обязанности платформ. В Республике Казахстан разработан специальный закон об ИИ, который подписан Главой государства 17 ноября 2025 года, однако он также не содержит прямые нормы в отношении правоохранительной деятельности.

На практике страны комбинируют общие нормы о данных и процессе с секторальными ограничениями и процедурами транспарентности для алгоритмических систем.

Степень научной разработанности обозначенных проблем в юридической науке на современном этапе развития национального законодательства остаётся недостаточной и требует углублённого теоретико-прикладного осмысления.

Стремительное развитие технологий и рост их применения в различных сферах обусловили активизацию научных исследований, посвящённых вопросам правового статуса систем ИИ, распределения ответственности за причинённый ими ущерб, обеспечения прозрачности и контроля алгоритмических решений. В зарубежной правовой литературе на протяжении последних десятилетий постепенно формируется особая предметная область – так называемое «робоправо» (robot law), ориентированное на выработку комплексных правовых механизмов регулирования отношений, возникающих в процессе создания и применения интеллектуальных систем, что отражает необходимость переосмысления традиционных юридических категорий в условиях цифровой трансформации общества.

В частности, вопросы юридических проблем, связанных с функционирование систем на основе ИИ и робототехники, исследованы в трудах таких ученых, как: W. Hoffmann-Riem, U. Pagallo, T. Wischmeyer, А.Г. Волеводз, В.А. Шестак.

Этические аспекты и вопросы защиты прав человека при применении искусственного интеллекта и робототехники в своих работах осветили G. Halevi, N. Marsch, C. Rudin, К.А. Амиянц, Д.В. Воронков. Правовые и этические механизмы минимизации рисков при применении искусственного

интеллекта затронули такие ученые, как: J. Bryson, C. Ernst, N. Rebe, T. Wischmeyer.

Следует отметить, что в Республике Казахстан научные публикации по указанным вопросам единичны и освещены в работах: С.А. Адилова, Е.Н. Бегалиева, М. Жаркынбекова, О. Кирилюка, Н.В. Сидоровой, М.К. Сулейменова, Ж.У. Тлембаевой, С.Ф. Ударцева, Е.П. Шульгина.

Вопросам информационной подготовки сотрудников отечественных и зарубежных правоохранительных органов, в том числе в Академии Федерального бюро расследований Соединенных Штатов Америки, а также совершенствования информационно-технического обеспечения судебно-экспертной деятельности посвящены работы К.К. Сейтенова.

Вместе с тем вопросы внедрения искусственного интеллекта в правоохранительную деятельность представляются не достаточно изученными, что обуславливает актуальность комплексного исследования данного направления. Названной тематике посвящены работы таких ученых, как: S. Raaijmakers, T. Rademacher, В.Б. Батоева, Д.В. Воронков, А.А. Бессонов, Ю.А. Евстратова, Степаненко Д.А.

Весьма обширное исследование на тему возможности внедрения иностранного опыта применения искусственного интеллекта в правоохранительную систему США, в том числе с использованием кейс-стади примера Эмирата Дубай, провела Ana Z. Lalley.

Следует отметить также, что организационно-тактические аспекты функционирования искусственного интеллекта в правоохранительных органах неразрывно связаны с личностью сотрудника правоохранительного органа. Вопросам анализа нравственно-психологических качеств личности прокурора посвящены работы А.А. Тынышбаевой.

Несмотря на то, что тема ИИ в правоохранительной деятельности была предметом исследования, говорить о том, что в настоящее время вопросы организации и тактики функционирования искусственного интеллекта в правоохранительной сфере охвачены в полной мере, пока не приходится. Исходя из вышеизложенного, тема монографии носит актуальный и своевременный характер.

Нормативной базой монографии являются Конституция Республики Казахстан, законы Республики Казахстан «О правоохранительной службе», «Об оперативно-розыскной деятельности», «О персональных данных и их защите», «О цифровизации», а также иные нормативные правовые акты, регулирующие использование информационных технологий в государственном управлении и правоохранительной системе. Также использованы стратегические и программные документы, направленные на развитие цифрового государства, в том числе в сфере искусственного интеллекта. В рамках сравнительно-правового анализа исследованы международные документы, а также нормативные подходы к регулированию ИИ, реализуемые в странах Европейского союза, США, Китая, Сингапура и других государствах.

Методологической и теоретической основой монографии послужили современные достижения теории государства и права, административного и информационного права, а также труды отечественных и зарубежных ученых в области цифровизации государственного управления, правового регулирования информационных технологий и искусственного интеллекта.

В процессе исследования использовались общенаучные методы – анализ, синтез, индукция, дедукция, обобщение и системный подход, а также частнонаучные методы, включая сравнительно-правовой анализ, формально-юридический и функциональный подходы. Использование комплексного метода позволило всесторонне раскрыть правовую и организационно-тактическую специфику применения ИИ в сфере обеспечения правопорядка и сформировать теоретически обоснованные предложения по совершенствованию правового регулирования в данной области.

Теоретическую основу исследования составили казахстанские и зарубежные научные труды (статьи, монографии, комментарии, диссертации и учебные пособия) в сфере искусственного интеллекта.

Эмпирическую базу монографии составили официальные документы и материалы правоохранительных органов Республики Казахстан, аналитические отчёты государственных и международных организаций по вопросам цифровизации и использования искусственного интеллекта, статистические данные, сведения из открытых информационных ресурсов, а также конкретные примеры применения ИИ-технологий в сфере обеспечения правопорядка. Кроме того, использовались материалы зарубежной практики, включая регуляторные подходы стран Европейского союза, США, Китая, Сингапура и России в области правового сопровождения искусственного интеллекта, а также данные социологического опроса сотрудников правоохранительных органов по вопросам функционирования ИИ.

1 КОНЦЕПТУАЛЬНО-ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

1.1 Философско-правовое осмысление феномена искусственного интеллекта

В последние годы наблюдается значительный рост интереса к технологиям ИИ, что обусловлено рядом факторов, включая качественное развитие алгоритмов машинного обучения, рост доступных вычислительных ресурсов, а также активную интеграцию интеллектуальных решений в различные сферы деятельности. Существенную роль в этом процессе сыграли экономические стимулы, в частности, высокая эффективность применения ИИ. Стратегическая поддержка со стороны частных инвесторов и государственных органов также способствовала его повсеместному распространению. На сегодняшний день ИИ закрепился в качестве одного из основных драйверов цифровых и управленческих трансформаций.

В рамках настоящего исследования подчёркивается важность сущностного понимания понятия «ИИ», которое представляется значимым в четырёх ключевых направлениях (таблица 1).

Таблица 1 – Четыре вектора важности определения понятия «ИИ»

Организация и координация научно-исследовательской деятельности	Согласование терминологии и процедур взаимодействия различных субъектов	Интеграция подходов и методов смежных научных дисциплин	Нормативное осмысление моральных, правовых и управленческих последствий
Определение ориентиров исследовательской деятельности предполагает постановку конкретных задач, установление методологических рамок и предметных границ. Иначе говоря, это обеспечивает ясное представление для научного сообщества о том, какие характеристики следует относить к	Четкое понятийное оформление ИИ способствует распространению достоверной информации о его функциональных возможностях и предельных ограничениях как среди профессионального сообщества, так и в обществе в целом. Осознанное восприятие технологии формирует обоснованные ожидания, позволяет трезво оценивать как потенциал, так и возможные угрозы,	Технологии ИИ развиваются на стыке различных научных направлений, включая вычислительные науки, когнитивистику, теорию коммуникации и нейронауку. Формирование согласованного понятийного аппарата создаёт основу для унифицированного подхода к его применению в смежных	Разработка нормативно-этических принципов и регуляторных политик невозможна без концептуально выверенного определения ИИ. Именно через категориальную определённость становится возможным содержательно обсуждать влияние интеллектуальных технологий на ключевые сферы общественной жизни – от защиты персональных данных и обеспечения

явлению ИИ, а какие выходят за пределы данной категории	сопряжённые с её внедрением	дисциплинах, способствуя углублению межотраслевого сотрудничества и реализации комплексных исследовательских и прикладных проектов	цифровой безопасности до вопросов занятости, социальной справедливости и технологической ответственности

Как отмечает судья Арбитражного суда Московской области П.М. Морхат, универсализация понятийной базы в сфере ИИ представляется затруднительной задачей, поскольку содержание термина напрямую зависит от конкретной сферы его применения [8]. Аналогичную позицию занимает и Ж.У. Тлембаева, подчёркивая контекстуальную обусловленность трактовки ИИ в правовой плоскости [9].

Как отмечают Д. Кастро и Д. Нью, вариативность определений ИИ в значительной степени связана с различием между концепцией так называемого слабого (узкоспециализированного) ИИ и сильного (универсального, общего) ИИ [10]. В рамках настоящего исследования предметом анализа выступает именно слабая форма ИИ, обладающая способностью решать ограниченный набор задач в строго определённой предметной области. В противоположность этому, сильный ИИ предполагает наличие универсальных когнитивных способностей, позволяющих адаптироваться к решению практически любых интеллектуальных задач, зачастую с превышением человеческих возможностей. Несмотря на то, что Илон Маск предсказывает реализацию такого ИИ уже в 2025-2026 годах [11], эта точка зрения вызывает определённую критику и скептицизм среди специалистов [12].

Проведённый анализ различных трактовок понятия ИИ позволяет выделить их условное деление на две группы: определения, основанные на родовом (системном) признаке, и подходы, акцентирующие внимание на функциональных характеристиках.

В рамках первого подхода ИИ описывается как разновидность интеллектуальной деятельности в широком смысле, при этом подчёркиваются его отличия от человеческого мышления, связанные с искусственной природой, отсутствием самосознания, неспособностью к эмоциональному восприятию, а также ограниченной универсальностью и адаптивностью.

К определениям данного типа относится, в частности, формулировка, предложенная Джоном Маккарти – исследователем, которому приписывается авторство самого термина «ИИ». Он характеризует ИИ как область науки и техники, направленную на создание интеллектуальных машин, в частности программ, обладающих способностью к разумному поведению. При этом подчёркивается, что ИИ изучает и моделирует человеческий интеллект, но не

обязательно следует исключительно тем механизмам, которые воспроизводимы или наблюдаемы в рамках биологических процессов [13].

В контексте функционального подхода к определению ИИ акцент смещается на способности системы к выполнению задач, которые традиционно ассоциируются с проявлениями человеческого интеллекта. Так, Рэй Курцвейл рассматривает ИИ как искусство конструирования машин, способных осуществлять действия, требующие интеллектуальных усилий со стороны человека, если бы эти действия выполнялись им самим [14]. Сходную позицию занимают Элейн Рич и Кевин Кнайт, подчёркивая, что ИИ представляет собой научное направление, направленное на обучение машин выполнению задач, в которых пока что преимущество остаётся за человеком [15].

Интересную концептуализацию предлагает болгарский исследователь Д. Добрев, подчеркивая моделируемую и средозависимую природу ИИ [16]. Его определение строится на трёх предпосылках: во-первых, интеллектуальная система может быть реализована в виде программы, эмулирующей вычислительное устройство; во-вторых, ИИ функционирует в дискретной (пошаговой) логике восприятия и реагирования; в-третьих, данная система включена в окружающую её среду (обозначаемую как «мир»), с которой она взаимодействует, влияя на неё через ввод и вывод информации. Таким образом, в рамках функционального подхода ИИ определяется через его операционную активность, направленную на обработку информации и целенаправленное воздействие на внешние условия.

Обобщая предложенные положения, Д. Добрев формулирует определение ИИ как программы, способной функционировать в произвольной среде с эффективностью, не уступающей человеку. Такое понимание отражает ориентацию на универсальность и автономность интеллектуального поведения, адаптированного к условиям внешнего мира.

Функциональный подход к определению ИИ акцентирует внимание на том, какие задачи способен решать интеллект, реализованный в программной или аппаратной форме, а также на результативности его применения в конкретных контекстах. Ключевым в этом случае становится не столько внутреннее устройство системы, сколько её практическая эффективность, целевая направленность и полезность в различных сферах деятельности. Такой подход подчёркивает прикладную сущность ИИ как инструмента, ориентированного на выполнение интеллектуально сложных операций.

Одним из ярких представителей этого направления является Ричард Беллман – исследователь, внёсший значительный вклад в разработку методов принятия решений в ИИ. Он определяет ИИ через способность автоматизировать действия, которые в человеческом контексте связываются с проявлением мыслительной деятельности, включая процессы обучения, логического вывода и решения задач [17].

В фундаментальной работе П. Норвига и С. Рассела, признанной одним из наиболее авторитетных источников в области ИИ, приводится классификация подходов к определению ИИ, сгруппированная по четырём

направлениям [18]. Эта типология охватывает как характеристики мышления, так и критерии поведения, а также различает ориентиры на человеческое подобие и рациональность.

Первая группа – это определения, основанные на идее человекоподобного мышления. В данном контексте ИИ рассматривается как система, стремящаяся к воспроизведению когнитивных функций человека, таких как рассуждение, обучение и способность к решению проблем. Ключевым критерием здесь выступает подобие процессов мышления, а не только результат. Примером может служить формулировка: «ИИ занимается созданием систем, которые мыслят подобно человеку».

Вторая группа фокусируется на рациональном мышлении. Здесь акцент сделан на применении формальной логики и выводов, направленных на достижение обоснованных и логически последовательных решений. В рамках этой группы ИИ определяется как интеллектуальный агент, принимающий решения на основе логических построений, вне зависимости от их сходства с человеческим мышлением.

Третье направление охватывает человекоподобное поведение. ИИ, согласно этому подходу, должен демонстрировать действия, схожие с теми, что характерны для человека. Основное внимание здесь уделяется не внутренним процессам, а способу внешнего проявления – насколько система ведёт себя как человек в типовых задачах. Типичная формулировка звучит так: «ИИ разрабатывает программы, способные выполнять задачи, с которыми сегодня лучше всего справляется человек».

Четвёртая группа объединяет определения, ориентированные на рациональное поведение. В этом случае ИИ рассматривается как система, способная предпринимать наилучшие возможные действия в заданных условиях, руководствуясь принципами максимизации целевых показателей или полезности. То, насколько поведение системы имитирует человеческое, отходит на второй план – основным критерием оценки становится её эффективность.

Авторы подчёркивают, что первые две группы акцентируют внимание на внутренних когнитивных процессах, в то время как третья и четвёртая – на результирующем поведении. Кроме того, подходы, основанные на человекоподобии, оценивают ИИ через призму имитации человеческой деятельности, тогда как рационалистские трактовки опираются на понятие идеальной рациональности, согласно которому интеллектуальная система должна действовать оптимально, исходя из доступной информации и заданных целей.

В рамках функционального подхода также заслуживают внимания определения, ориентированные на конкретные способности и операционные характеристики ИИ. Так, Д. Кастро и Д. Нью предлагают описывать ИИ через совокупность выполняемых им функций, включая обучение, понимание информации, необходимое для решения узкоспециализированных задач, логическое рассуждение и способность к взаимодействию с внешней средой [10, p. 32-34].

Аналогичную позицию развивает и судья Арбитражного суда Московской области П.М. Мохат, который в качестве определяющих характеристик ИИ выделяет такие свойства, как способность к обучению и самообучению, пониманию, рефлексивному анализу, выстраиванию логических рассуждений, а также внутреннему самоконтролю [8, с. 25-31]. Подобные трактовки подчёркивают ориентацию на автономную интеллектуальную активность системы, обеспечивающую адаптивность и гибкость в разнообразных условиях применения.

Интересную трактовку современного состояния ИИ предлагает Д. Воронков (Бахтеев), указывая, что наличие программной или программно-аппаратной основы – необходимое, но не достаточное условие для признания системы интеллектуальной. Он подчёркивает, что центральным компонентом, компенсирующим отсутствие сознания (в понимании, раскрытом в экспериментах Дж. Сёрла и Г. Лейбница), выступает способность к обучению и накоплению опыта. По его мнению, даже механическое следование инструкциям оставляет в системе следы, формирующие базу для последующего опыта, что сближает такие процессы с элементами обучения [19].

Следует оговориться, что в рамках настоящей монографии не ставится задача охватить весь спектр научных взглядов, представленных в современной литературе. Вместе с тем предпринята попытка провести классификацию существующих определений и обобщить ключевые теоретические подходы, отражающие текущее состояние научной дискуссии относительно сущности и признаков ИИ.

Полагаем, что достоинством определения ИИ с точки зрения его родового признака является его концентрация на дифференциации от интеллекта в общем и от человеческого – в частности. В этом свете можно рассматривать интеллект как базис, а искусственный интеллект – как надстройку. При этом, если брать за начальную точку отсчета интеллект, то по отношению к ИИ он будет родовым признаком, а ИИ будет его видовым проявлением. В системе координат, где за точку отсчета принимается ИИ, он является родовым признаком, его видовыми признаками можно считать конкретные реализации и направления развития (по уровню развития, методам реализации, области применения, способу обучения).

В своей диссертационной работе, посвящённой философским основаниям онтологии, Д. Родзинский обращается к категориям пустоты, простоты, покоя и бесконечности, рассматривая их как ключевые параметры небытия [20]. Согласно его интерпретации, небытие может быть охарактеризовано как абсолютно пустое по содержанию, простое по своей форме, пребывающее в состоянии покоя и не имеющее ограничений по размеру, то есть бесконечное. В этом контексте небытийная составляющая человеческой природы приобретает чёткие рациональные свойства, которые, по мнению автора, выполняют роль субстанциальной основы для всех переживаний, связанных с бытием.

Авторское осмысление бытия, представленное Д. Родзинским, опирается на структурные характеристики, противоположные свойствам небытия. Так, содержательно бытие определяется через различные уровни полноты, по форме – через усложнённость, в состоянии – через движение, а в пространственном измерении – через ограниченность. Эти параметры, согласно Д. Родзинскому, отражают рационализированную основу бытийственного существования человека, наполняя его жизненные переживания конкретным содержанием и философской артикуляцией [21].

С опорой на данную философскую конструкцию становится возможным интерпретировать методологические ограничения определения ИИ по родовому признаку. В этом контексте родовая характеристика может быть соотнесена с категорией простоты, отражающей исходную, неразвернутую сущность, тогда как функциональный признак выступает как выражение полноты, многомерности и прикладной конкретизации. Такое противопоставление позволяет взглянуть на определение ИИ сквозь призму закона единства и борьбы противоположностей, где взаимодействие абстрактной сущности и практической реализации обретает структуру философского синтеза.

Как подчёркивает сам Д. Родзинский, именно в этой диалектической связке проявляется логика рационального мышления, противоположная «простоте разума во сне без сновидений», и именно она даёт основание для появления третичного кода культуры – логико-структурной схемы, являющейся продуктом рассудочной деятельности и условием развития научного знания [21, с. 90-102].

В контексте философской интерпретации понятий, разработанной Д. Родзинским, родовой и функциональный признаки ИИ могут быть осмыслены как диалектически взаимосвязанные категории. Так, «пустота» как родовой признак символизирует базисную способность интеллектуальной системы – потенциальность к восприятию, анализу и интерпретации информации, выраженную в абстрактной и обобщённой форме. Это – структурный фундамент, на котором покоится вся система ИИ, своего рода «чистая форма разума», ещё не облечённая в конкретные функции.

Напротив, «полнота» как функциональный признак репрезентирует динамическое проявление этой способности – реализацию мыслительной деятельности в форме алгоритмов, логических структур и механизмов, направленных на выполнение конкретных задач. Именно через функциональные признаки интеллект приобретает содержательную определённость: способность к обучению, принятию решений, адаптации и взаимодействию со средой. Это не просто операционализация интеллекта, а его трансформация из потенциального в актуальное.

Функциональные признаки ИИ, таким образом, представляют собой его логику в действии – то, каким образом реализуется заложенная в родовом признаке способность к рациональному мышлению. Они не отрицают «простоту» как основу, но усложняют её, придавая ей содержательное наполнение. Родовой признак (простота) и функциональные признаки

(сложность) не противопоставлены, а находятся в состоянии взаимного напряжения и дополнения, реализуя диалектический принцип единства и борьбы противоположностей.

Следовательно, подход к определению ИИ, ограничивающийся исключительно одной из этих составляющих – либо абстрактной природой интеллекта, либо его функциональной результативностью, – оказывается неполным и односторонним. Полноценное понятийное осмысление ИИ возможно лишь при признании и концептуальном соединении обеих сторон – сущностной и операциональной, абстрактной и прикладной, «пустоты» и «полноты» в их неразрывном взаимодействии.

Исходя из вышеизложенного, представляется обоснованным вывод о том, что наиболее содержательным и концептуально целостным является такое определение ИИ, которое интегрирует в себе как родовой, так и функциональный признак. Универсальность и абстрактность родовой характеристики – той самой «простоты», связанной с интеллектуальной природой – создаёт основание для построения гибких, масштабируемых и технологически устойчивых моделей. В то же время функциональные признаки, воплощающие конкретные алгоритмы, процессы и механизмы взаимодействия с внешней средой, придают системе адаптивность, прикладную направленность и целевую эффективность.

Родовая простота обеспечивает системную стабильность и воспроизводимость, а функциональная сложность – вариативность, контекстуальную чувствительность и способность к саморазвитию. Их взаимосвязь формирует целостную архитектуру интеллектуальной системы, способную не только реагировать на внешние вызовы, но и осваивать новые задачи различного уровня сложности. В этом взаимодействии абстрактного и конкретного, устойчивого и изменчивого находит выражение не только философская диалектика, но и практическая сущность ИИ как явления, сочетающего в себе фундаментальную структуру и динамическую функциональность.

С целью формулирования интегрального и концептуально выверенного определения ИИ, свободного от односторонности ранее рассмотренных подходов и соответствующего принципу диалектического взаимодействия противоположностей, целесообразно обратиться к ряду свойств, определяющих сущностную природу ИИ.

В данном контексте предлагается опираться на четыре ключевые характеристики, которые, по мнению автора, составляют основание для комплексного понятийного осмысления ИИ. Следует подчеркнуть, что отбор данных свойств носит авторский характер и представляет собой попытку теоретического моделирования, а не претендует на исчерпывающее перечисление всех возможных признаков. Однако именно они, по нашему мнению, наилучшим образом отражают как родовую, так и функциональную структуру ИИ, позволяя конструировать определение, отражающее многогранность этого феномена.

Определены следующие основные свойства ИИ, которые мы условно разделяем на четыре группы:

1) объективные свойства;
2) функциональные свойства;
3) инструментальные свойства;
4) самореферентные свойства.

Остановимся подробнее на каждом из них.

Первым из выделенных свойств, лежащих в основе понятийного определения ИИ, является его *объективная характеристика*, связанная с формой реализации. Под этим свойством понимается внешняя, материально- или техноконструктивно-определённая оболочка, в которой интеллектуальная система получает фактическое воплощение. В большинстве рассматриваемых определений акцент делается на таких формах, как «интеллектуальные машины» или «автономные устройства» [13], [14], включая роботов, автоматизированные транспортные средства, промышленные комплексы и прочие физически осязаемые конструкции.

Однако, как показывает современная практика разработки и внедрения ИИ, на текущем этапе его реализация осуществляется в различных формах в программной, аппаратно-программной, сетевой, гибридной формах, способных выполнять интеллектуально насыщенные задачи в определённой предметной области [22], [23]. При технологически нейтральном подходе ИИ предстает как «техническая система» с присущей ей способностью к рациональной обработке данных и моделированию когнитивных функций, причем форма реализации значения не имеет. Таким образом, его объективное свойство может быть рассмотрено как способ присутствия в искусственно созданной материальной или цифровой среде, где ИИ выполняет роль посредника между человеческим мышлением и технологическим миром и формирует новый формат их взаимодействия.

Функциональные свойства ИИ отражают его прикладную сущность и выражаются в способности решать интеллектуальные задачи различной сложности, направленные на обработку, анализ и интерпретацию информации в условиях ограниченности ресурсов и/или неопределённости. Эти свойства проявляются через применение широкого спектра методов – от алгоритмов машинного и глубокого обучения до адаптивной оптимизации и эвристического поиска решений.

ИИ, как правило, используется для повышения эффективности процессов принятия решений, автоматизации рутинных операций и выявления скрытых закономерностей в больших массивах данных. Одним из ключевых функциональных аспектов является способность ИИ к рационализации процесса решения задач, предполагающего оптимальное распределение ограниченных ресурсов – временных, вычислительных, человеческих и иных. Кроме того, ИИ активно применяется в ситуациях, характеризующихся высокой степенью неопределённости, выступая в роли инструмента поддержки решений и снижая вероятность ошибок за счёт статистической оценки рисков и прогнозирования сценариев.

Таким образом, функциональные свойства характеризуют ИИ не только как инструмент технической автоматизации, но и как механизм интеллектуальной поддержки и усиления когнитивных возможностей человека.

Инструментальные свойства ИИ отражают его техническую природу как системы, функционирующей на основе формализованных методов логического вывода, вычислений и структурированных процедур обработки информации. Основанием для принятия решений в таких системах служат математические модели и алгоритмы, которые выступают в роли инструментария, позволяющего систематизировать, упрощать и интерпретировать сложные, многомерные и подчас неопределённые ситуации.

Благодаря встроенной алгоритмической логике, ИИ способен обеспечивать последовательность действий, адаптацию под входные параметры и целенаправленную обработку данных. Такой подход особенно востребован при анализе больших объёмов информации и в условиях дефицита времени на принятие решений. Однако при всей кажущейся объективности формализованной рациональности она не лишена уязвимостей – в частности, риска воспроизводства алгоритмической предвзятости, обусловленной особенностями обучающих данных, архитектурой моделей или допущениями разработчиков.

В связи с этим инструментальный характер ИИ требует постоянного человеческого участия и экспертного контроля, особенно в контекстах, связанных с правом, безопасностью, этикой или потенциальным воздействием на права человека. Человек в данном случае выполняет функцию критического фильтра, способного интерпретировать результаты, проверять обоснованность выводов и принимать окончательные решения в случаях, выходящих за пределы алгоритмической интерпретации.

Самореферентные свойства ИИ представляют собой наиболее сложный и концептуально нагруженный аспект его онтологии, связанный с вопросами субъективности, рефлексии и способности к внутренней самонастройке. В этой связи уместно обратиться к знаменитому тезису Р. Декарта – «Cogito, ergo sum» («Я мыслю, следовательно, существую»), который служит эпистемологическим основанием для различения субъекта и объекта и, если рассматривать шире – для постановки проблемы сознания как такового [24]. На современном этапе исследовательской дискуссии встаёт вопрос: может ли интеллектуальная система, функционирующая в цифровой среде, обладать хотя бы формализованной формой самосознания или когнитивной рефлексии, сравнимой с человеческой?

В рамках данной работы под самореферентными характеристиками ИИ понимаются его способности к обучению, анализу, интерпретации информации и самообновлению на основе внутренних механизмов адаптации. Выделяются следующие его признаки:

- обучаемость – способность ИИ к обучению под контролем внешнего субъекта (человека) или на основе заранее подготовленных датасетов. Это

обеспечивает первичную интеллектуализацию системы и возможность функционирования в заданной предметной области;

- самообучение – способность к автономному усовершенствованию собственных алгоритмов без внешнего управления и предопределённого массива данных. Данный признак отвечает за глубинную адаптивность и формирует предпосылки для эволюционного развития ИИ;

- интерпретация данных – интеллектуальная переработка информации с целью извлечения смыслов, закономерностей и структурных связей. Как подчёркивает Д. Воронков (Бахтеев), это не просто технический анализ, а своего рода «вовлечённое мышление», лежащее в основе проектирования интеллектуальных систем [19, с. 4-448];

- самоанализ и коррекция действий – способность ИИ не только фиксировать результаты своей деятельности, но и формировать оценочные механизмы, позволяющие вносить изменения в поведение и логику функционирования на основании прошлого опыта или внешней обратной связи.

Совокупность указанных признаков формирует основу для концептуального осмысления ИИ как самообучающейся и частично рефлексивной системы, обладающей способностью к формированию автономных стратегий поведения. Хотя в настоящий момент затруднительно говорить о наличии полноценного универсального определения ИИ, в рамках данной работы, не претендуя на всеобъемлющую универсальность, представляется возможным предложить определение, базирующееся на вышеописанных четырёх свойствах: объективном, функциональном, инструментальном и самореферентном.

Определение ИИ, основанное на его существенных свойствах, может быть сформулировано следующим образом: «ИИ – это техническая система, которая использует математические алгоритмы для решения познавательных задач, позволяя ей обучаться, принимать решения и взаимодействовать. Это позволяет ИИ эффективно анализировать данные, адаптироваться к изменяющимся условиям и выполнять задачи, требующие интеллектуальной деятельности».

Проведённый анализ позволил обосновать необходимость комплексного подхода к понятию искусственного интеллекта, в основе которого лежит соотнесение родовых и функциональных признаков. Родовой уровень отражает интеллектуальную природу ИИ как специфического феномена, отличного от человеческого сознания, но обладающего логической структурой и способностью к обработке информации. Функциональные признаки, в свою очередь, позволяют оценить ИИ через призму его прикладной результативности, то есть способности решать задачи, требующие интеллектуального участия. Такой подход обеспечивает методологическую гибкость и теоретическую полноту в описании природы ИИ.

В рамках данного подраздела автором предложена оригинальная концепция, основанная на диалектическом соотнесении категорий простоты и полноты, отражающих родовую и функциональную структуру ИИ

соответственно. Это позволило не только обобщить существующие научные подходы, но и сформулировать определение, раскрывающее ИИ как целостную систему, сочетающую в себе потенциал к восприятию и активную направленность на выполнение познавательных задач. При этом акцентировано, что анализ проведён без привязки к конкретной сфере применения – что создаёт теоретическую основу для дальнейшего исследования особенностей ИИ в контексте правоохранительной деятельности, которым посвящены следующие разделы монографии.

1.2 Задачи применения искусственного интеллекта в правоохранительной деятельности

Современные подходы к определению задач правоохранительной системы в условиях правового государства предполагают не только эффективное противодействие преступности, но и строгое соблюдение прав и свобод граждан. Как подчёркивает один из признанных специалистов в области изучения деятельности полиции Д.Х. Бэйли, основополагающими ориентирами для правоохранительных органов в демократическом обществе являются повышение результативности в обеспечении общественной безопасности и неукоснительное следование принципу верховенства закона, основанного на правах человека [25]. Ряд авторов ставит во главу угла защиту прав и свобод человека [26], [27], [28].

Научная точка зрения К.А. Ермолаева дополняет это понимание, акцентируя внимание на ряде конкретных направлений: правомерное и точное исполнение полномочий каждым из задействованных органов; соблюдение объективности и беспристрастности при осуществлении возложенных функций; своевременное обнаружение и пресечение противоправных деяний; установление причастных лиц и обеспечение их привлечения к установленной законом ответственности [29].

Учитывая задачи правоохранительной деятельности, можно дать определение ИИ в правоохранительной деятельности: ИИ в этом контексте означает интеграцию систем на основе ИИ для достижения целей и обязанностей правоохранительных органов по поддержанию общественного порядка и безопасности. Это включает такие направления, как профилактика правонарушений, аналитическое сопровождение расследований, обеспечение справедливости при отправлении правосудия, рационализация управленческих решений и укрепление общественного доверия. Интеграция ИИ в деятельность правоохранительных органов открывает возможности для повышения прозрачности, скорости и точности функционирования системы, при условии соблюдения юридических, этических и процедурных стандартов.

На наш взгляд, применение ИИ в правоохранительной системе должно анализироваться сквозь призму ключевых задач, традиционно возлагаемых на соответствующие органы. Такое структурирование позволяет более точно определить сферы, в которых интеллектуальные технологии могут быть наиболее результативны и допустимы с правовой и этической точек зрения.

В рамках настоящего исследования предлагается рассматривать применение ИИ в контексте выполнения следующих основных задач правоохранительной деятельности:

1) превенция;

2) раскрытие и расследование правонарушений;

3) осуществление правосудия;

4) исполнение судебных решений.

Каждое из указанных направлений обладает собственной спецификой и уровнем допустимого автоматизированного вмешательства. Далее они будут проанализированы более подробно с учётом их содержания, целей и технологических возможностей ИИ.

1. Превенция

Превенция как важнейшее направление в системе обеспечения правопорядка ориентирована на предупреждение противоправного поведения до момента его фактической реализации [30]. В этом контексте ИИ представляет собой не только эффективный инструмент, способствующий выявлению потенциальных угроз, но и платформу, на которой формируется современная модель оперативного реагирования правоохранительных органов. Применение ИИ позволяет перейти от реагирования на уже совершённые правонарушения к их предиктивному предотвращению, используя аналитику больших данных, поведенческие паттерны и автоматическое выявление отклонений от норм.

Т. Сринити и др. в одной из публикаций, посвящённой возможностям ИИ в сфере предупреждения преступности, подчёркивает потенциал ИИ в обработке и интерпретации больших объёмов данных для своевременного выявления рисков противоправной деятельности. Особое внимание в исследовании уделено проблемам алгоритмической предвзятости, а также необходимости разработки механизмов, обеспечивающих прозрачность и справедливость решений, принимаемых на основе ИИ. Авторы акцентируют важность соблюдения этических стандартов при внедрении подобных систем в практику правоохранительных органов, что рассматривается как ключевое условие их надёжного и социально приемлемого функционирования [31].

Согласно исследованию, подготовленному Центром по изучению технологий и безопасности, предотвращение серьёзных онлайн-преступлений требует не только адаптации законодательства, но и проактивного внедрения ИИ в практику правоохранительных органов. В отчёте подчёркивается, что современные угрозы в киберпространстве, включая мошенничество, фишинг, распространение вредоносных программ и создание дипфейков, приобретают новые формы благодаря алгоритмической автоматизации и масштабируемости. Для противодействия этим угрозам авторы рекомендуют создавать специализированные подразделения по борьбе с ИИ-преступностью, расширять технические возможности правоохранительных органов и налаживать международное сотрудничество. Особый акцент делается на необходимости раннего выявления инструментов, используемых преступниками, и построении барьеров для их распространения, включая

мониторинг даркнета, тестирование моделей на устойчивость к злоупотреблениям и развитие практик алгоритмической нейтрализации [32].

Одной из наиболее распространённых сфер превентивного применения ИИ является система интеллектуального видеонаблюдения. Алгоритмы, основанные на машинном обучении, способны анализировать визуальные потоки в режиме реального времени, выявляя признаки аномального поведения: от резких перемещений и агрессивной жестикуляции до потенциально опасных предметов в руках граждан. В метрополитене Лондона такие системы интегрированы в архитектуру городской безопасности: ИИ фиксирует и интерпретирует подозрительные действия пассажиров, включая попытки самоубийств, акты агрессии, либо наличие оружия, и незамедлительно уведомляет оперативные службы [33].

Одним из показательных примеров применения ИИ в целях предотвращения правонарушений является исследование Мартинеса-Маскорро и соавторов, в котором предложена модель на основе трёхмерных сверточных нейронных сетей, способная анализировать видеопотоки для выявления подозрительных поведенческих паттернов, предшествующих совершению краж в торговых точках. Разрабатываемая система фиксирует аномалии в перемещении клиентов – такие как повторяющиеся действия, длительное пребывание у товарных полок или резкие перемещения, – что позволяет персоналу оперативно реагировать на потенциальные угрозы. Данный подход демонстрирует, как ИИ может использоваться в качестве инструмента превентивного реагирования без вторжения в персональные данные [34].

В работе Адитьи и соавторов рассматриваются алгоритмы ИИ и машинного обучения, предназначенные для анализа видеопотоков в реальном времени с целью управления поведением толпы, выявления правонарушений и контроля производственных процессов. Разработанная система позволяет оперативно фиксировать потенциально опасные отклонения в поведении – будь то агрессивные действия, аномальные скопления людей или нарушение маршрутов движения – что даёт возможность предупредить развитие инцидентов ещё на стадии их формирования. Такой подход демонстрирует высокую эффективность ИИ как инструмента превенции в условиях динамично меняющейся среды – как в общественных пространствах, так и на промышленных объектах [35].

В исследовании, представленном компанией IronYun (2022), рассматриваются возможности использования ИИ для повышения эффективности локальных стратегий обеспечения общественной безопасности. Особое внимание уделяется инструментам, основанным на видеоаналитике и распознавании лиц, которые позволяют в реальном времени отслеживать происходящее в общественных пространствах, выявлять подозрительные действия и реагировать до совершения правонарушений. Кроме того, анализ данных социальных сетей и мониторинг ситуаций в режиме 24/7 дают возможность правоохранительным органам оперативно распределять ресурсы и предотвращать инциденты. Публикация

подчёркивает, что ИИ может стать не только технологическим помощником, но и важным компонентом системно ориентированной превентивной политики [36].

Успешный опыт применения ИИ в целях превенции демонстрирует и практика города Сан-Франциско, где внедрены мобильные платформы наблюдения с интеллектуальным ядром. Эти комплексы не только фиксируют происходящее, но и анализируют поведенческие аномалии – резкие групповые перемещения, скопления людей в нетипичных локациях, признаки паники или намерения скрыться. ИИ способен интерпретировать поведенческие сигналы и заранее информировать службы реагирования о возможной эскалации ситуации. Такая интеграция позволила, согласно официальным данным, снизить показатели уличной преступности на 20% в течение первого года после внедрения [37].

Цифровая среда также становится пространством, где ИИ успешно реализует задачи превентивного характера. Так, интеллектуальные системы выявляют признаки мошенничества, вмешательства в личную цифровую сферу, кибербуллинга и иной антиобщественной онлайн-активности. Ярким примером служит инициатива компании Meta, внедрившей ИИ для анализа рекламного контента. Программа фиксирует попытки использования изображений знаменитостей в фальшивых инвестиционных предложениях и, опираясь на алгоритмы распознавания лиц, блокирует подобные объявления ещё до их распространения [38].

Значимым направлением является и применение ИИ в сфере дорожной безопасности. В Казахстане функционирует система Sergek, объединяющая данные с множества источников: от камер видеонаблюдения и светофоров до беспилотных дронов. Интеллектуальные алгоритмы анализируют трафик, прогнозируют пробки, фиксируют нарушения правил дорожного движения и обеспечивают информационную поддержку для принятия решений в условиях чрезвычайных ситуаций. В случае природных или техногенных катастроф система способна формировать оптимальные маршруты эвакуации и координировать действия экстренных служб [39].

А. Ешназаров справедливо подчёркивает, что реализация проектов, направленных на разработку и интеграцию технологий блокчейн и ИИ в деятельность правоохранительных органов, сопряжена с объективной необходимостью привлечения значительных материальных ресурсов, специализированных кадров в области программирования, а также существенных временных затрат.

В целях минимизации указанных вызовов целесообразным видится институционализация партнерских связей между ведомственными образовательными организациями, осуществляющими подготовку кадров для системы правопорядка, и профильными техническими вузами Республики Казахстан, ориентированными на развитие компетенций в сфере информационных технологий, что позволит обеспечить системное повышение квалификационного уровня сотрудников и организацию эффективного обмена профессиональными знаниями [40].

Комплексная реализация предложенных мер может служить катализатором технологической модернизации правоохранительной системы.

Еще одна сфера, где ИИ демонстрирует значимый превентивный потенциал – раннее выявление случаев домашнего насилия. В Германии действует система Lizzy, предназначенная для прогнозирования риска повторных эпизодов. На основании анкетных данных жертв система формирует поведенческие профили и предлагает меры вмешательства до наступления новой угрозы. Эмпирические данные показывают, что в регионах, где система применялась, число повторных случаев сократилось почти на половину [41].

Несмотря на изначально высокий уровень доверия к алгоритмам предиктивного анализа, который активно транслировался в научных и прикладных публикациях 2010-х годов, последующий этап развития показал гораздо более сложную картину. Если в отчёте RAND Corporation подчеркивалась эффективность систем типа PredPol в локализации «горячих точек» и более рациональном распределении патрульных маршрутов, то по мере накопления практического опыта и появления независимых оценок выявились глубокие изъяны в концептуальной основе предиктивной полиции [42].

Современные исследования, включая критические обзоры С. Эгберт и М. Лизе, а также А. Фергюсона, всё чаще демонстрируют, что на практике алгоритмы предсказания преступности далеко не всегда обеспечивают ту результативность, которая заявлялась на этапе их разработки и внедрения [43, 44]. Более того, выяснилось, что эффективность PredPol и LASER в ряде случаев не превышала статистической погрешности: по результатам внутренних проверок, менее 1% прогнозов действительно приводили к выявлению новых правонарушений, а многие участки «высокой криминальной активности» повторялись на протяжении месяцев без изменения условий.

Особую обеспокоенность вызывал тот факт, что алгоритмы основывались на исторически накопленных данных, которые содержали в себе отражение структурного неравенства, расовой дискриминации и дисбаланса в реагировании на преступления в разных районах города. Это порождало «замкнутый круг»: одни и те же кварталы попадали в список патрулирования, тем самым усиливая полицейское присутствие и потенциально провоцируя рост инцидентов с участием правоохранителей, что затем снова фиксировалось системой как «повышенная активность».

В ответ на растущую критику в ряде муниципалитетов США, таких как Санта-Круз, Новый Орлеан и Лос-Анджелес, данные системы были полностью или частично выведены из эксплуатации. Кроме того, на уровне Европейского союза был закреплён частичный запрет на предиктивную аналитику, использующую персональные характеристики граждан, что закреплено в положениях итогового текста Закона ЕС «Об ИИ (AI Act)». Аналитические платформы указывают на системную непрозрачность логики алгоритмов, невозможность независимого аудита и отсутствие механизмов апелляции для

лиц, оказавшихся в зоне интереса алгоритма. Подобные программы, как подчёркивается в научной литературе, создают «технологическую видимость рациональности» – то есть формируют у общества иллюзию объективного, беспристрастного контроля, хотя фактически воспроизводят уже существующие неравенства и уязвимости [45], [46], [47], [48], [49].

В результате накопленного эмпирического опыта произошло значительное переосмысление самой идеи предиктивной полицейской деятельности. Если ранее она воспринималась как нейтральный инструмент превентивного управления, то сегодня она всё чаще рассматривается как источник потенциальных угроз правам человека, особенно в контексте дискриминации, нарушения презумпции невиновности и подрыва общественного доверия. Это требует от разработчиков и правоприменителей не только технической доработки алгоритмов, но и выработки чётких юридических и этических рамок их использования, исключающих произвол и обеспечивающих подотчётность на всех этапах – от программирования до практического внедрения.

Таким образом, практика применения ИИ в рамках превентивной деятельности демонстрирует его многоплановую полезность – от обработки визуальных сигналов и поведенческих аномалий до анализа цифровой активности и координации экстренных служб. ИИ постепенно становится частью инфраструктуры обеспечения общественной безопасности, помогая в оперативной фиксации отклонений, автоматизации наблюдения и формировании алгоритмов раннего реагирования. Его интеграция наблюдается как в сфере офлайн-пространства – городского видеонаблюдения, дорожной аналитики и патрульного мониторинга, так и в цифровом пространстве, включая противодействие киберугрозам и распространению противоправного контента.

Однако растущий интерес к ИИ в превентивных целях сопровождается не только положительными примерами, но и критическими случаями, обнажающими системные риски. Отказ от неэффективных и предвзятых систем, таких как PredPol и LASER, а также введение нормативных ограничений в странах ЕС подтверждают необходимость сдержанного и взвешенного подхода. ИИ может стать не только эффективным помощником, но и фактором неоправданного вмешательства в права граждан, если использовать его вне прозрачных правовых и этических рамок. Проблемы алгоритмической предвзятости, ограниченной верифицируемости решений и усиления социального неравенства требуют особого внимания со стороны разработчиков, правоприменителей и законодателей.

В свете вышеизложенного, дальнейшее использование ИИ в целях превенции должно сопровождаться разработкой комплексной нормативной архитектуры, включающей стандарты прозрачности, механизмы аудита и меры защиты от дискриминационных практик. Только при наличии таких институтов ИИ способен выполнять свою функцию – не как инструмент цифрового надзора, а как современное средство поддержки правопорядка, действующее в интересах общества и в рамках законности.

2. Раскрытие и расследование правонарушений

Одним из ключевых направлений деятельности правоохранительных органов остаётся выявление уголовных правонарушений, установление их характера, масштабов и лиц, причастных к их совершению. Эта задача прочно закреплена в действующем законодательстве, формируя нормативную основу для раскрытия уголовных правонарушений с учётом современных цифровых реалий. Сегодня, в условиях стремительного внедрения технологий ИИ, соответствующая деятельность обретает новые организационно-аналитические формы, интегрирующие традиционные правовые инструменты с алгоритмическими средствами анализа данных.

Согласно положениям Уголовно-процессуального кодекса Республики Казахстан (УПК РК), досудебное расследование направлено на всестороннее установление обстоятельств совершённого преступления, фиксацию доказательств, выявление личности подозреваемого и оценку факторов, повлиявших на правонарушение. В частности, статья 8 УПК РК определяет задачи уголовного процесса: «Задачами уголовного процесса являются пресечение, беспристрастное, быстрое и полное раскрытие, расследование уголовных правонарушений, изобличение и привлечение к уголовной ответственности лиц, их совершивших, справедливое судебное разбирательство и правильное применение уголовного закона, защита лиц, общества и государства от уголовных правонарушений» [50]. В условиях цифровизации эти задачи всё чаще могут быть решены с привлечением ИИ-систем, способных обрабатывать массивы данных о поведении, связях и цифровом следе подозреваемых, тем самым ускоряя раскрытие уголовных правонарушений.

Кроме того, ст. ст. 59-63 УПК РК очерчивают полномочия органов досудебного расследования, к примеру, ч.3 ст.60 УПК: «Следователь обязан принимать все меры к всестороннему, полному и объективному исследованию обстоятельств дела, осуществлять уголовное преследование лица, в отношении которого собраны достаточные доказательства, указывающие на совершение им уголовного правонарушения, путем квалификации деяния подозреваемого, избрания ему в соответствии с настоящим Кодексом меры пресечения, составления отчета о завершении досудебного расследования с изложением обстоятельств уголовного правонарушения, описанием собранных доказательств».

Согласно ч.1 ст.126 УПК РК, «Научно-технические средства в процессе доказывания по уголовному делу могут быть использованы органом, ведущим уголовный процесс, адвокатом, являющимся защитником, представителем потерпевшего, а также экспертом и специалистом при исполнении ими процессуальных обязанностей, предусмотренных настоящим Кодексом» [50].

Кроме того, согласно ч.3 вышеуказанной статьи, «Применение научно-технических средств признается допустимым, если они:

1) прямо предусмотрены законом или не противоречат его нормам и принципам;

2) научно состоятельны;

3) обеспечивают эффективность производства по уголовному делу;

4) безопасны» [50].

В современных условиях эти положения становятся предпосылками для легитимного включения в практику ИИ-инструментов, направленных на интеллектуальную обработку доказательств, моделирование преступных сценариев, а также автоматическое выделение признаков серийности преступлений.

Подпункт 2 п.1 ст. 4 Закона Республики Казахстан «О правоохранительной службе» гласит: «Сотрудники обязаны: обеспечивать соблюдение и защиту прав и свобод человека и гражданина, а также законных интересов физических и юридических лиц, государства» [51]. Сегодня эта функция всё чаще реализуется через внедрение интеллектуальных систем анализа видеонаблюдения, прогнозной аналитики и цифровой криминалистики, которые позволяют не только реагировать на уже совершённое деяние, но и своевременно идентифицировать признаки его подготовки.

Уголовный кодекс Республики Казахстан (УК РК), в свою очередь, в ст. 2 фиксирует охранительную функцию уголовного законодательства: «Задачами настоящего Кодекса являются: защита прав, свобод и законных интересов человека и гражданина, собственности, прав и законных интересов организаций, общественного порядка и безопасности, окружающей среды, конституционного строя и территориальной целостности Республики Казахстан, охраняемых законом интересов общества и государства от общественно опасных посягательств, охрана мира и безопасности человечества, а также предупреждение уголовных правонарушений» [52]. Включение ИИ в сферу раскрытия преступлений требует переосмысления этой нормы с учётом алгоритмической интерпретации фактов, что влечёт необходимость выработки новых подходов к допустимости цифровых доказательств и гарантии прав человека в условиях машинного анализа.

Таким образом, в современных условиях задачи по раскрытию преступлений, установленные национальным законодательством, приобретают новое измерение. Традиционная правовая конструкция дополняется элементами интеллектуальной автоматизации, что требует от правоохранительных органов не только соблюдения законности, но и компетентного взаимодействия с алгоритмическими инструментами, способными усиливать как точность выявления преступлений, так и риск правовых ошибок при их расследовании. В результате раскрытие преступлений становится неотъемлемым компонентом более широкой концепции цифровой уголовной юстиции, где ИИ выступает не заменой, а усилителем аналитического потенциала следствия.

Выявление и расследование уголовных правонарушений представляет собой одну из ключевых функций правоохранительных органов и направлено на обеспечение законности, восстановление нарушенных прав и привлечение виновных к ответственности. На практике этот процесс включает оперативное выявление событий, обладающих признаками противоправности,

систематический сбор доказательной базы, а также комплексный анализ обстоятельств совершения деяния.

Д.В. Бахтеев полагает, что применение ИИ должно сопровождаться процедурной надёжностью: каждый этап анализа должен быть воспроизводим и верифицируем, особенно в части интерпретации цифровых доказательств [53].

Л. Флориди обращает внимание на необходимость этического сопровождения применения интеллектуальных систем, особенно в контексте автономного анализа и использования биометрических данных, что требует учёта принципов неприкосновенности частной жизни и справедливого процесса [54].

Таким образом, исследования последних лет подчёркивают, что эффективное расследование уголовных правонарушений в условиях цифровизации немыслимо без учёта достижений в области ИИ, которые, с одной стороны, открывают новые горизонты для оперативности и точности, а с другой – порождают вызовы, связанные с правовыми и этическими ограничениями, требующими постоянного научного осмысления и нормативной конкретизации.

М. Иннес акцентирует внимание на важности модернизации полицейских подходов с учётом современных технологических условий при неизменном соблюдении ключевых принципов расследования преступлений [55].

Установление и детальное расследование правонарушений остаются базовыми составляющими правоохранительной деятельности. Эта работа включает в себя своевременное выявление противоправных деяний, анализ их признаков и обстоятельств, а также последовательный сбор и интерпретацию доказательств, необходимых для установления истины. Целью является не только фиксация факта нарушения, но и оценка его тяжести, масштабов и последствий в рамках правовой квалификации.

В современных условиях особую роль играет использование ИИ и других высокотехнологичных решений, позволяющих существенно повысить точность, скорость и обоснованность оперативно-следственных мероприятий. Такие технологии применяются при восстановлении хронологии событий, идентификации подозреваемых, анализе цифровых следов, а также в процессах автоматизированной экспертизы. Как правило, успешное расследование требует согласованной работы различных ведомств и специалистов, включая экспертов-криминалистов, судебно-медицинских экспертов и аналитиков данных, что особенно актуально в условиях цифровизации и роста объёмов обрабатываемой информации.

Процесс раскрытия уголовных правонарушений представляет собой первичную стадию реагирования системы правопорядка, в рамках которой осуществляется незамедлительное выявление лиц, предположительно причастных к совершению противоправных деяний, а также реализуются меры, направленные на исключение повторных инцидентов. Эта фаза включает в себя анализ места происшествия, оперативную фиксацию следов

преступления, сбор первичной информации от очевидцев и потерпевших, а также использование технологических решений для идентификации подозреваемых. Особое значение в данной плоскости приобретает применение систем на основе ИИ, способных обрабатывать большие объёмы данных в реальном времени и выявлять корреляции, ускользающие от традиционных методов расследования.

На следующем этапе осуществляется непосредственное расследование, представляющее собой комплексную деятельность, ориентированную на восстановление полной картины произошедшего. В рамках данного этапа формируется доказательная база, выдвигаются и проверяются версии, осуществляется правовая квалификация действий субъектов, а также подготавливаются материалы, служащие основанием для возбуждения уголовного дела и последующего судебного рассмотрения. Расследование предполагает не только глубинный аналитический подход, но и координацию между различными ведомственными структурами, включая органы досудебных расследований, криминалистические подразделения, а также экспертные учреждения. Здесь ИИ также находит широкое применение – от алгоритмической реконструкции событий на основе цифровых следов до интеллектуального анализа содержания документов и аудиовизуальных материалов.

ИИ в правоохранительной практике выполняет одновременно профилактическую и аналитико-выявляющую функцию, демонстрируя свою эффективность как на этапе предупреждения, так и в процессе раскрытия уже совершённых правонарушений. Особенность таких технологий заключается в том, что инструменты, изначально предназначенные для фиксации преступной активности, часто обладают потенциалом раннего реагирования и позволяют предотвратить противоправные действия ещё до их реализации. Таким образом, функциональные границы между превенцией и расследованием в рамках применения ИИ нередко размываются, формируя единую, взаимодополняющую стратегию обеспечения общественной безопасности, основанную на анализе и прогнозировании данных в реальном времени.

Комплексный характер задач, решаемых с использованием ИИ, обусловливает необходимость систематизации его функций на различных этапах правоохранительной деятельности. Многие технологии, задействованные в рамках превенции, одновременно применимы и в процессе расследования, что свидетельствует о высокой степени взаимосвязанности этих направлений. Для наглядного представления таких перекрёстных применений ИИ целесообразно выделить ключевые функции интеллектуальных систем и отразить их роль как в профилактике правонарушений, так и в их последующем раскрытии (таблица 2).

Таблица 2 – Соотношение функций ИИ в сфере превенции и раскрытия правонарушений

Функция ИИ	Функция в превенции	Функция в раскрытии правонарушений
Автоматизированное наблюдение и обнаружение аномалий	Системы видеонаблюдения, использующие алгоритмы ИИ, способны в режиме реального времени фиксировать нетипичную активность, такую как продолжительное пребывание вблизи банкоматов или скопление людей в потенциально уязвимых зонах. Эти сигналы рассматриваются как индикаторы возможной дестабилизации обстановки, что позволяет оперативным службам вмешаться на раннем этапе и предотвратить развитие инцидентов.	Алгоритмы ИИ, применяемые при анализе видеонаблюдения, позволяют автоматически распознавать признаки противоправных действий, включая порчу имущества, хищения и акты физической агрессии. Такая технологическая поддержка существенно ускоряет процесс установления ключевых обстоятельств происшествия и содействует более оперативному раскрытию правонарушений.
Прогнозная аналитика и распознавание моделей преступлений	На основе накопленных статистических и поведенческих данных ИИ-системы способны выявлять территориальные зоны, характеризующиеся повышенным риском правонарушений. Такой аналитический подход позволяет прогнозировать вероятные очаги преступной активности и заблаговременно направлять туда ресурсы правоохранительных органов для предупреждения противоправных деяний.	После фиксации противоправного деяния ИИ может использоваться для ретроспективного анализа аналогичных инцидентов, с целью выявления устойчивых поведенческих паттернов и скрытых взаимосвязей. Это способствует установлению связей между различными эпизодами, включая случаи серийных преступлений, и повышает эффективность следственной работы.
Распознавание лиц и биометрических данных	Системы ИИ, интегрированные в средства наблюдения, позволяют проводить автоматическое распознавание лиц в общественных пространствах с целью идентификации лиц, ранее привлекавшихся к ответственности или находящихся под оперативным наблюдением. Такой механизм способствует раннему выявлению потенциальных угроз и оперативному информированию	Алгоритмы ИИ используются для сопоставления визуальных данных, зафиксированных на месте правонарушения, с имеющимися в распоряжении правоохранительных органов базами изображений и биометрической информации. Такой подход ускоряет процедуру идентификации подозреваемых и способствует оперативному раскрытию преступлений.

	правоохранительных органов до наступления негативных последствий.	
Мониторинг социальных сетей и киберпреступности	Интеллектуальные системы используются для мониторинга цифрового пространства, включая социальные сети, тематические форумы и закрытые каналы коммуникации, с целью выявления индикаторов подготовки противоправных действий. Такие технологии позволяют заблаговременно фиксировать потенциальные угрозы, связанные с кибератаками, деятельностью организованных преступных группировок или признаками экстремистской активности.	В сфере киберпреступности ИИ применяется для анализа цифровых следов, оставленных в результате противоправной деятельности, включая мошеннические транзакции, фишинговые атаки и несанкционированный доступ к персональным данным. Обработка таких цифровых свидетельств позволяет оперативно выявлять лиц, причастных к правонарушениям, и восстанавливать цепочку событий, связанных с их совершением.
ИИ при анализе экстренных вызовов	Системы ИИ, задействованные в анализе обращений в экстренные службы, способны выявлять повторяющиеся паттерны коммуникации – в частности, частые звонки и сообщения, указывающие на возможные случаи домашнего насилия. Такая автоматизированная обработка сигналов тревоги даёт возможность оперативного реагирования со стороны правоохранительных органов ещё на стадии развития угрозы, до её эскалации	При обработке звонков в экстренные службы ИИ способен распознавать не только содержание речи, но и акустические параметры – интонацию, эмоциональные оттенки, а также фоновую аудиосреду. Такая многослойная аналитика позволяет более точно интерпретировать ситуацию, выявлять признаки стресса или угрозы, и при необходимости оперативно инициировать выезд экстренных служб на место предполагаемого происшествия.

Современная парадигма аналитической поддержки деятельности правоохранительных органов всё чаще исходит из необходимости концептуального и институционального оформления обратной связи между стадиями постфактум-анализа и превентивного реагирования. В рамках этой логики цифровые следственные данные, извлекаемые в ходе раскрытия уголовных правонарушений, обретают не только ретроспективную значимость, но и превращаются в предиктивные индикаторы, обуславливающие конфигурацию будущих стратегий безопасности. Так, в исследовании Ф. Экундайо и соавторов подчёркивается, что сочетание методов цифровой криминалистики с алгоритмами машинного обучения позволяет формировать адаптивные модели, интегрирующие выводы из завершённых дел в архитектуру превентивных вмешательств [56].

Аналогично, А. Тамир и соавторы обосновывают применимость прогнозной логики, построенной на постраскрывательских массивах данных, как средства уточнения пространственно-временных параметров будущих правонарушений [57].

Д. Энсин и соавторы в работе о так называемых «самоподкрепляющихся петлях предсказательной полицейской аналитики» акцентируют внимание на том, что необоснованное замыкание потока данных между раскрытием и профилактикой без должной нормативной фильтрации может привести к усилению институциональной предвзятости [58].

Особое значение в поддержании обоснованности подобной обратной связи приобретают теоретические положения криминологического паттернового анализа. Данные, генерируемые на стадии раскрытия преступлений, при должной агрегации и пространственной интерпретации становятся основой картографической репрезентации зон рисков и механизмов их распространения. Такая модель мышления постепенно вытесняет традиционно реактивные подходы к правопорядку, формируя логику предикативной обусловленности управленческих решений [59].

Одним из ключевых направлений прикладного взаимодействия между этапами раскрытия правонарушений и формированием эффективной превентивной политики является аналитическая переработка данных, полученных в ходе криминалистических процедур с участием ИИ. Современные методы цифровой судебной экспертизы, включая автоматизированное сопоставление отпечатков пальцев, биометрический анализ ДНК и баллистическую реконструкцию, позволяют не только идентифицировать субъектов преступной деятельности, но и выявлять устойчивые поведенческие и пространственно-временные закономерности, имеющие прогностическую ценность для будущих стратегий профилактики.

Так, сведения, извлечённые в ходе анализа правонарушений в сфере дорожного движения, подвергнутые интеллектуальной обработке на базе ИИ, дают возможность не только выявить наиболее проблемные участки транспортной инфраструктуры, но и предложить алгоритмически обоснованные варианты их реконфигурации. Это, в свою очередь, способствует снижению вероятности повторных инцидентов путём инженерного воздействия на внешнюю среду и повышения соблюдаемости правил. Подобный подход апробирован в ряде крупных мегаполисов с высокой плотностью трафика и доказал свою результативность в снижении аварийности.

Особый интерес представляет применение ИИ в сфере расследования экономических и финансовых преступлений, где алгоритмические решения позволяют вскрывать латентные схемы мошенничества, включая аномальные транзакции, схемы обналичивания и скрытого перевода активов. Анализ этих данных способствует не только изобличению конкретных лиц, но и модификации нормативно-правовых механизмов регулирования финансовых потоков. Таким образом, информация, полученная в рамках одной функции –

раскрытия, трансформируется в инструмент адаптивного управленческого воздействия в сфере предупреждения.

Например, выявление преступлений с помощью криминалистического анализа с использованием ИИ (сопоставление отпечатков пальцев, распознавание ДНК, баллистический анализ) помогает выявлять тенденции, что приводит к совершенствованию политики предупреждения преступности. Данные о нарушениях правил дорожного движения, обрабатываемые с помощью ИИ, позволяют городам перестраивать дорожную разметку и улучшать соблюдение правил дорожного движения, сокращая количество аварий и нарушений в будущем. Расследование финансовых преступлений с помощью ИИ помогает выявлять новые схемы мошенничества, позволяя государственным и правоохранительным органам применять адаптировать существующие правила для предотвращения подобных случаев.

Конкретные примеры практического использования ИИ в целях раскрытия правонарушений и последующего совершенствования превентивных механизмов демонстрируют трансформацию правоохранительных стратегий от реактивного к проактивному формату. Благодаря способности интеллектуальных систем извлекать закономерности из эмпирически зафиксированных инцидентов, становится возможным выстраивание циклов обратной связи, в рамках которых каждый успешно раскрытый случай подпитывает стратегическое планирование.

Так, в области криминалистики применение ИИ в автоматизированной интерпретации биологических следов уже позволяет детализировать профили подозреваемых без вмешательства эксперта: алгоритмы, базирующиеся на биосенсорах, в ряде случаев способны выявлять пол, возраст, наличие заболеваний, медикаментозную историю, что значительно сокращает временные затраты на идентификацию и усиливает доказательственную основу (см.: 10 Modern Forensic Science Technologies, forensicscolleges.com). Как свидетельствует информация, представленная на официальном ресурсе Федерального бюро расследований США, технология Rapid DNA (или экспресс-генетическая идентификация) представляет собой высокоавтоматизированный протокол молекулярно-генетического анализа, позволяющий в течение 1–2 часов без участия специалиста в лабораторных условиях извлекать и обрабатывать ДНК-профили, полученные, как правило, из биологического материала ротовой полости. В опубликованном FBI руководстве детализируются как технические параметры, так и регуляторные процедуры внедрения данной технологии в рамках функционирования национальной базы CODIS (Combined DNA Index System), включая её сопряжение с механизмами биометрической идентификации, в частности – с дактилоскопической регистрацией.

Дополнительное методологическое обоснование применения технологии Rapid DNA содержится в аналитических материалах Национального института юстиции США (NIJ), где подчёркивается значительный потенциал данной процедуры в контексте оптимизации доказательной базы и существенного сокращения сроков установления

личности фигурантов уголовного судопроизводства. В совокупности это открывает новые горизонты для её использования в рамках следственно-оперативной деятельности, особенно в условиях ограниченного временного ресурса [59];, [60], [61].

В сфере обеспечения безопасности дорожного движения ИИ задействован не только для фиксации нарушений, но и как инструмент обратной инженерии дорожной инфраструктуры. Так, в Филадельфии внедрена система камер с ИИ-модулем, фиксирующим водителей, не останавливающихся перед школьными автобусами с выдвинутыми ограничителями. Собранные данные, кроме штрафных мер, используются для выявления небезопасных участков, требующих дополнительной разметки или контроля [62]. В испанской Барселоне специалисты из Университета Оберта де Каталония разработали алгоритмы прогнозного анализа аварийности, позволяющие муниципалитетам на основании выявленных паттернов внедрять меры инфраструктурного характера и снизить вероятность аварий [63].

Что касается финансовой сферы, здесь ИИ выступает не просто средством детекции, но и аналитической платформой для обновления контрмошеннических протоколов. Так, Банк HSBC в сотрудничестве с Google Cloud внедрил систему обработки более миллиарда транзакций в месяц, с акцентом на снижение ложноположительных инцидентов и одновременное выявление нестандартных схем [64]. Одновременно, Citi Group инвестировал в платформу Feedzai, применяющую машинное обучение для сквозного мониторинга платежей в режиме реального времени, обеспечивая сдерживание финансовых преступлений до их полномасштабной реализации [65].

Именно благодаря совмещению процедур детекции, аналитики и экстраполяции выявленных схем, формируется замкнутый цикл правоприменительной практики, в котором каждое следственное действие обогащает базы данных для будущей превенции. Тем самым, ИИ перестаёт быть исключительно инструментом технической поддержки, превращаясь в фактор интеллектуализации правоохранительной архитектуры.

Функции ИИ, используемые для раскрытия и расследования правонарушений

В современных условиях обеспечения общественного порядка *системы видеонаблюдения*, интегрированные с технологиями ИИ, приобретают статус одного из центральных инструментов аналитико-оперативного реагирования в правоохранительной практике. Благодаря алгоритмам компьютерного зрения, ИИ способен осуществлять автоматизированный анализ видеопотоков в режиме реального времени, идентифицируя лица, подозреваемые в противоправной деятельности, фиксируя отклонения в поведенческой модели, а также отслеживая перемещения объектов в пространстве. Так, система Clearview AI демонстрирует высокую эффективность в сопоставлении лиц, изображённых на видеозаписях, с базами данных, содержащими миллионы

фотографий, что позволяет существенно ускорить процесс идентификации подозреваемых лиц и лиц, находящихся в розыске [66].

Не меньший интерес представляет использование систем от ImageVision, ориентированных на автоматическое выявление аномалий в поведении субъектов – от резких движений и скоплений людей до подозрительных предметов. Такие системы способны в режиме реального времени сигнализировать о потенциально опасных ситуациях, облегчая работу оперативных служб [67]. Британская практика интеграции ИИ в архитектуру городского наблюдения, в частности в Лондоне, также демонстрирует высокую результативность: ИИ используется для идентификации признаков агрессии, ношения оружия, попыток самоубийства на станциях метрополитена и иных ситуаций, несущих угрозу общественной безопасности [68].

Примечательно, что технологии распознавания лиц, признанные международным сообществом и активно применяемые под эгидой Интерпола, основываются на обработке морфологических признаков, полученных с видеозаписей, и обладают высокой точностью при сопоставлении с криминалистическими базами данных [69]. Такие технические решения служат важным звеном в цепочке мероприятий по раскрытию преступлений, снижая временные и ресурсные издержки правоохранительных органов и повышая оперативность принятия решений.

Таким образом, видеонаблюдение с элементами ИИ уже перестаёт быть вспомогательным инструментом и становится центральным элементом цифровой трансформации уголовно-правовой сферы [70]. Однако его использование должно сопровождаться регламентированной процедурой контроля, направленной на соблюдение прав и свобод граждан и исключение дискриминационных практик, что подчёркивается в ряде международных правозащитных обзоров.

Так, в отчёте Управления Верховного комиссара ООН по правам человека подчёркивается, что технологии, основанные на ИИ, включая системы распознавания лиц, способны усиливать уже существующие предвзятости и социальные искажения, особенно в отношении расовых и этнокультурных меньшинств. Более того, в другом докладе УВКПЧ прямо указывается, что применение ИИ в рамках уголовного правосудия потенциально чревато воспроизводством структурной дискриминации и подрывает принципы справедливого судебного разбирательства [71], [72].

Организация Amnesty International также фиксирует высокие риски, связанные с использованием ИИ в системах социального обеспечения. В частности, в исследовании, посвящённом практике автоматизированного принятия решений в Дании, подчёркивается, что алгоритмы, применяемые в цифровом управлении благосостоянием, создают условия для массовой слежки и системной дискриминации уязвимых категорий граждан [73].

Важным вектором развития технологий в раскрытии и расследовании уголовных правонарушений занимает применение ИИ в *биометрической идентификации и цифровой криминалистике*, что обусловлено способностью

данных технологий существенно оптимизировать процедуры сбора, обработки и анализа доказательственной информации. Указанные направления обладают высоким потенциалом не только в контексте оперативного установления личности подозреваемых и документирования событий, но и в обеспечении целостности доказательственной базы при минимизации субъективного влияния человеческого фактора.

Применению ИИ в судебной экспертизе посвящен ряд публикаций, что косвенно подтверждает интерес научного сообщества к этой теме [74], [75], [76].

Применение ИИ в области биометрии основывается на анализе и интерпретации уникальных физиологических и поведенческих параметров, таких как отпечатки пальцев, параметры радужной оболочки глаза, голосовые характеристики и особенности походки. Современные системы, оснащённые ИИ-модулями, способны выполнять автоматизированную верификацию личности с использованием алгоритмов глубокого обучения, что обеспечивает высокий уровень точности и устойчивость к внешним помехам. Подобные решения уже интегрированы в судебно-экспертную практику ряда стран, включая США, Великобританию и государства Евросоюза, где применяются при миграционном контроле, в учреждениях пенитенциарной системы, а также в ходе досудебных расследований [77].

Распознавание лиц как один из ключевых инструментов биометрической идентификации продемонстрировало высокую эффективность в правоохранительной деятельности. Например, системы вроде Face++ и NEC NeoFace применяются для сопоставления визуальных данных с базами разыскиваемых лиц. Как отмечается в аналитическом отчёте Управления уполномоченного по информационной свободе Австралии, растущая точность таких алгоритмов делает их незаменимыми при обеспечении общественной безопасности, одновременно порождая риски неконтролируемого наблюдения [78]. ИИ-технологии, использующие голосовую биометрию, позволяют анализировать акустические параметры речи и выявлять конкретных лиц даже при наличии фонового шума, что актуализировано в борьбе с телефонным мошенничеством и киберпреступностью [79].

Ещё одним значимым направлением является цифровая криминалистика, в которой ИИ обеспечивает автоматизированный анализ данных, полученных с электронных устройств. Такие системы способны восстанавливать удалённые или повреждённые файлы, расшифровывать зашифрованные коммуникации, выявлять следы вредоносной активности, а также анализировать поведенческие шаблоны в цифровом пространстве. В частности, исследование, опубликованное в журнале Electronics, демонстрирует, как алгоритмы машинного обучения применяются для выявления признаков кибербуллинга, онлайн-экстремизма и социальной инженерии на цифровых платформах [80].

Современные ИИ-платформы для цифровой криминалистики, такие как Magnet AXIOM и Cellebrite UFED, активно применяются в международной

практике для анализа цифровых следов на мобильных устройствах, ноутбуках и облачных хранилищах. Их потенциал подтверждается эмпирическими данными, согласно которым обработка цифровых улик с использованием ИИ сокращает время расследования до 40% [81]. Особое значение имеет возможность выявления скрытых взаимосвязей между цифровыми объектами, например, связи между подозреваемыми и событиями, геолокацией и временными последовательностями взаимодействий.

Кроме того, технологии ИИ позволяют формировать так называемые поведенческие профили пользователей, выявлять аномалии и потенциальные признаки инсайдерских угроз, что особенно востребовано при расследовании корпоративного мошенничества и экономических преступлений. Такие подходы, как показано в исследовании Б. Гупты, позволяют интерпретировать логи событий, распределённые по нескольким цифровым источникам, и реконструировать хронологию действий подозреваемых [82].

Одной из системообразующих задач в процессе внедрения технологий искусственного интеллекта в сферы биометрической идентификации и криминалистического анализа является обеспечение неукоснительного соблюдения правовых и этических стандартов, выработанных в международной правозащитной практике. Компетентные органы, в том числе Управление Верховного комиссара ООН по правам человека и Amnesty International, последовательно указывают на необходимость институционализации нормативных рамок использования ИИ в данных областях, исходя из принципов пропорциональности, целенаправленности, прозрачности и подотчётности алгоритмических решений. Специальные доклады ООН подчёркивают, что недостаточная калибровка или непрозрачность функционирования ИИ-систем способна индуцировать системные риски, связанные с дискриминацией отдельных категорий лиц, ошибочной идентификацией подозреваемых и подрывом презумпции невиновности как фундаментального постулата международного права [83].

Таким образом, применение технологий искусственного интеллекта в сферах биометрической идентификации и цифровой криминалистики должно основываться на интегративном балансе между стремлением к максимизации технологической продуктивности и императивом обеспечения всесторонней защиты основополагающих прав и свобод личности, включая право на неприкосновенность частной жизни, презумпцию невиновности и принцип недискриминации.

Объективизация процедур сбора и анализа доказательств с помощью интеллектуальных алгоритмов повышает надёжность и достоверность следственных мероприятий, но требует постоянного экспертного мониторинга, включая регулярные аудиты, верификацию обучающих датасетов и многоуровневое юридическое регулирование. Лишь в условиях институциональной подконтрольности и научной обоснованности возможно гармоничное развитие данных направлений без нарушения базовых принципов правопорядка.

Существенное значение для повышения эффективности в раскрытии и расследовании уголовных правонарушений является использование ИИ в *анализе больших массивов данных*. Эта технология позволяет осуществлять многомерную обработку информации, поступающей из разнородных источников – от телекоммуникационных операторов и социальных сетей до видеонаблюдения и транзакционных платформ. Объединение таких источников в единую аналитическую архитектуру позволяет выявлять скрытые корреляции, реконструировать связи между участниками преступных схем и формировать доказательственную базу высокой степени достоверности.

Наиболее распространённым направлением является использование ИИ для автоматического выявления аномалий в транзакциях и коммуникациях. Согласно данным Межамериканского банка развития, внедрение ИИ-решений в странах Латинской Америки позволило существенно повысить эффективность выявления преступных паттернов в деятельности организованных групп, включая отслеживание каналов перемещения средств, логистики и передвижения подозреваемых лиц [84]. Эта практика основывается на корреляционном анализе больших данных и формировании визуализированных карт преступных сетей, что в значительной степени облегчает действия правоохранительных органов.

Немаловажное значение имеет и сфера финансового мониторинга. Использование ИИ в борьбе с отмыванием доходов и финансовыми махинациями получило широкое распространение благодаря способности интеллектуальных систем распознавать нелинейные цепочки транзакций. Так, в исследовании, представленном в цифровой библиотеке ACM, подчеркивается, что применение алгоритмов глубокого обучения позволяет эффективно идентифицировать подозрительные финансовые потоки в среде криптовалютных операций, что ранее было затруднено из-за анонимности таких транзакций [85].

Интеграция ИИ в процесс анализа цифровых следов оказывает значительное влияние и на оперативную работу правоохранительных органов. По данным платформы Cognyte, передовые ИИ-системы способны в режиме реального времени идентифицировать поведенческие аномалии, сигнализирующие о подготовке преступных действий, либо указывающие на участие лиц в незаконных схемах [86]. Использование таких систем не только ускоряет расследование, но и минимизирует нагрузку на сотрудников, поскольку интеллектуальная платформа самостоятельно предлагает направления дальнейшего анализа и расследования.

Значимым направлением интеграции ИИ в деятельность органов, осуществляющих досудебное расследование уголовных правонарушений, выступает автоматизированная *обработка аудиозаписей и текстовых массивов* с применением технологий обработки естественного языка (Natural Language Processing, NLP). Эти технологии позволяют в режиме реального времени анализировать поступающую речевую и письменную информацию с целью выявления признаков противоправного деяния, определения его

характера и классификации по правовым основаниям. Среди ключевых задач ИИ в данном аспекте – семантический анализ телефонных обращений, дешифровка зашифрованных сообщений, детектирование языковых маркеров угроз, шантажа и вербальных индикаторов насильственного поведения [87].

Так, ИИ-системы, ориентированные на аудиоформат, позволяют производить трансформацию устной речи в текст с сохранением интонационной и контекстуальной нагрузки, что особенно важно при анализе обращений в экстренные службы, где каждое слово может содержать критическую информацию. Одним из примеров успешной имплементации таких решений является система Dragon Law Enforcement, разработанная Nuance Communications. Эта платформа обеспечивает высокоточный автоматический перевод устной речи в текст, что существенно сокращает время на оформление рапортов, объяснительных и протоколов, одновременно минимизируя вероятность потери или искажения фактической информации [88].

Кроме того, использование ИИ в анализе цифровой переписки и социальных сетей предоставляет возможность заблаговременного выявления индикаторов готовящихся уголовных правонарушений. Алгоритмы NLP эффективно идентифицируют ключевые слова и выражения, характерные для обсуждений противоправной активности, включая незаконный оборот наркотических средств, оружия, угрозы причинения вреда и проявления агрессии. Эти функции особенно актуальны в условиях роста онлайн-коммуникаций, охватывающих как открытые платформы, так и зашифрованные мессенджеры.

Система может быть запрограммирована на выявление как прямых, так и завуалированных признаков возможного насилия или координации противоправных действий. Так, в докладе RAND Corporation подчёркивается необходимость интеграции инструментов речевой аналитики и поведенческой оценки в практику работы экстренных служб [89]. Исследователи отмечают, что обработка аудиопотока с применением методов анализа эмоционального и когнитивного состояния заявителя может существенно повысить точность принятия решений на стадии диспетчеризации. Хотя термин ИИ напрямую не используется, суть описываемых подходов предполагает использование технологий, относящихся к области ИИ, в частности алгоритмов классификации, обработки естественного языка и предиктивной аналитики. В данном контексте ИИ рассматривается как связующее звено между оценкой обращений и выбором подходящей модели реагирования, что особенно актуально в условиях динамизации угроз и увеличения числа нестандартных инцидентов, требующих гибкого и точного реагирования. Также можно выделить платформу Case Service**,** разработанную компанией Versaterm [90]. Этот программно-аналитический комплекс использует методы обработки естественного языка (NLP) для автоматической интерпретации как голосовых, так и текстовых обращений граждан. Система выполняет семантическую разметку и тематическую категоризацию поступающей информации, выделяя ключевые параметры – характер угрозы, тип инцидента и контекст. Такая

структуризация аудиоданных существенно облегчает последующий анализ и позволяет перераспределить ресурсы оперативных подразделений с учётом приоритетности вызовов. Внедрение аналогичных решений в отечественную практику досудебного производства открывает возможности для повышения качества аналитического сопровождения расследований, оперативной фильтрации сигналов и проактивного реагирования на наиболее значимые угрозы общественной безопасности.

Следует отметить, что эффективность таких решений во многом зависит от качества языковой модели, объёма обучающего корпуса и способности алгоритмов учитывать социокультурный контекст. Применение нейросетей последнего поколения (включая трансформеры) позволяет достигать высоких результатов в выявлении ключевых смыслов даже в неполных, фрагментарных или намеренно искажённых высказываниях. В отчёте Национального института юстиции США подчёркивается, что системы, использующие ИИ для анализа текстов и аудио, демонстрируют до 94% точности при определении категории вызова и соответствующего риска при правильно обученной модели [91].

Одной из существенных проблем при разработке и внедрении языковых моделей для казахского языка является ограниченность обучающих корпусов, что затрудняет формирование устойчивых и качественных лингвистических представлений в рамках искусственного интеллекта. В частности, исследователи проекта KazMMLU подчёркивают дефицит высококачественных и тематически разнообразных датасетов, что значительно снижает способность моделей к точной генерации и интерпретации текста [92]. Дополнительной трудностью выступает морфологическая сложность казахского языка, связанная с его агглютинативной природой и отсутствием полноценных морфоанализаторов, что снижает эффективность систем распознавания именованных сущностей [93]. Также важно учитывать ограничения технической и вычислительной инфраструктуры в регионе, что затрудняет реализацию масштабных языковых моделей: модели, такие как KazLLM и IrbisGPT, сталкиваются с нехваткой вычислительных ресурсов и кадровой экспертизы в области нейросетевой дообучаемости [94]. Кроме того, текущие версии языковых моделей демонстрируют слабую адаптацию к прикладным профессиональным областям, включая юридическую, медицинскую и административную речь, а также уязвимы к подмене казахской терминологии заимствованиями из русского языка [95]. Отдельного внимания требует проблема объяснимости – большинство доступных моделей не предоставляют прозрачности в принятии решений, что делает их менее пригодными для использования в правоприменительной или судебной деятельности [96].

Таким образом, автоматизированная обработка аудио- и текстовых данных с использованием ИИ формирует новый уровень эффективности и точности в системе досудебного реагирования. Эти технологии позволяют в короткие сроки обрабатывать огромные объёмы речевой информации, оперативно выявлять критические сигналы и способствуют формированию

доказательной базы, соответствующей требованиям уголовно-процессуального законодательства.

Экспоненциальное расширение виртуальной коммуникационной среды неизбежно создало предпосылки для необходимости использования ИИ-инструментария для анализа *цифровой активности в сети, охватывающей как открытые онлайн-платформы, так и закрытые сегменты, включая даркнет***.** Указанное направление деятельности правоохранительных органов предполагает постоянное адаптирование к трансформирующейся цифровой среде и требует автоматизированной интерпретации больших массивов информации в условиях высокой скорости её обновления. Именно в таких условиях ИИ демонстрирует наибольшую аналитическую продуктивность, обеспечивая интеллектуальное сопровождение при выявлении индикаторов правонарушений.

Одним из ключевых аспектов применения ИИ в данной области является автоматизированное отслеживание поведенческих паттернов пользователей социальных сетей. Алгоритмы машинного обучения и методы NLP позволяют в реальном времени фиксировать и интерпретировать отклонения от типичной пользовательской активности, включая проявления экстремистских настроений, признаки вовлечённости в противозаконные действия, а также координацию противоправных действий. Например, платформа Dataminr, внедрённая в ряде правоохранительных органов США, осуществляет мониторинг потоков сообщений в Twitter, анализируя их на предмет потенциальных угроз [97].

Значительное внимание также уделяется возможностям ИИ по идентификации фальсифицированных учётных записей, координируемых бот-сетей и иных форм манипулятивной онлайн-активности. Так, Cyabra обеспечивает комплексный поведенческий анализ и выявление скоординированных аномалий в цифровом взаимодействии, что критически важно в контексте нейтрализации информационно-психологических угроз и деструктивного влияния на общественное мнение [98].

Даркнет как пространство с повышенным уровнем анонимности представляет собой особую зону интереса правоохранительных органов, где осуществляется широкий спектр нелегальных транзакций. Инструменты ИИ, реализованные в системах Bolster и ZeroFox, обеспечивают анализ сетевой инфраструктуры, отслеживание торговых операций, а также интерпретацию зашифрованных каналов коммуникации с целью выявления и пресечения уголовных правонарушений [99], [100].

При этом необходимо учитывать, что активное внедрение ИИ в практику цифрового мониторинга сопряжено с высоким риском нарушения прав граждан на неприкосновенность частной жизни. В исследовании, подготовленном Brennan Center for Justice, подчёркивается необходимость нормативного ограничения алгоритмического вмешательства, особенно в части предиктивного анализа и массовой персонализированной слежки, поскольку данные практики потенциально могут привести к системным злоупотреблениям [101].

Еще одним прикладным назначением использования ИИ является *предиктивная аналитика*, основанная на алгоритмической интерпретации поведенческих и криминологических данных. В частности, автоматизированные методы профилирования, базирующиеся на ИИ-моделях, позволяют формировать обоснованные гипотезы о потенциальной угрозе противоправных деяний и повышать точность оперативного реагирования на уже совершённые уголовные правонарушения [102].

Значимым направлением является пространственно-временное моделирование криминогенной активности. Современные предиктивные платформы, интегрированные с геоинформационными системами, способны анализировать не только места совершения правонарушений, но и прогнозировать вероятные локации будущих эпизодов с учётом топографических, социальных и поведенческих переменных. Эффективность такого подхода подтверждается в отчётах Национального института юстиции США [103].

В своей работе Э. Цекич [104] рассматривает потенциал ИИ в области психологического профилирования правонарушителей, включая анализ мотивационных паттернов и скрытых поведенческих структур. Использование алгоритмов машинного обучения и обработки естественного языка позволяет выявлять риски и предикторы преступного поведения, при этом подчёркивается необходимость этической регламентации и обеспечения прозрачности решений.

ИИ также расширяет возможности перекрёстного анализа дел, не связанных прямыми признаками. Выявление общих методик совершения противоправных деяний – будь то способ проникновения, тип используемого орудия или структура действий – способствует формированию более обоснованных версий и повышает вероятность раскрытия серийных уголовных правонарушений [105].

А.А. Бессонов, внёсший значительный вклад в исследование применения ИИ в криминалистике, особенно в области предиктивной аналитики и профилирования правонарушителей, в своей статье показал, что применение алгоритмической аналитики на основе нейросетевых и статистических моделей позволило реконструировать поведенческие и биографические характеристики правонарушителей с высокой степенью достоверности. В условиях серийной преступности ИИ-технологии продемонстрировали эффективность в выявлении скрытых корреляций между действиями преступника и его личностными, пространственными и социальными параметрами [106].

В своей работе А.А. Бессонов, внёсший весомый вклад в развитие криминалистических исследований, связанных с использованием ИИ, убедительно демонстрирует, что применение алгоритмических методов, основанных на нейросетевых и статистических моделях, позволяет с высокой степенью достоверности реконструировать поведенческие и биографические характеристики преступников. В контексте серийной преступности технологии ИИ показали высокую эффективность при выявлении скрытых

взаимосвязей между действиями правонарушителя и его личностными, территориальными и социальными особенностями [106, с. 45-52].

Кроме того, А.А. Бессонов подчёркивает необходимость интеграции ИИ-инструментов в практику предварительного расследования, указывая на важность адаптации методов машинного обучения к специфике юридических задач [107].

Машинное обучение в правоохранительной практике требует оценки справедливости, поскольку может воспроизводить системные предвзятости; необходимы стандарты и междисциплинарный подход для этичного использования предиктивных технологий [108].

Таким образом, интеграция ИИ в процесс предиктивного анализа и профилирования в уголовно-правовой практике создаёт значительные возможности для повышения результативности правоохранительной деятельности.

Применение ИИ в расследовании *правонарушений, совершаемых в киберпространстве*, позволяет существенно повысить как скорость, так и точность идентификации источников угроз. Киберпреступность как трансграничный феномен требует комплексного подхода к идентификации и деконструкции цифровых следов, оставляемых правонарушителями в распределённых информационных средах. ИИ-инструменты позволяют автоматизировать обработку сетевого трафика, осуществлять детектирование фишинговых атак, проводить декомпозицию вредоносных программ и отслеживать криптовалютные транзакции, используемые в целях отмывания доходов, полученных преступным путём. Как подчёркивают Л.В. Бертовский и Б.Р. Сембекова, высокотехнологичные преступления уже сегодня представляют собой не только криминальную, но и значимую угрозу национальной безопасности, требующую институционального переосмысления методов их выявления и процессуального сопровождения [109].

В отчёте Европола подчёркивается, что ИИ значительно усиливает возможности организованной преступности, позволяя проводить более точные и разрушительные кибератаки, направленные на правительства, бизнес и частных лиц [110].

На практике эффективность подобных подходов подтверждается реальными случаями. В 2024 году в Гонконге сотрудница компании была обманута мошенниками, использовавшими технологии deepfake для создания видеоконференции с участием «руководителей» компании, в результате чего было переведено около 20 миллионов фунтов стерлингов. Подобные инциденты обостряют потребность в совершенствовании алгоритмов ИИ, направленных на раннее выявление подобных мошеннических схем [111].

Кроме того, ИИ активно применяется в цифровой криминалистике. Исследование, опубликованное в журнале Forensic Science International: Digital Investigation, анализирует роль ИИ и машинного обучения в современных цифровых расследованиях, подчёркивая их потенциал в реконструкции временных линий киберпреступлений и анализе больших данных [112].

В 2024 году южнокорейская полиция с помощью ИИ проанализировала более 300 000 транзакций, что позволило выявить вьетнамскую фишинговую группировку, похитившую 10 млрд вон через поддельные SMS-приглашения [113]. В 2018 году исследователи из Нидерландов продемонстрировали, что ИИ способен с точностью до 98,7% отслеживать перемещение пользователей даркнета между форумами, сопоставляя почерковую манеру сообщений при наличии от 25 постов [114]. В 2023 году в Германии Deutsche Bank внедрил ИИ-модель поведенческого анализа, которая позволила сократить число ложных срабатываний на 60% и повысить точность выявления мошенничества, усилив защиту цифровых транзакций в режиме реального времени [115].

Однако внедрение ИИ в расследование киберпреступлений сопряжено с рядом вызовов. Необходимость обеспечения прозрачности алгоритмов, защиты персональных данных и соблюдения этических норм требует разработки соответствующих нормативных и правовых рамок. В этом контексте важно учитывать рекомендации, изложенные в исследовании, опубликованном в Cogent Engineering, где акцентируется внимание на рисках и правовом статусе применения интеллектуальных технологий в цифровой защите [116].

Таким образом, интеграция ИИ в процессы расследования киберпреступлений представляет собой перспективное направление, способное значительно повысить эффективность правоохранительных органов. Однако для успешной реализации этого потенциала необходимо учитывать как технологические, так и правовые аспекты, обеспечивая надёжную защиту прав граждан и государства.

ИИ-технологии, задействованные в *анализе речевых и текстовых коммуникаций*, предоставляют правоохранительным органам инструменты для расшифровки аудиозаписей, интерпретации зашифрованных цифровых сообщений, а также машинного перевода материалов с иностранных языков. Одним из ключевых направлений выступает автоматическая транскрипция телефонных переговоров, что позволяет не только документировать содержание коммуникаций, но и анализировать его в юридическом контексте. Применение ИИ уже выходит за рамки теоретических разработок. Например, исследование Д. Косты и коллег убедительно демонстрирует, как технологии машинного анализа аудио могут играть ключевую роль в контексте обработки данных экстренных вызовов [117].

Технологии ИИ обеспечивают синтаксически точную и семантически релевантную передачу текста, включая обнаружение ключевых фраз, потенциально указывающих на противоправную деятельность. В дополнение к этому, всё большее значение приобретает автоматическая интерпретация эмоционального состояния говорящего. В. Ву и соавторы разработали систему, автоматически определяющую эмоции, речь и личность говорящего в аудиозаписях [118]. Полагаем, что это важно для оценки достоверности показаний и анализа поведения в правоохранительной практике.

Систематический обзор и метаанализ Г. Алхуссейна и др. выявили потенциал ИИ в распознавании эмоций, но также указали на методологические проблемы: предвзятость, низкую воспроизводимость и ограниченность моделей. Для применения в правоохранительной сфере требуется повышение объективности и правовой приемлемости алгоритмов [119].

Использование нейросетевых систем машинного перевода также подтверждает свою актуальность в условиях глобализированной преступности. Развитие ИИ в области автоматического перевода, субтитрирования и озвучивания способствует более точной передаче контекста и культурных особенностей речи, что может быть полезно при обработке мультиязычных аудиовизуальных материалов в рамках международных расследований и судебной практики [120].

Современные технологии анализа тональности речи на основе ИИ позволяют в реальном времени определять эмоциональное состояние собеседника по голосовым характеристикам. Однако сохраняются вызовы, включая точность, межкультурные различия, акустические и технические искажения, а также риски нарушения конфиденциальности и этических стандартов [121].

Таким образом, автоматизированные инструменты расшифровки, перевода и анализа тональности становятся важной частью современной криминалистической и оперативно-розыскной практики, обеспечивая более глубокое понимание контекста коммуникации и содействуя построению обоснованных версий при расследовании уголовных правонарушений.

Трансформация подходов к расследованию уголовных правонарушений в условиях цифровизации криминалистики обусловлена активным внедрением технологий ИИ в процесс визуального анализа и проверки подлинности цифровых доказательств. Особо значимое место в этом контексте занимает использование интеллектуальных алгоритмов для пространственно-временной реконструкции инцидентов, позволяющей моделировать криминальные события с высокой степенью достоверности. Инновационные ИИ-системы, интегрированные с геоинформационными платформами (ГИС), создают интерактивные 3D-сценарии, в которых последовательно визуализируются действия правонарушителей, потерпевших и свидетелей на основе видеонаблюдения, цифровых следов, координат GPS и временных меток. Такие решения способствуют формированию обоснованных версий произошедшего и сопоставлению вербальных показаний с эмпирическими данными. Один из примеров – проект VALCRI (Visual Analytics for Sense-making in Criminal Intelligence Analysis), разработанный при поддержке Европейской комиссии и направленный на визуализацию и осмысление больших массивов криминальной информации [122].

Дополнительным направлением является детектирование подделок и манипуляций с цифровыми объектами доказательственного значения. Современные ИИ-модели на основе глубокого обучения обладают высокой

чувствительностью к аномалиям в структурах изображений, аудио- и видеоматериалов, что делает их эффективными инструментами в выявлении дипфейков, поддельных документов и фальсифицированных записей. ИИ позволяет выявлять фальсификации судебно-медицинских экспертиз через анализ текстовых аномалий и несоответствий [123]. Алгоритмы ИИ успешно применяются для автоматической диагностики подделок по структуре и стилистике заключений.

Программное обеспечение компании Cognitec Systems GmbH, в частности система FaceVACS, успешно применяется в практике идентификации лиц, включая оперативную сверку изображений с полицейскими базами данных и видеопотоками с общественных камер наблюдения [124]. Эти технологии были апробированы, в частности, в 2023 году в рамках операции «Renewed Hope», в ходе которой удалось идентифицировать сотни правонарушителей и жертв преступлений по цифровым следам [125].

ИИ также находит применение в сфере анализа обращений граждан и автоматической обработки текстовых массивов. Использование языковых моделей нового поколения (таких как GPT, LLaMA и их модификации), позволяющих анализировать смысловые паттерны, выделять ключевые сигналы и аномалии, усиливает аналитический потенциал при обработке больших объёмов жалоб, заявлений и текстовых свидетельств. Однако исследователи подчёркивают необходимость экспертной модерации таких решений, поскольку контекстно-семантические искажённые интерпретации могут повлиять на достоверность и правовую допустимость сформулированных выводов [126], [127], [128].

Киберфизические технологии, направленные на аудиодетекцию, такие как от компании Flock Safety, предоставляют примеры успешной интеграции ИИ в акустический мониторинг уличной преступности. Эти платформы позволяют локализовать источник выстрела с высокой точностью и передавать координаты в режиме реального времени полицейским подразделениям. В ряде американских городов они стали частью комплексных центров городской безопасности, подтвердив свою практическую ценность [129].

3. Осуществление правосудия

Одним из ключевых направлений внедрения ИИ в судебную сферу выступает повышение эффективности и обоснованности процедур правосудия, особенно на стадии судебного разбирательства. Использование ИИ в данном контексте направлено не только на автоматизацию рутинных операций, но и на поддержку принятия решений на основе комплексного анализа правовой информации, что способствует обеспечению принципов правовой определённости, транспарентности и справедливости [130].

Особое внимание в исследовательской и прикладной практике уделяется применению ИИ для обработки и анализа массивов юридических документов. Современные ИИ-системы, построенные на базе алгоритмов NLP, обеспечивают высокоточное распознавание и интерпретацию текстов законов,

судебных решений, подзаконных и иных правовых актов [131]. В частности, система LexisNexis использует ИИ для поиска релевантной судебной практики и выявления логических связей между делами на основании семантического анализа [132].

Одним из значимых кейсов в этой области является разработка платформы ROSS Intelligence, функционирующей на основе модели IBM Watson. Эта система ориентирована на юрисдикцию США и позволяет адвокатам и судьям быстро получать ответы на правовые вопросы, базируясь на содержании тысяч прецедентных решений и законодательных актов. Как показано в анализе Сасскинда, ROSS успешно интегрируется в адвокатскую и судебную деятельность, повышая скорость правового анализа и снижая риск пропуска релевантной информации [133].

Применение ИИ также позволяет повысить объективность судебных заключений за счет оценки вероятностей тех или иных исходов на основе статистических данных. Например, в исследованиях Европейского суда по правам человека использовалась система предиктивной аналитики на основе ИИ, которая с высокой точностью предсказывала решения Суда, анализируя текстовые и контекстуальные характеристики дел [134].

В то же время необходимо отметить, что внедрение ИИ в сферу правосудия требует строгого соблюдения правовых и этических стандартов. Особое значение приобретают вопросы обоснованности алгоритмических решений, прав человека на справедливый суд и процедурной прозрачности. Автоматизация судебной аналитики требует нормативной регламентации, в том числе в части ответственности за ошибочные выводы, сделанные алгоритмом [135].

Еще одним направлением выступает ускорение процессов *подготовки и структурирования типовых судебных документов*. Инструменты ИИ позволяют обрабатывать текстовую информацию, извлекать релевантные правовые нормы и формировать юридические конструкции в автоматизированном режиме с учётом заданных параметров.

Так, современные модели на базе NLP демонстрируют высокую способность к генерации и корректировке юридических текстов на основании анализа массивов нормативных актов и судебной практики [136]. Автоматизированные платформы, интегрированные в судебные информационные системы, способны генерировать шаблонные исковые заявления и договоры с уровнем точности, удовлетворяющим базовые критерии юридической корректности [137], [138].

В странах с континентальной правовой системой автоматизированное составление судебных документов основано преимущественно на нормативно-фактологическом сопоставлении, а не на прецедентном праве. Это обеспечивает более стабильную архитектуру автоматических шаблонов.

Наряду с техническими преимуществами, автоматизация документооборота требует учёта рисков, связанных с юридической ответственностью за возможные ошибки в составленных документах. Критически важным аспектом остаётся обеспечение надлежащего контроля со

стороны профессионала на заключительном этапе подготовки правовых актов [139].

ИИ анализирует исторические данные о судебных процессах, чтобы *предсказать вероятность успешного рассмотрения дела*. Современные алгоритмы машинного обучения, применяемые в системах юридического анализа, позволяют моделировать возможные сценарии судебных решений на основе обширных массивов данных.

Одним из наиболее авторитетных исследований в этой области является работа Д.М. Каца и М.Дж. Боммарито, где на материале решений Верховного суда США продемонстрирована возможность прогнозирования судебных исходов с точностью до 70% [140]. Несмотря на специфику англосаксонской системы, полученные выводы нашли отражение в последующих исследованиях, адаптирующих модели ИИ к особенностям континентального права. В частности, Гарри Сёрден подчёркивает роль ИИ в оценке правовых рисков, формировании правовых стратегий и автоматизации правового анализа [141].

На практике алгоритмические инструменты всё чаще используются юридическими компаниями и государственными структурами. Так, канадская платформа Blue J Legal разработала систему, позволяющую с высокой степенью вероятности предсказывать налоговые решения и судебные исходы по трудовым спорам [142]. Важно обеспечивать баланс между эффективностью ИИ и уважением к судебной автономии, особенно в делах, требующих индивидуальной правовой оценки [143].

Важным шагом в направлении адаптации технологий ИИ в условиях Республики Казахстан стало внедрение специализированной аналитической платформы «Цифровая аналитика судебной практики». Как отметил официальный представитель судебного сообщества, данная система используется в практике судей-примирителей и предназначена для анализа судебных решений с целью оценки перспектив разрешения споров в досудебном порядке [144]. ИИ в данном контексте выполняет функцию интеллектуального помощника, позволяя сторонам получить представление о возможных правовых исходах и тем самым стимулировать переход к альтернативным способам урегулирования разногласий до стадии формального принятия иска к производству.

Также, согласно докладу председателя Верховного суда РК Асламбека Мергалиева, озвученному в начале 2025 года, с использованием ИИ было обработано 665 тысяч дел и материалов из 2 миллионов, что составляет почти треть от общего количества. Внедрение автоматизированной системы «Цифровая аналитика судебной практики» позволило роботизированным модулям формировать прогнозы исходов гражданских дел на основе анализа судебных решений, выявления аномалий и прецедентов. Как подчёркивается в официальном сообщении, «программа обучена понимать суть судебных решений, сравнивать их между собой, выявлять аномалии и прогнозировать исход гражданского дела. И судья при поступлении иска видит судебную практику по схожим делам, вплоть до кассации» [145].

Такой подход отражает важную тенденцию к расширению функционала ИИ в сфере правосудия не только в части автоматизации и прогнозирования, но и в качестве инструмента обеспечения процессуальной экономии, укрепления доверия к судебной системе и повышения правовой предсказуемости. Интеграция предиктивной аналитики в контексте разрешения гражданских дел способствует снижению нагрузки на судебную систему и формированию устойчивой культуры медиации и правового диалога.

Особый интерес представляет также практика применения ИИ в рамках системы уголовного правосудия США, где используется модель COMPAS (Correctional Offender Management Profiling for Alternative Sanctions – Система оценки риска и поведения осуждённых для выбора альтернативных санкций). Эта система прогнозирует вероятность рецидива – повторного совершения уголовного правонарушения – и применяется судами при вынесении решений о мерах пресечения, досрочном освобождении и условиях пробации. В то же время исследование ProPublica вызвало широкую дискуссию о справедливости и прозрачности подобных алгоритмов. Было показано, что алгоритм допускает систематические ошибки, завышая оценки риска для определённых этнических групп, что ставит под сомнение его пригодность для использования в целях правосудия без надлежащего институционального контроля [146].

Применение ИИ в прогнозировании исходов дел имеет и практико-ориентированное значение. Такие системы могут предоставить сторонам процесса оценку вероятности успеха и предложить оптимальные стратегии – как в части доказывания, так и в части защиты, особенно в условиях перегрузки судов и ограниченности ресурсов.

Внедрение интеллектуальных систем *автоматического контроля* способствует не только повышению организационной дисциплины в рамках судопроизводства, но и обеспечивает дополнительную гарантию соблюдения прав сторон.

ИИ-инструменты, интегрированные в электронные судебные платформы, позволяют формализовать и автоматизировать контроль за соблюдением процессуальных сроков, включая подачу заявлений, предоставление доказательств, а также направление апелляций и кассационных жалоб. Такие системы способны в режиме реального времени отслеживать ход дела, уведомлять участников процесса о наступлении критически важных дат и обнаруживать пропуски, связанные с несоблюдением обязательных требований.

Особое внимание уделяется функциям верификации процессуальных документов. Системы ИИ анализируют полноту предоставленных материалов, сверяют наличие обязательных реквизитов, проверяют соответствие установленным нормативам. Это позволяет избежать возвратов заявлений по формальным основаниям, а также минимизирует риск затягивания сроков разбирательств.

На практике в нашей стране контрольные функции частично реализованы через платформу «Төрелік», обеспечивающую автоматизированное управление судебным документооборотом и синхронизацию процессуальных действий с календарными графиками судопроизводства [147].

В международной практике аналогичные функции реализуются, например, в платформе Case Center и европейской системе e-CODEX, где ИИ участвует в формализации делопроизводства и автоматизированной валидации документов, способствуя более эффективному процессуальному менеджменту [148], [149].

Автоматизация *юридических консультаций*, прежде всего в части разрешения типовых правовых вопросов, не требующих индивидуального толкования сложных норм материального или процессуального права, – еще одно поле для деятельности ИИ. Использование ИИ-ботов, функционирующих на основе алгоритмов обработки естественного языка и обученных на корпусах юридических текстов, позволяет осуществлять первичную правовую навигацию для граждан и организаций, существенно снижая нагрузку на традиционные каналы юридической помощи.

Такие ИИ-системы могут предоставлять предварительные консультации по вопросам защиты прав потребителей, спорам в сфере трудового права, нарушениям договорных обязательств и аналогичным категориям дел, в которых структура правового конфликта имеет стандартный и повторяющийся характер [130, p. 1305-1339]. Например, платформа DoNotPay позиционируется как «первый в мире робот-юрист», предоставляющий помощь в подготовке исков, обжаловании штрафов, запросах о возврате средств и пр. [150]. Аналогичные решения реализуются в рамках правительственных инициатив по обеспечению доступа к правосудию: в Канаде, Нидерландах, Эстонии и Сингапуре внедрены пилотные проекты, ориентированные на цифровую трансформацию юридических консультаций [151].

В феврале 2025 года Министр юстиции Республики Казахстан Ерлан Сарсембаев заявил о планах по внедрению чат-бота для предоставления гражданам бесплатной юридической помощи в рамках государственной гарантии: «Для оптимизации данной процедуры предлагается внедрить чат-бот для консультаций граждан ″не выходя из дома″. Высвобождаемые средства от правового консультирования предлагается направить на увеличение тарифов оплаты труда на судебное представительство» [152].

Несмотря на очевидные преимущества – скорость отклика, масштабируемость и возможность функционирования в режиме 24/7 – автоматизированные консультации требуют нормативного разграничения между информацией и юридическим советом, а также надлежащей ответственности за предоставленные сведения. Европейская комиссия по эффективности правосудия (CEPEJ) подчёркивает необходимость обеспечения прозрачности, обратной связи и возможности эскалации вопроса к человеку-юристу при использовании ИИ в правовых консультациях [153].

Функциональные возможности ИИ в данном контексте позволяют отслеживать сроки подачи процессуальных документов, в том числе жалоб, ходатайств и возражений, проверять полноту доказательной базы на соответствие требованиям конкретной категории дела, выявлять возможные нарушения – такие как пропущенные сроки или отсутствие обязательных документов, а также осуществлять контроль качества судебных актов с точки зрения их логической согласованности, корректности правовой аргументации и точности ссылок на нормы права.

В Китае функционируют так называемые «умные суды» (smart courts), которые в автоматизированном режиме проверяют соответствие сроков и процессуальных норм, используя централизованные алгоритмы анализа данных [154].

Таким образом, применение ИИ в целях мониторинга соблюдения процессуального законодательства усиливает институциональные гарантии справедливого разбирательства, способствует стандартизации процедур и укреплению доверия граждан к судебной системе.

В условиях многоязычного судопроизводства и увеличивающегося объёма аудиовизуальных данных судебные органы различных стран внедряют технологии ИИ для автоматизации перевода юридических документов и расшифровки аудиозаписей судебных заседаний. К примеру, платформа Rask AI предоставляет услуги по транскрипции казахской речи [155].

Более того, в 2024 году в Республике Казахстан был запущен проект по тестированию «интернет-суда» с использованием технологий ИИ и распознавания речи. Этот проект предусматривает онлайн-формат судебных заседаний, в которых автоматизированные решения фиксируют речь участников, синхронизируют её с процессуальными действиями и формируют протокол заседания в реальном времени. Указанная инициатива направлена на сокращение бюрократической нагрузки и ускорение правосудия в делах незначительной сложности [156].

В ЕС Европейская комиссия в рамках стратегии цифровизации правосудия подчёркивает необходимость внедрения технологий машинного перевода и автоматической дешифровки судебных процессов с целью обеспечения многоязычия, прозрачности и доступа к правосудию. Это включает разработку мультимодальных переводческих систем, адаптированных к юридическим задачам [157].

В Китае концепция «умных судов» включает применение ИИ для автоматической расшифровки аудио- и видеозаписей судебных процессов. Такие системы, как, например, «206», способны распознавать речь и идентифицировать участников процесса по ролям, что способствует повышению эффективности судебного разбирательства [158].

ИИ также может быть использован для выявления фальсифицированных доказательств, так как традиционные методы верификации документов и свидетельств требуют значительных временных и человеческих ресурсов, в то время как ИИ предлагает автоматизированные, более точные и масштабируемые решения.

Интеллектуальные системы с использованием алгоритмов машинного обучения и нейросетевых моделей способны выявлять поддельные документы, включая изменённые или сгенерированные договоры, постановления, удостоверения. Особую ценность представляют технологии, ориентированные на анализ цифровых подписей, которые фиксируют уникальные паттерны поведения пользователя при подписании документов (скорость, ритм, нажим, динамика движений), что делает невозможным их подделку вручную.

Особый интерес в этом контексте представляет концепт «электронного почерка», разработанный в рамках исследований А.В. Цветковой, согласно которому поведенческие характеристики пользователя при работе с цифровыми документами (включая микродвижения, траектории курсора и паузы между нажатиями клавиш) могут быть использованы в качестве уникального идентификатора, не поддающегося простому воспроизведению и являющегося новым направлением в криминалистической идентификации [159].

ИИ также применяется для проверки аутентичности свидетельских показаний, сравнивая их с массивами ранее зафиксированных данных (видеозаписей, аудиофайлов, текстов), выявляя несоответствия, а также анализируя эмоциональные и поведенческие маркеры при даче показаний.

Кроме того, алгоритмы компьютерного зрения используются для анализа изображений, видеозаписей и отсканированных документов, позволяя обнаруживать цифровые следы редактирования, признаки наложения, неестественные шрифты и метаданные, не соответствующие оригинальному источнику.

В качестве примеров можно привести инициативу Adobe Content Authenticity Initiative, обеспечивающую верификацию происхождения и истории изменений цифровых материалов [160]; технологию Truepic, основанную на использовании криптографических стандартов для защиты изображений от подделки [161]; решения компании Cognitec, специализирующейся на биометрической идентификации с помощью лицевого анализа [162]; а также платформу Pangea, предоставляющую API для верификации цифровой идентичности и борьбы с документарным мошенничеством [163].

Таким образом, использование ИИ в борьбе с фальсификациями позволяет значительно снизить риск процессуальных ошибок, повысить достоверность доказательной базы и укрепить правовую защиту участников судопроизводства.

4. Исполнение судебных решений

Исполнение судебных решений является завершающим и критически важным этапом правосудия, от которого напрямую зависит фактическое восстановление нарушенных прав. В условиях цифровой трансформации правовой системы технологии искусственного интеллекта находят всё большее применение в сфере мониторинга и обеспечения исполнения судебных актов.

В нашей стране внедряются цифровые решения, направленные на автоматизацию процессов исполнения судебных решений. В частности, Министерство юстиции представило инициативу по модернизации правовой системы, включающую запуск цифрового помощника для кредиторов и должников, а также обновление системы «Робот-судебный исполнитель» с целью повышения эффективности взыскания задолженностей. Цифровизация затрагивает всё больше сфер, включая и сферу юстиции. Так, за последние полгода в Казахстане был внедрён «Робот-судебный исполнитель», который оформил свыше 125 тысяч процессуальных документов. По оценкам Министерства юстиции, это позволило сэкономить более 600 миллионов тенге. В связи с высокой эффективностью планируется расширение его функциональных возможностей. Поэтому в Министерстве юстиции намерены расширить его полномочия. Эти меры направлены на улучшение системы исполнения, внедрение цифровых технологий и автоматизацию процессов, таких как снятие арестов и ограничений на выезд за границу [164].

Электронные браслеты, оснащённые модулями GPS-навигации и интегрированные в централизованные цифровые платформы, позволяют в режиме реального времени отслеживать перемещения поднадзорных лиц. ИИ, применяемый в таких системах, не только фиксирует геолокацию, но и анализирует маршруты передвижения, выявляет отклонения от предписанных судом зон и временных интервалов, а также формирует автоматические сигналы тревоги при нарушениях условий наказания. При этом алгоритмы самообучения позволяют системам адаптироваться к индивидуальным поведенческим особенностям осуждённых, минимизируя ложноположительные срабатывания и тем самым снижая вероятность избыточного вмешательства со стороны сотрудников службы пробации.

ИИ способен выявлять как единичные, так и повторяющиеся попытки нарушения ограничений, определять риск рецидива, формировать поведенческий профиль каждого поднадзорного и обеспечивать принятие превентивных мер. На основе накопленных данных создаются аналитические карты и сценарии отклоняющегося поведения, что позволяет выстраивать эффективную превентивную модель реагирования. Кроме того, интеграция ИИ с другими базами данных правоохранительных органов способствует быстрому выявлению лиц, уклоняющихся от контроля, и автоматическому инициированию мер по их задержанию.

Это снижает нагрузку на сотрудников уголовно-исполнительной системы и повышает надёжность контроля за осуждёнными, что особенно важно при необходимости предотвращения повторных правонарушений. Таким образом, применение ИИ в данной сфере является примером синергии технологий и безопасности, обеспечивая не только цифровой мониторинг, но и элементы интеллектуального предсказания потенциальных нарушений.

Например, британская система Buddi позволяет в режиме реального времени отслеживать перемещение осуждённых, направляя автоматические уведомления при пересечении границ установленных зон [165]. В Канаде применяется программа Correctional Service Canada's Electronic Monitoring

Program, которая не только обеспечивает GPS-наблюдение, но и интегрирована с аналитическими модулями для оценки риска нарушений [166]. В США, помимо системы SmartLink, используется BI TotalAccess от компании BI Incorporated, включающая мобильные приложения, видеосвязь и биометрические проверки, синхронизированные с браслетами [167]. Эти технологии не только обеспечивают контроль, но и формируют цифровую среду ресоциализации, позволяя отслеживать поведенческую динамику поднадзорного лица и взаимодействовать с ним дистанционно.

В Финляндии активно развиваются системы предиктивного реагирования, которые позволяют оценивать риск повторного правонарушения на основании поведенческих и социальных факторов, автоматически формируя для сотрудников службы пробации алгоритм дальнейших действий [168].

Таким образом, ИИ в системах контроля за передвижением осуждённых становится не только инструментом технического наблюдения, но и частью более широкой системы адаптивного правоприменения, обеспечивая баланс между общественной безопасностью и правами человека [169], [170], [171].

Современные технологии искусственного интеллекта позволяют применять методы предиктивной аналитики в сфере исполнения судебных решений и контроля за осуждёнными. Это направление основано на анализе большого объёма данных, включающих как персональные характеристики осуждённых, так и поведенческие маркеры, полученные в процессе исполнения наказания.

ИИ-модели способны с высокой степенью вероятности прогнозировать риск побега, нарушения условий условно-досрочного освобождения, неуплаты административных штрафов или уклонения от выполнения других обязательств, наложенных судом. Для этого используются алгоритмы машинного обучения, которые выявляют закономерности и скрытые взаимосвязи на основе исторических данных о правонарушителях.

Особенность предиктивных систем заключается в их способности учитывать не только формальные показатели, но и динамические изменения в поведении осуждённого в процессе исполнения наказания. Например, увеличение частоты контактов с контролирующими органами, нарушение графика явок, изменение маршрутов передвижения – всё это может служить маркерами, сигнализирующими о потенциальном уклонении.

Примером является система HART (Harm Assessment Risk Tool), разработанная полицией Дарема в Великобритании. Она использует машинное обучение для прогнозирования вероятности повторного правонарушения в течение двух лет после освобождения, классифицируя правонарушителей по уровням риска: высокий, средний или низкий [172]. Система внедряется в рамках политики «умного правосудия», ориентированной на снижение повторных преступлений путём индивидуального подхода.

В Канаде в качестве альтернативы широко используется система LS/CMI (Level of Service/Case Management Inventory), разработанная Andrews

and Bonta, и официально внедрённая в уголовно-исполнительную систему страны. Она включает модуль оценки риска уклонения и нарушений условий условного освобождения и активно применяется службами пробации [173]. Модель интегрирована с фискальными базами данных и позволяет выявлять группы лиц, подверженных риску неисполнения финансовых обязательств, с последующим направлением таких дел на приоритетное реагирование.

В Германии в рамках инициативы Predictive Policing пилотный проект реализуется в сотрудничестве с полицейскими управлениями Баварии и Гессена. Используются предиктивные алгоритмы для оценки вероятности повторных имущественных преступлений на основе анализа временно-пространственных закономерностей [174].

Прогностическая аналитика на основе ИИ используется также для оптимизации нагрузки на сотрудников службы исполнения наказаний, позволяя им сосредоточиться на работе с осуждёнными, имеющими высокий риск нарушений. Кроме того, предиктивные инструменты способствуют снижению рецидива и экономии государственных ресурсов за счёт адресного подхода к надзору.

Прогностическая аналитика на основе ИИ используется также для оптимизации нагрузки на сотрудников службы исполнения наказаний, позволяя им сосредоточиться на работе с осуждёнными, имеющими высокий риск нарушений. Кроме того, предиктивные инструменты способствуют снижению рецидива и экономии государственных ресурсов за счёт адресного подхода к надзору. В частности, как отмечается в отчётах EMHIC Global, подобные алгоритмы используются для прогнозирования поведения заключённых и оптимизации графиков смен, что снижает эмоциональную нагрузку на персонал и повышает безопасность учреждения [175].

ИИ также рассматривается в Великобритании в качестве инструмента предотвращения насилия и членовредительства в пенитенциарных учреждениях на основе анализа видеопотока с помощью нейросетевых моделей, что позволяет оперативно выявлять признаки потенциально опасного поведения [176].

В последние годы автоматизация процессов взыскания задолженностей становится всё более актуальной задачей в правоохранительной и судебной системах. Использование ИИ в этой сфере позволяет значительно повысить эффективность взыскания штрафов, налоговых долгов, алиментов и других обязательств.

ИИ-системы обеспечивают *автоматическую генерацию уведомлений должникам о наличии задолженности*, сроках её уплаты и возможных правовых последствиях неисполнения. Эти уведомления могут направляться как через электронную почту, так и посредством SMS или мессенджеров, что обеспечивает охват широкой аудитории в оперативные сроки. Такие решения реализованы, например, в платформе Beam AI, которая полностью автоматизирует взаимодействие с должниками [177].

Одним из ключевых направлений применения ИИ является распознавание платежных данных. Современные решения, такие как Level AI и Convin AI, интегрируются с государственными и банковскими системами, отслеживая статус платежей и определяя приоритет взыскания [178-180]. Например, алгоритмы могут автоматически распознавать задержки и отличать технические сбои от фактов уклонения. Помимо этого, ИИ способен анализировать повторяемость задолженностей, наличие просрочек и другие показатели, формируя кредитный профиль гражданина в рамках государственного контроля.

На основе собранных данных формируется единый реестр нарушителей платёжной дисциплины. Такие реестры позволяют быстро реагировать на системные нарушения и направлять соответствующие уведомления в надзорные и судебные органы. Информационная взаимосвязь между государственными и финансовыми структурами усиливает межведомственную координацию и позволяет сокращать сроки исполнения взысканий.

ИИ также используется для формирования судебных запросов на взыскание задолженности в упрощённом порядке. Алгоритмы формируют проекты обращений в суд на основе шаблонов и информации о должнике, что минимизирует участие человека в рутинных действиях.

Потенциал интеграции ИИ в процедуры автоматической идентификации лиц, отбывших наказание или находящихся на контроле в рамках условно-досрочного освобождения, заключён в возможности повышения институциональной эффективности механизмов пенитенциарного надзора и укрепления гарантий общественной безопасности. Применение соответствующих технологических решений, основанных на биометрических методах верификации личности (включая распознавание радужной оболочки глаза, лица, отпечатков пальцев), а также на автоматизированных системах контроля доступа, обеспечивает не только минимизацию рисков ошибочной идентификации, но и создание единого цифрового контекста взаимодействия между осуждёнными и уполномоченными государственными органами.

В США ФБР внедрило систему Next Generation Identification (NGI), которая включает в себя модуль распознавания радужной оболочки глаза. Эта технология используется для быстрой и точной идентификации осуждённых при их перемещении или освобождении из мест лишения свободы, а также в рамках пробации и условно-досрочного освобождения. Сканирование радужной оболочки позволяет обеспечить высокую точность идентификации и снизить риск ошибок при освобождении или переводе заключённых. Согласно информации на официальном сайте ФБР, NGI Iris Service предоставляет возможность захвата, каталогизации и быстрого сравнения изображений радужной оболочки глаза с высокой точностью, что способствует эффективной идентификации в различных сценариях [181].

Стремление к повышению эффективности исполнения наказаний подталкивает к мысли потенциального использования ИИ в целях мониторинга цифрового поведения осуждённых, особенно в контексте

условно-досрочного освобождения и наказаний, не связанных с лишением свободы. Учитывая ограничения традиционных механизмов надзора, основанных преимущественно на физическом присутствии или периодической отчётности, технологии ИИ могут служить инструментом косвенного, но устойчивого контроля через анализ цифровых следов.

Предполагается, что в будущем системы, базирующиеся на алгоритмах NLP и методах поведенческого анализа, смогут использоваться для выявления признаков нарушений установленных ограничений, включая контакты с потерпевшими, участие в запрещённых мероприятиях, а также распространение информации, свидетельствующей о рецидивных тенденциях. В частности, анализ открытых источников, таких как социальные сети, мессенджеры и иные онлайн-платформы, может позволить отслеживать потенциальные отклонения в поведении условно освобождённых лиц.

На современном этапе в практику уголовно-исполнительной системы США, в частности в штате Калифорния, активно внедряются технологии в целях повышения эффективности контроля за лицами, находящимися под пробационным контролем [182]. Одним из направлений является применение систем мониторинга, осуществляющих анализ активности поднадзорных субъектов в социальных сетях. Такие платформы обеспечивают автоматизированную обработку открытых данных и идентификацию потенциальных нарушений условий освобождения – например, посещение запрещённых территорий либо взаимодействие с лицами, с которыми общение ограничено или запрещено решением суда. В частности, платформа Guardian Alliance Technologies предлагает программное обеспечение, основанное на использовании искусственного интеллекта и настраиваемых ключевых слов, позволяющее выявлять подозрительную онлайн-активность лиц, находящихся под надзором [183].

С учётом возрастающей сложности форм социальной девиации и увеличения нагрузки на правоохранительные органы, цифровизация процедур исполнения наказаний, не сопряжённых с лишением свободы, при участии технологий ИИ, обретает всё большую практическую значимость и представляет собой новое концептуальное направление в развитии систем уголовного правосудия.

Лица, осуждённые к исправительным и общественным работам, требуют эффективного и в то же время ненавязчивого мониторинга поведения в условиях свободы. Применение ИИ-технологий позволяет автоматизировать ключевые элементы надзора и тем самым повысить как дисциплинарную подотчётность осуждённых, так и эффективность функционирования уголовно-исполнительной системы.

Один из перспективных векторов – использование ИИ для автоматического учёта явки на место исполнения исправительных работ. Системы способны верифицировать личность при помощи биометрических данных (распознавание лиц, отпечатков пальцев, радужной оболочки глаза), а также вести непрерывную регистрацию времени присутствия осуждённого на рабочем месте с точностью до минут.

Современное переосмысление задач правоохранительной деятельности в условиях цифровой трансформации правового государства требует системного подхода к оценке потенциала и ограничений ИИ. Правоохранительная система, действующая в интересах общества, должна быть не только эффективной, но и подотчётной, соблюдающей принципы законности, справедливости и прав человека. В этом контексте ИИ уже не воспринимается исключительно как вспомогательный инструмент, а становится одним из ключевых факторов трансформации институтов безопасности, правосудия и общественного контроля.

Проведённый анализ позволяет утверждать, что задачи применения ИИ в правоохранительной сфере охватывают весь жизненный цикл реагирования на противоправные деяния: от их предиктивного предупреждения до исполнения судебных решений. При этом в каждом из направлений реализуются специфические функции: превенция опирается на прогнозную аналитику и анализ поведенческих паттернов; расследование – на обработку цифровых следов, криминалистический анализ и интеллектуальную реконструкцию событий; судопроизводство – на автоматизацию юридического анализа, подготовку судебных документов и прогнозирование решений; а исполнение наказаний – на предиктивный надзор и цифровой мониторинг поведения осуждённых.

Одним из ключевых положений, подтверждённых в рамках данной главы, является то, что ИИ не должен восприниматься как универсальное средство решения всех задач правоохранительных органов. Его использование должно быть обосновано с учётом характера поставленной задачи, юридического контекста и уровня допустимого вмешательства в сферу прав и свобод личности. Это особенно актуально в условиях правового государства, где любое ограничение прав должно быть пропорциональным, необходимым и легитимным.

Определение задач применения ИИ сквозь призму стадий правоохранительной деятельности позволяет выработать более взвешенные критерии допустимости и эффективности его интеграции. Превенция как стратегически приоритетное направление открывает перспективы для формирования устойчивых и гибких моделей предупреждения угроз, но требует особо тщательного контроля за соблюдением принципа недискриминации. В то время как сферы раскрытия и расследования правонарушений демонстрируют высокую востребованность ИИ в части ускорения процедур и повышения аналитической точности, они требуют развития нормативных механизмов допустимости цифровых доказательств, воспроизводимости алгоритмических решений и процедурной надёжности.

Судебная деятельность, несмотря на свою формализованную природу, также оказалась восприимчивой к цифровизации, что подтверждается внедрением систем прогнозного анализа, автоматизации подготовки решений и контроля за соблюдением процессуальных норм. Здесь ИИ может служить не только инструментом повышения эффективности, но и механизмом

обеспечения правовой определённости – при условии сохранения автономии судейского усмотрения.

Наконец, в сфере исполнения судебных решений ИИ демонстрирует значительный потенциал для формирования системы интеллектуального надзора, адаптивного к индивидуальным характеристикам осуждённых и обеспечивающего баланс между контролем и гуманностью. В этом контексте технологии ИИ могут стать основой для формирования «цифрового гуманизма» – концепции, при которой цифровые технологии служат не инструментом давления, а средством обеспечения законности, справедливости и реабилитации.

Таким образом, задачи применения ИИ в правоохранительной деятельности необходимо рассматривать не как изолированные технические нововведения, а как элементы целостной правовой и институциональной эволюции системы обеспечения общественного порядка. Такой подход требует междисциплинарного научного осмысления, разработки нормативной архитектуры, обеспечения прозрачности и подотчётности используемых решений. Только в условиях гармоничного сочетания технологических возможностей и юридических гарантий ИИ может стать не просто помощником в правоохранительной деятельности, а полноценным фактором устойчивого и справедливого правопорядка в условиях цифровой эпохи.

1.3 Параметризация использования искусственного интеллекта в правоохранительной деятельности

В связи с внедрением технологий ИИ в сферу государственного управления и обеспечения правопорядка возникает объективная потребность в разработке универсальных и одновременно гибких критериев допустимости алгоритмически опосредованных решений. Особенно остро эта проблема проявляется в контексте правоохранительной деятельности, где любое технологическое вмешательство сопряжено с потенциальным затрагиванием основополагающих прав и свобод личности. В связи с этим систематическая параметризация ИИ – как концептуальный и прикладной подход – приобретает фундаментальное значение, выходя за пределы узкотехнического дискурса и переходя в сферу юридической теории, философии права и институционального проектирования. Теоретической основой предлагаемого подхода выступают положения двух взаимодополняющих концептуальных рамок: теории процедурной справедливости и подхода к праву как инструменту управления рисками. Обе теории позволяют рассматривать алгоритмическое регулирование не как нейтральную технологическую инновацию, а как социально чувствительный процесс, требующий нормативной верификации, институциональной прозрачности и воспроизводимой логики принятия решений.

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 [184]. Как отмечает Т. Тайлер: «Процедурная справедливость – это восприятие людьми справедливости процессов, с помощью которых принимаются решения и разрешаются споры [185]». 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 дискриминации и нормативная обоснованность, играют решающую роль в легитимации ИИ-систем, позволяя согласовать 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 неопределённости, право должно выполнять не только функцию нормоустановления, но и функцию минимизации институциональных рисков [186], [187]. По этой логике параметризация ИИ выступает как способ введения контролируемых границ технологической неопределённости. Каждая категория параметров (точность, надёжность, интерпретируемость, справедливость) может быть понята как нормативный предел, за который алгоритм не имеет права выходить. Параметризация позволяет задать формализованные индикаторы допустимого уровня риска, тем самым создавая основу для регуляторного вмешательства. Например, если ИИ-система демонстрирует высокий уровень ложноположительных решений, выходящий за пределы допустимой нормы, это может служить основанием для её приостановки, доработки или отклонения от внедрения. Таким образом, параметризация функционирует как правовой фильтр, предотвращающий включение в правоохранительный процесс алгоритмов, не соответствующих критериям допустимого риска и нормативной устойчивости. Особенно важно подчеркнуть, что в теории управления рисками акцент смещается с абсолютной эффективности на допустимость действия в условиях неопределённости. Это значит, что даже высокоэффективный алгоритм может быть признан нежелательным, если он сопряжён с непрозрачными источниками ошибок, социальной дискриминацией или технической нестабильностью. Системная параметризация позволяет заранее задать набор ограничителей и критериев, определяющих порог принятия таких решений,

тем самым обеспечивая баланс между инновацией и правовой предсказуемостью.

Интеграция подходов процедурной справедливости и управления рисками позволяет сконструировать комплексную параметризационную модель, ориентированную на соблюдение как технологических, так и правовых стандартов. В её основе лежит представление о параметре не только как о числовом индикаторе, но как о правовом и этическом ориентире, встраивающем алгоритмические решения в пространство институциональной подотчётности. Так, количественные параметры (точность, полнота, стабильность) обеспечивают метрическую верификацию модели и её соответствие инженерным критериям. Качественные параметры (интерпретируемость, правовая релевантность, этическая допустимость) обеспечивают нормативную приемлемость решений. Аналитические параметры (способность к обобщению, устойчивость к ошибкам в условиях неполных данных, адаптивность к контексту) отражают когнитивную гибкость модели. Показатели надёжности и масштабируемости служат индикаторами эксплуатационной состоятельности алгоритма и его способности функционировать в изменяющейся институциональной среде. Вместе они формируют архитектуру правомерного алгоритмического регулирования, в которой эффективность не противостоит справедливости, а соотносится с ней через систему параметров и нормативных допущений.

На практике подобная параметризационная модель может быть использована при нормативном допуске ИИ-систем в разные сферы правоохранительной деятельности – от оперативно-розыскной аналитики и цифрового профилирования до автоматизации уголовного преследования и распределения следственной нагрузки. При этом каждая система ИИ должна сопровождаться пакетом параметров, подтверждённых тестированием, аудитом и экспертной оценкой, с последующим внесением в реестр допустимых моделей. Таким образом создаётся инфраструктура алгоритмической подотчётности, аналогичная сертификации экспертных методик или процессуального допуска доказательств в суде. Внедрение такой модели позволит не только формализовать границы допустимости ИИ, но и повысить доверие общества к технологиям, снижая риски технологической стигматизации и правового нигилизма. Кроме того, параметризация служит инструментом превентивного регулирования, позволяя не дожидаться правонарушения или ошибки, а работать на опережение, исключая заранее потенциально недопустимые технологические решения.

Интеграция подходов процедурной справедливости и управления рисками позволяет сконструировать комплексную параметризационную модель, ориентированную на соблюдение как технологических, так и правовых стандартов. В её основе лежит представление о параметре не только как о числовом индикаторе, но как о правовом и этическом ориентире, встраивающем алгоритмические решения в пространство институциональной подотчётности. Комплексное использование этих параметров позволяет сформировать полноценную оценочную матрицу, в которой эффективность

ИИ трактуется не в узкофункциональном, а в нормативно-институциональном смысле – как совокупность технологической продуктивности, социальной справедливости и правовой допустимости. Тем самым параметризация превращается в ключевое условие правомерного, обоснованного и этически выверенного внедрения ИИ в правоохранительную деятельность.

Как справедливо подчёркивают Д.А. Степаненко и соавторы, перед современным правоведением, особенно в тех его отраслях, которые ориентированы на практическое применение и непосредственное взаимодействие с социальными процессами, неизменно стоит задача переосмысления и совершенствования применяемого методологического инструментария. Указанная необходимость обусловлена стремительной эволюцией общественных и институциональных реалий, требующих от правовых систем способности к адаптации, инновационной трансформации и гибкому реагированию на новые вызовы. В этом контексте развитие юридических механизмов, включая их интеграцию с цифровыми технологиями, выступает не просто как направление модернизации, а как императив, обеспечивающий устойчивость и функциональную релевантность правовой регуляции в условиях постиндустриальной динамики [188].

В трудах Н. Гарупы акцентируется внимание на том, что оценка результативности деятельности правоохранительных органов не может ограничиваться юридическими или формально-статистическими категориями, она должна опираться также на принципы экономической рациональности. Исследователь исходит из предпосылки, согласно которой каждое управленческое или принудительное воздействие должно оцениваться с точки зрения соотношения затрат и достигнутого общественного эффекта. В условиях ограниченности ресурсов чрезмерное применение карательных мер не только ведёт к значительным финансовым и социальным издержкам, но и способно оказаться контрпродуктивным, подрывая общественное доверие к институтам правопорядка. В то же время недооценка необходимого уровня вмешательства чревата увеличением уровня преступности и ослаблением превентивного потенциала государства. Таким образом, по мысли Гарупы, правоохранительная политика должна быть соотнесена с логикой предельной эффективности: ресурсы следует перераспределять таким образом, чтобы достигался наибольший общественный эффект при минимально допустимых издержках [189].

Р. Бхарати обосновывает, что применение ИИ в деятельности правоохранительных органов представляет собой качественно новый этап в развитии управленческих и аналитических механизмов, направленных на преодоление институциональных перегрузок. Согласно его позиции, интеграция интеллектуальных алгоритмов в процессы обработки поступающих материалов, стратегического распределения ресурсов и сокращения административных издержек формирует условия для существенного повышения функциональной результативности и операционной устойчивости всей системы. Эти технологические преобразования не следует рассматривать как второстепенные инновации;

напротив, они обладают потенциалом структурного переосмысления механизма функционирования правоохранительных институтов, в частности в части разрешения системных проблем, таких как перегрузка следственных подразделений и хронический дефицит квалифицированных кадров.

Ключевым преимуществом ИИ в этом контексте выступает его способность к высокоскоростной обработке масштабных объёмов неструктурированных данных и выявлению латентных закономерностей, которые зачастую оказываются недоступными в рамках классических методов аналитики. Такая технологическая возможность не только расширяет интеллектуальный потенциал правоприменительных практик, но и способствует переходу к более взвешенным, логически непротиворечивым и институционально согласованным решениям на различных стадиях оперативно-розыскной и процессуальной деятельности. В перспективе подобная алгоритмическая реконфигурация может обеспечить повышение уровня транспарентности, воспроизводимости и нормативной обоснованности решений, одновременно минимизируя риски субъективных искажений. Это делает ИИ не просто вспомогательным техническим средством, а полноправным компонентом обновлённой архитектуры правоохранительного управления [190].

В рамках научных разработок, посвящённых цифровой трансформации уголовно-процессуальной деятельности, Д.В. Бахтеев (Воронков) подчёркивает необходимость придания алгоритмизированным элементам правоприменения черт нормативной рациональности. Согласно его позиции, как действия субъектов уголовного процесса, так и функционирование цифровых решений, интегрированных в соответствующие институциональные контуры, должны быть организованы в соответствии с принципами логической обоснованности, структурной последовательности и целесообразности. Под рациональностью в данном контексте понимается не только соответствие внутренней логике процедур, но и их сопряжённость с правовыми принципами, критериальной воспроизводимостью и устойчивостью к произвольным отклонениям. Это требование в равной степени относится как к человеческому элементу правоприменения, так и к интеллектуальным системам, предназначенным для поддержки процессуальных решений, будь то в форме аналитических платформ, алгоритмов оценки рисков или систем рекомендательного типа.

Построение надёжных механизмов цифрового сопровождения деятельности правоохранительных органов возможно лишь при условии, если алгоритмы будут разрабатываться и применяться на базе формализованных параметров рациональности, исключающих спонтанность, неопределённость и зависимость от внеправовых факторов. Такая рационализация предполагает не абстрактное стремление к технологической эффективности, а сознательное стремление к институциональной и правовой воспроизводимости действий, что является основой процедурной легитимности и доверия к алгоритмическому правоприменению [191].

Канадский исследователь В. Чайо последовательно развивает концепт отказа от универсалистских подходов при определении роли ИИ и человека в процессе принятия решений в сфере правоохранительной деятельности. По его мнению, невозможно сформулировать однозначный нормативный принцип, в соответствии с которым на всех этапах правоприменительного процесса предпочтение должно отдаваться либо исключительно алгоритмическим системам, либо исключительно субъективному усмотрению человека. Каждая стадия требует отдельного анализа с учётом специфики поставленных задач, уровня допустимой неопределённости и вероятности ошибок.

В. Чайо предлагает осуществлять оценку применимости различных подходов через призму параметров точности, таких как доля ложноположительных и ложноотрицательных решений, а также их взвешенное соотношение. Такой подход позволяет с высокой степенью эмпирической достоверности сравнивать решения, принимаемые с использованием ИИ, и суждения, формируемые на основе профессионального опыта и внутреннего убеждения представителей правоохранительной системы. В качестве показательной ситуации рассматривается сравнение алгоритма оценки риска повторного правонарушения с судебным усмотрением, в рамках которого ключевыми становятся два аспекта: вероятность проявления расовой предвзятости и уровень прогностической точности. Принятие решения в подобных условиях может быть значительно облегчено, если один подход превосходит другой по обеим метрикам или хотя бы по одной из них при сопоставимом результате по второй.

Тем не менее, подчёркивает исследователь, даже при наличии статистического преимущества алгоритмических решений окончательное определение допустимого компромисса между точностью и этической нейтральностью не может быть сведено к техническому выбору. Это уже политико-правовой вопрос, находящийся в сфере общественной морали и социальной ответственности. Например, алгоритм, демонстрирующий высокую точность, но обладающий встроенным уклоном в отношении определённых категорий граждан, может быть отвергнут в пользу менее точной, но более справедливой модели. Таким образом, В. Чайо делает акцент на необходимости широкой общественной легитимации решений о внедрении ИИ в практику правоохранительных органов, подчёркивая, что подобные решения должны быть основаны не только на вычислительной эффективности, но и на общепринятых ценностях правовой справедливости и социальной допустимости [192].

В рамках критического переосмысления оснований алгоритмического правоприменения Б. Харкорт предлагает парадоксальную, на первый взгляд, альтернативу – институционализированную рандомизацию как форму принятия решений в контексте деятельности правоохранительных органов и назначения уголовных санкций. С его точки зрения, стремление к максимизации формальной рациональности через автоматизацию и алгоритмизацию может, вопреки ожиданиям, не устранить предвзятости, а

напротив – воспроизвести и зафиксировать существующие социальные и правовые искажения в цифровом формате. Рандомизация в данном случае предлагается не как отказ от логики, а как способ нейтрализации структурных перекосов, которые укореняются в системах, опирающихся на исторически накопленные данные и предопределённые правила принятия решений [193].

Данная концепция обостряет вопрос о сущностных критериях оценки эффективности ИИ в сфере правоприменения. Если в инженерном дискурсе эффективность традиционно связывается с показателями точности, скорости и надёжности, то в правовом контексте к этим метрикам добавляются такие качественные характеристики, как справедливость, нейтральность и социальная допустимость. В частности, важнейшими индикаторами становятся степень предвзятости и уровень соответствия базовым принципам равенства перед законом.

В этой связи подчеркивается, что ИИ, внедряемый в практику правоохранительных органов, не должен воспроизводить или усиливать уже существующие формы дискриминации – будь то на расовой, гендерной, этнической или социально-экономической основе. Алгоритмическая справедливость в данном контексте предполагает наличие встроенных механизмов контроля и коррекции предвзятости, а также нормативно закреплённую возможность независимой оценки и пересмотра решений, принятых при участии автоматизированных систем. Таким образом, с точки зрения Б. Харкорта, переход к цифровой рациональности должен сопровождаться не только технологической модернизацией, но и глубоким институциональным переосмыслением оснований справедливого правоприменения, в рамках которого допустимость автоматизированных решений определяется не их скоростью или точностью, а их соответствием этическим и правовым критериям легитимности.

Одним из ключевых критериев, подлежащих обязательному учёту при оценке пригодности ИИ к интеграции в процессы правоприменения, выступает его масштабируемость. Речь идёт о способности системы сохранять стабильность, функциональную целостность и допустимый уровень производительности в условиях увеличения объёма обрабатываемых данных, роста нагрузки и расширения организационной инфраструктуры. По мере того, как цифровые платформы проникают в глубинные слои административно-управленческой деятельности, возрастает значимость гибкости архитектуры ИИ-систем и их способности адаптироваться к изменяющимся параметрам среды – от количества пользователей и подключённых баз до сложности оперативных задач [194].

Именно в этом контексте особо показательной представляется позиция С.А. Курочкина, который подчёркивает, что эффективность судебной защиты, обеспечиваемой с использованием ИИ, может рассматриваться как центральное условие его легитимного применения в таких юрисдикционных формах, как административное, гражданское и арбитражное судопроизводство. Данный тезис логично экстраполируется и на более широкий контекст – деятельность правоохранительных органов в целом, где

значимость эффективности, устойчивости и масштабируемости ИИ-систем приобретает ещё более критическое значение в силу оперативного характера задач, наличия высокой правовой чувствительности и непрерывной работы с разнообразными массивами данных [195].

Относительно определения производительных характеристик систем можно рассмотреть следующее мнение: «Сравним алгоритм, ″заточенный″ на точность, и другой, который не должен вносить больший расовый перекос (входные данные ограничивают выходные данные). Безусловно, подобные сравнения алгоритмов покажут, на какие компромиссы нужно идти для внедрения того или иного подхода. А вот вопрос, на какой компромисс идти, уже выходит за область технического решения, переходя в область морали, и нуждается в политическом решении, да еще таком, с которым согласится общественность» [196].

Следовательно, оценка масштабируемости в условиях внедрения ИИ в правоохранительную практику должна включать в себя не только технико-функциональные параметры, но и институциональные показатели – такие как способность системы интегрироваться в уже существующие процессы без нарушения процедурной логики, расширяться без снижения правовой предсказуемости и поддерживать баланс между технологической автономией и нормативной подконтрольностью.

Таким образом, представляется обоснованным утверждение, что внедрение ИИ в деятельность правоохранительных органов должно сопровождаться системной параметризацией, выступающей в качестве базового инструмента для многоуровневой оценки его функциональной результативности, этической приемлемости и эксплуатационной надёжности. Речь идёт не о формальной технико-статистической процедуре, а о содержательно насыщенной методике, обеспечивающей как внутреннюю согласованность алгоритмов, так и их соответствие внешним – правовым и общественным – ожиданиям.

В рамках предлагаемого подхода к параметризации эффективности применения ИИ в правоохранительной деятельности целесообразно выделить две ключевые группы оценочных показателей. Первая группа включает количественные метрики, предоставляющие объективные, статистически воспроизводимые данные о результативности алгоритмов. К ним относятся показатели точности, полноты, прецизионности, средней продолжительности безотказной работы, доверительного интервала, а также устойчивости к внешним и внутренним воздействиям. Вторая категория охватывает качественные параметры, отражающие степень интерпретируемости решений, их соответствие нормам юридической логики и общепринятым принципам справедливости. Внутри этой категории особую значимость приобретают так называемые аналитические параметры, характеризующие способность алгоритма к смысловой реконструкции, обобщению, адаптации к контексту и квазииндуктивной обработке информации.

Комплексное использование этих параметров позволяет сформировать полноценную оценочную матрицу, в которой эффективность ИИ трактуется

не в узкофункциональном, а в нормативно-институциональном смысле – как совокупность технологической продуктивности, социальной справедливости и правовой допустимости. Тем самым параметризация превращается в ключевое условие правомерного, обоснованного и этически выверенного внедрения ИИ в правоохранительную деятельность.

1. Количественные показатели эффективности

В системе количественной оценки эффективности применения ИИ в правоохранительной деятельности важнейшую роль играют метрики, предоставляющие объективные, статистически воспроизводимые показатели результативности алгоритмов.

Одним из базовых параметров является *частота обнаружения* (ЧО), определяемая как доля корректно выявленных инцидентов правонарушений или угроз в общем потоке проанализированных ситуаций. Например, если система видеонаблюдения с функцией ИИ за сутки обработала 10 тысяч эпизодов, из которых 100 содержали признаки противоправного поведения, и 85 из них были корректно зафиксированы, то показатель ЧО составит 85%. Этот индикатор демонстрирует чувствительность алгоритма к криминогенным паттернам в исходных данных и позволяет судить о его способности выполнять функцию своевременного предупреждения рисков [197], [198].

Неотъемлемо связанный с ним показатель – это *частота ложных срабатываний* (ЧЛС), фиксирующая долю ситуаций, в которых ИИ ошибочно интерпретирует поведение как подозрительное или опасное. К примеру, если та же система зафиксировала 300 тревожных эпизодов, но из них 215 оказались ложными (например, человек наклонился, чтобы поднять вещь, а система распознала это как драку), то ЧЛС составит около 71%. Высокий уровень ложноположительных результатов приводит к перерасходу ресурсов и может дискредитировать саму систему в глазах оперативных сотрудников [199], [200], [201].

Третьей метрикой является *время отклика* (ВО), то есть временной промежуток между поступлением входных данных и генерацией системой релевантного аналитического вывода. В ситуации, когда ИИ установлен на городских камерах для автоматического выявления оставленных предметов в общественных местах, критически важно, чтобы система реагировала не через 5-10 минут, а в течение секунд. Если, к примеру, на платформе метро осталась сумка, а система срабатывает через 8 секунд после её появления в кадре – это и будет значением ВО [197, p. 21-1-21-16], [202].

Особое значение среди количественных показателей эффективности функционирования ИИ в правоохранительной деятельности приобретает такой параметр, как *эффективность раскрытия дел* (ЭРД). Данный показатель позволяет оценить прикладную результативность использования интеллектуальных систем по сравнению с традиционными методами оперативно-розыскной и следственной работы. По сути ЭРД отражает долю уголовных дел, успешно раскрытых при непосредственном участии ИИ, в общем количестве расследованных дел определённой категории в заданный

временной период. Формально он может быть выражен следующей формулой: ЭРД = (число раскрытых дел с участием ИИ / общее число раскрытых дел данной категории) × 100% [203].

Например, в делах о квартирных кражах ИИ может автоматически сопоставлять временные интервалы отключения сигнализации с геолокационными данными мобильных устройств, находившихся вблизи объекта. Такой подход позволяет в кратчайшие сроки сузить круг подозреваемых и ускорить возбуждение уголовного дела.

В делах о киберпреступлениях система ИИ способна анализировать большие объёмы сетевого трафика, выявляя подозрительные транзакции и аномальное поведение пользователей. Так, если при расследовании эпизодов фишинга ранее требовалось вручную просматривать тысячи записей веб-активности, то теперь интеллектуальный алгоритм способен отобрать из них те, которые совпадают по структуре, ключевым словам и IP-логике. Это сокращает сроки расследования с недель до нескольких часов.

В делах, связанных с мошенничеством в сфере госзакупок, ИИ может анализировать структуру связей между поставщиками, участниками тендеров и госорганами. Например, когда алгоритм выявляет цепочку взаимозависимых юридических лиц, участвующих в конкурсе с минимальным шагом понижения цены, это позволяет установить признаки сговора, которые сложно выявить вручную.

Ещё одним наглядным примером является использование ИИ при расследовании нападений в общественных местах. Если раньше для установления личности нападавшего по видеозаписи требовалось вручную сверять кадры с паспортной базой или запрашивать розыск, то сейчас система распознавания лиц может мгновенно найти совпадение в базе биометрии и выдать точные данные. Это увеличивает раскрываемость по горячим следам и повышает общую динамику успешного преследования [204].

Кроме того, в делах о семейно-бытовом насилии ИИ может обрабатывать жалобы, поступающие на горячие линии, выделяя из них наиболее опасные ситуации по совокупности ключевых слов и интонации голоса. Это позволяет своевременно направлять наряды полиции, предотвращая эскалацию конфликта и в ряде случаев спасая жизни.

Применение этой метрики возможно при наличии сопоставимых массивов данных. Так, например, если за квартал в городе было зарегистрировано 500 преступлений, связанных с кражами автотранспорта, из которых 240 удалось раскрыть с использованием интеллектуальных систем видеонаблюдения, интегрированных с программой распознавания номерных знаков и алгоритмами маршрутизации, то показатель ЭРД составит 48%. Это свидетельствует о высокой результативности применения алгоритмического инструментария в решении конкретной правоохранительной задачи. Аналогично в рамках дел о телефонных и интернет-мошенничествах, где ранее доля раскрытых эпизодов не превышала 20-25%, внедрение ИИ, способного анализировать транзакционные данные и выявлять аномалии в поведении картодержателей, к примеру, может увеличить показатель ЭРД до

40% и выше. Подобная динамика отражает не просто количественное улучшение статистики, но и качественный сдвиг в методике уголовного преследования.

Кроме того, показатель ЭРД позволяет проводить территориальные или институциональные сравнительные исследования. Например, в двух районах с сопоставимым уровнем преступности может быть зафиксирована значимая разница в уровне раскрываемости дел, если в одном из них задействован ИИ-модуль анализа IMEI-идентификаторов мобильных устройств, украденных в результате уличных грабежей. Такая дельта в показателях раскрываемости – при прочих равных условиях – свидетельствует о высокой степени влияния цифрового компонента на эффективность правоохранительной деятельности.

При этом важно учитывать, что сам по себе рост ЭРД не должен интерпретироваться исключительно как заслуга ИИ: методически корректное измерение требует фиксации дополнительного влияния иных факторов, таких как кадровое обеспечение, сезонность, интенсивность правоприменительной активности и др.

Следует согласиться с позицией Д.В. Бахтеева (Воронкова), который справедливо указывает на то, что одним из значимых критериев оценки эффективности систем искусственного интеллекта является сопоставление их результатов с качеством выполнения аналогичных задач человеком. По результатам проведённого анкетирования экспертов установлено, что в среднем специалисты по почерковедческой экспертизе распознавали случаи подделки подписи в 69 % случаев. Соответственно, если система ИИ демонстрирует показатель выше данного значения, это свидетельствует о её высокой операционной надёжности и обоснованности использования в правоохранительной деятельности [191, с. 179-184].

Таким образом, показатель ЭРД может служить ключевым индикатором не только технологической результативности, но и стратегической целесообразности масштабирования алгоритмических решений в правоохранительных органах. При правильной методологической фиксации он позволяет выстроить систему сравнительной оценки внедрённых ИИ-модулей, повысить обоснованность управленческих решений и, в конечном счёте, способствовать формированию цифровой доказательной экосистемы в сфере обеспечения правопорядка.

Еще одним из ключевых количественных индикаторов, определяющих надёжность функционирования ИИ в правоохранительной деятельности, является показатель *точности*. Эта метрика отражает способность алгоритма правильно классифицировать события, объекты или поведенческие модели в рамках заранее определённого набора данных. По существу, точность фиксирует долю корректно принятых решений – как в части положительных, так и отрицательных результатов – среди всех случаев, подвергшихся обработке [205].

Формально этот показатель рассчитывается по следующей формуле: Точность = (ИП + ИО) / (ИП + ЛП + ИО + ЛО), где ИП – число истинно положительных случаев, ИО – истинно отрицательных, ЛП –

ложноположительных, ЛО – ложноотрицательных. Иными словами, точность определяется как отношение суммы верно классифицированных положительных и отрицательных случаев к общему количеству всех проанализированных ситуаций.

Например, если система, установленная в транспортном узле, анализирует потоки видеонаблюдения и из тысячи записей верно интерпретирует 850 (определяя наличие или отсутствие признаков правонарушений), её точность составляет 85 %. Такой показатель считается приемлемым для задач предварительного мониторинга, где критична скорость и масштаб охвата.

В другой практической ситуации, связанной с анализом аудиоданных, например, при прослушивании обращений на горячую линию, система может эффективно выделять тревожные сигналы среди общего массива записей. Допустим, из 200 входящих звонков ИИ точно определил 180 как подлежащие реагированию и при этом ошибочно обозначил 10 нейтральных разговоров как критические. В таком случае уровень точности составит около 90 %, что особенно важно в условиях, где человек-оператор может быть ограничен в ресурсах или подвержен усталости.

Кроме того, показатель точности применим при работе с биометрическими данными. В ситуациях, когда ИИ анализирует большое количество видеокадров – например, в периметре охраны важных объектов или вокзалов – и из 10 тысяч единиц визуальной информации правильно обрабатывает 9 тысяч 200, можно говорить о точности на уровне 92 %. Это повышает обоснованность доверия к алгоритму со стороны сотрудников правоохранительных органов, особенно при решении задач, связанных с розыском и контролем доступа.

Как отмечают М.Б. Садыков и соавторы: «ИИ-системы в правоохранительных органах должны быть примером надежности и точности. В конце концов, кому нужен сотрудник правоохранительных органов, которому нельзя доверять? Точно так же, как отсутствие информации о безопасности может повлиять на целостность вашей точки доступа, любые ошибки в алгоритме или обучающих данных могут привести к высокому риску принятия несправедливых решений» [206].

Однако важно учитывать, что высокая точность сама по себе не является универсальным показателем эффективности. Существует риск, что алгоритм, стремясь избегать ошибок, будет излишне осторожен и пропускать важные случаи, что приведёт к снижению показателя полноты. Таким образом, оценка точности должна сопровождаться анализом других метрик, в частности интегрального показателя F1, который позволяет сбалансировать соотношение между количеством правильно выявленных случаев и объёмом пропущенной информации.

В конечном итоге точность представляет собой один из наиболее наглядных и легко интерпретируемых параметров оценки интеллектуальных систем, используемых в правоохранительной сфере. Её корректная интерпретация позволяет установить границы допустимости применения ИИ

в тех или иных оперативных условиях и обосновать необходимость их адаптации или доработки с точки зрения правовой и этической приемлемости.

Наряду с общей точностью важным показателем эффективности интеллектуальной системы является показатель *прецизионности*. Прецизионность отражает долю истинно положительных классификаций относительно всех классификаций, определённых системой как положительные. Иными словами, прецизионность позволяет определить, насколько среди всех срабатываний системы на наличие правонарушения преобладают действительно верные случаи [207].

Формула расчёта выглядит следующим образом: Прецизионность = ИП / (ИП + ЛП), где ИП – число истинно положительных классификаций, а ЛП – количество ложноположительных результатов.

Практический пример применения этой метрики может выглядеть следующим образом: если система наблюдения за периметром охраняемого объекта за сутки зарегистрировала 100 тревожных событий, из которых 80 оказались реальными угрозами, а 20 – ошибочными тревогами (например, движением животных), то прецизионность данной системы составит 80 %. Высокий уровень прецизионности критически важен для обеспечения оперативной эффективности и оптимизации реагирования сил правопорядка.

Прецизионность особенно важна в тех сценариях правоохранительной деятельности, где ложные срабатывания могут повлечь за собой серьёзные последствия: необоснованную проверку, задержание или иные ограничения прав граждан. Например, в системах автоматического распознавания лиц в общественных местах высокий уровень прецизионности позволяет минимизировать случаи ошибочной идентификации и избежать репутационных и правовых рисков для правоохранительных органов.

Однако следует учитывать, что высокая прецизионность при низкой полноте может свидетельствовать о чрезмерной осторожности алгоритма, при которой многие реальные инциденты остаются незамеченными. Поэтому для всесторонней оценки эффективности интеллектуальной системы необходимо анализировать прецизионность в совокупности с показателем полноты и интегральной F1-мерой.

Таким образом, прецизионность является одним из наиболее значимых количественных индикаторов надёжности ИИ в правоохранительной деятельности. Её комплексная оценка в сочетании с другими параметрами позволяет объективно определить пригодность алгоритма к применению в практической деятельности, выявить возможные риски его использования и сформировать рекомендации по адаптации или доработке цифровых систем в целях обеспечения баланса между эффективностью и соблюдением прав человека.

Наряду с общей точностью важным показателем эффективности интеллектуальной системы является показатель *полноты*. Полнота отражает долю истинно положительных результатов относительно всех фактических положительных случаев в данных. Иными словами, полнота позволяет

определить, насколько хорошо система ИИ выявляет все случаи реального наличия правонарушений или угроз [208].

Формула расчёта полноты выглядит следующим образом: Полнота = ИП / (ИП + ЛО), где ИП – число истинно положительных результатов, а ЛО – количество ложноотрицательных случаев.

Практический пример применения этой метрики может выглядеть следующим образом: если система мониторинга видеонаблюдения в течение суток имела 120 реальных случаев подозрительного поведения и при этом верно зафиксировала 90 из них, пропустив 30, то показатель полноты составит 75 %. Это значит, что четверть реальных инцидентов остались без автоматического обнаружения, что может быть критическим фактором для оценки надёжности и допустимости применения такой системы в правоохранительной деятельности.

Другой пример может быть связан с использованием ИИ в системах контроля пересечения границ. Если из 50 попыток нелегального пересечения, зафиксированных по данным наземных сенсоров и дронов, система обнаружила лишь 35, полнота её работы составит 70 %. Это свидетельствует о необходимости либо доработки алгоритма, либо усиления систем внешнего контроля.

Также полнота важна при анализе сообщений о правонарушениях, поступающих через цифровые платформы. Например, при автоматическом анализе жалоб на кибербуллинг в социальных сетях алгоритм может быть настроен на высокую полноту: если за сутки было размещено 200 обращений с признаками агрессии и система корректно выявила 180 из них, полнота работы составит 90 %, что допустимо для обеспечения своевременной реакции правоохранительных органов.

Полнота приобретает особую значимость в сценариях, где упущение реальной угрозы может иметь тяжёлые последствия. Например, в системах автоматического мониторинга за общественной безопасностью, направленных на выявление признаков насильственного поведения или террористической активности, высокий уровень полноты является приоритетной задачей. Даже при определённой допустимой доле ложных срабатываний критически важно минимизировать случаи, когда потенциально опасное событие остаётся незамеченным.

Тем не менее, чрезмерная ориентация исключительно на повышение полноты без учёта других метрик может привести к лавинообразному росту количества ложных тревог, что негативно скажется на оперативной деятельности сотрудников правоохранительных органов. Поэтому полнота должна оцениваться в комплексе с прецизионностью и F1-мерой, обеспечивая сбалансированную характеристику качества работы алгоритма.

Таким образом, полнота является одним из важнейших количественных индикаторов, позволяющих оценить способность ИИ-систем к выявлению реальных инцидентов в правоохранительной практике. Её комплексный анализ совместно с другими параметрами позволяет более обоснованно решать вопрос о допустимости и масштабируемости внедрения

алгоритмических решений в деятельность по обеспечению общественного порядка и безопасности.

Среди интегральных показателей, применяемых для оценки эффективности интеллектуальных систем, особое место занимает *F1-мера*. Данный параметр представляет собой среднее гармоническое между показателями прецизионности и полноты, обеспечивая тем самым сбалансированную оценку качества функционирования алгоритма [209].

Формула расчёта F1-меры выглядит следующим образом: F1 = 2 × (Прецизионность × Полнота) / (Прецизионность + Полнота). В отличие от отдельных метрик точности или полноты, F1-мера позволяет комплексно учитывать как способность системы минимизировать ложные срабатывания, так и её умение охватывать все фактические случаи правонарушений или угроз.

Практическое значение F1-меры особенно проявляется в ситуациях, где необходимо найти оптимальный баланс между риском пропуска инцидентов и риском избыточных тревог. Например, если система видеонаблюдения на массовом мероприятии демонстрирует прецизионность в 80 % и полноту в 70 %, то F1-мера составит около 74 %, отражая сбалансированное качество её работы в реальных условиях высокой социальной чувствительности.

В другом случае, при анализе сетевой активности в целях выявления киберугроз, алгоритм может достигать высокой полноты (например, 90 %) за счёт снижения прецизионности до 60 %. В таком случае F1-мера даст усреднённую объективную оценку функционирования системы и укажет на необходимость корректировки её параметров для повышения практической применимости.

F1-мера приобретает особую практическую важность в процессе интеграции ИИ в правоохранительную деятельность, поскольку позволяет одновременно минимизировать риск пропуска серьёзных угроз и избежать чрезмерной перегрузки оперативных служб вследствие многочисленных ложных срабатываний. Например, в системах автоматизированного распознавания лиц на вокзалах или стадионах высокая F1-мера свидетельствует о том, что система одновременно эффективно выявляет разыскиваемых лиц и минимизирует ошибки при идентификации обычных граждан. Именно в условиях правоохранительной деятельности, где цена ошибки может быть крайне высокой как для общества, так и для конкретных лиц, F1-мера становится критическим инструментом, позволяющим выстроить объективную оценку качества алгоритмических решений.

Кроме того, F1-мера позволяет выявить скрытые недостатки систем, которые при высоком значении отдельной прецизионности или полноты могли бы остаться незамеченными. Так, алгоритм, демонстрирующий высокую прецизионность, но низкую полноту, будет пропускать значительное количество правонарушений, в то время как высокий уровень полноты при низкой прецизионности приведёт к чрезмерной нагрузке на оперативные службы. F1-мера, объединяя оба аспекта, служит универсальным инструментом оценки реальной практической ценности интеллектуальных

решений, особенно в правоохранительной среде, где необходимо одновременно обеспечивать безопасность и соблюдать принципы справедливости, правовой определённости и уважения прав личности.

Наконец, в условиях комплексных угроз и динамично меняющейся оперативной обстановки использование F1-меры позволяет создавать системы ИИ, ориентированные не на узковедомственную эффективность, а на достижение общественно значимых целей – защиты прав и свобод граждан, поддержания общественного порядка и обеспечения безопасности в соответствии с принципами справедливости и пропорциональности.

Таким образом, F1-мера представляет собой один из наиболее универсальных и сбалансированных индикаторов, применяемых для всесторонней оценки качества работы интеллектуальных систем в правоохранительной деятельности. Её использование в практике анализа позволяет не только повысить объективность выводов о пригодности алгоритмов, но и сформировать обоснованные рекомендации по их доработке, адаптации и масштабированию в интересах эффективного и правомерного обеспечения общественной безопасности.

Среднее время между отказами является важным показателем надёжности функционирования интеллектуальных систем, внедряемых в правоохранительную деятельность. Этот параметр характеризует средний временной интервал между двумя последовательными сбоями или ошибками работы системы, измеряемый, как правило, в часах или днях. Чем выше значение среднего времени между отказами, тем более стабильной и предсказуемой считается работа алгоритма в реальных условиях эксплуатации [210].

Практическое значение данного показателя особенно велико в правоохранительной сфере, где перебои в функционировании ИИ-систем могут приводить к серьёзным последствиям: пропуску инцидентов, задержке оперативного реагирования, нарушению процессуальных сроков. Например, если система распознавания лиц на контрольных пунктах безопасности работает в среднем без ошибок 720 часов (30 дней), то такой показатель может считаться приемлемым для её применения в оперативной деятельности. В то же время, если система аварийно выходит из строя каждые 48 часов, это свидетельствует о необходимости её модернизации или замены.

Среднее время между отказами позволяет не только оценить устойчивость алгоритмических решений, но и прогнозировать расходы на техническую поддержку, планировать графики профилактического обслуживания и определять регламенты резервирования систем. В системах интеллектуального видеонаблюдения, автоматизированного анализа звонков на горячие линии, биометрической идентификации граждан высокое значение данного параметра напрямую коррелирует с эффективностью обеспечения общественной безопасности.

Таким образом, среднее время между отказами выступает одним из ключевых количественных индикаторов эксплуатационной надёжности ИИ-систем. Его регулярная оценка позволяет своевременно выявлять риски

деградации качества работы алгоритмов, оптимизировать техническую инфраструктуру правоохранительных органов и повышать уровень доверия к использованию цифровых технологий в обеспечении законности и общественного порядка.

Доверительный интервал является важной статистической мерой, применяемой для оценки степени уверенности в предсказаниях интеллектуальных систем. Он показывает диапазон значений, в пределах которого с заданной вероятностью (например, 95 %) находится истинное значение параметра, полученного в результате работы алгоритма. Чем уже доверительный интервал и чем выше уровень доверия, тем большей достоверностью обладают результаты прогноза [211], [212].

Проще говоря, если система прогнозирует вероятность совершения рецидива преступления для определённой группы лиц в диапазоне от 60 до 70 % с уровнем доверия 95 %, это означает, что в 95 из 100 аналогичных выборок реальная вероятность действительно будет находиться между 60 и 70 %. Такой подход позволяет не полагаться на одно фиксированное значение, а учитывать возможные колебания, делая выводы более обоснованными и надёжными.

В правоохранительной практике использование доверительного интервала критически важно при оценке рисков. Например, при прогнозировании вероятности совершения новых правонарушений лицами, находящимися под административным надзором, доверительный интервал помогает объективно судить о степени угрозы. Если два подозреваемых имеют одинаковую среднюю прогнозируемую вероятность рецидива – 65 %, но один имеет доверительный интервал от 63 до 67 %, а другой от 45 до 85 %, то очевидно, что первый прогноз намного надёжнее и позволяет принимать решение с меньшим риском ошибки.

Ещё один наглядный пример: в системе предиктивного патрулирования районов города алгоритм оценивает вероятность возникновения уличных правонарушений. Если для одного района предсказание составляет 20-25 % с доверительным интервалом 95 %, а для другого – 10-40 %, то при одинаковой средней вероятности первый район будет рассматриваться как более приоритетный для усиленного патрулирования, поскольку предсказание для него значительно стабильнее.

Таким образом, доверительный интервал служит фундаментальным инструментом для повышения обоснованности решений в правоохранительной деятельности, минимизации рисков ошибочных действий и оптимизации распределения ресурсов. Его правильное использование позволяет интегрировать интеллектуальные системы в процесс оперативно-розыскной и следственной работы без ущерба для прав граждан и правовой определённости.

Устойчивость к атакам является важным параметром оценки надёжности интеллектуальных систем, особенно в контексте их применения в правоохранительной деятельности. Этот показатель отражает способность алгоритма противостоять попыткам манипуляции или обмана, которые могут

быть предприняты злоумышленниками для искажения работы системы. Устойчивость оценивается, как правило, через тестирование на проникновение, создание специальных искусственных воздействий (adversarial attacks) и анализ сценариев обучающих атак (adversarial training).

Проще говоря, если система видеонаблюдения или распознавания лиц подвержена тому, что небольшое изменение изображения – например, изменение угла съёмки или наложение малозаметных меток – способно привести к неправильной идентификации подозреваемого, такая система считается уязвимой к атакам. Устойчивость в этом случае будет измеряться степенью сохранения точности распознавания при наличии подобных попыток манипуляций [213].

В правоохранительной практике проверка устойчивости критически важна. Например, если подозреваемый может с помощью определённого вида одежды, очков или маски обмануть систему биометрической идентификации и избежать задержания, это ставит под угрозу всю эффективность использования ИИ в оперативной деятельности. Поэтому тестирование на устойчивость должно входить в обязательный цикл проверки всех интеллектуальных систем перед их внедрением.

Наглядный пример: при обучении алгоритмов анализа аудиозаписей для выявления угроз в телефонных переговорах необходимо проверять, не удастся ли с помощью изменения тембра или наложения фонового шума обмануть систему и скрыть тревожные сигналы. Системы с высокой устойчивостью сохраняют способность правильно интерпретировать содержание даже при наличии подобных искажений.

Таким образом, устойчивость к атакам является одним из важнейших критериев качества интеллектуальных решений, используемых в обеспечении общественной безопасности. Её оценка позволяет предотвратить технологические риски, повысить доверие к алгоритмическим системам со стороны общества и обеспечить надёжность работы ИИ в критически значимых сферах правоохранительной деятельности.

Эффективность использования ресурсов является важнейшим показателем результативности применения интеллектуальных систем в правоохранительной деятельности. Этот параметр отражает способность ИИ-технологий сокращать объём человеческих трудозатрат, временных и финансовых расходов за счёт автоматизации рутинных процедур и оптимизации процессов принятия решений. Эффективность использования ресурсов обычно выражается через соотношение затрат на внедрение и эксплуатацию системы к достигнутым выгодам в виде ускорения работы, повышения раскрываемости, снижения затрат на обслуживание или уменьшения нагрузки на персонал [214].

Практическое значение этой метрики проявляется в самых разных аспектах правоохранительной деятельности. Например, автоматизация процесса первичного анализа заявлений о правонарушениях позволяет существенно сократить количество сотрудников, необходимых для ручной обработки обращений граждан. Если ранее на обработку 1000 заявлений

требовалось 20 человек, а с использованием ИИ – всего 5, ресурсная эффективность возрастает в четыре раза.

Другой пример: применение систем автоматического распознавания номерных знаков на въездах в населённые пункты. Ранее для контроля транспортных потоков требовались патрульные экипажи, несущие круглосуточное дежурство. Интеллектуальная система, фиксирующая нарушения автоматически, позволяет перераспределить силы оперативных подразделений на более сложные задачи, одновременно увеличивая охват и точность контроля.

Кроме того, системы автоматического анализа телефонных звонков на горячие линии, оснащённые модулями обработки естественного языка, позволяют в режиме реального времени сортировать поступающие сообщения по степени срочности. Это сокращает время реагирования на экстренные вызовы, а также снижает нагрузку на операторов колл-центров, освобождая их ресурсы для работы со сложными случаями.

Ещё один показательный пример – внедрение ИИ в процесс обработки видеодоказательств. Ранее для анализа многосуточных записей видеонаблюдения требовались значительные трудозатраты следственных групп. Применение интеллектуальных алгоритмов, способных в автоматическом режиме выделять подозрительные фрагменты (например, аномальное поведение, пересечение запрещённых зон), позволяет сократить продолжительность анализа с нескольких недель до нескольких дней, что существенно ускоряет расследование уголовных дел.

В сфере кибербезопасности ИИ используется для автоматизированного выявления вредоносной активности в корпоративных сетях правоохранительных органов. Это даёт возможность оперативно локализовать угрозы без необходимости постоянного ручного мониторинга со стороны специалистов ИТ-отделов, что также увеличивает ресурсную эффективность.

Ресурсная эффективность важна и в контексте финансового планирования. Например, если внедрение алгоритмов интеллектуального анализа видеонаблюдения позволяет за год предотвратить ущерб от преступлений на сумму, превышающую совокупные затраты на установку и эксплуатацию системы, это свидетельствует о положительном балансе и стратегической целесообразности вложений в ИИ.

Таким образом, эффективность использования ресурсов является одним из ключевых критериев оценки практической пользы внедрения ИИ в правоохранительные органы. Высокие показатели по этому параметру свидетельствуют не только о технологической зрелости решений, но и об их способности обеспечивать устойчивое развитие системы обеспечения правопорядка в условиях ограниченности бюджетных и кадровых ресурсов.

2. Качественные показатели эффективности

Качественные метрики оценивают неколичественные аспекты функционирования систем искусственного интеллекта, уделяя при этом внимание их социальной, этической и операционной приемлемости в условиях правоохранительной деятельности. В отличие от количественных

показателей, качественные индикаторы позволяют выявить глубинные закономерности восприятия, доверия и интеграции ИИ в процесс обеспечения правопорядка.

К основным направлениям качественной оценки относятся:

Индекс доверия населения представляет собой интегральный показатель, направленный на оценку уровня общественного доверия к системам искусственного интеллекта, внедряемым в деятельность правоохранительных органов. Этот индекс строится на основании данных, получаемых в результате регулярных опросов, социологических исследований и фокус-групп, в которых анализируется отношение граждан к использованию ИИ для обеспечения общественной безопасности [215].

Индекс доверия населения включает в себя такие компоненты, как восприятие честности алгоритмических решений, степень обеспокоенности возможными ошибками или предвзятостью ИИ, а также общий уровень уверенности населения в том, что новые технологии используются справедливо и в интересах общества. Шкала оценки может быть представлена в процентном выражении или по уровневым категориям (например, высокий, средний, низкий уровень доверия).

Практический пример применения индекса доверия населения может быть следующим: после внедрения системы распознавания лиц в общественных местах проводится опрос населения, в ходе которого выясняется, что 68% респондентов считают использование технологии оправданным и безопасным, 20% относятся к нему нейтрально, а 12% выражают недоверие или обеспокоенность. В этом случае индекс будет находиться на высоком уровне, что свидетельствует о социальной легитимности применяемой технологии.

Примерная методика расчёта индекса доверия населения может включать следующие этапы: проведение репрезентативных опросов с использованием шкал оценки доверия (например, от 1 до 5 баллов), последующая нормализация полученных данных и агрегирование их в сводный индекс. В дополнение к количественным оценкам могут учитываться качественные показатели – например, степень осведомлённости населения о работе ИИ-систем, уровень прозрачности процедур их внедрения, количество зарегистрированных жалоб и обращений граждан по вопросам использования алгоритмов. Для обеспечения объективности и репрезентативности результатов рекомендуется осуществлять расчёт индекса доверия населения с учётом региональных различий, социально-демографических характеристик и временной динамики. Такой подход позволяет выявлять скрытые закономерности и изменения в общественных установках. В частности, следует учитывать, что различные возрастные группы могут по-разному воспринимать внедрение ИИ в правоохранительную деятельность. К примеру, молодёжь, обладающая более высоким уровнем цифровой грамотности и склонная к восприятию инноваций, может демонстрировать большую готовность к принятию интеллектуальных систем и оценивает их использование более позитивно. Представители старших поколений,

напротив, могут проявлять повышенную настороженность и критичность, обусловленную меньшим доверием к автоматизированным процессам и большей приверженностью традиционным формам правоприменительной практики.

Индекс доверия населения позволяет отслеживать динамику общественного мнения во времени, выявлять проблемные зоны в восприятии ИИ и своевременно корректировать политику внедрения технологий для повышения их социальной приемлемости. Например, снижение показателя после серии негативных инцидентов, связанных с ошибочными задержаниями на основе алгоритмических предсказаний, будет сигналом для проведения дополнительных мер по повышению прозрачности систем и улучшению механизмов объяснения их решений.

Таким образом, индекс доверия населения играет ключевую роль в обеспечении баланса между технологическим прогрессом и защитой фундаментальных прав граждан, служит индикатором социальной устойчивости и способствует выстраиванию доверительных отношений между правоохранительными органами и обществом в условиях цифровой трансформации.

Оценка соответствия этическим нормам представляет собой качественную характеристику, отражающую степень соблюдения системой искусственного интеллекта таких фундаментальных принципов, как справедливость, подотчетность и уважение прав человека. Оценка обычно проводится посредством экспертных обзоров или специализированных аудиторских процедур.

Оценка соответствия этическим нормам представляет собой качественную характеристику, отражающую степень соблюдения системой ИИ таких фундаментальных принципов, как справедливость, подотчетность и уважение прав человека. Эта оценка направлена на выявление потенциальных рисков нарушения прав и свобод личности, возникающих вследствие автоматизированного принятия решений, а также на определение уровня соответствия работы системы установленным правовым и этическим стандартам. Оценка соответствия проводится посредством экспертных обзоров или специализированных аудиторских процедур, включающих комплексный анализ алгоритмических моделей, используемых данных и логики принятия решений. При проведении проверки особое внимание уделяется таким аспектам, как обоснованность и прозрачность критериев обработки информации, наличие механизмов оспаривания решений ИИ, обеспечение прав граждан на защиту персональных данных и соблюдение принципа недискриминации [216], [217].

Проверка ориентируется на несколько ключевых критериев, включая наличие документированных правил, регулирующих работу алгоритмов, наличие механизмов внутреннего контроля и этического аудита, уровней объяснимости решений, доступных для конечных пользователей, а также процедур защиты прав на обжалование и пересмотр автоматизированных

выводов, соблюдение стандартов международного права в области защиты прав человека.

Важной частью оценки является тестирование алгоритмов на предмет скрытой предвзятости по социально-демографическим признакам, что осуществляется посредством методики сравнительного анализа ошибок первого и второго рода среди различных категорий населения, а также проведения экспертного анализа потенциальных рисков необоснованного вмешательства в частную жизнь и непропорционального ограничения гражданских свобод.

Результаты оценки оформляются в виде заключения, в котором отражаются выявленные несоответствия, уровни их критичности и рекомендации по их устранению. При выявлении существенных нарушений этических принципов может приниматься решение о приостановлении эксплуатации системы до проведения необходимых корректирующих мероприятий.

Таким образом, оценка соответствия этическим нормам служит эффективным инструментом превентивного контроля, минимизации правовых рисков и обеспечения баланса между развитием технологий и защитой фундаментальных прав и свобод личности в условиях цифровизации правоохранительной деятельности.

Уровень удовлетворенности пользователей представляет собой качественную характеристику, направленную на оценку восприятия сотрудниками правоохранительных органов удобства использования, практической применимости, надёжности и эффективности систем ИИ в их профессиональной деятельности. Этот показатель отражает не только субъективную оценку комфорта взаимодействия с системой, но и объективное восприятие её вклада в повышение эффективности оперативно-служебной деятельности. Оценка уровня удовлетворенности проводится с использованием стандартизированных методов, включая анкетирование с применением шкал Лайкерта, проведение фокус-групп и индивидуальных интервью, что позволяет получить разностороннюю информацию о реальном опыте использования ИИ в правоохранительной практике [218].

В рамках исследования анализируются такие аспекты, как интуитивная понятность интерфейса, скорость освоения функционала, стабильность работы системы при выполнении типичных служебных задач, восприятие точности и обоснованности алгоритмических выводов, а также влияние использования ИИ на сокращение временных и трудовых затрат сотрудников. Дополнительно учитывается уровень доверия к рекомендациям, выдаваемым интеллектуальной системой, и степень готовности сотрудников полагаться на результаты автоматизированного анализа при принятии процессуальных решений.

Высокий уровень удовлетворенности пользователей свидетельствует о технологической зрелости внедренных решений, их соответствии реальным потребностям правоохранительной деятельности и эффективной интеграции в существующие рабочие процессы. Низкие показатели, напротив, могут

указывать на необходимость доработки интерфейсов, улучшения алгоритмов, расширения функциональных возможностей или проведения дополнительного обучения пользователей. В частности, неудовлетворенность сотрудников может проявляться в жалобах на сложность навигации, высокую частоту сбоев, недостаточную интерпретируемость решений или избыточную трудоёмкость отдельных операций.

Полученные результаты анализа уровня удовлетворенности подвергаются статистической обработке для выявления устойчивых закономерностей и формулирования обоснованных рекомендаций по оптимизации внедренных систем ИИ. Регулярное проведение таких оценок позволяет не только оперативно устранять возникающие проблемы, но и выстраивать стратегию дальнейшего развития цифровой инфраструктуры правоохранительных органов на основе реальных потребностей и ожиданий персонала.

Таким образом, оценка уровня удовлетворенности пользователей является важнейшим индикатором успешности интеграции систем ИИ в правоохранительную практику. Она обеспечивает обратную связь, необходимую для совершенствования алгоритмических решений, способствует повышению их социальной легитимности и эффективности, а также играет ключевую роль в формировании устойчивой, доверительной и высокотехнологичной цифровой среды органов правопорядка.

Индекс снижения предвзятости представляет собой качественную характеристику, направленную на оценку способности систем ИИ минимизировать вероятность возникновения дискриминационных результатов в процессе обработки данных и принятия решений. Этот показатель служит индикатором степени соблюдения принципов справедливости и равного отношения ко всем социальным, этническим, гендерным и возрастным группам при эксплуатации алгоритмических систем в правоохранительной практике.

Как справедливо отмечают М.Б. Садыков и Р.Р. Жилкайдаров: «Запись данных с помощью технологий искусственного интеллекта и последующая проверка фактов не только сокращают затраты времени. Это также позволяет свести к минимуму вероятность человеческой ошибки или предвзятости в отчете» [219].

Оценка индекса снижения предвзятости осуществляется через комплексный анализ практических кейсов применения ИИ, сопоставление результатов работы алгоритмов по различным демографическим критериям, а также тестирование интеллектуальных систем в контролируемых условиях. Особое внимание уделяется выявлению статистически значимых различий в уровне ложных срабатываний, пропусков событий или ошибочных решений в отношении разных категорий граждан. Например, может анализироваться, склонен ли алгоритм систематически переоценивать риски, связанные с определёнными этническими группами, или, напротив, демонстрировать заниженную чувствительность к отдельным видам правонарушений.

Важной частью методологии является применение методов стресс-тестирования, при которых в систему вводятся контролируемые изменения входных данных с целью оценки стабильности и нейтральности её поведения. Также используются методы анализа отклонений в выдаче результатов и их сопоставление с реальными статистическими характеристиками изучаемых групп.

Высокий уровень индекса снижения предвзятости свидетельствует о том, что система ИИ демонстрирует устойчивость к внешним и внутренним факторам, способным вызвать дискриминационные последствия. Низкие значения индекса указывают на необходимость пересмотра алгоритмических моделей, улучшения процедур подготовки обучающих данных и внедрения дополнительных механизмов контроля за соблюдением принципов недискриминации [220].

Таким образом, индекс снижения предвзятости играет важнейшую роль в обеспечении справедливости алгоритмических решений в правоохранительной деятельности. Его регулярная оценка позволяет минимизировать риски системной дискриминации, повысить качество оказываемых услуг в сфере правопорядка и укрепить общественное доверие к применению интеллектуальных технологий в обеспечении безопасности.

Рейтинг прозрачности и объяснимости представляет собой качественную характеристику, направленную на оценку степени, в которой процессы принятия решений системой ИИ являются интерпретируемыми и понятными для конечных пользователей. Этот показатель служит индикатором доступности логики функционирования алгоритма, обоснованности результатов и способности системы предоставить проверяемые объяснения своих выводов, что критически важно для обеспечения доверия к ИИ в правоохранительной практике [221].

Оценка рейтинга прозрачности и объяснимости осуществляется через анализ технической документации, проведение независимого тестирования алгоритмов, а также опросы сотрудников правоохранительных органов относительно их восприятия понятности решений, принимаемых ИИ. В рамках аудита изучается структура принятия решений, наличие встроенных механизмов объяснения выводов, качество представляемых пользователю отчётов и возможность проследить логическую цепочку от исходных данных к итоговому результату [222].

Как отмечают А.В. Сырбу и М.Б. Садыков: «Процесс принятия решений ИИ, особенно в сложных алгоритмах, часто трудно интерпретировать. Из-за этого ″черного ящика″ трудно доверять или понимать процесс принятия решений, который система принимала или не выполняет. ИИ нетрудно быстро вычислить входящие и исходящие сигналы, поскольку они описывают процесс, происходящий в черном ящике, с помощью системы математических уравнений, которая уже используется в некоторых криптовалютных системах для ″взлома криптосмикшеров″» [223].

Особое внимание уделяется тому, насколько алгоритмы позволяют идентифицировать использованные критерии и переменные, каким образом

формируются промежуточные выводы и в какой степени пользователь способен понять причины того или иного решения без глубоких специальных знаний в области машинного обучения. Проверяется, имеются ли адаптированные средства визуализации решений, краткие объяснительные справки, обучающие модули или другие инструменты повышения алгоритмической прозрачности.

Высокий рейтинг прозрачности и объяснимости свидетельствует о зрелости системы ИИ, её готовности к внедрению в сферы, требующие высокой ответственности и соблюдения процессуальных стандартов, таких как раскрытие преступлений или принятие процессуальных решений. Низкие показатели рейтинга указывают на необходимость доработки архитектуры алгоритма, упрощения объяснительных механизмов и повышения доступности пользовательского интерфейса.

Таким образом, рейтинг прозрачности и объяснимости играет важнейшую роль в процессе оценки пригодности систем ИИ для применения в правоохранительной деятельности. Его регулярный мониторинг позволяет не только повысить доверие сотрудников и граждан к интеллектуальным технологиям, но и укрепить правовые гарантии соблюдения справедливости и процессуальной прозрачности в ходе использования алгоритмических решений.

В рамках качественных показателей эффективности также выделяется группа аналитических параметров, которые фокусируются на технических и операционных характеристиках функционирования ИИ. Они позволяют комплексно оценивать надежность, устойчивость, масштабируемость и адаптивность интеллектуальных решений в реальных условиях правоохранительной деятельности. Данные параметры охватывают такие аспекты, как вычислительная сложность алгоритмов, качество исходных данных, способность систем эффективно масштабироваться при увеличении объема обрабатываемой информации, интеграционная совместимость с существующей инфраструктурой правоохранительных органов, а также способность к непрерывному обучению и адаптации к изменяющимся типологиям угроз. Систематическая оценка этих характеристик обеспечивает надёжность эксплуатации ИИ, минимизацию технологических рисков и устойчивость цифровых платформ в долгосрочной перспективе.

Сложность алгоритмов представляет собой характеристику, отражающую, насколько быстро и с какими затратами система ИИ способна обрабатывать информацию и выполнять поставленные задачи. При этом под затратами понимается как время обработки данных, так и объём задействованных технических ресурсов – например, оперативной памяти. Чем выше сложность алгоритма, тем больше времени и вычислительных мощностей требуется для выполнения анализа, и наоборот. Для ориентировки часто используется так называемая оценка порядка роста алгоритма, которая помогает понять, насколько возрастёт нагрузка при увеличении объема обрабатываемых данных [224].

В правоохранительной практике оценка сложности алгоритмов имеет большое значение, поскольку от неё зависит, насколько быстро и стабильно будут работать системы ИИ в реальных условиях. Например, в системах видеонаблюдения, установленных в общественных местах, медленная работа алгоритма поиска по базе данных может приводить к задержкам в выявлении подозрительных лиц. Если система обрабатывает каждую новую запись слишком долго, это может препятствовать своевременному реагированию сотрудников на потенциальные угрозы. Напротив, использование более «быстрых» алгоритмов позволяет за доли секунды находить совпадения даже в очень больших базах данных.

Подобная проблема может возникнуть и при анализе финансовых транзакций для выявления мошеннических схем. Если система требует много времени и ресурсов на проверку каждой операции, это создаёт задержки в обработке потоков данных и снижает шансы на быстрое выявление подозрительных действий. Оптимизация алгоритмов позволяет значительно ускорить этот процесс без увеличения затрат на оборудование.

Также оценка сложности необходима при планировании работы серверных мощностей в правоохранительных органах: зная примерные требования системы, можно заранее предусмотреть необходимые объёмы хранения данных и вычислительные ресурсы, чтобы избежать перегрузок и сбоев.

Таким образом, сложность алгоритмов является важнейшим параметром, который напрямую влияет на надёжность, скорость и экономичность работы интеллектуальных систем в правоохранительной деятельности. Правильная оценка и контроль этого показателя позволяют не только повысить эффективность работы ИИ, но и оптимизировать затраты и повысить устойчивость технологических решений в условиях роста нагрузки или непредвиденных ситуаций.

Индекс качества данных представляет собой характеристику, оценивающую качество, релевантность и разнообразие данных, используемых для обучения и функционирования системы ИИ. Надёжность алгоритмов напрямую зависит от того, насколько полно, корректно и сбалансированно представлены данные, на которых производится их обучение и последующая адаптация к реальной среде. Высокий уровень качества данных обеспечивает большую точность, устойчивость и справедливость принимаемых системой решений.

Оценка *индекса качества данных* проводится посредством статистического анализа массивов информации и аудита процедур сбора данных. Проверяются наличие пропущенных или ошибочных записей, выявляются дубликаты, оценивается полнота атрибутов и их актуальность, проводится тестирование на наличие системных искажений. Особое внимание уделяется репрезентативности обучающих выборок: важно, чтобы данные охватывали все релевантные социальные, демографические и географические группы, отражали специфику различных категорий правонарушений и учитывали возможные контекстные особенности [225].

В правоохранительной практике качество данных имеет критическое значение, поскольку на основе обучающих массивов формируются прогнозные модели преступной активности, системы оценки риска, механизмы автоматизированного анализа видеоматериалов и другие инструменты, влияющие на безопасность общества. Например, если в обучающих данных о преступлениях отсутствуют точные сведения о месте и времени инцидентов, это способно привести к неправильной идентификации зон повышенного риска и неэффективному распределению полицейских патрулей. В практике одной из западных стран имели место случаи, когда система предиктивного патрулирования, обученная на неполных данных, направляла ресурсы в районы с исторически завышенными показателями преступности, игнорируя новые очаги роста угроз.

Или, если в системе распознавания лиц обучающая база недостаточно разнообразна и представляет преимущественно определённую этническую группу, это может вызвать рост числа ложных срабатываний при проверке представителей иных групп населения, что нарушает принципы равенства и недискриминации. Подобный случай был зафиксирован в экспериментах по оценке алгоритмов распознавания, где точность идентификации лиц афроамериканского происхождения была на 20-30% ниже, чем лиц европейцев, что вызвало серьёзные дискуссии о допустимости использования таких технологий в сфере правоохранительной деятельности [226].

Кроме того, при формировании систем раннего выявления коррупционных рисков качество данных о государственных контрактах и структурах собственности поставщиков напрямую влияет на точность аналитических выводов. Неполные или устаревшие сведения могут привести к пропуску существенных аномалий и упущению признаков коррупционных схем.

Анализ индекса качества данных позволяет заблаговременно выявить эти риски, корректировать массивы информации, устранять искажения и добиваться более сбалансированного представления данных в алгоритмических системах. На практике это достигается через регулярные аудиты баз данных, введение процедур предварительной очистки информации, внедрение автоматизированных механизмов контроля качества данных и обеспечение прозрачности источников информации.

Таким образом, индекс качества данных является одним из фундаментальных параметров, определяющих объективность, надёжность и правовую допустимость функционирования систем ИИ в правоохранительной деятельности. Его системная оценка и регулярный мониторинг позволяют значительно повысить эффективность цифровых технологий при сохранении принципов справедливости, равенства и уважения прав человека.

Фактор масштабируемости представляет собой характеристику, отражающую способность системы ИИ обрабатывать растущие объемы данных и увеличивающиеся нагрузки без ухудшения качества работы. В правоохранительной деятельности это качество особенно важно, поскольку цифровые системы нередко сталкиваются с резким увеличением количества

информации, например, при массовых мероприятиях, чрезвычайных происшествиях или проведении крупных следственных мероприятий [227].

Оценка масштабируемости проводится через испытания на устойчивость: создаются условия повышенной нагрузки, чтобы проверить, как система справляется с увеличением числа запросов или объема данных. Одновременно анализируется, насколько эффективно распределяются ресурсы – вычислительная мощность, пропускная способность каналов связи, память серверов.

На практике масштабируемость определяет, насколько правоохранительные системы готовы к реальным вызовам. Например, в городских центрах система интеллектуального видеонаблюдения должна сохранять стабильную работу даже в моменты, когда одновременно обрабатываются десятки тысяч видеопотоков – во время праздников, митингов или спортивных событий. Недостаточная масштабируемость может привести к потере видеоданных, замедлению аналитики и снижению эффективности реагирования на инциденты.

Иной пример касается систем анализа интернет-трафика для выявления киберугроз. В случае атак типа «отказ в обслуживании» объём передаваемых данных резко возрастает. Платформа, неспособная масштабироваться, может быть парализована в критический момент, что откроет путь для проникновения злоумышленников. Системы, прошедшие проверку на масштабируемость, способны автоматически перераспределять нагрузку между серверами и продолжать функционирование даже при резком росте атакующего трафика.

Также важным примером является работа баз данных розыска лиц. В обычное время система обрабатывает запросы в стандартном объеме, однако в случае теракта или крупной аварии количество запросов к базе возрастает в разы. Если архитектура системы позволяет динамически наращивать ресурсы без перебоев, это значительно повышает шансы на быструю идентификацию подозреваемых.

Таким образом, фактор масштабируемости является важнейшей характеристикой для оценки реальной пригодности систем ИИ в правоохранительной деятельности. Высокая масштабируемость обеспечивает устойчивую работу цифровых платформ при росте нагрузки, повышает оперативность реагирования органов правопорядка и минимизирует риск технологических сбоев в критических ситуациях.

Оценка совместимости представляет собой характеристику, отражающую способность системы ИИ интегрироваться с уже существующей технической инфраструктурой и базами данных правоохранительных органов без необходимости глубокой переработки или модернизации окружающей среды. Проверка уровня совместимости осуществляется через тестирование взаимодействия с различными цифровыми системами, базами данных, каналами связи и программным обеспечением, используемыми в правоохранительной практике.

На практике высокий уровень совместимости означает, что новая система ИИ способна беспрепятственно обмениваться данными с реестрами розыска лиц, базами ДНК-профилей, архивами видеонаблюдения, информационными порталами органов внутренних дел и судебными системами. Например, при подключении интеллектуальной платформы для анализа отпечатков пальцев важно, чтобы её модули без сбоев взаимодействовали с уже действующими автоматизированными дактилоскопическими базами.

Отсутствие должной совместимости приводит к необходимости дополнительной переработки информационных систем, увеличению расходов, замедлению обмена данными и риску появления технологических «разрывов», когда критически важная информация не может быть своевременно получена или передана между подразделениями.

Примером последствий недостаточной совместимости может служить ситуация, когда система ИИ для анализа подозрительных финансовых операций не синхронизируется с базами данных налоговых органов или служб безопасности банков, что приводит к утере части важной информации о подозреваемых транзакциях.

Таким образом, оценка совместимости является важнейшим условием успешной интеграции новых интеллектуальных решений в существующие правоохранительные процессы. Высокий уровень совместимости позволяет сократить сроки внедрения ИИ-систем, повысить надёжность межведомственного взаимодействия, а также минимизировать финансовые и организационные издержки при переходе к цифровым форматам обеспечения правопорядка.

Коэффициент адаптивности отражает способность системы ИИ своевременно подстраиваться под изменения в сфере правоохранительной деятельности. В условиях, когда преступные схемы и модели поведения быстро меняются, особенно важно, чтобы цифровые технологии могли оперативно реагировать на новые угрозы без необходимости полного пересмотра своих алгоритмов.

Оценка адаптивности основывается на наблюдении за тем, насколько быстро и эффективно система способна учитывать новые данные и обновлять свои действия. Для правоохранительных органов это означает, что ИИ должен без промедления распознавать новые типы преступлений, а не полагаться только на старые шаблоны. Например, при появлении новых способов краж или мошенничества интеллектуальные системы должны своевременно анализировать новые случаи и встраивать их в свою модель работы.

На практике высокая адаптивность особенно важна в борьбе с киберпреступностью. Новые методы атак появляются практически ежедневно, и системы защиты должны уметь быстро учиться на реальных инцидентах, чтобы оперативно блокировать новые схемы мошенничества или хакерских вторжений. В аналогичном ключе действует ИИ при выявлении изменений в поведении преступных группировок: когда меняется тактика совершения

преступлений, интеллектуальные системы должны своевременно фиксировать эти изменения и корректировать рекомендации для оперативных служб.

Примером успешной адаптации можно считать ситуацию, когда система анализа документов своевременно обновляет алгоритмы обнаружения фальсификаций по мере появления новых техник подделки, не требуя сложной переработки всей платформы.

Таким образом, коэффициент адаптивности является одним из важнейших показателей пригодности ИИ для правоохранительной сферы. Высокая адаптивность позволяет быстрее реагировать на изменения в преступной активности, эффективно перераспределять усилия и ресурсы, а также снижать вероятность промедлений при выявлении новых угроз.

Системная параметризация ИИ в правоохранительной деятельности представляет собой не просто технический инструмент оценки его результативности, но и фундаментальный механизм обеспечения правовой допустимости, социальной справедливости и институциональной подотчётности алгоритмических решений. Формирование комплексной системы количественных и качественных показателей позволяет не только объективно измерять эффективность ИИ, но и выстраивать нормативные границы его применения в социально чувствительных сферах.

Предложенный подход к классификации параметров от базовых метрик точности и полноты до интегративных индикаторов доверия, прозрачности и адаптивности демонстрирует необходимость многомерного анализа алгоритмов, учитывающего как инженерные, так и правовые, социальные и этические аспекты их функционирования. Эффективность интеллектуальных систем должна оцениваться не только с позиций технологической продуктивности, но и сквозь призму их влияния на права человека, общественное доверие и устойчивость институтов правопорядка.

Институционализация параметризации ИИ в форме обязательных процедур тестирования, аудита и сертификации является важнейшим направлением развития современной цифровой правоприменительной политики. Она создаёт условия для внедрения ИИ-технологий на основе принципов процедурной справедливости и риск-ориентированного регулирования, минимизируя технологические, правовые и социальные риски. В перспективе такой подход способен не только повысить качество и предсказуемость алгоритмических решений, но и укрепить легитимность цифровых инноваций в обеспечении общественного порядка и защиты прав и свобод личности.

2 ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

2.1 Предмет нормативного регулирования искусственного интеллекта в правоохранительной деятельности

Полагаем, что при исследовании предмета нормативного регулирования ИИ в правоохранительной деятельности следует принимать во внимание то, что ИИ – это не просто технология, а феномен, который меняет природу человеческого общества, взаимоотношения между людьми, государством и машинами. Более того, вопрос о нормативном регулировании ИИ в правоохранительной деятельности имеет еще более глубокий смысл, поскольку затрагивает фундаментальные принципы справедливости, свободы, морали и ответственности.

Право по своей природе отражает общественные представления о справедливости, морали и этике, закрепляя их в юридических нормах. Внедрение ИИ в правоохранительную сферу радикально меняет характер взаимодействия права и человека. Правовая система традиционно базируется на человеческом восприятии справедливости и ответственности, однако с распространением ИИ возникает необходимость юридически переосмыслить эти понятия [228].

Сегодняшние правовые решения в этой области формируют прецеденты, определяя направление будущего законодательства. Это означает, что мы не просто создаем правила регулирования технологии, но закладываем фундамент новой юридической культуры, где субъектом правового взаимодействия может выступать не только человек, но и технология.

Правовые решения должны быть ориентированы не только на разрешение текущих задач, но и учитывать долгосрочные последствия, включая влияние на фундаментальные права и свободы граждан. Использование ИИ в правоохранительной деятельности напрямую затрагивает права на частную жизнь, свободу от дискриминации, право на справедливое судебное разбирательство и презумпцию невиновности. Если алгоритм принятия решений непрозрачен или содержит встроенные системные ошибки, это не только подрывает доверие к правоохранительной системе, но и может спровоцировать кризис всей правовой системы в долгосрочной перспективе.

ИИ, особенно в контексте правоохранительной деятельности, не является нейтральным инструментом. Алгоритмы обработки информации, принятия решений, а также методы сбора, анализа и интерпретации данных приобретают правовую значимость тогда, когда их применение влияет на права и свободы граждан. Следовательно, правовое регулирование необходимо не ради контроля над программным обеспечением как таковым, а ради обеспечения легитимности, справедливости, подотчетности и правовой определенности в процессе использования этих технологий.

Предмет нормативного регулирования в данном контексте охватывает весь спектр отношений, возникающих в процессе создания, внедрения и использования интеллектуальных систем в правоохранительной сфере. В первую очередь это касается установления допустимых границ алгоритмического вмешательства в частную и общественную жизнь граждан. ИИ, особенно при использовании технологий обработки больших данных, биометрической идентификации, анализа поведения и прогнозирования риска, способен проникать в ранее недоступные сферы частной жизни, что требует строгого правового контроля, направленного на недопущение произвольного вмешательства в личную свободу индивида.

На практике это означает необходимость установления чётких регламентов использования систем видеонаблюдения с функцией автоматического распознавания лиц, анализа передвижений граждан, мониторинга активности в сети Интернет, обработки звонков на горячие линии и других форм оперативного контроля. Каждое такое применение должно быть строго ограничено целями, прямо установленными законом, а также подчинено принципам необходимости, пропорциональности и минимизации вторжения в частную жизнь.

Как отмечают Д.Р. Нуркеева и М.Б. Садыков: «Несмотря на то что регулирование применения ИИ является важнейшим инструментом для обеспечения принципа законности, оно имеет свои ограничения. Понимание этих ограничений необходимо для выработки справедливой и адекватной нормативно-правовой основы: – Серые зоны этики. Законодательные рамки, как правило, чётко очерчены, тогда как в вопросах этики применения ИИ в правоохранительной практике границы существенно размыты. Такая дихотомия порождает значительные пробелы в разрешении ситуаций, не имеющих однозначного правового решения» [229].

Важным направлением регулирования является определение условий и порядка применения ИИ при осуществлении оперативно-розыскных мероприятий, надзора, задержаний, расследования уголовных правонарушений и использования полученных данных в доказательственном процессе. Применение ИИ в этих стадиях должно быть сопоставимо с процессуальными гарантиями, традиционно предусмотренными уголовно-процессуальным законодательством. Например, автоматизированное профилирование лиц, подозреваемых в совершении преступлений, не должно служить единственным основанием для возбуждения уголовного дела или применения мер процессуального принуждения без дополнительной проверки и верификации данных.

Одной из центральных задач регулирования является формирование механизмов защиты граждан от потенциальных злоупотреблений со стороны алгоритмических систем. В первую очередь это касается предотвращения алгоритмической дискриминации, которая может проявляться в предвзятости в отношении отдельных этнических, социальных, гендерных или возрастных групп. Исторические примеры, такие как использование системы COMPAS в США, которая демонстрировала систематическое завышение уровня

рецидивного риска для представителей афроамериканского населения, показывают, насколько реальной является угроза переноса социального неравенства в автоматизированные решения. В этой связи необходимо обязательное тестирование ИИ-систем на предмет наличия скрытых предвзятостей и дискриминационных эффектов ещё на стадии разработки и в процессе эксплуатации.

Необходимость нормативного регулирования также обусловлена рисками, связанными с непрозрачностью алгоритмических моделей. В условиях, когда решения принимаются на основе моделей машинного обучения, внутренний механизм функционирования которых остаётся недоступным для интерпретации («эффект чёрного ящика»), возникают серьёзные угрозы процессуальной справедливости. В уголовно-процессуальной практике каждый субъект, в отношении которого принимается ограничивающее его права решение, должен иметь возможность понять основание принятия такого решения и обжаловать его в суде. Применительно к ИИ это означает требование к объяснимости алгоритмов, используемых в правоохранительных органах: системы должны предоставлять проверяемые основания для своих выводов.

Особую тревогу вызывает риск постепенной утраты человеческого контроля над процессами правоприменения. При отсутствии чётких нормативных рамок может сложиться практика делегирования принятия критически важных решений исключительно алгоритмам, что подрывает принципы индивидуализации ответственности и подотчётности. Например, если вопрос о мере пресечения, месте содержания под стражей или уровне риска рецидива будет решаться автоматически, без участия компетентного процессуального субъекта, это приведёт к размыванию института презумпции невиновности и нарушению базовых стандартов справедливого правосудия.

Не менее серьёзным фактором является правовая неопределённость для разработчиков и операторов ИИ-систем. В отсутствие чётких регуляторных требований они вынуждены действовать в условиях высокой неопределённости относительно допустимых целей использования технологий, стандартов обеспечения безопасности, процедур сертификации решений и критериев допустимости их применения в судебных и административных процессах. Это тормозит развитие технологий, снижает готовность компаний к инвестициям в разработку правоприменительных решений и создаёт риски для государства, которое в будущем будет вынуждено устранять последствия неурегулированных технологических практик.

Таким образом, создание эффективной системы правового регулирования применения искусственного интеллекта в правоохранительной сфере требует разработки комплексного нормативного подхода, включающего установление обязательных требований к прозрачности, объяснимости, справедливости и подотчётности алгоритмических решений. Законодатель должен исходить из того, что использование ИИ в правоохранительной практике может быть допустимо только при условии соблюдения жёстких

стандартов защиты прав и свобод человека, а не только на основании критериев технологической эффективности или оперативной целесообразности.

Предмет правового регулирования в контексте применения технологий ИИ в правоохранительной деятельности охватывает не только вопросы установления допустимых пределов алгоритмического вмешательства в сферу государственного управления и индивидуальной автономии, но и формирование комплексных требований к условиям, в рамках которых такое применение может быть признано юридически допустимым. В этом контексте регулирование должно предусматривать нормативное определение правового статуса и степени ответственности субъектов, вовлечённых в процесс разработки, внедрения и эксплуатации систем ИИ, включая государственные органы, частных разработчиков, операторов алгоритмических платформ, а также надзорные и контрольные структуры. Необходимо обеспечить детальную регламентацию процедур и процессуальных стадий, на которых допустимо задействование интеллектуальных технологий, таких как обработка, интерпретация и оценка доказательственной информации, анализ рисков и угроз, идентификация и розыск лиц, подозреваемых в совершении правонарушений. Важнейшим элементом нормативной конструкции является закрепление чётких правовых гарантий для физических лиц, чьи интересы могут быть затронуты в результате применения алгоритмических решений, включая право на защиту, оспаривание автоматизированных выводов и обеспечение прозрачности процедур вмешательства. Регулятивная рамка должна предусматривать установление форм и уровней многоуровневого контроля за функционированием систем ИИ, включая судебный, прокурорский, общественный и независимый экспертный надзор, направленных на обеспечение открытости, подотчётности и предотвращение злоупотреблений. Кроме того, обязательным требованием является установление стандартов верифицируемости и объяснимости функционирующих алгоритмов, обеспечивающих возможность ретроспективного анализа оснований принятых решений, их воспроизводимости и нормативной обоснованности, что является неотъемлемым условием поддержания процедурной справедливости и укрепления доверия общества к цифровой трансформации правоохранительных механизмов.

Таким образом, нормативное регулирование функционирует в качестве основного механизма поддержания динамического равновесия между критериями технологической эффективности и правовой допустимости, формируя институциональные условия для легитимного и обоснованного использования ИИ в сфере осуществления государственного управления.

При этом следует особо подчеркнуть, что ИИ в контексте правоохранительной деятельности представляет собой сложный двойственный объект регулирования: с одной стороны, он выступает как информационно-технический продукт, на который распространяются требования обеспечения безопасности, стандартизации, сертификации и

качества функционирования, а с другой стороны как правооформляющий феномен, обладающий способностью трансформировать принципы уголовной политики, изменять методы правоприменения и оказывать существенное воздействие на общественное восприятие легитимности и справедливости институтов государственной власти.

Вследствие такой двойственной природы ИИ предмет правового регулирования не может быть ограничен исключительно технико-правовыми параметрами или стандартами программно-аппаратной безопасности: он требует применения междисциплинарного подхода, синтезирующего усилия юристов, специалистов в области информационных технологий, этиков, социологов и представителей иных наук, обеспечивающих всестороннее осмысление социальных последствий алгоритмизации властных функций. Только в рамках такой комплексной нормативной стратегии возможно построение системы регулирования, способной одновременно учитывать специфику технологических процессов, гарантировать защиту прав и свобод личности и обеспечивать устойчивость общественных институтов в условиях цифровой трансформации.

Сложная природа и высокая социальная чувствительность алгоритмически опосредованных решений обусловливают необходимость формирования многоуровневой системы нормативного регулирования. На национальном уровне данная система предполагает принятие фундаментальных правовых актов, устанавливающих общие рамки допустимости применения ИИ в сфере обеспечения правопорядка, а также создание специализированных регуляторных органов, уполномоченных на осуществление лицензирования, сертификации и надзора за алгоритмическими системами. На институциональном уровне регулятивные усилия сосредоточены на разработке локальных актов, таких как внутренние инструкции, кодексы профессионального поведения, алгоритмы процессуальной интеграции ИИ в правоохранительные процедуры, обеспечивающие адаптацию общих нормативных требований к специфике деятельности конкретных ведомств. На международном уровне формируется согласованная система совместимых подходов, основанная на выработке минимальных стандартов допустимости алгоритмических решений и установлении механизмов трансграничного контроля, призванных предотвращать правовые лакуны и регулировать вопросы ответственности в случае применения ИИ в межгосударственном правовом взаимодействии. Таким образом, многоуровневая архитектура регулирования становится необходимым условием обеспечения целостности, правомерности и социальной легитимности интеграции интеллектуальных технологий в сферу государственного управления и уголовного права.

Без такого многоуровневого подхода возможна фрагментация правоприменительной практики, рост конфликтов между техническими возможностями и юридическими ограничениями, а также снижение доверия граждан к институтам правосудия.

Особое внимание при определении предмета нормативного регулирования в сфере ИИ следует уделить не только технологическим параметрам функционирования интеллектуальных систем, но и практическим ожиданиям от их использования в профессиональной среде. В этой связи репрезентативное значение приобретают результаты анкетирования, проведённого среди сотрудников правоохранительных органов Республики Казахстан (100 респондентов), отражающие отношение к перспективам внедрения ИИ в различные сегменты уголовной юстиции. Опрос позволил выявить уровень осведомлённости, отношение и готовность к использованию технологий искусственного интеллекта (ИИ) в профессиональной практике (Приложения В, Г).

Анализ стажа правоохранительной службы показывает, что наибольшую долю респондентов составляют сотрудники со стажем от года до трёх лет – 21%. Существенную часть представляют также респонденты со стажем свыше десяти лет (19%) и от семи до десяти лет (17%). Молодые специалисты со стажем до года составляют 16%, а сотрудники со стажем от трёх до пяти лет – 15%. Наименьшую долю составляют респонденты со стажем от пяти до семи лет – 12%. Таким образом, выборка сбалансирована и охватывает как молодых сотрудников, находящихся на этапе профессионального становления, так и опытных работников, обладающих устойчивыми профессиональными взглядами. Это позволяет более объективно оценить восприятие технологий искусственного интеллекта представителями разных поколений правоохранителей.

По занимаемым должностям среди респондентов наибольшую долю составляют оперативные сотрудники – 32%. Дознаватели представлены в количестве 25%, прокуроры – 22%, следователи – 21%. Это распределение демонстрирует, что в исследовании широко представлены ключевые должностные лица функциональных ролей в системе уголовного преследования. Присутствие как оперативных, так и процессуальных работников позволяет более полно отразить специфику отношения к применению искусственного интеллекта на различных этапах работы с правонарушениями – от первичного реагирования до судебного надзора.

Что касается степени знакомства с технологиями ИИ, наибольшая доля респондентов – 27%, указала, что обладают хорошими знаниями и активно отслеживают развитие данной области. Базовые знания отметили 26% опрошенных, ещё 25% находятся на стадии изучения темы. При этом 22% респондентов признали, что имеют лишь незначительное представление об ИИ и не проявляют интереса к его дальнейшему изучению. Это подтверждает, что в целом среди сотрудников правоохранительных органов формируется позитивная тенденция в сторону цифровой компетентности, однако сохраняется потребность в системной образовательной поддержке и институциональных мерах по повышению квалификации.

Отношение к ИИ среди сотрудников правоохранительных органов оказалось достаточно неоднородным. 26% респондентов высказали негативное отношение, ещё 17% – крайне негативное, что в совокупности

составляет 43% участников опроса. В то же время 24% респондентов продемонстрировали позитивное восприятие ИИ, а 16% – крайне позитивное. Нейтральную позицию заняли 17% опрошенных. Эти данные свидетельствуют о том, что отношение к ИИ в профессиональной среде во многом поляризовано и зависит, вероятно, от индивидуального опыта, уровня цифровой грамотности и специфики служебных обязанностей. Такая картина подчёркивает необходимость формирования устойчивой культуры доверия к ИИ и широкого профессионального диалога о его возможностях и рисках.

Навыки работы с системами на основе ИИ среди респондентов распределились следующим образом: 25% сообщили об отсутствии каких-либо навыков в этой области, 24% обладают минимальным практическим опытом. Базовые навыки, включающие использование популярных ИИ-инструментов (таких как ChatGPT или Midjourney), отметили 16% опрошенных. 14% указали на наличие ограниченного опыта. Примечательно, что 21% респондентов заявили о наличии навыков программирования и обучения ИИ-систем – этот показатель демонстрирует высокую техническую вовлеченность определённой части правоохранительного сообщества. В целом данные указывают на разнообразие компетенций и подтверждают актуальность специализированных обучающих программ, направленных на развитие цифровой грамотности и прикладных умений работы с ИИ.

На вопрос о способности ИИ заменить оперативного сотрудника мнения респондентов разделились. 37% считают, что ИИ способен лишь частично заменить оперативную работу, 35% высказали мнение о полной заменяемости этой должности технологиями. Вместе с тем 28% опрошенных уверены, что ИИ не может заменить оперативного работника. Такое распределение отражает амбивалентность профессионального восприятия – с одной стороны, признаётся потенциал ИИ в обработке информации, выявлении закономерностей и быстром реагировании, с другой – сохраняется убеждение в уникальности человеческого фактора, необходимого для принятия нестандартных решений, моральной оценки и тактической гибкости в ситуациях реального взаимодействия.

Относительно профессии следователя 42% респондентов выразили мнение, что ИИ способен полностью заменить эту должность. Такой высокий показатель демонстрирует значительное доверие к автоматизации аналитической и процессуальной работы, связанной с построением версий, систематизацией доказательств и логическим моделированием преступных событий. В то же время 30% считают, что замещение возможно лишь частично, а 28% – что ИИ не способен заменить следователя. Таким образом, несмотря на определённый оптимизм в отношении автоматизации следственной функции, сохраняется доля специалистов, акцентирующих внимание на необходимости сохранения человеческого контроля и профессионального суждения при решении сложных правовых вопросов и оценке доказательств.

Оценка перспектив замены прокурора ИИ продемонстрировала почти равномерное распределение мнений: по 34% респондентов считают, что ИИ

может либо полностью, либо частично заменить прокурора. Вместе с тем 32% выразили уверенность в том, что полная замена невозможна. Эти данные отражают, с одной стороны, растущее признание потенциала ИИ в правовой аналитике, надзорных функциях и подготовке процессуальных решений, а с другой – осознание важности институциональной роли прокурора как носителя ответственности, субъекта судебной инициативы и гаранта соблюдения прав. Таким образом, подавляющее большинство респондентов рассматривают ИИ как вспомогательный инструмент, но не как независимый правовой субъект в сфере надзора.

Анализ ответов на вопрос о степени готовности использовать технологии искусственного интеллекта при раскрытии уголовных правонарушений выявил наличие противоречивых установок среди респондентов. Наиболее распространёнными оказались оценки «2» (26%) и «1» (22%), что может свидетельствовать о настороженности, недостатке опыта или сомнениях в эффективности ИИ на этапе оперативной работы. Вместе с тем значительная часть участников (19% и 18% соответственно) указали на высокую степень готовности, выбрав оценки «5» и «4». Ещё 15% респондентов заняли умеренную позицию, оценив свою готовность на «3». Таким образом, около трети сотрудников демонстрируют высокую мотивацию к интеграции ИИ в практику раскрытия преступлений, тогда как почти половина нуждается в дополнительных условиях для формирования готовности: доступ к обучению, наглядные кейсы эффективности и регламентированное внедрение. Полученные результаты подчёркивают важность системного внедрения технологий ИИ не только на уровне инструментов, но и на уровне формирования профессиональной уверенности в их применимости и правовой защищённости действий, основанных на алгоритмической поддержке.

Оценка степени готовности использовать информацию, полученную от систем искусственного интеллекта при расследовании уголовных правонарушений, показала, что мнения респондентов распределены достаточно равномерно. Наивысшую готовность («5») продемонстрировали 14% участников, ещё 22% оценили её на «4». При этом наибольшая доля пришлась на оценку «3» – 28%, что указывает на умеренно-позитивную установку при наличии определённых сомнений. Низкую готовность выразили 24% (оценка «1») и 12% (оценка «2»). Эти данные показывают, что, несмотря на относительную заинтересованность в использовании ИИ, сотрудники правоохранительных органов сохраняют настороженность при доверии к алгоритмически полученной информации в доказательственном процессе. Вероятной причиной является отсутствие устоявшихся процедур правовой проверки и процессуальной допустимости такой информации. Это подчёркивает необходимость формирования нормативных механизмов, определяющих пределы использования, достоверность и верифицируемость данных, полученных с помощью ИИ.

На вопрос о предполагаемой роли искусственного интеллекта в системе правоохранительных органов респонденты продемонстрировали широкий

спектр представлений. По 20% опрошенных считают, что ИИ может выступать в роли следователя, либо, напротив, вовсе не видят перспектив его применения в данной сфере. 17% респондентов указали на возможность использования ИИ в качестве судебного эксперта, 16% – как помощника следователя, а 13% – как инструмента для сбора и обработки информации (например, прогнозирование преступности, выявление серийности, формирование досье). Ещё 14% предложили иные варианты, что свидетельствует о наличии собственного видения, не укладывающегося в типовую классификацию. Подобное распределение говорит о двойственной установке: с одной стороны, фиксируется вера в потенциал ИИ как активного участника процессуальных действий, с другой – выражено существенное сомнение в правовой, этической и практической допустимости полной его интеграции. Это подтверждает необходимость институционального обсуждения пределов допустимости автономных алгоритмов в уголовной юстиции и выработки моделей их ответственности, подотчётности и процессуальной легитимности.

Анкетирование подтверждает, что предмет нормативного регулирования ИИ в правоохранительной деятельности охватывает не только технологические решения, но и вопросы допустимости, пределы функционального замещения, процедуры доказательной верификации и кадровую адаптацию. Речь идёт о формировании нормативной среды, которая будет учитывать реальную степень готовности системы, обеспечивая законность, этичность и эффективность применения ИИ в правоохранительной сфере.

Таким образом, предмет нормативного регулирования искусственного интеллекта в правоохранительной деятельности представляет собой комплексный и динамичный правовой феномен, охватывающий не только технологические аспекты, но и социальные, этические, институциональные последствия его применения. Основной задачей нормативного воздействия в данной области должно стать обеспечение законности, справедливости и прозрачности в условиях цифровой трансформации правоохранительной деятельности. Без этого невозможно сохранить баланс между эффективностью государственного реагирования и сохранением правовой безопасности личности.

2.2 Пределы использования искусственного интеллекта в правоохранительной деятельности

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 процедурной справедливости. 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 контексте 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 её 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» [230], [231].

Есть цитаты Р.Ф. Иеринга, также посвященные праву: «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» [232].

Применительно к современным вызовам, связанным с внедрением ИИ в практику правоприменения, данная позиция требует жёсткого ограничения технической автономии алгоритмов, поскольку ни одна, даже самая совершенная технологическая система, не способна заменить интуитивное, ценностное и этическое измерение человеческого правосудия. ИИ в данном контексте может быть признан допустимым исключительно в качестве вспомогательного средства, служащего достижению высших целей права –

справедливости, гуманности, правовой определённости и защиты человеческой свободы.

Допущение ИИ в процессы, имеющие значение для правового статуса личности, возможно лишь при условии строгой нормативной подчинённости 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, наделённым профессиональной, правовой и моральной ответственностью. В противном случае возникает опасность технологической подмены права – подчинения правоприменительной деятельности механистической эффективности в ущерб её гуманитарному содержанию.

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

Теория управления рисками, подробно рассмотренная нами ранее в подразделе 1.3, является одной из ключевых методологических основ осмысления допустимости применения искусственного интеллекта в правоохранительной сфере. Здесь же дополнительно упомянем монографию Ортвина Ренна, которая представляет собой одну из наиболее авторитетных и концептуально насыщенных работ, посвящённых проблематике управления рисками в условиях экспоненциального технологического развития [233].

В контексте правоохранительной деятельности, где под угрозой оказываются такие базовые ценности, как личная свобода, безопасность, неприкосновенность частной жизни и презумпция невиновности, применение технологий искусственного интеллекта 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 всё 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 искусственного интеллекта в правоохранительной деятельности, в рамках которой интенсивность регулятивного вмешательства должна находиться в прямой зависимости от уровня потенциальной угрозы правам, свободам и законным интересам субъектов права.

Ренн подчёркивает, 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. В этой логике возникает необходимость выстраивания многоуровневых регулятивных режимов, адекватных различным уровням риска, что особенно актуально в контексте 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 своё органичное продолжение в исследовании допустимости и пределов применения технологий искусственного интеллекта в сфере правоохранительной деятельности. Как уже отмечалось в разделе, посвящённом параметризации эффективности алгоритмических систем, 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.

Тайлер пишет: «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» [234].

В условиях внедрения ИИ в процессы правоприменения требования процедурной справедливости приобретают ещё 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, полученных с помощью алгоритмических инструментов.

ИИ, даже будучи высокотехнологичным и функционально надёжным, 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, лишённых способности к оценке справедливости, соразмерности и уважения к человеческому достоинству.

Таким образом, пределы допустимости применения искусственного интеллекта 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 искусственного интеллекта в зависимости от уровня риска воздействия на права человека, о чём речь шла в разделе о параметризации, приобретает в этом контексте 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 искусственного интеллекта в правоохранительной деятельности сквозь призму философии права и морально-этической рефлексии, следует подчеркнуть, что мы вступаем в сферу, находящуюся на пересечении технологического прогресса и глубоко укоренённых оснований человеческой цивилизации – таких как достоинство личности, верховенство права, общественная мораль и универсальные ценности справедливости. Этот контекст 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 – замещение человеческого начала или его технологическое дополнение?

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 контексте конкретных человеческих ситуаций. В этом контексте встают 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 искусственный интеллект интерпретировать норму с учётом её этического содержания, контекста, целей и ценностей, которые зачастую выходят за пределы формально-логического анализа?

Ещё более остро встаёт 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 ключевых пределов применения искусственного интеллекта в правоохранительной практике. Алгоритм, как бы высоко ни была развита его способность к обработке информации, не способен заместить моральную интуицию, ценностное осмысление и способность к справедливой интерпретации уникальных жизненных ситуаций, которые являются сутью правоприменения. Искусственный интеллект 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 ткани 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 их критическому осмыслению в контексте 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 искусственного интеллекта в правоохранительную деятельность 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.

Как отмечает М.Б. Садыков: «Таким образом суммируя вышесказанное, на наш взгляд, 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 технологий искусственного интеллекта. 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 технологий искусственного интеллекта следует воспринимать данные системы как помощника в принятии решений, а не как замену человеку. Финальное решение всегда должен принимать человек» [235].

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 совершённые ошибки. Однако функциональное участие ИИ в процессах, имеющих юридически значимые последствия для прав и свобод личности, создаёт иллюзию распределённой, а в действительности часто – утраченной ответственности, скрытой в технологическом «чёрном 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 последствий.

Человеческая ответственность за действия искусственного интеллекта 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 остаётся на стороне человека. Только в этом случае возможно избежать трансформации права в безликий технологический механизм, лишённый ценностного содержания и подотчётности перед обществом.

Внедрение технологий 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, лишённое 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. Этот контекст формирует принципиальное ограничение 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 подчинённым 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 ключевых 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 своё сущностное предназначение.

В свете проникновения ИИ в правоохранительную систему 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 учётом 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 в этом контексте 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 серьёзным организационным вызовом становится обеспечение прозрачности и подотчётности алгоритмических процессов в правоохранительной деятельности. По мере усложнения архитектуры машинного обучения и увеличения числа уровней нейронных сетей алгоритмы становятся всё 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 чётко 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, который 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 датасет для обучения.

Результаты работы ИИ должны перепроверяться соответствующими должностными лицами. Кроме того, выходные данные ИИ не должны быть единственной основой для принятия процессуальных решений, затрагивающих права и свободы людей [236].

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, сопряжённой 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 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 идёт о применении ИИ в оценке доказательств, поддержке решений об аресте, инициировании следственных действий и других действиях, непосредственно влияющих на свободу и честь гражданина. Здесь технология 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 в данном контексте несёт особо тяжёлые 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 её основы в стремлении к технологической эффективности.

Полагаем, что развитие технологий ИИ требует развития правовой инфраструктуры ИИ, внедрения этических стандартов, усиления механизмов подотчётности и, главное, сохранения человеческого измерения правосудия в эпоху цифровизации.

Таким образом, осмысление пределов и ограничений использования искусственного интеллекта 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.

2.3 Компаративный анализ зарубежного опыта правового регулирования искусственного интеллекта в правоохранительной деятельности

Стремительное развитие ИИ требует от государств по всему миру решить вопрос с адаптацией своей действующей нормативно-правовой базы. Для удобства отслеживания постоянно изменяющегося законодательства в различных странах в сети Интернет можно найти несколько ресурсов, которые осуществляют мониторинг законодательства. Одними из них, например, являются ресурсы известной юридической компании White and Case [237], Международной ассоциации специалистов по конфиденциальности (International Association of Privacy Professionals) [238], Legal Nodes [239] и другие.

Наряду с государствами, такие международные организации, как Организация Объединенных Наций (ООН), Совет Европы, Организация экономического сотрудничества и развития (ОЭСР), также выпускают свои рамочные документы. Однако темпы развития ИИ заставляют усомниться в способности как государств, так и международных объединений успевать за ними.

Также следует учитывать необходимость скоординированного приложения усилий по выработке единых подходов к регулированию отношений в сфере ИИ, иначе в мире может сложится ситуация фрагментации международного права. Одним из примеров попытки объединения международного сообщества является прошедшее в конце 2023 года в Великобритании глобальное мероприятие, направленное на содействие безопасному и ответственному развитию ИИ в мире [240].

В нашей стране каркасным актом, задающим институциональные и процедурные правила развития государственной цифровой среды является Закон Республики Казахстан «Об информатизации» №418-V от 24 ноября 2015. Он фиксирует понятийный аппарат *(«автоматизация», «информатизация»)* и регулирует создание, развитие и эксплуатацию объектов ИКТ; архитектуру электронного правительства и межведомственную интероперабельность; жизненный цикл ИТ-проектов и реестровую дисциплину, а также режим киберустойчивости, включая классификацию, аттестацию, аудит и реагирование на инциденты. Закон разграничивает компетенции и ответственность владельца, оператора и уполномоченного органа, придавая управлению ясную иерархию. Предусмотренные меры государственной поддержки ИКТ-отрасли напрямую увязаны с задачами устойчивого роста и международной конкурентоспособности Казахстана. Нормативная ткань акта пронизана принципами законности, приоритета прав и свобод, равенства участия и открытого доступа к электронным информационным ресурсам государственных органов.

Правовой блок цифровизации в Республике Казахстан опирается также на пять системообразующих актов:

1) Закон «Об электронном документе и электронной цифровой подписи» №370-II от 7 января 2003 года закрепляет юридическую силу электронных документов, правила их создания, обращения и хранения, инфраструктуру доверия (национальный удостоверяющий центр), а также требования к ЭЦП, отметкам времени и ответственности участников;

2) Закон Республики Казахстан «О персональных данных и их защите» №94-V от 21 мая 2013 года определяет правовые основания и процедуры сбора, обработки, хранения и передачи персональных данных, устанавливает права субъектов и обязанности операторов, режим безопасности и ответственность за нарушения;

3) Закон Республики Казахстан «О государственных услугах» от 15 апреля 2013 года №88-V институционализирует сервисную модель государства: дефинирует услугу как индивидуализированную форму реализации функций, закрепляет права услугополучателей (включая участие в публичном обсуждении стандартов), распределяет компетенции органов и регламентирует омниканальное, включая электронное, предоставление;

4) Закон Республики Казахстан «О цифровых активах в Республике Казахстан» №193-VII от 6 февраля 2023 года формирует режим выпуска/оборота и майнинга: лицензирование майнеров, аккредитация пулов, фискальные требования и реализация ≥75% добытых активов через биржи МФЦА;

5) Закон Республики Казахстан «О связи» №567-II от 5 июля 2004 года устанавливает основы регулирования сетей и услуг связи: лицензирование, распределение ресурсов нумерации и радиочастот, межсетевое присоединение, качество и устойчивость, а также порядок взаимодействия с государственными органами. Совокупно эти нормы обеспечивают юридическую валидность электронных сделок, защиту данных и надежность коммуникационной инфраструктуры. Предусмотрены согласие, анонимизация, трансграничная передача и уведомление уполномоченного органа в установленных законом случаях.

24 сентября 2025 года Мажилис во втором чтении одобрил проект Закона «Об искусственном интеллекте» и сопутствующие поправки. Документ формализует понятийный аппарат *(определения «искусственный интеллект», «библиотека данных», «синтетические результаты деятельности систем искусственного интеллекта»)*, формирует условия для внедрения ИИ в различные сферы и вводит запрет на создание систем, способных нарушать права и свободы человека *(манипулирование, дискриминация, сбор биометрических данных без согласия, использование ИИ для распознавания лиц в общественных местах в режиме реального времени за исключением случаев, разрешённых законом и др.)*. Предусмотрены требования к прозрачности, управляемости и безопасности, особые условия применения технологий государственными органами и субъектами квазигоссектора, а также расширение полномочий правительства по формированию и координации политики в сфере ИИ [241]. Однако 23 октября законопроект был

возвращен Сенатом в Мажилис на доработку. В частности, предложена новая редакция отдельных статей законов:

- объектом авторского права станет произведение, созданное с использованием ИИ только при наличии творческого вклада человека;

- собственники и владельцы ИИ обязаны будут принимать меры не только по минимизации, но и предотвращению возможного ущерба, в том числе в части защиты прав, свобод и законных интересов физических лиц;

- уточнено, что страхование ответственности за вред, причиненный ИИ, осуществляется «в соответствии с законами Республики Казахстан [242].

В августе 2025 года депутатами Мажилиса инициирован проект Цифрового кодекса. Разработка осуществляется эволюционным путем с общей части и далее будет дополняться отраслевыми частями. Цифровой кодекс определяет четыре вида цифровых объектов, связанных с цифровыми данными: записи, ресурсы, платформы и системы, а также инфраструктуру. В будущем допускается расширение перечня. Цифровое государство предлагается рассматривать как систему публичного управления. Вводится понятие «цифровая зрелость» – инструмент для оценки отраслей и организаций по уровню их цифрового развития. Документ содержит также ряд других норм, направленных на комплексное регулирование цифровой среды.

Вместе с тем рядом юристов высказана критика Кодекса. В частности, Заслуженный юрист Республики Казахстан С. Темирбулатов выразил мнение, что проект Цифрового кодекса «по своему содержанию, объему и конструкции даже не приближен к кодексу. Нет в нем и последовательной согласованности норм, логической связанности между текстом отдельных глав, правовой определенности по многим вопросам. Этот проект представляет собой совокупность отдельных положений из популярных изданий по IT-сфере, информации о цифровых объектах и конструкциях, не несущей правовой нагрузки, а также положений об экспериментальном правовом регулировании в цифровой сфере. И все это перечисленное не имеет определенной взаимосвязи внутри одного сводного акта.» [243].

На заседании Общественной палаты при Мажилисе ассоциированный профессор Университета КазГЮУ им. М.С. Нарикбаева М. Хасенов выразил поддержку идее законодательного регулирования цифровых отношений, отметив масштаб и стратегический подход авторов проекта, Эксперт, однако, обратил внимание на ряд юридических недоработок. Так, опасной он назвал норму о том, что цифровые данные не являются объектами гражданских прав, не регулируются гражданским законодательством и могут свободно создаваться, собираться, обрабатываться и передаваться, за исключением случаев, установленных законами. М. Хасенов призвал также сосредоточиться на содержательной стороне документа. «Сейчас мы не можем принимать кодекс авансом, ссылаясь на будущее, что остальное допишем позже. Так это не работает. Кодекс уже сегодня должен соответствовать названию и статусу», – считает эксперт [244].

Правительства и регулирующие органы по всему миру в спешном порядке адаптируют свою нормативно-правовую базу к стремительному

развитию ИИ. Международные организации, такие как G7, ООН, Совет Европы и ОЭСР, также выпустили свои собственные руководства по ИИ. Однако быстрое развитие технологий ИИ означает, что эти усилия могут столкнуться с трудностями. Чтобы способствовать международному сотрудничеству, правительство Великобритании организовало в ноябре 2023 года первый Глобальный саммит по безопасности ИИ, целью которого является содействие безопасному и ответственному развитию ИИ во всем мире.

Европейский союз

Европа лидирует в разработке законодательства по регулированию искусственного интеллекта. Закон ЕС об ИИ (Regulation (EU) 2024/1689), принятый в июле 2024 года, является первым законодательным актом, создающим единую нормативную базу для развития искусственного интеллекта в Европейском союзе [245]. Он направлен на гарантирование защиты основных прав, демократии, верховенства закона и экологическую устойчивость от высокого риска ИИ, одновременно стимулируя инновации и делая Европу лидером в этой области. Также устанавливаются обязательства для ИИ, исходя из его потенциальных рисков и уровня воздействия.

Согласованный текст теперь должен быть официально принят как Парламентом, так и Советом, чтобы стать законом ЕС. Парламентские комитеты по внутреннему рынку и гражданским свободам проголосуют по соглашению на предстоящем заседании.

Цель законодательства – гарантировать контроль человека над системами ИИ, обеспечивая их безопасность, прозрачность, прослеживаемость, недискриминацию и экологичность. Кроме того, существует желание создать единообразное определение ИИ, которое может быть адаптировано к различным технологиям, охватывающим как нынешние, так и будущие системы ИИ.

Закон Европейского союза «Об искусственном интеллекте» делит компьютерные программы на основе ИИ на три уровня риска (неприемлемый риск, приложения с высоким риском и приложения, которые явно не запрещены или не классифицируются как приложения с высоким риском), и степень регулирования различается в зависимости от этого.

Статья 5 Закона ЕС об ИИ (AI Act, Регламент 2024 года) определяет перечень практик, строго запрещённых на территории ЕС. Эти запреты критически важны для правоохранительных органов, поскольку устанавливают четкие юридические и этические границы допустимости применения ИИ в сфере уголовного правосудия и обеспечения общественной безопасности.

Основные запрещённые практики, касающиеся правоохранительной деятельности:

«1. Сублиминальные (не фиксируемого сознанием воздействия на психику) техники, искажающие поведение (ст. 5(1)(a))

Запрещаются ИИ-системы, использующие сублиминальные методы, способные существенно искажать поведение человека и причинять физический или психологический вред.

Для правоохранительной деятельности это означает:

– запрещается использование ИИ, скрыто влияющего на поведение подозреваемых или граждан (например, эмоционально манипулятивного контента при допросах или наблюдении);

– манипуляции с помощью распознавания эмоций и поведенческого профилирования могут быть юридически сомнительными.

2. Использование уязвимостей отдельных групп (ст. 5(1)(b))

Запрещаются ИИ-системы, использующие уязвимости конкретных групп населения (например, детей или лиц с инвалидностью) с целью искажения их поведения.

Для правоохранительной деятельности это означает:

Правоохранительные органы не должны применять ИИ, нацеленный на уязвимые категории (например, в школах, при работе с несовершеннолетними или в сфере социальной защиты).

3. Социальный скоринг (ст. 5(1)(c))

Запрещается использование ИИ для универсальной системы социального скоринга (оценки благонадёжности) со стороны государственных органов.

Для правоохранительной деятельности это означает:

– запрещается практика предсказательной оценки поведения на основе социальных, экономических или поведенческих факторов;

– нельзя использовать общие ″индексы риска″ при принятии решений, не связанных с конкретными правонарушениями (например, отказ в УДО на основании поведения в соцсетях).

4. Биометрическая идентификация в реальном времени в общественных местах (ст. 5(1)(d))

Запрещается использование ИИ-систем, предназначенных для биометрической идентификации в реальном времени в общедоступных местах, за исключением строго определённых случаев.

Исключения (ст. 5(1)(d), пп. i–iii):

- поиск пропавшего лица или жертвы (например, похищенного ребёнка);

- предотвращение конкретной, существенной и неминуемой угрозы (например, теракта);

- идентификация подозреваемого в тяжком преступлении по судебному решению» [245].

Для правоохранительной деятельности это означает:

1. Повсеместное использование распознавания лиц в городах или общественном транспорте запрещено, если отсутствует основание, предусмотренное законом.

2. Массовая слежка через ИИ признана незаконной.

3. Применение требует судебного разрешения и строгой соразмерности.

Статья 5 Закона ЕС об ИИ устанавливает красные линии, за которые ИИ в правоохранительной деятельности выходить не может. Эти запреты базируются на необходимости защищать основные права, и соблюдение их критично для сохранения общественного доверия, судебного надзора и легитимности цифрового правоприменения.

При этом автор книги «Уклончивые предприниматели» А. Тьерер считает, что инновации в ИИ, появившиеся в США, никогда не появятся в Европе по определению, так как законы этого просто не позволяют. Он считает, что европейский подход к регулированию ИИ только укрепит мощь глобальных IT-гигантов, потому что только они могут содержать юридические службы, способные привести все в соответствие с нормами AI Act [246].

Соединенные Штаты Америки

В то же время США, которые до сих пор считались своеобразным «пристанищем» для инноваций в области ИИ, при либеральном подходе к регулированию этой сферы предпринимают первые предварительные шаги по установлению правил для инструментов ИИ, так как ажиотаж вокруг генеративного ИИ и чат-ботов достиг своего апогея.

Одним из ключевых событий стало издание в январе 2025 года Президентом Дональдом Трампом Указа «О снятии барьеров для американского лидерства в ИИ» (Removing Barriers Executive Order), который отменил Указ Президента Джо Байдена «О безопасной, надёжной и заслуживающей доверия разработке и применении ИИ» (Biden EO). Новый указ ориентирован на снятие административных и нормативных ограничений, противоречащих идее усиления глобального доминирования США в области ИИ. Это свидетельствует о резком сдвиге в сторону проинновационного и экономически ориентированного подхода к ИИ, в котором интересы национальной конкурентоспособности ставятся выше этико-правовых ограничений [247].

По данным Bloomberg, по состоянию на январь 2024 года в США не было федерального законодательства в области ИИ, но в октябре 2023 года президент Джо Байден в своем административном указе (англ. executive order) призвал к внедрению стандартов и тестированию моделей ИИ. Законы также появляются на уровне штатов и на местном уровне, ассоциации адвокатов некоторых штатов пишут этические рекомендации для юристов, использующих эту технологию, а суды взвешивают последствия применения ИИ для авторских прав.

По данным Белого дома, административный Указ президента Джо Байдена от 30 октября 2023 года «О безопасной, надежной и заслуживающей доверия разработке искусственного интеллекта и его использовании» (англ. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence) устанавливает новые стандарты безопасности и защиты ИИ, защищает частную жизнь американцев, продвигает равенство и гражданские права, отстаивает интересы потребителей и работников, способствует инновациям и конкуренции, укрепляет американское лидерство во всем мире и многое другое.

Являясь частью комплексной стратегии администрации Байдена-Харриса по ответственным инновациям, Указ опирается на предыдущие действия президента, включая работу, которая привела к добровольным обязательствам 15 ведущих компаний по обеспечению безопасного, надежного и заслуживающего доверия развития ИИ.

Здесь стоит остановиться на том, чем является административный указ. Административный приказ – это заявление президента или губернатора, имеющее силу закона, обычно основанное на существующих законодательных полномочиях. Для вступления в силу исполнительного приказа не требуется никаких действий со стороны Конгресса или законодательного органа штата, и законодательный орган не может его отменить.

Несмотря на то, что в Конституции США нет прямого упоминания об административном указе, однако в статье II есть упоминание о том, что исполнительная власть принадлежит президенту США. На эту норму ссылаются при наделении президента полномочиями по изданию административных указов.

Федеральные агентства уже начали принимать меры в отношении ИИ, в том числе Комиссия по равным возможностям в области трудоустройства стала бороться с предвзятостью при приеме на работу.

Многие законодатели США также призывали Конгресс принять меры. Без законодательства последствия Указа моглит оказаться кратковременными, если бы Байден потерял свой пост в 2024 году.

11 апреля 2023 года Министерство торговли США объявило, что официально запрашивает у общественности комментарии о том, как создать меры подотчетности для ИИ, и просит помощи в том, как посоветовать политикам США подходить к этой технологии.

Белый дом предложил «План Билля о правах ИИ», в котором изложены пять принципов предотвращения дискриминации и защиты конфиденциальности и безопасности пользователей, а Национальный институт стандартов и технологий выпустил структуру управления рисками ИИ.

Однако до сих пор Вашингтон придерживался добровольного подхода к соблюдению требований, в то время как эксперты говорят, что существует необходимость в более обязательном подходе к регулированию ИИ.

Окружной судья Вашингтона Берил Хауэлл 21 августа постановила, что произведение искусства, созданное искусственным интеллектом без участия человека, не может быть защищено авторским правом в соответствии с законодательством США, подтвердив отклонение Управлением по авторским правам заявки, поданной специалистом по компьютерам Стивеном Талером от имени его системы DABUS.

Федеральная торговая комиссия США (FTC) начала в июле масштабное расследование в отношении OpenAI по заявлениям о том, что она нарушила законы о защите прав потребителей, подвергнув риску личную репутацию и данные.

Генеративный ИИ вызывает опасения по поводу конкуренции и находится в центре внимания Бюро технологий FTC наряду с его Управлением технологий, сообщило агентство в блоге в июне.

В июне сенатор Майкл Беннет обратился с письмом к ведущим технологическим фирмам, призвав их маркировать контент, созданный искусственным интеллектом, и ограничить распространение материалов, направленных на введение пользователей в заблуждение. В апреле он внес законопроект о создании целевой группы для изучения политики США в области искусственного интеллекта [248].

Федеральный акт Соединённых Штатов «TAKE IT DOWN» от 19 мая 2025 года создал самостоятельный состав правонарушения, связанный с распространением интимных изображений без согласия, включая синтетические изображения, созданные средствами ИИ. Запрещено как размещение, так и угроза размещения; для взрослых предусмотрены штраф и лишение свободы до двух лет, для случаев с участием несовершеннолетних санкции строже. Закон опирается на проверяемый признак отсутствия согласия и очевидную приватность изображения, что устраняет прежний пробел между этикой площадок и публичным правом. Документ принят единодушно в Сенате и подавляющим большинством в Палате представителей, затем подписан президентом страны.

На площадки с пользовательским контентом возложены процессуальные обязанности: создать понятный порядок уведомления, удалить оспариваемый материал в течение сорока восьми часов после надлежащего обращения, пресекать повторные загрузки и принимать заявления от самого потерпевшего или уполномоченного представителя. Контроль осуществляет Федеральная торговая комиссия, отсутствует замещение права штатов, что сохраняет для потерпевших параллельные траектории защиты. Как нам представляется, нормативная логика объединяет восстановительную направленность в пользу жертвы и управленческую дисциплину для платформ.

Политическая и социальная поддержка была необычно широкой. Палата представителей проголосовала практически единогласно, значимые площадки и общественные фигуры публично поддержали инициативу, а история Эллистон Берри придала проблеме человеческое измерение и видимую срочность. Вместе с тем эксперты указывают на риски чрезмерного удаления, недостаточную процедурную защиту при ошибочных блокировках и потенциальное давление на частные каналы связи при внедрении инструментов выявления. Именно на этом участке, по нашему ощущению, будет проходить проверка устойчивости новой модели соотношения согласия, личности и сетевого распространения [249], [250], [251].

Китайская Народная Республика

В 2025 г. КНР демонстрирует существенный технологический прорыв (кейс с DeepSeek) и последовательно реализует «трёхшаговую» стратегию развития ИИ (план 2017-2030), что требует всестороннего правового обеспечения.

Требования к комплаенсу подробно описаны для провайдеров GAI-сервисов: алгоритмическая регистрация и оценка (CAC), маркировка контента, этическая экспертиза, жёсткие ограничения на сбор/обработку персональных данных.

КНР принял ряд нормативных актов, регулирующих цифровую трансформацию:

1. Закон КНР о защите персональных данных (PIPL, 2021) – регулирует сбор, обработку и защиту персональных данных.

2. Закон о безопасности данных (2021) – устанавливает правила обращения с чувствительной информацией.

3. Закон о кибербезопасности (2017) – регулирует защиту информационных систем и сетей.

4. Закон о научно-техническом прогрессе (2022).

Эти законы формируют основу цифровой правовой среды, в том числе при использовании ИИ. Однако они в меньшей степени охватывают конкретные особенности применения ИИ в уголовной юстиции.

Также существует ряд административных положений (2018-2023) и более чем десяток региональных регламентов (Шанхай, Шэньчжэнь, Фуцзянь, Чжэцзян и др.) [252], [253].

В 2021 году КНР опубликовала «Этические нормы ИИ нового поколения», где подчёркиваются следующие принципы: ориентация на человека, прозрачность, подотчётность, справедливость, недискриминация.

Эти положения служат ориентиром для разработчиков и государственных структур, однако пока не имеют обязательной силы в правоохранительной практике.

13 июля 2023 года Администрация киберпространства Китая опубликовала регулятивный документ под названием «Административные меры для генеративных услуг искусственного интеллекта», который вступил в силу 15 августа 2023 года.

Меры по генеративному ИИ применяются к «использованию технологии генеративного ИИ (относится к алгоритмам, моделям или другим правилам) для предоставления услуг по генерации текста, изображений, звуков, видео и другого контента на территории Китая». Требования этого постановления будут применяться к отечественным компаниям и зарубежным поставщикам услуг генеративного ИИ, предлагающим услуги генеративного ИИ широкой публике в Китае. Важно также отметить, что меры генеративного ИИ применяются к услугам, предлагаемым населению, а не к использованию услуг генеративного ИИ предприятиями.

Вот некоторые особенности постановления:

1. При разработке и использовании услуг генеративного ИИ поставщики услуг генеративного ИИ должны:

- не создавать незаконный контент, например, ложную или вредную информацию;

- принять эффективные меры по предотвращению создания дискриминационного контента;

- не использовать преимущества в алгоритмах, данных или платформах, если это ведет к монополии и недобросовестному конкурентному поведению;

- не нарушать права на портреты, права на репутацию, права чести, права на неприкосновенность частной жизни и права на личную информацию;

- принять эффективные меры в зависимости от типов услуг для повышения прозрачности услуг генеративного ИИ, а также точности и надежности контента генеративного ИИ.

2. В отношении данных обучения поставщики услуг генеративного ИИ должны:

- использовать данные и базовые модели из законных источников;

- не нарушать законную интеллектуальную собственность других лиц;

- получать персональные данные с согласия или в случаях, предусмотренных законом или административными мерами;

- принять эффективные меры по повышению качества обучающих данных, их правдивости, точности, объективности и разнообразия.

3. При предоставлении услуг генеративного ИИ поставщики услуг генеративного ИИ несут обязательства по кибербезопасности как производители онлайн-информационного контента и обязательства по защите личной информации как обработчики личной информации и должны:

- заключать договоры на обслуживание с зарегистрированными пользователями услуг генеративного ИИ, в которых определяются права и обязанности обеих сторон;

- направлять пользователей по законному использованию генеративной технологии искусственного интеллекта и принимать эффективные меры для предотвращения чрезмерной зависимости пользователей от созданных услуг искусственного интеллекта или «зависимости от них»;

- не собирать второстепенную личную информацию, не хранить незаконно входную информацию и записи об использовании, которые могут быть использованы для идентификации пользователя, а также не предоставлять незаконным образом входную информацию пользователей и записи об использовании другим лицам;

- получать и удовлетворять запросы субъектов данных;

- должны обеспечивать маркировку тегами контента, такого как фотографии и видео, созданного ИИ в соответствии с «Административными положениями о глубоком синтезе информационных услуг Интернета (Положения о глубоком синтезе)»;

- в случае обнаружения незаконного контента принять меры по прекращению создания, передачи и удалению незаконного контента, принять меры по исправлению ситуации, такие как улучшение модели, и сообщить об этом соответствующим компетентным органам;

- в случае обнаружения пользователей, использующих генеративные услуги искусственного интеллекта для ведения незаконной деятельности, принять меры по предупреждению пользователя или ограничению,

приостановке или прекращению предоставления услуги, сохранить записи и сообщить об этом соответствующим компетентным органам;

- создать механизм приема и обработки жалоб пользователей.

4. В отношении других юридических обязательств и надзора за исполнением поставщики услуг генеративного ИИ должны:

- если услуга генеративного ИИ обладает атрибутом общественного мнения или способностью к социальной мобилизации, выполнить обязательство по оценке безопасности и (в течение десяти рабочих дней с даты предоставления услуг) пройти формальности по регистрации в соответствии с Административными положениями по рекомендации алгоритма, для информационных услуг Интернета (положения алгоритмов);

- в случае, когда соответствующие компетентные органы (например, CAC) начинают надзорные проверки службы генеративного ИИ, сотрудничать с ними, объяснить источник, размер и типы обучающих данных, правила маркировки, а также механизмы и принципы алгоритма и предоставить необходимые технологии, данные и т.д. для поддержки и помощи.

После одобрения правительством четыре китайские технологические фирмы, включая Baidu Inc и SenseTime Group, 31 августа 2023 года запустили свои чат-боты с искусственным интеллектом для широкой аудитории.

На момент подготовки данного анализа отсутствует специальный закон, определяющий границы и процедуры применения ИИ в правоохранительных органах.

Главным регулирующим органом выступает Канцелярия по вопросам киберпространства Китая (CAC), которая утверждает модели ИИ перед внедрением в общественные сферы, осуществляет надзор, аудит и определяет штрафные санкции [245].

Хотя указанные правовые акты не ориентированы напрямую на полицию, они прямо регулируют:

1. Использование систем видеонаблюдения с ИИ-распознаванием лиц.

2. Применение ИИ при анализе данных в расследованиях.

3. Правила использования ИИ в предиктивном (превентивном) правопорядке.

Любые системы ИИ, применяемые органами правопорядка, обязаны:

1) проходить аудит и проверку на соответствие ценностям и безопасности;

2) обеспечивать прозрачность и защиту данных.

Необходимо найти оптимальный баланс между стимулированием инноваций и минимизацией рисков, связанных с развитием ИИ. Данная дилемма напоминает парадокс Коллинриджа, где свобода воли (предполагается, что ИИ обладает определенной степенью автономности и может принимать нестандартные решения, что можно сравнить со свободой воли) сталкивается с предопределенностью (алгоритмы ИИ часто работают на основе детерминированных процессов, что можно сравнить с предопределенностью) [254], [255].

С одной стороны, чрезмерное регулирование может стать барьером для новых идей в сфере ИИ. С другой стороны, отсутствие контроля может привести к созданию технологий, угрожающих безопасности и этике.

В ответ на неправомерное использование ИИ Китай законодательно закрепил «прозрачность происхождения» цифровых артефактов через специальные «Меры по обозначению синтетического контента, созданного средствами искусственного интеллекта», вступившие в силу 1 сентября 2025 г. Правовой акт требует двухконтурной идентификации для текста, изображений, аудио, видео и «виртуальных сцен»: явные пометки (надписи, графические и звуковые сигналы) и скрытые пометки (метаданные, в том числе сведения об изготовителе и уникальный идентификатор). Обязанности распределены по всей экосистеме: разработчики, службы распространения и каталоги приложений несут установленные функции; при скачивании и экспорте пометки должны сохраняться. Одновременно введён обязательный национальный стандарт GB 45438-2025, который детализирует формат явных и скрытых пометок (например, высота текстовой метки на изображении не менее 5 % короткой стороны; для аудио допустим голосовой маркер или ритмический сигнал). Эти Меры институционально опираются на ранее принятые акты о «глубоком синтезе» и управлении генеративными сервисами.

Регуляторная логика представляется двойственной: эпистемическая компонента обеспечивает распознаваемость и трассируемость синтетики, а превентивная компонента снижает риски дезинформации, манипуляций и нарушений прав. Показательно, что до вступления норм в силу регулятор удалил свыше 960 тысяч единиц неправомерного контента в рамках целевой кампании; крупные платформы объявили о внедрении механизмов пометок и дообозначения материалов пользователей. При сравнении с европейским правом наблюдается различие в темпе и степени императивности: в Европейском союзе обязательства по прозрачности вводятся поэтапно в 2025–2026 гг., тогда как китайская модель сразу задаёт детальные технологические параметры и распределённую ответственность. На наш взгляд, практическая развилка теперь в устойчивости пометок при агрессивной обработке и в калибровке «ложноположительных» срабатываний детекторов, так как именно здесь будет решаться баланс между инновацией и нормативной определённостью [256].

Сингапур

Как и во многих других странах, в Сингапуре отсутствует всеобъемлющий закон или нормативная база, специально посвященная ИИ. Вместо этого в настоящее время он опирается на существующие законы, принципы общего права, регулирующие органы и недавно ввел национальные руководящие принципы для регулирования вопросов, связанных с ИИ [194, p. 156-168].

В апреле 2023 года министр связи и информации заявил на заседании парламента, что Сингапур поддерживает ответственную разработку и развертывание ИИ, чтобы его преимуществами можно было пользоваться в обстановке доверия и безопасности. Для достижения этой цели была внедрена

модель управления фреймворком ИИ. Такие компании, как DBS, HSBC, Visa и Microsoft, внедрили эту структуру для решения ключевых этических и управленческих проблем при внедрении решений ИИ. Еще одним инструментом является AI Verify, система самотестирования и инструментарий для демонстрации ответственного внедрения ИИ. Им заинтересовались более 50 компаний. Комиссия по защите персональных данных (PDPC) в течение года выдаст консультативные рекомендации по использованию персональных данных в системах искусственного интеллекта в соответствии с Законом о защите персональных данных (PDPA). Они взаимодействуют с отраслевыми и международными партнерами по вопросам, связанным с ИИ, через наш Консультативный совет по этичному использованию ИИ и данных и Глобальное партнерство по искусственному интеллекту. Подобно тому, как правительство Сингапура регулирует использование данных, кибербезопасность, дезинформацию и онлайн-вред, они будут продолжать анализировать состояние технологий, подход к регулированию и его эффективность для поддержания доверия и безопасности в цифровых разработках [257], [258].

Российская Федерация

Национальная стратегия развития искусственного интеллекта до 2030 года является ключевым документом, создающим в Российской Федерации благоприятную среду для создания и внедрения интеллектуальных систем. Государство, его ведомства и крупные корпорации вкладывают значительные средства в сбор наборов данных и разработку моделей машинного обучения в различных отраслях экономики, как в государственном, так и в частном секторах [259].

Ключевой фигурой в этическом и правовом регулировании деятельности по развитию искусственного интеллекта в России является Альянс по искусственному интеллекту.

В соответствующем этическом кодексе, разработанном этой организацией, оговариваются только случаи гражданского (невоенного) использования, что представляется существенным упущением. Кроме того, с позиций юридической техники документ, по сути, призывает к коллективному внешнему воздействию на участников этой технологии, что, на примере многих международных договоров, не является оптимальным: в логике развития любой критической технологии достаточно одному нарушителю задать другой вектор ее формирования. На наш взгляд, этико-правовое регулирование должно осуществляться «снизу» и исходить от непосредственных лиц, участвующих в разработке интеллектуальных систем. В то же время вышеперечисленные недостатки рассматриваемого документа легко объясняются широким кругом его подписантов. В настоящее время данный кодекс предусматривает обязательный учет свойств подотчетности и справедливости при развитии систем искусственного интеллекта в России. Мы считаем, что игнорирование критерия прозрачности связано с осознанием того, что на данном этапе технологического развития его соблюдение представляется маловероятным [194, p. 156-168].

Важным аспектом развития систем искусственного интеллекта в России является изучение рисков и ограничений внедрения этой технологии. Так, А. Бессонов и Д. Бахтеев (Воронков) в своих работах, связанных с развитием прикладных систем в правоохранительной деятельности, неоднократно указывали на необходимость предварительного изучения аспекта человеческой деятельности, который оптимизируется с помощью интеллектуальных систем; необходимость обучения сотрудников правоохранительных органов основам технологии перед внедрением ее в правовые процессы; соотнесение принципов формирования системных выводов с критериями оценки [260], [261].

Из трех критериев, заявленных в начале статьи, справедливость воспринимается в России как ключевая: системы искусственного интеллекта воспринимаются как способ обеспечения точности и эффективности юридических процедур. Большинство опросов общественности и юристов показывают положительное отношение граждан к таким системам. В то же время попытки внедрения систем машинного обучения в судебные и экспертные системы наталкиваются на невыполнение критериев подотчетности и прозрачности, что может замедлить внедрение интеллектуальных технологий в российскую правовую систему. Соответственно, необходимо соблюдать принцип: если принятие большого количества решений может быть оценено статистически, то индивидуальное решение, не может быть исследовано на предмет правильности его логики, и в этом случае должна оставаться возможность изучения ситуации квалифицированным специалистом-человеком.

Анализ национальных моделей регулирования применения технологий искусственного интеллекта в правоохранительной сфере позволил выделить разносторонние и контрастные подходы, формирующиеся под влиянием различий в правовых системах, политико-административных установках и степени зрелости цифровых экосистем.

В правопорядке Европейского союза преобладает превентивно-защитная парадигма, где вопросы технологического развития подчинены задачам охраны фундаментальных прав и свобод личности. Регуляторные инициативы здесь нацелены на ограничение избыточных или рискоориентированных форм ИИ-применения, особенно в случаях, затрагивающих приватность, недискриминацию и автономию индивида.

Американская юрисдикция, в противоположность европейской, опирается на децентрализованный механизм, в котором ключевую роль играют корпоративные инициативы, негосударственные стандарты и внутренняя правовая адаптация действующих норм под реалии автоматизации. Прагматическая ориентация на технологическое лидерство нередко отодвигает вопросы регулирования на второй план.

Китайский опыт демонстрирует противоположную модель, основанную на институциональном доминировании государства и приоритете национальной безопасности. Здесь ИИ интегрируется в практики повседневного надзора, анализа поведения и оперативной идентификации,

при этом вопросы прозрачности и гражданского контроля находятся в зачаточном состоянии.

Сингапур выступает в роли своеобразного медиатора между Востоком и Западом, реализуя технократически выверенную стратегию, сочетающую эффективность с элементами этико-юридической культуры. Разработанные рамки управления ИИ акцентируют внимание на доверии, подотчетности и возможности адаптации к изменяющимся социальным условиям.

Правовая архитектура Российской Федерации в рассматриваемой области характеризуется инерционной институционализацией ИИ-инструментов без унифицированного нормативного фреймворка. Использование алгоритмических систем ограничивается рамками отраслевых законов, в то время как механизмы подотчётности и гражданского контроля пока остаются недостаточно разработанными.

Итогом проведённого сравнительного анализа стало выделение трёх основных подходов к регулированию искусственного интеллекта в правоохранительной сфере:

– правозащитный подход (Европейский союз), где ИИ применяется с приоритетом на защиту прав и свобод человека;

– инновационно-гибкий подход (США и Сингапур), ориентированный на развитие технологий с минимальными ограничениями;

– подход с государственным доминированием и контролем (Китай и Россия), при котором ИИ используется преимущественно в целях обеспечения безопасности и работает под управлением государственных органов.

Каждая из этих моделей содержит как положительные стороны, так и потенциальные риски. Их осмысленное сопоставление с правовыми традициями и особенностями государственного управления позволяет разрабатывать более сбалансированные и эффективные механизмы регулирования ИИ с учётом потребностей Республики Казахстан.

3 ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

3.1 Применение искусственного интеллекта в судебной деятельности

Интеграция технологий ИИ в сферу судебной деятельности представляет собой одно из наиболее значимых направлений цифровизации правосудия, сопряжённое с трансформацией традиционных процессуальных механизмов и переосмыслением роли субъективного усмотрения. В условиях усложнения социальной реальности, возрастания объёмов информации и требований к оперативности принятия решений ИИ-технологии приобретают всё большую значимость в обеспечении аналитической поддержки судей, автоматизации рутинных процедур и оптимизации администрирования судебных процессов.

Тем не менее, процесс интеграции ИИ в судебную сферу не может рассматриваться в категориях простой технической модернизации традиционных институтов. Он неизбежно обостряет комплекс правовых, этических и институциональных дилемм, требующих критического осмысления через призму фундаментальных принципов правосудия, таких как независимость судебной власти, равенство процессуальных сторон, презумпция невиновности и право на справедливое судебное разбирательство. Применение алгоритмически опосредованных решений в рамках судопроизводства объективно обусловливает необходимость формирования нормативной архитектуры, способной одновременно минимизировать риски алгоритмической предвзятости, гарантировать прозрачность процедур и сохранить пространство для индивидуализированного судебного усмотрения в условиях нарастающей технологической медиатизации процессуальной деятельности.

Именно в этом контексте особую значимость приобретает направление, связанное с использованием технологий ИИ для создания механизмов выявления отклонений от стандартов надлежащего осуществления судебной деятельности. Внедрение интеллектуальных систем в процессы мониторинга правосудия предполагает разработку механизмов, способных в автоматизированном режиме выявлять возможные отклонения от стандартов надлежащего отправления правосудия, при этом не затрагивая основополагающий принцип независимости судей. Речь идет не о вмешательстве в существо принимаемых решений, а об аналитической поддержке институтов правового надзора, направленной на обеспечение единообразия судебной практики и повышение уровня процедурной справедливости.

Интеллектуальные технологии в данном случае используются для систематического анализа принятых судебных актов, сопоставления их с установленными стандартами процессуального права и выявления аномалий,

которые могут свидетельствовать о рисках нарушения принципов равенства сторон, презумпции невиновности или иных гарантий справедливого разбирательства. Например, система может фиксировать случаи систематического несоблюдения процессуальных сроков, частого отказа в удовлетворении определённых категорий ходатайств без достаточной мотивации либо значительные расхождения в санкциях за аналогичные деяния в пределах одной юрисдикции.

В качестве примера можно привести использование ИИ для анализа решений по уголовным делам о кражах: если интеллектуальная система выявит, что за одинаковые по сути эпизоды в аналогичных обстоятельствах в одном суде выносятся мягкие наказания, а в другом – значительно более строгие, это может стать поводом для дополнительного изучения ситуации компетентными органами, без какого-либо давления на судей в рамках конкретного дела. Ещё один пример – анализ решений о мере пресечения: если система обнаруживает, что определённый судья значительно чаще других выбирает содержание под стражей, даже при наличии альтернативных мер, это также может быть предметом обсуждения на уровне судебной статистики или внутреннего аудита.

Подобные инструменты способствуют повышению институциональной транспарентности, укрепляют доверие общества к судебной системе и обеспечивают дополнительные механизмы раннего выявления возможных проблем в правоприменительной практике. При этом важно подчеркнуть, что использование таких аналитических систем требует чёткого нормативного регулирования: алгоритмы не должны становиться основанием для автоматического вынесения суждений о профессионализме судьи без всестороннего анализа контекста дела, а выводы, полученные в результате интеллектуального анализа, должны рассматриваться исключительно в качестве одного из источников информации для принятия управленческих решений в рамках установленных процедур независимого надзора.

Одной из ключевых угроз, сопровождающих интеграцию искусственного интеллекта в судебную деятельность, является феномен так называемого «эффекта автоматического согласия» (automation bias) [262]. Под данным явлением понимается склонность судебных акторов – судей, прокуроров, адвокатов – придавать чрезмерное значение рекомендациям и заключениям, сформулированным алгоритмическими системами, нередко в ущерб самостоятельной критической оценке правовых ситуаций. Такая тенденция способствует формированию ложного представления о непогрешимости алгоритмических решений, что объективно ведет к девальвации фундаментальных процессуальных принципов, включая презумпцию невиновности, состязательность сторон и право на судебную защиту. Автоматизация процесса принятия решений, при всей внешней эффективности, может нивелировать требуемую законом степень индивидуализации подхода к каждому делу, подменяя сложный правовой анализ статистическими корреляциями и вероятностными оценками, что, в

конечном итоге, угрожает институционализацией алгоритмической предвзятости.

На фоне данных рисков возникает объективная необходимость разработки и внедрения комплексных этических кодексов, регламентирующих применение технологий искусственного интеллекта в судопроизводстве. Этические кодексы должны содержать положения, направленные на обеспечение транспарентности алгоритмических процедур, установление обязательности информирования участников процесса о факте использования ИИ, закрепление права на оспаривание автоматизированных рекомендаций, а также сохранение пространства для самостоятельного принятия решений судьями. Немаловажным является также требование предупреждения алгоритмической дискриминации, защиты персональных данных, соблюдения процессуальных прав сторон и обеспечения аудируемости алгоритмических процедур. Следует подчеркнуть, что подобные стандарты должны быть интегрированы не только на уровне внутренних актов судебных органов, но и иметь надлежащую правовую регламентацию в национальном и международном законодательстве.

Важным направлением является также определение разумных пределов автоматизации механизмов анализа судебной деятельности. Применение искусственного интеллекта для мониторинга и анализа судебных актов на предмет системных ошибок, нарушений сроков рассмотрения дел, соблюдения единообразия правоприменительной практики может способствовать повышению эффективности и транспарентности судопроизводства. Однако замена экспертной оценки профессиональной компетентности судей исключительно алгоритмическими средствами представляется концептуально недопустимой. Искусственный интеллект, фиксируя отдельные факты и выявляя статистические аномалии, не обладает возможностью адекватно учитывать специфику конкретных дел, изменчивость правовой практики и значимость социального контекста рассматриваемых споров. Следовательно, автоматизированные средства должны рассматриваться исключительно как вспомогательные инструменты, дополняющие, но не подменяющие суждение компетентных коллегиальных органов судебного сообщества.

Особое значение в условиях цифровизации приобретает сохранение индивидуализированного подхода в судебной практике. Судебная деятельность требует деликатного учета уникальности фактических обстоятельств каждого дела, правовых позиций сторон, общественной значимости и социального контекста спора. Индивидуализация судебных решений не только служит гарантией справедливости в конкретном процессе, но и укрепляет общественное доверие к судебной власти, обеспечивая восприятие суда как института, способного учитывать человеческий фактор и многообразие жизненных ситуаций. В этой связи внедрение технологий искусственного интеллекта должно строиться на принципах субсидиарности, при которых ИИ рассматривается как вспомогательный элемент судебной деятельности, а решающее значение в осуществлении правосудия остается за

человеком, обладающим необходимым уровнем профессиональной интуиции, правовой эрудиции и нравственной ответственности.

Таким образом, интеграция ИИ в механизмы обеспечения качества судебной деятельности открывает новые возможности для развития правосудия, но одновременно требует соблюдения высоких стандартов правовой определённости, процессуальной справедливости и уважения к принципу судебной независимости.

Одним из ключевых направлений применения технологий искусственного интеллекта в области правосудия становится переводческое сопровождение и языковое обеспечение судебных процедур. В условиях глобализации, увеличения миграционных потоков и роста числа участников судебного процесса, не владеющих государственным языком, вопросы эффективного языкового посредничества приобретают всё большую значимость. Решение данных задач имеет принципиальное значение для обеспечения справедливого судебного разбирательства, равенства сторон и недискриминационного доступа к правосудию.

Исторически переводческое сопровождение судебных процедур осуществлялось исключительно с привлечением профессиональных переводчиков, обладающих специализированной подготовкой в области юридического языка. Однако современные реалии, характеризующиеся резким увеличением объемов документооборота и усложнением языкового взаимодействия в многонациональных юрисдикциях, объективно требуют автоматизации ряда процессов. В этой связи всё большую роль начинают играть интеллектуальные технологии, прежде всего системы машинного перевода и обработки естественного языка, способные значительно ускорить и упростить решение переводческих задач в рамках судопроизводства.

Применение технологий искусственного интеллекта в данной сфере реализуется в нескольких направлениях. Одним из них является автоматизация перевода письменных процессуальных документов, включая исковые заявления, судебные акты, протоколы заседаний и материалы доказательственного характера. Современные интеллектуальные системы машинного перевода, обученные на юридических корпусах текстов, обеспечивают не только механический перенос информации с одного языка на другой, но и адекватную передачу юридического содержания, что критически важно для сохранения точности и недвусмысленности процессуальных актов.

Другим направлением становится внедрение технологий автоматического синхронного перевода в режиме реального времени в ходе судебных заседаний. Системы распознавания речи и обработки естественного языка позволяют оперативно обеспечивать перевод высказываний участников процесса на необходимый язык, что особенно востребовано при рассмотрении дел с участием иностранных граждан, мигрантов и лиц без гражданства. Такое технологическое сопровождение даёт возможность оперативно устранять языковые барьеры, минимизируя необходимость привлечения большого числа переводчиков и ускоряя процессуальные процедуры.

Тем не менее, использование интеллектуальных технологий в сфере переводческого сопровождения судебных процедур сопряжено с рядом правовых, этических и технических рисков. Прежде всего, возникает проблема точности автоматизированных переводов: даже незначительные ошибки в передаче юридической информации могут повлечь существенные нарушения процессуальных прав участников дела. Ошибочный перевод обвинения, показаний свидетеля или содержания судебного акта способен деформировать весь ход разбирательства, поставить под сомнение его справедливость и привести к нарушениям основополагающих принципов права. В связи с этим в нормативном регулировании необходимо закрепить обязательные требования к проверке и верификации результатов машинного перевода, особенно в случаях, когда от качества перевода зависит судьба правового положения лица в процессе.

Дополнительной проблемой является защита персональных данных, обрабатываемых в процессе автоматического перевода судебных документов. Системы ИИ должны функционировать в рамках жёстких требований конфиденциальности и обеспечивать невозможность утечки чувствительной информации, затрагивающей права сторон, содержание доказательств или иные сведения, составляющие предмет судебной тайны.

Отдельное внимание должно быть уделено адаптации интеллектуальных переводческих систем к особенностям юридического языка и культурно-языковым спецификам различных групп населения. Юридическая терминология нередко оперирует концептами, не имеющими точных аналогов в других языках, что требует от интеллектуальных систем не только лингвистической, но и правовой интерпретационной компетентности. Ошибочная трактовка таких понятий способна существенно исказить правовое содержание текста и повлечь нарушение принципа справедливого разбирательства.

На практике внедрение технологий ИИ в переводческое сопровождение судебных процедур требует построения комплексной системы обеспечения качества переводов. Эта система должна включать первичную автоматическую обработку текста, обязательную экспертную проверку результатов квалифицированными судебными переводчиками, разработку специализированных юридических глоссариев и постоянное обучение алгоритмов на основе утвержденных судебных текстов. Также необходимо внедрить процедуры системной корректировки и обратной связи, позволяющие интеллектуальным системам постоянно улучшать свои результаты в соответствии с практическими требованиями судопроизводства.

Следует особо подчеркнуть, что автоматизация переводческого сопровождения судебных процедур не может полностью заменить участие человека. Технологии должны использоваться в качестве вспомогательных инструментов, призванных повышать скорость и удобство работы, но окончательная ответственность за корректность перевода должна оставаться за профессиональными судебными переводчиками. В делах особой социальной чувствительности, связанных с правами человека, депортацией,

международной правовой помощью, участие профессионала является обязательным элементом процессуальной защиты.

Таким образом, применение технологий искусственного интеллекта в переводческом сопровождении и языковом обеспечении судебных процедур представляет собой важный этап развития цифрового правосудия, направленный на расширение доступности судебной защиты для всех категорий населения. Вместе с тем такая интеграция требует выверенного нормативного регулирования, устанавливающего чёткие стандарты качества, механизмы контроля, гарантии защиты прав участников процесса и процедурные требования к функционированию интеллектуальных систем. Только при соблюдении этих условий возможно гармоничное сочетание технологической эффективности и обеспечения фундаментальных прав и свобод личности в рамках цифровой трансформации судебной системы.

В контексте цифровой трансформации правосудия всё большее значение приобретает административное и ресурсное сопровождение судебной деятельности с использованием технологий ИИ. Речь идёт о внедрении интеллектуальных решений, направленных на оптимизацию управленческих процессов внутри судебной системы, повышение эффективности распределения ресурсов, автоматизацию рутинных процедур и обеспечение устойчивой институциональной инфраструктуры для осуществления правосудия. В современных условиях административное сопровождение включает в себя не только классические элементы организационного обеспечения – такие как планирование судебных заседаний, распределение дел между судьями, учёт процессуальных сроков, но и более сложные функции, связанные с предиктивной аналитикой нагрузки на суды, оптимизацией кадровых и материально-технических ресурсов, прогнозированием потребностей в инфраструктурном развитии на основе обработки больших массивов данных. Интеллектуальные системы способны анализировать статистику поступления дел, оценивать динамику процессуальных действий, выявлять закономерности перераспределения деловой активности по регионам или юрисдикциям, тем самым предоставляя руководителям судов инструменты для более обоснованного и оперативного принятия административных решений. Например, алгоритмы могут моделировать сценарии изменения судебной нагрузки при изменении законодательства или судебной практики, что позволяет заранее планировать перераспределение ресурсов, своевременно увеличивать штат сотрудников либо оптимизировать внутренние процессы.

Отдельным направлением ресурсного сопровождения с участием ИИ является автоматизация документооборота и процедур обеспечения открытости судебной деятельности. Интеллектуальные платформы позволяют систематизировать архивы судебных актов, автоматизировать их публикацию с соблюдением требований обезличивания данных, оптимизировать процессы приёма обращений граждан и организаций, а также обеспечивать оперативное взаимодействие судов с иными государственными органами через интегрированные цифровые экосистемы. Существенное значение имеет и

использование ИИ для логистического обеспечения судебной деятельности – например, при планировании маршрутов доставки процессуальных документов, оптимизации использования залов судебных заседаний или управлении судебными вызовами сторон и свидетелей.

Организация процессов обработки информации и документации в судопроизводстве представляет собой один из краеугольных аспектов обеспечения эффективного функционирования судебной системы в условиях её цифровой трансформации. В современных условиях, когда объемы информации, циркулирующей в рамках судебных процедур, многократно возросли, а требования к оперативности и точности документооборота значительно ужесточились, традиционные методы работы с информацией становятся недостаточными. Это обстоятельство предопределяет необходимость внедрения комплексных систем автоматизированной обработки данных и оптимизации процедурного документооборота с использованием технологий искусственного интеллекта (ИИ) и интеллектуальных систем управления процессами.

Эффективная организация информационных потоков в судебной деятельности включает в себя создание и сопровождение электронных делопроизводственных систем, которые обеспечивают централизованное хранение, систематизацию, классификацию, поиск, передачу и архивирование судебной документации. В рамках таких систем обеспечивается возможность быстрого доступа к процессуальным материалам для судей, помощников, секретарей судебных заседаний, сторон и их представителей, при этом реализуются необходимые уровни доступа и механизмы защиты конфиденциальной информации. Автоматизация документооборота позволяет минимизировать временные и трудовые издержки на подготовку, пересылку и обработку бумажных носителей, что особенно актуально в условиях роста числа рассматриваемых дел и увеличения процессуальной сложности.

Технологии ИИ, интегрированные в систему электронного судопроизводства, способны автоматизировать процессы сортировки документов по категориям дел, выявления дубликатов, проверки полноты поданных материалов, а также предварительного анализа содержания документов для оптимизации их обработки на последующих этапах. Например, интеллектуальные алгоритмы могут автоматически распознавать реквизиты процессуальных документов, сопоставлять их с базой действующих процессуальных требований и сигнализировать о наличии нарушений либо недочетов, требующих устранения. В ряде юрисдикций уже применяются пилотные проекты по автоматической разметке поступающих исковых заявлений, жалоб и ходатайств с привязкой к соответствующим процессуальным кодексам, что значительно ускоряет начальную обработку материалов и сокращает вероятность человеческих ошибок.

Организация процессов обработки судебной информации также предполагает создание и поддержание баз данных судебной практики, доступных как для внутреннего пользования судами, так и для публичного ознакомления в целях обеспечения транспарентности и единообразия

правоприменения. Электронные архивы судебных актов с возможностью поиска по различным критериям – времени, типу спора, применённым нормам права, позиции суда по аналогичным делам – служат важнейшим ресурсом для подготовки обоснованных решений и повышения качества судебного правосудия. Интеллектуальные системы могут анализировать эти массивы данных для выявления отклонений от устоявшейся практики, что, в свою очередь, помогает в обеспечении процессуальной справедливости и стабильности судебной практики.

Необходимо отметить, что оптимизация обработки информации в судопроизводстве должна сопровождаться строгим соблюдением принципов процессуальной законности, сохранения тайны личной жизни, адвокатской тайны и других видов защищённой информации. Технологическая модернизация не должна нарушать права участников процесса на равный доступ к информации и на защиту от неправомерного использования персональных данных. Поэтому внедрение систем автоматизированной обработки судебной информации должно предусматривать многоуровневую систему защиты данных, процедуры аутентификации пользователей, шифрование каналов связи и ведение журналов доступа для последующего контроля.

Кроме того, процессы цифровизации документооборота требуют совершенствования внутреннего организационного регулирования: разработки и утверждения стандартов электронного судопроизводства, инструкций по работе с электронными документами, регламентов хранения и уничтожения электронных материалов. В условиях постоянного развития технологий необходимо предусматривать механизмы регулярной актуализации этих стандартов, чтобы поддерживать их соответствие требованиям процессуальной эффективности и информационной безопасности.

Таким образом, организация процессов обработки информации и документации в судопроизводстве является системным элементом обеспечения эффективности, прозрачности и доступности судебной деятельности в цифровую эпоху. Она направлена на повышение скорости и качества рассмотрения дел, сокращение административной нагрузки на судебных работников, создание предпосылок для более объективного и обоснованного отправления правосудия, при неукоснительном соблюдении правовых стандартов защиты информации и процессуальной справедливости.

Однако интеграция интеллектуальных систем в сферу административного сопровождения судопроизводства требует соблюдения целого ряда принципов. Прежде всего, это обеспечение процессуальной независимости судей, исключение любого давления через административные алгоритмы, а также прозрачность критериев, на основании которых принимаются управленческие решения с использованием ИИ. Любая автоматизация должна допускать возможность человеческой коррекции и апелляции, особенно в случаях, когда алгоритмические рекомендации затрагивают вопросы распределения дел, рассмотрения обращений либо

организационных решений, влияющих на права сторон. Кроме того, необходимо учитывать риски технологического неравенства, когда несбалансированное внедрение цифровых решений может усиливать различия между отдельными судами в зависимости от их технического оснащения, кадрового потенциала и уровня цифровой зрелости.

Таким образом, административное и ресурсное сопровождение судебной деятельности с применением технологий ИИ представляет собой важнейшее направление модернизации судебной системы, способствующее повышению её эффективности, прозрачности и устойчивости. При этом его развитие должно основываться на принципах правового равенства, технологической нейтральности, уважения к независимости суда и обязательного учёта человеческого фактора на всех этапах цифровизации судебного управления. Только при соблюдении этих условий возможно гармоничное сочетание технологического прогресса с сохранением фундаментальных гарантий справедливого правосудия в условиях цифровой эпохи.

В условиях нарастающей сложности общественных процессов и увеличения объема юридически значимой информации особое значение приобретает развитие аналитической обработки данных для нужд судопроизводства. Интеграция технологий ИИ в судебную сферу открывает новые горизонты для повышения качества, обоснованности и эффективности судебных решений, обеспечивая возможность глубокой систематизации, интерпретации и прогнозирования на основе масштабных массивов данных. Применение интеллектуальных аналитических платформ позволяет не только автоматизировать поиск релевантной судебной практики и правовых норм, но и выявлять скрытые корреляции между обстоятельствами дел, динамикой изменения судебных подходов и тенденциями правоприменительной практики в различных юрисдикциях. В частности, системы интеллектуального анализа могут строить профили правовых рисков, оценивать вероятность определённых процессуальных исходов на основе исторических данных, выявлять паттерны изменения судебной нагрузки, а также прогнозировать влияние новых законодательных инициатив на судебную практику.

На уровне практического применения аналитическая обработка данных в судопроизводстве позволяет, например, формировать автоматизированные подборки прецедентов, структурировать аргументацию сторон, выявлять ошибки в применении норм права или логические противоречия в судебных актах. Кроме того, интеллектуальные системы способны поддерживать процесс вынесения судебных решений путём предоставления судье информации о ранее рассмотренных аналогичных делах, статистике удовлетворения определённых видов требований, средней продолжительности рассмотрения аналогичных процессов, что, при соблюдении необходимых процессуальных гарантий, может повысить единообразие и предсказуемость судебной практики. Примером эффективного применения аналитики является использование интеллектуальных систем для оценки обоснованности мер пресечения: анализируя сотни тысяч решений, ИИ

может выявлять тенденции и обоснованные критерии, минимизируя субъективизм и способствуя соблюдению принципа пропорциональности ограничительных мер.

При этом следует подчеркнуть, что внедрение аналитической обработки данных в судебную деятельность не должно вести к снижению уровня индивидуализации судебного усмотрения или к механическому следованию статистическим выводам. ИИ в данном контексте должен восприниматься как вспомогательный инструмент поддержки судебного решения, а не как его автоматизированный заместитель. Судебная власть, обладающая особыми полномочиями в обеспечении прав и свобод личности, обязана сохранять приоритет человеческого разума, нравственного суждения и процессуальной справедливости перед алгоритмическими рекомендациями.

Особую важность имеет и вопрос верифицируемости аналитических выводов, формируемых ИИ-системами. Все результаты интеллектуального анализа должны быть прозрачными, обоснованными и воспроизводимыми в условиях судебного контроля, а применяемые алгоритмы подлежат проверке на соответствие принципам недискриминации, нейтральности и процедурной допустимости. Кроме того, необходимо учитывать этическую и правовую ответственность разработчиков и операторов систем аналитической обработки данных, поскольку результаты, формируемые ИИ, могут оказывать значительное влияние на процессуальные позиции сторон и итоговые судебные решения.

Таким образом, развитие аналитической обработки данных для нужд судопроизводства представляет собой неотъемлемый элемент современной цифровой трансформации системы правосудия. Оно должно осуществляться на основе комплексного баланса между технологическими возможностями, правовыми стандартами и фундаментальными принципами справедливого судебного разбирательства, обеспечивая тем самым повышение качества судебной деятельности, укрепление её транспарентности и доверия со стороны общества.

Таким образом, интеграция технологий ИИ в сферу судебной деятельности представляет собой сложный и многоплановый процесс, охватывающий как технические, так и глубинные правовые, этические и институциональные аспекты функционирования правосудия. ИИ открывает новые возможности для повышения эффективности, транспарентности и доступности судебных процедур, автоматизации рутинных процессов, оптимизации административного сопровождения и углубления аналитической обработки правовой информации.

В то же время он ставит перед судебной системой вызовы, требующие системного нормативного ответа: обеспечение индивидуализации судебного усмотрения, недопущение алгоритмической предвзятости, защита процессуальных прав сторон, сохранение судебной независимости и укрепление принципов справедливого судебного разбирательства. Особое значение приобретает выстраивание правового и этического регулирования применения ИИ, включающего механизмы проверки достоверности

алгоритмических решений, обеспечение транспарентности процедур, защиту персональных данных и обязательную верификацию переводческих и аналитических операций, осуществляемых с использованием интеллектуальных систем.

Приоритетным остаётся утверждение подхода, при котором ИИ используется как вспомогательный инструмент, дополняющий профессиональное правосудие, но не заменяющий самостоятельное и ответственное решение судьи. В конечном итоге успешная цифровая трансформация судебной системы возможна лишь при соблюдении баланса между технологическим прогрессом и фундаментальными принципами правового государства, что требует комплексного, междисциплинарного и ориентированного на защиту прав человека подхода к регулированию применения ИИ в судопроизводстве.

3.2 Применение искусственного интеллекта в прокурорском надзоре

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.

Согласно ст.1 Конституционного закона Республики Казахстан «О прокуратуре» от 5 ноября 2022 года (ЗРК «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» [263].

В условиях роста информационной нагрузки, усложнения правоприменительных процессов и усиления требований к оперативности реагирования технологии ИИ начинают рассматриваться в качестве вспомогательного механизма, способствующего укреплению аналитической и прогностической составляющей надзорной деятельности. Интеграция ИИ позволяет повысить эффективность мониторинга исполнения законодательства, осуществлять углублённый 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 чётком 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 технологий 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.

Согласно п.1 ст.1 ЗРК «О прокуратуре», «Систему актов прокуратуры составляют:

1) акты прокурорского надзора: протест, санкция, указание, представление, постановление;

2) акты прокурорского реагирования: ходатайство, заявление (иск), обращение, разъяснение о недопустимости нарушений законов Республики Казахстан;

3) акты, регулирующие вопросы организации и деятельности органов прокуратуры: приказы, распоряжения, положения, инструкции, регламенты и другие» [263].

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 контексте 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 остаётся 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.

Благодаря обучению на обширных массивах правовых документов, актов судебной практики и материалов прокурорских проверок, интеллектуальные системы приобретают способность выявлять устойчивые правовые конструкции, повторяющиеся аргументативные шаблоны и типовые формальные признаки, характерные для различных категорий правонарушений в сфере трудового, экологического, бюджетного, административного, уголовного и антикоррупционного законодательства. Применение технологий искусственного интеллекта (ИИ) в автоматизации подготовки актов прокурорского надзора позволяет существенно повысить качество, обоснованность и единообразие документов, а также сократить временные затраты на их составление.

Так, 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 причинённого 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 волокиты или необоснованного прекращения уголовных дел. Интеллектуальные системы способны оперативно сопоставить действия (или бездействие) следственных органов с процессуальными требованиями Уголовно-процессуального кодекса, 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 контекстуальные нюансы, такие как социальная значимость выявленного нарушения, характер и степень причинённого 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 отдалённых 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.

Следовательно, автоматизация составления актов прокурорского надзора и реагирования посредством применения технологий 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 ключевых 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 контекстного анализа и искажением принципа соразмерности реагирования по отношению к конкретным правонарушениям.

Вторым важным 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 её сформировал алгоритм, что связано с проблемой «чёрного 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 важной является проблема юридической ответственности. Вопрос о том, кто несёт ответственность за юридическую ошибку в акте прокурорского надзора, сформированном с участием ИИ – разработчик, оператор, прокурор или ведомство в целом – до сих пор остаётся без нормативного разрешения. Это создаёт неопределённость, 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, обобщённых и адресных мер прокурорского реагирования.

Согласно ст.20 ЗРК «О прокуратуре», «Анализ состояния законности проводится без посещения прокурорами субъектов (объектов) путем изучения статистических данных, сведений государственных и международных организаций, средств массовой информации, материалов гражданских и уголовных дел, дел об административных правонарушениях, а также иных источников информации» [263].

ИИ-системы, обученные на репрезентативных выборках нормативных правовых актов, судебных решений, статистических данных, материалов прокурорских проверок и обращений граждан, способны формировать комплексные аналитические отчёты 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 определённом 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 загрязнённости, 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 искажённые 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 «чёрного 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.

Ещё одним критическим 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, контекстуальным пониманием ситуации и правовой ответственностью.

Таким образом, эффективное использование ИИ в анализе состояния законности требует соблюдения целого комплекса организационных и правовых условий. Прежде всего, это разработка нормативных регламентов, определяющих сферы допустимого применения ИИ, процедуры верификации результатов и порядок привлечения алгоритмов к принятию 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 соблюдения прав человека, интеграция ИИ в функции анализа состояния законности может стать устойчивым инструментом повышения эффективности и обоснованности прокурорского надзора. ИИ не должен заменять человека, но обязан усиливать его способность видеть картину в целом, ориентироваться в сложных массивах информации и принимать решения, соответствующие принципам правового государства.

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, путём 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 путём 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 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 контексте 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.

Ещё одним вызовом является алгоритмическая непрозрачность, 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, к примеру, о возбуждении уголовного дела, наложении ареста на имущество или направлении запроса о возврате активов из-за рубежа. Следовательно, используемые алгоритмы должны быть подотчетными, интерпретируемыми и подлежащими аудиту, а механизмы их применения – чётко регламентированными.

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 этом контексте развитие отечественных решений и платформ становится ключевым условием обеспечения информационной безопасности в сфере мониторинга активов.

Таким образом, интеллектуальные технологии обладают значительным потенциалом в сфере анализа информации, связанной с незаконным приобретением и трансграничным перемещением активов, но их применение должно быть встроено в чёткую 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 восстановлением социальной справедливости.

Установление 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 учётом 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.

Согласно ст. 10 Конституционного закона Республики Казахстан «О прокуратуре», «прокурор в праве: требовать незамедлительной отмены мер запретительного или ограничительного характера, приостановления полностью или частично действия незаконного акта при наличии оснований и в порядке, предусмотренном законом Республики Казахстан». В соответствии со ст. 37 «прокурор выносит постановление: об отмене действий и мер запретительного либо ограничительного характера, необоснованно осуществляемых государственными, местными представительными и исполнительными органами, органами местного самоуправления, организациями, субъектами квазигосударственного сектора, а также их должностными и иными лицами».

Однако по мере устранения обстоятельств, послуживших основанием для введения ограничительных или запретительных мер, перед правоприменительными органами, в том числе прокуратурой, встаёт 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 этом контексте 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 обновлённые 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 – продолжение 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 Конституционного Суда или изменённой практики применения норм, на которых основывался приостановленный акт. Всё 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, 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.

Проверка материалов уголовных дел прокурором является одной из ключевых форм надзорной деятельности, направленной на обеспечение законности в уголовном судопроизводстве. В соответствии с положениями статьи 193 УПК Республики Казахстан прокурор, в частности: «9) получает для проверки от органов уголовного преследования уголовные дела, документы, материалы, в том числе результаты оперативно-розыскных, контрразведывательных мероприятий и негласных следственных действий, направляет уголовные дела, по которым прерваны сроки для производства дальнейшего расследования; …11) возвращает уголовное дело для производства дополнительного расследования либо прекращает досудебное расследование в полном объеме или в отношении конкретных лиц» [50].

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.

Согласно ст.301 УПК РК, «Прокурор изучает поступившее с отчетом о завершении досудебного расследования уголовное дело и проверяет:

1) имело ли место деяние и содержит ли это деяние состав уголовного правонарушения;

2) нет ли в деле обстоятельств, влекущих его прекращение;

3) подлежит ли деяние подозреваемого переквалификации;

4) подтверждается ли инкриминируемое лицу деяние имеющимися в деле доказательствами;

5) по всем ли установленным уголовно наказуемым деяниям лицо признано подозреваемым;

6) приняты ли меры для привлечения к уголовной ответственности всех лиц, в отношении которых по делу добыты доказательства о совершении ими уголовных правонарушений;

7) нет ли в деле оснований для избрания, изменения либо отмены меры пресечения;

8) приняты ли меры обеспечения гражданского иска и возможной конфискации имущества;

8-1) связано ли имущество подозреваемого, обвиняемого с уголовным правонарушением, являющимся основанием для возможной конфискации, в случаях, предусмотренных статьей 48 Уголовного кодекса Республики Казахстан, и представлены ли доказательства относимости данного имущества к предмету конфискации;

9) не допущены ли в производстве досудебного расследования существенные нарушения уголовно-процессуального закона;

10) приняты ли органом уголовного преследования меры по установлению сумм процессуальных издержек и других сумм для обеспечения их взыскания судом;

11) имеются ли основания для заключения процессуального соглашения» [50].

При наличии нарушений прокурор обязан возвратить уголовное дело для устранения недостатков. Так, согласно ч.1 ст.302 УПК РК, «1. По результатам изучения материалов уголовного дела прокурор производит одно из следующих действий: …3) направляет уголовное дело лицу, осуществляющему досудебное расследование, для производства дополнительного расследования» [50].

Интеграция технологий искусственного интеллекта (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 по ст. 189 УК РК интеллектуальная система может выявить отсутствие заключения финансово-экономической экспертизы [52].

Также отсутствие протокола допроса лиц, выполняющих функции финансового контроля в организации, свидетельствует о неполной реализации принципа всесторонности при сборе доказательственной базы [52].

Во-вторых, интеллектуальные алгоритмы позволяют оперативно обнаруживать процессуальные ошибки, которые в дальнейшем могут повлечь признание доказательств недопустимыми по основаниям, указанным в ст. 112 УПК РК. 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 влечёт необходимость соответствующего прокурорского реагирования в рамках надзора за соблюдением процессуального законодательства.

В-третьих, ИИ может служить инструментом проверки соблюдения процессуальных прав участников процесса. Путём 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, предусмотренный ст. 129 УПК РК.

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 (ст. 382 УПК РК) или заключения соглашения о признании вины (ст. 612 УПК РК) [50]. 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 даёт основание для объединения

производств в порядке ст. 43 УПК РК или возбуждения новых уголовных дел по выявленным эпизодам [50].

Дополнительно интеллектуальные системы могут предлагать проекты процессуальных решений: постановлений о возврате дела для дополнительного расследования (ст. 302 УПК РК), об изменении меры пресечения (ст. 153 УПК РК), о прекращении уголовного дела за отсутствием состава уголовного правонарушения (п. 2 ч. 1 ст. 35 УПК РК) [50]. 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 оценки конкретных обстоятельств дела.

Например, в практике может возникнуть ситуация, когда дело о мошенничестве в сфере страхования (ст. 190 УК РК) поступает в прокуратуру для составления обвинительного акта [52]. ИИ-система, анализируя материалы дела, выявляет, что все допросы потерпевших проведены без соблюдения положений о разъяснении их прав и обязанностей, предусмотренных ст. 71 УПК РК [50]. 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 путём (ст. 218 УК РК). 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.

Тем не менее, 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 технологий искусственного интеллекта 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.

Формирование линии обвинения является одним из центральных этапов досудебного производства, определяющим структуру и качество последующего судебного разбирательства. В соответствии со ст.ст. 301 и 302

УПК прокурор после изучения материалов уголовного дела, поступившего с отчетом о завершении досудебного расследования, 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. Особую роль на этом этапе играют не только объём собранных доказательств, но и их юридическая значимость, относимость и допустимость, как это прямо предусмотрено ст.ст. 112 и 113 УПК РК.

Интеграция технологий 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, в соответствии с требованиями Общей части Уголовного кодекса Республики Казахстан.

Например, в делах о коррупционных преступлениях (глава 15 УК РК) 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 причинённого ущерба, ИИ может рекомендовать проведение дополнительного допроса либо экономической экспертизы, что способствует своевременному устранению пробелов в доказательственной базе.

Отдельного внимания заслуживает возможность применения ИИ для подготовки проектов процессуальных документов: обвинительных актов, ходатайств о применении мер пресечения, представлений о привлечении дополнительных доказательств. В этих проектах автоматически учитываются требования ст.ст. 302–303 УПК РК 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, установленных ст. 19 УПК РК.

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.

Одним из показательных примеров экспериментальной интеграции технологий ИИ в процесс формирования линии обвинения является китайский проект создания так называемого «прокурора на основе ИИ». Как сообщается в публикации South China Morning Post, учёные Китайской академии наук разработали нейросетевую систему, способную на основе анализа материалов уголовного дела формулировать версии обвинения с высокой степенью точности. Система прошла апробацию в Народной прокуратуре Шанхая и демонстрирует способность идентифицировать восемь наиболее распространённых категорий преступлений, включая мошенничество, участие в азартных играх, опасное вождение, умышленное причинение вреда

здоровью, воспрепятствование выполнению служебных обязанностей и ряд других правонарушений. Алгоритмы системы были обучены на массиве из более чем 17 тысяч реальных уголовных дел, рассмотренных в период с 2015 по 2020 годы, что позволило добиться прогностической точности, превышающей 97% по заявленным категориям дел.

Тем не менее, несмотря на впечатляющие результаты, реальный масштаб применения данной технологии остаётся ограниченным как по кругу анализируемых преступлений, так и по процессуальным возможностям. В соответствии с действующей китайской практикой окончательное решение о возбуждении уголовного дела и формулировании обвинения по-прежнему принимается судьёй или прокурором, а нейросетевая система рассматривается лишь в качестве вспомогательного инструмента поддержки их решений. Это обстоятельство подчёркивает важнейший принцип: искусственный интеллект в уголовном процессе должен играть исключительно субсидиарную роль, не подменяя собой профессиональное суждение правоприменителя [264], [265].

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 подкреплённым допустимыми доказательствами, соответствующими требованиям процессуального закона.

Таким образом, формирование линии обвинения с использованием технологий 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.

3.3 Применение искусственного интеллекта в следственной деятельности

Интеграция технологий искусственного интеллекта (ИИ) в следственную деятельность открывает новые горизонты для модернизации уголовного судопроизводства, предлагая качественно иные инструменты для повышения эффективности, обоснованности и оперативности принимаемых процессуальных решений. Современные интеллектуальные системы, обладающие возможностями машинного обучения, анализа больших массивов данных и выявления скрытых закономерностей, способны не только автоматизировать рутинные аналитические процедуры, ранее отнимавшие значительные ресурсы, но и существенно обогащать процесс формирования следственных версий, оценки доказательственной базы и построения целостной логики расследования.

В условиях постоянного усложнения криминогенной среды, возрастания масштабов и сложности преступных схем, а также стремительного роста объёмов доступной информации, включая цифровые следы, метаданные и

данные из открытых источников, традиционные методы расследования всё в большей степени испытывают перегрузку. В этих реалиях использование ИИ становится не просто технологической опцией, а стратегической необходимостью для следственных органов, стремящихся обеспечивать высокий уровень процессуальной справедливости и эффективность уголовного преследования.

Анализ имеющихся материалов уголовного дела с целью построения простых и сложных следственных гипотез и определения направлений их проверки является одной из центральных задач следственной деятельности, направленной на обеспечение полноты, всесторонности и объективности досудебного расследования. Следователь обязан выдвигать версии о событиях преступления, проверять их и принимать решения, основанные на допустимых и достоверных доказательствах. При этом особую актуальность приобретает системный, аналитический подход к обработке больших массивов информации, что в современных условиях возможно при интеграции технологий ИИ.

На ранней стадии досудебного расследования следователь анализирует первичные материалы – заявления о преступлении, объяснения очевидцев, результаты осмотра места происшествия, экспертные заключения. На основании этих данных формулируются гипотезы относительно механизма совершения преступления, мотивации подозреваемого, способов сокрытия преступления. Простые следственные гипотезы касаются отдельных элементов преступления: например, способа взлома в деле о краже либо предмета посягательства при расследовании хищения. Сложные гипотезы включают в себя предположения о структуре преступной группы, уровне организованности, наличии предварительного сговора, особенностях распределения ролей среди участников.

ИИ-платформы, основанные на анализе больших данных и машинном обучении, позволяют оперативно обрабатывать массивы информации, выявлять нетипичные корреляции, скрытые зависимости и аномалии в поведении участников событий. Например, в деле о получении взятки должностным лицом в одном из акиматов ИИ, анализируя биллинги телефонных переговоров, перемещения по базам видеонаблюдения «Сергек» и данные о сделках с недвижимостью, может помочь установить, что контакт между должностным лицом и посредником происходил значительно чаще вблизи объектов, связанных с государственными закупками.

В качестве другого примера можно привести расследование факта серии мошенничеств с использованием цифровых платформ. Изначально следователь на основе заявлений потерпевших формирует гипотезу о действии одного злоумышленника. Однако интеллектуальная система, анализируя схожесть цифровых следов – IP-адресов, паттернов текстов сообщений, способов передачи денег через электронные кошельки, – выявляет существование сети связанных между собой аккаунтов, что позволяет выдвинуть более сложную версию о наличии организованной преступной группы, действующей на территории нескольких регионов страны.

ИИ также может использоваться для сопоставления имеющихся доказательств с правоприменительной практикой судов Казахстана. Например, если в деле о хищении ИИ фиксирует аналогичные обстоятельства в ранее рассмотренных Верховным Судом РК делах, он может подсказать следователю направления для дополнительной проверки фактов, необходимых для доказывания наличия состава преступления (например, корыстной цели, предварительного умысла).

Результаты анализа ИИ не могут сами по себе являться доказательствами, а служат лишь вспомогательным средством для обоснования следственных действий, которые затем должны быть закреплены процессуальными способами: протоколами, заключениями экспертов, показаниями.

При этом необходимо учитывать ограничение на вмешательство в частную жизнь граждан, требующее получения судебного санкционирования для доступа к сведениям о телефонных переговорах, переписке или банковских операциях. Использование ИИ должно быть встроено в процессуальные рамки: если интеллектуальный анализ выявил необходимость получения дополнительных данных, следователь обязан оформить соответствующее ходатайство в суд.

Гипотетический пример, характерный для казахстанской практики: при расследовании дела о самовольном захвате земельного участка в пригороде Алматы ИИ, сопоставляя данные кадастрового учета, записи нотариусов и сведения об участниках электронных торгов, может выявить, что за юридическим лицом, оформившим документы, стоит лицо, ранее судимое за аналогичные действия. Такая информация позволяет выдвинуть обоснованную сложную гипотезу о систематическом характере преступной деятельности.

Ещё один пример: в деле о дорожно-транспортном происшествии с тяжкими последствиями ИИ анализирует не только показания участников ДТП, но и данные с камер «Сергек», скорость движения автомобиля по данным GPS-логов, характер тормозного пути. Результаты анализа могут подтолкнуть следователя к версии о наличии предварительного употребления алкоголя водителем либо сокрытия факта технической неисправности автомобиля.

Следует подчеркнуть, что использование ИИ при построении следственных версий в Казахстане требует учёта ряда рисков. Во-первых, существует риск некорректной интерпретации результатов интеллектуального анализа, если следователь без должной критики перенимает выводы алгоритма. Во-вторых, алгоритмическая непрозрачность некоторых систем затрудняет процесс обоснования процессуальных решений перед судом. В-третьих, существует угроза несанкционированного доступа к обработанным данным, что требует соблюдения требований Закона РК «О персональных данных и их защите».

Одним из наиболее сложных этапов расследования уголовных правонарушений является воссоздание события преступления и его следовой

картины в условиях ограниченности, противоречивости или фрагментарности исходных данных. Следователь обязан обеспечить полноту, всесторонность и объективность исследования обстоятельств дела, что в современных условиях многократно затрудняется усложнением способов совершения преступлений, развитием технологий их сокрытия и увеличением объёма обрабатываемой информации. В этом контексте ИИ открывает новые возможности для аналитической реконструкции событий, используя опыт, накопленный в ходе расследования множества уголовных дел.

Применение ИИ в процессе воссоздания следовой картины предполагает использование алгоритмов машинного обучения, обученных на больших массивах данных, включающих в себя судебные решения, материалы следствия, заключения экспертиз и другие источники процессуальной информации. Такие интеллектуальные системы способны выявлять устойчивые модели поведения преступников, закономерности взаимодействия между различными элементами преступной деятельности, а также сопоставлять имеющиеся в деле признаки с типовыми сценариями аналогичных правонарушений.

Гипотетическим примером может служить ситуация с расследованием разбойного нападения на ювелирный магазин в городе А. При осмотре места происшествия обнаружены лишь частичные следы обуви и осколки витрин, а видеонаблюдение отсутствует из-за преднамеренного выведения камер из строя. Интеллектуальная система, опираясь на базу аналогичных дел, может предположить участие нескольких лиц, спрогнозировать возможные маршруты отхода, а также предложить гипотезу о применении заранее подготовленного транспортного средства. Эти выводы, разумеется, должны быть проверены в ходе последующих следственных действий, но позволяют оптимизировать план расследования уже на начальной стадии.

Другой пример связан с делами о дорожно-транспортных происшествиях со смертельным исходом в условиях отсутствия прямых свидетелей. При расследовании аварии в А., когда на месте происшествия обнаружены лишь обрывки лакокрасочного покрытия и фрагменты фар, интеллектуальная система может смоделировать вероятный тип транспортного средства, установить возможное направление движения и предположить механизм столкновения. Это даёт возможность быстрее определить круг подозреваемых транспортных средств и организовать их проверку.

ИИ также способен строить альтернативные версии событий, если исходная информация допускает несколько возможных интерпретаций. Например, при обнаружении тела с признаками падения с высоты в многоэтажном доме система может предложить несколько сценариев: самоубийство, несчастный случай или насильственное причинение смерти. На основе анализа сопутствующих факторов – наличия следов борьбы, предшествующего поведения потерпевшего, содержания его социальных сетей – система поможет приоритезировать версии и определить направления проверки.

Следует подчеркнуть, что реконструкции, осуществляемые с помощью ИИ, носят вероятностный характер и не могут служить самостоятельными доказательствами. Их роль заключается в аналитической поддержке следствия, выявлении логических связей между фактами и оптимизации планирования следственных действий. Именно человек – следователь, обладающий юридической квалификацией и опытом правоприменения, принимает окончательные решения о выдвижении гипотез и способах их проверки.

Применение интеллектуальных систем в воссоздании следовой картины также позволяет более эффективно работать с ситуациями, когда преступники намеренно искажают обстановку места происшествия. В случаях инсценировки кражи или сокрытия следов убийства ИИ способен за счёт выявления нестандартных аномалий в структуре события предположить наличие преднамеренного искажения действительности, что требует от следствия особой внимательности.

Особую ценность ИИ имеет при расследовании сложных экономических, коррупционных и организованных преступлений, где события растянуты во времени, пространстве и имеют множественные пересечения участников. Здесь интеллектуальные алгоритмы могут моделировать цепочки действий, выявлять ключевых фигурантов и указывать на критические временные промежутки, требующие дополнительной проверки.

Наряду с очевидными преимуществами, интеграция ИИ в процессы реконструкции событий несёт и определённые риски. Основной из них – вероятность чрезмерного доверия к алгоритмическим моделям при игнорировании уникальности конкретного уголовного дела. Существует также риск алгоритмической предвзятости, когда система, обученная на неполных или искажённых данных, может ошибочно придавать избыточное значение несущественным признакам.

Кроме того, важным этическим требованием является соблюдение конфиденциальности персональных данных, содержащихся в материалах уголовных дел, что особенно актуально в условиях использования технологий больших данных. В случае анализа материалов, касающихся частной жизни граждан, должна быть обеспечена максимальная защита информации от несанкционированного доступа и неправомерного использования.

Перспективным направлением развития технологий ИИ в сфере воссоздания следовой картины является интеграция интеллектуальных систем с электронными базами уголовных дел, базами криминалистических учётов и архивами судебной практики. Это позволит формировать более полные, актуализированные и достоверные модели событий, существенно повышая качество предварительного расследования.

Таким образом, использование ИИ в воссоздании событий преступления и его следовой картины на основе неполных данных представляет собой мощный инструмент аналитической поддержки следствия, способствующий более полному, всестороннему и объективному исследованию обстоятельств дела. Однако эффективность такого подхода напрямую зависит от

профессионализма следователя, способности критически воспринимать результаты интеллектуального анализа и строго соблюдать баланс между технологическими возможностями и принципами уголовного процесса.

Поиск признаков серийности при расследовании уголовных правонарушений представляет собой одну из наиболее сложных задач следственной аналитики, особенно в условиях фрагментарной или противоречивой исходной информации. Это обстоятельство требует от органов досудебного расследования высокой степени системности, способности к выявлению скрытых взаимосвязей между эпизодами преступной деятельности и применения методов многокритериального анализа.

В этой связи интеграция ИИ в процесс выдвижения и проверки следственных версий серийного характера приобретает особую актуальность. В условиях отечественной правоохранительной практики, особенно в регионах с высокой территориальной дисперсией и ограниченными кадровыми ресурсами, интеллектуальные системы могут выполнять вспомогательные функции по раннему распознаванию повторяемых паттернов преступного поведения, выявлению схожих обстоятельств совершения деяний и формированию обоснованных предположений о наличии связи между инцидентами.

Так, например, при наличии серии краж из частных домов в пригородах К., совершённых без свидетелей, в ночное время и с использованием схожего способа взлома (через пластиковые окна), интеллектуальный анализ позволяет систематизировать эти эпизоды и рассмотреть возможность их объединения в одно производство по признакам серийности. При этом в условиях отсутствия прямых улик (отпечатков пальцев, ДНК, видеозаписей) система может обратить внимание на косвенные признаки: временные интервалы, географическую близость, специфику похищенного имущества, наличие похожих средств сокрытия.

Далее, алгоритмы, обученные на базе уголовных дел аналогичной категории, способны предложить типовые направления проверки – например, установление передвижений лиц, ранее судимых за аналогичные преступления, мониторинг продаж похищенного имущества на онлайн-площадках или сопоставление с ранее прекращенными делами по формальным основаниям. Кроме того, ИИ может предлагать нестандартные гипотезы: например, если временной промежуток между преступлениями строго цикличен, это может указывать на распорядок трудовой деятельности преступника. Применение таких подходов позволяет компенсировать дефицит информации за счёт вовлечения скрытых закономерностей, неочевидных для анализа традиционными методами.

При этом необходимо подчеркнуть, что ИИ не заменяет следователя в выдвижении окончательных версий, а лишь помогает структурировать данные, выделить ключевые индикаторы серийности и снизить вероятность упущения важных связей.

Вместе с тем необходимо чётко осознавать, что применение ИИ в целях выявления признаков серийности преступлений сопряжено с целым рядом как технических, так и правовых ограничений. Одной из серьёзных угроз является возможность алгоритмической ошибки, в том числе вследствие переобучения моделей на нерепрезентативных или искажённых данных. В условиях, когда система анализирует массив уголовных дел, содержащий в себе предвзятости, ошибки протоколирования или неполную информацию, существует риск ложной корреляции – объединения в одну серию эпизодов, объективно не связанных между собой. Такая ошибка способна исказить общую картину расследования, привести к выдвижению неверных следственных версий, неправомерному расширению предмета доказывания или даже к предъявлению необоснованных подозрений в отношении непричастных лиц.

Особое внимание следует уделить этическим аспектам применения интеллектуальных технологий. Одним из краеугольных камней уголовного судопроизводства в Республике Казахстан, как и в международной правовой практике, остаётся принцип презумпции невиновности. Любая аналитика, основанная на вероятностных выводах ИИ, не может и не должна подменять собой фактическое установление обстоятельств дела надлежащими процессуальными средствами. Иными словами, даже при высокой степени вероятности, рассчитанной интеллектуальной системой, любое объединение дел в серию, как и любые последующие процессуальные решения, должны основываться исключительно на результатах традиционных следственных действий: осмотра места происшествия, допросов, экспертиз и других проверенных методов.

Дополнительным риском является снижение уровня критического восприятия у следователя при высокой кажущейся объективности алгоритмического вывода. Психологический эффект «автоматического согласия» может привести к тому, что следователь будет склонен безусловно доверять предложенным ИИ гипотезам, воспринимая их как «научно обоснованные», тогда как на практике они требуют не меньшей, а зачастую даже большей степени проверки. В особенности это касается ситуаций, когда на основе ограниченного объёма данных формируются выводы о причастности конкретного лица к серии эпизодов, что требует особой процессуальной аккуратности и верификации.

В целях минимизации указанных рисков использование интеллектуальных систем должно сопровождаться чётко установленными регламентами, предусматривающими, что любые алгоритмические выводы рассматриваются исключительно в качестве вспомогательных предпосылок для дальнейшей ручной аналитики и оперативно-следственных мероприятий. В каждом конкретном случае необходимо проведение дополнительной проверки полученных данных с использованием комплекса средств, предусмотренных уголовно-процессуальным законодательством: оперативных мероприятий, следственных экспериментов, дополнительных допросов потерпевших и свидетелей, сравнительных криминалистических экспертиз.

В практическом контексте правоохранительной деятельности эти требования означают необходимость внедрения внутренних стандартов работы с системами аналитического сопровождения следствия, ориентированных на процессуальную допустимость и защиту прав лиц, вовлечённых в уголовное производство. Например, в случае, если интеллектуальная система указала на вероятность серийности в ряде краж с проникновением в жилища в городе А., следователь обязан не просто принять это к сведению, но и провести комплексный сравнительный анализ всех материалов дел: методов проникновения, характера похищенного имущества, способов сокрытия следов, времени и места совершения преступлений, профиля предполагаемого преступника.

Важно подчеркнуть, что автоматизация этапа формирования следственных гипотез, даже при её высокой технологической оснащенности, не отменяет необходимости профессионального следственного суждения, которое опирается на юридическое образование, опыт расследования аналогичных преступлений и умение видеть нюансы, не отражаемые в цифровых данных. Таким образом, внедрение ИИ в сферу выявления серийности преступлений действительно способно значительно повысить эффективность следственной работы, но лишь при условии строгого соблюдения требований правовой допустимости, сохранения человеческого контроля и обеспечения технологической прозрачности процессов.

Повторная оценка полноты и допустимости доказательств с целью принятия решения о предъявлении обвинения либо направлении уголовного дела в прокуратуру представляет собой одну из ключевых стадий следственного процесса, требующую особой тщательности, системности и соответствия принципам процессуальной справедливости. В период перехода к использованию ИИ в следственной деятельности данная процедура получает новые инструменты аналитической поддержки, способные существенно повысить качество и оперативность подготовки окончательных процессуальных решений.

Применение интеллектуальных систем в этом контексте заключается, прежде всего, в автоматизированной обработке массивов следственных материалов: протоколов допросов, результатов экспертиз, заключений специалистов, вещественных доказательств и иных процессуальных документов. ИИ способен выявлять внутренние логические несоответствия между доказательствами, фиксировать отсутствие ключевых элементов доказательственной базы, сопоставлять фактические данные с требованиями уголовно-процессуального законодательства о допустимости, относимости и достаточности доказательств. Например, интеллектуальная система может сигнализировать о ситуации, когда показания свидетеля, положенные в основу обвинения, не были подтверждены независимыми источниками информации либо когда протокол осмотра места происшествия не содержит обязательных реквизитов, необходимых для признания его процессуально допустимым.

В практическом контексте использование ИИ может существенно способствовать повышению стандартов доказывания, требуемых для

последующего судебного разбирательства. Так, интеллектуальные алгоритмы способны автоматически проверять полноту выполнения следственных действий, обязательных для определённых категорий дел (например, проведение судебно-медицинской экспертизы по делам о причинении тяжкого вреда здоровью или об изнасиловании), а также сопоставлять собранные доказательства с элементами состава преступления, предусмотренными Уголовным кодексом. При выявлении пробелов в доказательственной базе система может рекомендовать проведение дополнительных процессуальных действий: допросов, очных ставок, дополнительных экспертиз, что способствует минимизации рисков возвращения дела прокурором для дополнительного расследования или прекращения производства в суде в связи с недостаточностью доказательств.

Тем не менее, следует подчеркнуть, что применение ИИ в оценке полноты и допустимости доказательственной базы не освобождает следователя от обязанности осуществлять собственную юридическую квалификацию материалов дела и принимать решения на основе внутреннего убеждения, сформированного с соблюдением всех процессуальных гарантий. ИИ может выступать эффективным вспомогательным инструментом структурирования информации, выявления аномалий и логических несоответствий, но не может подменить собой оценочное усмотрение следственного органа. Особенно это актуально в случаях, когда отдельные доказательства обладают высокой степенью субъективной оценки их достоверности и допустимости (например, показания несовершеннолетних свидетелей, результаты сложных криминалистических экспертиз).

Особую актуальность в современных условиях приобретает также использование интеллектуальных технологий для проверки процессуальных сроков и стадийности уголовного преследования. ИИ может автоматически отслеживать соблюдение сроков досудебного расследования, выявлять случаи их превышения без должной правовой мотивации, а также сигнализировать о рисках нарушения разумных сроков рассмотрения дела, что имеет важное значение как для соблюдения прав подозреваемого, так и для поддержания легитимности всего уголовного процесса.

Кроме того, в условиях цифровизации следственной деятельности особенно важным становится обеспечение технологической прозрачности и проверяемости работы интеллектуальных систем. Все заключения и рекомендации, сформулированные ИИ, должны быть подвержены верификации человеком – следователем, и не иметь самостоятельной юридической силы без соответствующего процессуального оформления. На законодательном уровне требуется установление стандартов по фиксации работы интеллектуальных систем в уголовном процессе: например, в виде автоматизированных отчётов, приобщаемых к материалам дела и позволяющих в дальнейшем оценить корректность работы алгоритмов в случае обжалования итоговых процессуальных решений.

Говоря о гипотетических примерах, можно привести ситуацию, когда следователь, расследующий дело о крупной растрате в государственном

учреждении, использует интеллектуальную систему для повторной оценки имеющихся доказательств перед принятием решения о предъявлении обвинения. Система выявляет, что протоколы выемки финансовых документов, на которых основывается обвинение, содержат процедурные нарушения, связанные с отсутствием понятых при изъятии. В результате следователь проводит дополнительную выемку с соблюдением всех требований закона и устраняет риск признания ключевых доказательств недопустимыми в суде. В другом примере ИИ может обратить внимание на отсутствие процессуальной связи между результатами аудиторской проверки и установленными в ходе следствия фактами причинения ущерба, что требует проведения дополнительного допроса эксперта-аудитора для устранения противоречий.

Таким образом, повторная оценка полноты и допустимости доказательств с использованием технологий ИИ в следственной деятельности способна стать важнейшим инструментом повышения качества уголовного преследования, при условии соблюдения принципов процессуальной законности, уважения к правам сторон и сохранения решающего значения человеческого профессионального усмотрения. В условиях цифровизации правосудия в Республике Казахстан развитие подобных интеллектуальных решений должно сопровождаться формированием нормативных рамок, обеспечивающих баланс между эффективностью автоматизации и незыблемыми гарантиями справедливого судебного разбирательства.

Интеграция ИИ и цифровых инструментов в сферу расследования уголовных дел открывает новые возможности для оперативного уточнения фактических обстоятельств посредством анализа данных, размещённых в социальных сетях, архивных копиях интернет-страниц, результатах поисковых систем и других открытых онлайн-ресурсах. В современных условиях значительная часть социальной и деловой активности субъектов переносится в виртуальную среду, что делает цифровые следы важным источником информации для следственных органов.

Использование ИИ в данном контексте позволяет автоматизировать сбор, систематизацию и предварительную аналитику данных из многообразных цифровых источников. Интеллектуальные системы способны, например, выявлять публикации, фотографии, видеофайлы, комментарии и иные формы цифровой активности, релевантные расследуемым событиям, а также сопоставлять эти данные с другими материалами уголовного дела. Такие технологии могут фиксировать факты взаимодействия между фигурантами дела, подтверждать или опровергать наличие между ними социальной связи, устанавливать их местоположение в определённый временной промежуток, а также выявлять сведения о потенциальных свидетелях.

На практике это может выражаться, например, в анализе геолокационных меток в публикациях социальных сетей, подтверждающих или опровергающих алиби подозреваемого; в восстановлении удалённых постов или сообщений через кэш поисковых систем; в анализе временных

метаданных цифрового контента для определения последовательности событий. При расследовании преступлений, связанных с мошенничеством или киберпреступностью, интеллектуальные системы могут выявлять закономерности в структуре интернет-коммуникаций, а при расследовании преступлений против личности – фиксировать признаки конфликтных взаимоотношений, угроз или иных признаков предшествующего инцидента.

Однако применение данных из онлайн-источников сопряжено с целым рядом правовых и этических ограничений. Прежде всего, возникает вопрос допустимости использования такой информации в качестве доказательств в уголовном процессе, что требует строгого соблюдения процессуальных норм, касающихся источников получения доказательств, их подлинности, относимости и допустимости. Фиксация и извлечение информации из сети должны осуществляться с соблюдением процессуальных формальностей – с составлением соответствующих протоколов осмотра, привлечением понятых либо применением инструментов электронного нотариата.

Вторым важным аспектом является обеспечение конфиденциальности и защиты персональных данных, особенно если речь идёт о сборе сведений о третьих лицах, не являющихся фигурантами дела. Использование данных должно быть строго ограничено рамками установленной законом цели расследования и соответствовать принципу пропорциональности вмешательства в частную жизнь.

Кроме того, следует учитывать риск манипулирования цифровыми данными: возможность их удаления, изменения, фальсификации требует применения специальных методов верификации цифровых доказательств, в том числе с использованием технологий блокчейна для фиксации метаданных и историчности контента.

Применение ИИ в анализе онлайн-ресурсов не освобождает следственные органы от необходимости критической проверки и юридической оценки полученной информации. Автоматизированные выводы должны рассматриваться лишь в качестве отправной точки для последующей процессуальной проверки: допросов участников событий, проведения экспертиз, осмотров мест происшествия и иных следственных действий.

В условиях Республики Казахстан использование цифровых источников информации в уголовном процессе опосредуется требованиями процессуального законодательства, касающегося допустимости доказательств, защиты личной жизни и обеспечения процессуальной справедливости. В этом контексте требуется дальнейшая разработка специализированных методических рекомендаций, регламентирующих порядок обращения с цифровыми доказательствами, в том числе полученными из интернета и социальных сетей, а также внедрение обучающих программ для следственных работников по вопросам фиксации и анализа цифровых следов.

Таким образом, использование данных из социальных сетей, интернет-архивов, поисковых систем и иных онлайн-ресурсов в следственной деятельности при поддержке технологий ИИ открывает качественно новые возможности для уточнения фактических обстоятельств уголовных дел, но

требует соблюдения высокого стандарта процессуальной добросовестности, технической компетентности и уважения к фундаментальным правам личности.

Прогнозирование вероятности совершения новых преступлений с использованием технологий ИИ представляет собой одно из перспективных направлений развития следственной аналитики в условиях цифровой трансформации уголовного судопроизводства. Основываясь на анализе признаков ранее совершённых преступлений, интеллектуальные системы способны выявлять закономерности, тенденции и скрытые взаимосвязи, что позволяет более обоснованно оценивать риск повторных правонарушений и оптимизировать превентивные меры.

Прогнозная аналитика осуществляется путём обработки комплексных массивов данных, включающих сведения о месте совершения преступления, времени, социально-демографических характеристиках фигурантов, способах совершения деяния, а также уровне его информационного резонанса в средствах массовой информации и социальных сетях. Такие параметры, как концентрация преступлений в определённых районах, участие в деяниях лиц, ранее привлекавшихся к ответственности, наличие аффилированности с криминальными группировками или участие в организованных схемах, могут быть учтены интеллектуальными алгоритмами для построения вероятностных моделей риска.

Например, в случае выявления серии краж из автомобилей в одном из спальных районов города А. в вечернее время интеллектуальная система может сопоставить локализацию эпизодов, профили подозреваемых, их передвижения, характер похищенного имущества и наличие информации о подобных случаях в социальных сетях. На основе таких данных возможно прогнозирование вероятных точек совершения новых преступлений, что позволяет органам внутренних дел заранее усилить меры патрулирования, провести оперативно-розыскные мероприятия и минимизировать ущерб.

Иной пример касается преступлений, связанных с мошенничеством в интернет-пространстве. Системы ИИ могут анализировать публикации в социальных сетях, форумы, а также жалобы граждан в онлайн-приёмных государственных органов, выявляя на ранней стадии признаки появления новых схем обмана, моделируя риск их распространения в зависимости от социальной уязвимости населения определённых регионов и доступности интернет-услуг.

Особую значимость прогнозная аналитика приобретает в сфере предупреждения тяжких насильственных преступлений. Анализируя факторы риска, такие как наличие заявлений о домашнем насилии, предыдущие административные взыскания, участие в конфликтах, интеллектуальная система может формировать ранние сигналы о повышенной вероятности совершения повторных актов насилия, что требует превентивного вмешательства уполномоченных органов с соблюдением законодательства о защите жертв.

Тем не менее, использование ИИ для прогнозирования преступности сопряжено с рядом принципиальных правовых и этических ограничений. Прежде всего, возникает риск «профилирования» лиц и групп на основе вероятностных выводов, что может вступать в противоречие с принципом презумпции невиновности и недопустимостью наказания за предполагаемые деяния. Прогнозные модели могут ошибочно классифицировать лицо как потенциального правонарушителя, опираясь на неполные или искажённые данные, что недопустимо в условиях уголовного судопроизводства, основанного на конкретных доказательствах факта совершения преступления.

Кроме того, существенным вызовом является проблема алгоритмической предвзятости: если обучающие выборки содержат исторические перекосы (например, по социальному статусу, месту проживания, национальности), интеллектуальная система может воспроизводить эти искажения, усугубляя социальное неравенство. Поэтому важно обеспечивать многоступенчатую верификацию моделей ИИ, регулярную проверку их нейтральности, привлечение экспертов из числа юристов, социологов и специалистов по правам человека к процессу разработки и внедрения таких систем.

Необходимо подчеркнуть, что в условиях Республики Казахстан правоприменение в сфере прогнозирования преступности должно строго соответствовать основным принципам Уголовно-процессуального кодекса, в том числе принципам уважения чести и достоинства личности, обеспечения равенства перед законом и судом, недопустимости ограничения прав без достаточных законных оснований. Прогнозные данные могут использоваться исключительно в качестве ориентировочной информации для принятия решений о проведении профилактических мероприятий или оперативных проверок, но не могут служить основанием для возбуждения уголовного дела, применения мер процессуального принуждения или ограничения конституционных прав без установленных процессуальных процедур.

Таким образом, применение ИИ для прогнозирования вероятности совершения новых преступлений на основе анализа признаков ранее совершённых деяний представляет собой эффективный инструмент в арсенале превентивной деятельности правоохранительных органов. Однако его использование требует строгого соблюдения стандартов законности, этической ответственности и научной обоснованности, чтобы обеспечить баланс между эффективностью борьбы с преступностью и защитой фундаментальных прав и свобод граждан в условиях построения правового государства.

Таким образом, интеграция технологий искусственного интеллекта (ИИ) в следственную деятельность открывает качественно новые возможности для повышения эффективности, полноты и обоснованности уголовного преследования в условиях усложняющейся криминальной реальности. Применение ИИ способствует оптимизации процессов построения следственных версий, реконструкции событий преступления, выявления серийных деяний, оценки полноты доказательств и уточнения фактических

обстоятельств на основе анализа цифровых следов. Вместе с тем интеллектуальные технологии не заменяют профессиональное следственное суждение, а служат лишь инструментом его усиления, требующим строгого соблюдения норм процессуального законодательства, стандартов защиты прав личности и этических принципов.

Использование ИИ в следствии сопровождается не только перспективами, но и серьёзными вызовами – рисками алгоритмической ошибки, непрозрачности выводов, угрозой нарушения презумпции невиновности и угрозами конфиденциальности персональных данных. В этой связи эффективность цифровой трансформации расследования напрямую зависит от соблюдения баланса между технологическими возможностями и принципами уголовного процесса, профессиональной ответственности следователей и создания надёжной нормативной рамки, обеспечивающей законность, справедливость и доверие к результатам следственной деятельности.

Развитие интеллектуальных инструментов должно сопровождаться не только техническим совершенствованием, но и формированием правовой культуры работы с ИИ, развитием методического сопровождения и повышением квалификации сотрудников правоохранительных органов. Лишь в этом случае цифровизация следственной деятельности станет не угрозой процессуальным гарантиям, а ресурсом укрепления справедливости, транспарентности и эффективности уголовного судопроизводства в Республике Казахстан.

3.4 Применение искусственного интеллекта в судебно-экспертной деятельности

Интеграция технологий ИИ в сферу судебно-экспертной деятельности представляет собой одну из наиболее перспективных тенденций цифровизации системы правосудия. В условиях усложнения структуры преступности, роста объёмов обрабатываемой информации и необходимости оперативного проведения экспертных исследований использование интеллектуальных систем становится важнейшим инструментом повышения точности, объективности и скорости экспертных заключений. ИИ в данном контексте не заменяет специалиста-эксперта, а выполняет вспомогательную функцию, усиливая аналитические возможности человека, минимизируя риск ошибок и сокращая время проведения экспертиз.

Формирование экспертных заключений в рамках проведения судебных экспертиз по вопросам, требующим специальных знаний, представляет собой сложный многоэтапный процесс, лежащий на стыке научного анализа, практической интерпретации фактических данных и соблюдения процессуальных норм. В условиях цифровизации и стремительного развития технологий особую значимость приобретает интеграция ИИ в экспертную деятельность, направленную на обеспечение объективности, полноты и обоснованности выводов, принимаемых в рамках судебного разбирательства.

На первоначальном этапе формирования экспертного заключения ключевую роль играет корректное определение предмета и объёма исследования. Эксперт обязан ясно сформулировать вопросы, поставленные перед ним органами досудебного расследования, судом или сторонами процесса, и определить методы, адекватные задачам экспертизы. При этом технологии ИИ могут быть использованы для систематизации материалов дела, предварительного анализа данных, классификации объектов исследования и выявления скрытых взаимосвязей, требующих экспертной оценки. Например, в рамках почерковедческой экспертизы ИИ способен заранее обработать представленные на исследование образцы, выделив их структурные и графические особенности, тем самым облегчая дальнейший аналитический этап.

На стадии непосредственного исследования объектов экспертизы ИИ может использоваться для автоматизированной обработки визуальных, текстовых, аудиовизуальных или иных цифровых данных. В криминалистической практике это проявляется в применении программ машинного зрения для анализа следов на местах происшествий, в биологической экспертизе – в использовании алгоритмов для интерпретации генетических профилей, в судебной экономике – в автоматической верификации финансовых документов и выявлении аномалий в бухгалтерских записях. Тем самым интеллектуальные системы становятся не заменой, а эффективным вспомогательным ресурсом, повышающим качество и скорость исследования.

Особую важность имеет этап формирования выводов, где от эксперта требуется не только изложить фактические результаты проведённого анализа, но и дать обоснованное суждение на основе специальных знаний, при строгом соблюдении требований научной обоснованности и процессуальной допустимости. В этом контексте ИИ может предлагать вероятностные модели интерпретации данных, выявлять статистически значимые корреляции, а также формировать гипотезы, подлежащие последующей верификации экспертом-человеком. Однако окончательное заключение должно основываться на профессиональной оценке эксперта, который принимает решение с учётом всех аспектов конкретного дела, правового регулирования и принципов судебной справедливости.

Применение ИИ в процессе формирования экспертных заключений, безусловно, расширяет возможности судебной экспертизы, однако оно сопряжено с необходимостью соблюдения ряда принципиальных требований. Прежде всего, выводы, полученные с использованием интеллектуальных технологий, должны быть воспроизводимыми и проверяемыми и не могут носить характер недоступных для критической оценки «чёрных ящиков». Все применяемые методы и алгоритмы должны быть описаны в заключении таким образом, чтобы их корректность могла быть проверена как сторонами процесса, так и судом. Более того, эксперт обязан указать пределы применимости методов, использованных в ходе экспертизы, возможные

погрешности, ограничения, а также дать оценку степени достоверности полученных результатов.

Необходимо также подчеркнуть, что использование ИИ должно полностью соответствовать действующим процессуальным требованиям, регулирующим порядок назначения, проведения и оценки судебных экспертиз. В частности, в Республике Казахстан нормативные требования установлены в Уголовно-процессуальном кодексе, Гражданском процессуальном кодексе, Кодексе об административных правонарушениях, а также в соответствующих ведомственных инструкциях и методических рекомендациях, утверждённых органами судебной экспертизы. Таким образом, интеграция искусственного интеллекта в процесс формирования экспертных заключений требует выверенного нормативного сопровождения, а также развития внутриотраслевых стандартов и этических кодексов, направленных на сохранение высокого уровня достоверности и научной добросовестности в экспертной практике.

Особую актуальность приобретают вопросы защиты конфиденциальности данных, обрабатываемых в рамках судебной экспертизы с применением интеллектуальных систем. Поскольку в ходе экспертных исследований нередко используются персональные данные, сведения о частной жизни, коммерческая тайна и иные охраняемые законом секреты, технологии ИИ должны функционировать в условиях строгого соблюдения норм о защите информации, а также обеспечивать аудит действий систем и исключение несанкционированного доступа.

Таким образом, формирование экспертных заключений с использованием технологий искусственного интеллекта открывает новые перспективы для повышения научной обоснованности, точности и эффективности судебных экспертиз. Вместе с тем это требует строжайшего соблюдения принципов процессуальной допустимости, прозрачности методологии и подотчётности полученных результатов. Только в условиях надлежащего правового регулирования, этического контроля и сохранения приоритета профессионального экспертного суждения возможно гармоничное внедрение интеллектуальных технологий в судебно-экспертную практику, направленное на укрепление справедливости и правовой определённости в процессе отправления правосудия.

Одним из ключевых векторов трансформации традиционных методов криминалистики становится интеграция технологий ИИ, в частности – систем компьютерного зрения, обработки изображений и интеллектуального анализа структурированных и неструктурированных данных. Современные алгоритмы способны не только обрабатывать колоссальные массивы информации в считанные секунды, но и выявлять закономерности, остающиеся недоступными при использовании классических экспертных подходов.

Одним из приоритетных направлений является применение ИИ при формировании экспертных заключений по делам, требующим анализа сложных визуальных данных. Например, в рамках трасологической экспертизы интеллектуальные системы, обученные на тысячах изображений

следов обуви и транспортных средств, могут с высокой степенью точности соотносить обнаруженные на месте происшествия следы с базами имеющихся образцов, исключая человеческий фактор при предварительном сопоставлении.

Технологии компьютерного зрения также находят применение при исследовании материалов видеонаблюдения. В ходе расследования серии квартирных краж в городе К. интеллектуальный модуль был использован для автоматического распознавания лиц, фигурирующих в кадрах с камер подъездов. Система успешно выделила одного и того же подозреваемого в записях с четырёх различных адресов, что позволило оперативно скоординировать действия следственной группы и получить разрешение на обыск, закончившийся изъятием похищенного имущества.

В области баллистической экспертизы ИИ используется для автоматизированного сопоставления следов на гильзах и пулях, оставленных различными образцами огнестрельного оружия. Обладая возможностью точного сопоставления микротрещин и технологических дефектов, системы компьютерного анализа обеспечивают не только ускорение процесса сравнения, но и снижение вероятности субъективной ошибки. В городе М. подобная система позволила связать три ранее не связываемых между собой преступления, совершённых с использованием одного и того же оружия, что дало основания для выдвижения версии о серийности.

Не менее перспективным направлением остаётся интеллектуальный анализ цифровых доказательств – от электронной переписки до геолокационных данных и логов сотовой связи. В рамках одного из расследований в городе Н. ИИ-модуль был применён для выявления скрытых связей между фигурантами по 26 уголовным делам, объединённым общей схемой мошенничества с банковскими переводами. Алгоритм выявил общие IP-адреса, аналогичные поведенческие паттерны и пересекающиеся контактные цепочки, что в дальнейшем легло в основу представленного суду обвинения.

Тем не менее, при всех достоинствах внедрение ИИ в сферу криминалистики сопряжено с рядом ограничений. Во-первых, существует риск алгоритмической предвзятости: если система обучалась на нерепрезентативных данных, её выводы могут быть ошибочными или содержать скрытые формы дискриминации. Во-вторых, сохраняется проблема объяснимости: при использовании сложных нейросетевых моделей невозможно верифицировать, каким образом был получен тот или иной вывод, что осложняет судебную процедуру оценки допустимости доказательств. В-третьих, существует опасность переоценки точности таких систем, когда следственные органы полагаются на результаты ИИ в ущерб традиционным процессуальным стандартам.

Особое значение приобретает вопрос нормативного регулирования использования ИИ в криминалистической экспертизе. Требуется разработка специальных методических рекомендаций, которые определят допустимые пределы автоматизации, процедуры верификации и принципы

взаимодействия между техническими средствами и экспертами-людьми. Использование ИИ должно носить вспомогательный характер и ни в коем случае не заменять правовое суждение эксперта, особенно в контексте сложных и социально значимых дел.

Таким образом, применение ИИ в криминалистических исследованиях представляет собой важнейший этап модернизации экспертной практики. Это направление, при грамотной институционализации и юридическом сопровождении, способно радикально повысить эффективность и достоверность судебных экспертиз, сохраняя при этом принципы законности, справедливости и процессуальной допустимости доказательств.

Одним из наиболее перспективных направлений применения ИИ в судебно-экспертной и криминалистической деятельности становятся выявление, обработка и интерпретация файлов и цифровых данных, недоступных при использовании стандартных средств анализа. Развитие цифровых технологий и повышение уровня технологической оснащенности преступлений приводит к усложнению задач, стоящих перед экспертами-криминалистами. Стремление скрыть следы цифровой активности, использование средств шифрования, программ для сокрытия файлов, а также активное применение стеганографии обуславливает необходимость внедрения интеллектуальных систем, способных выявлять данные, ускользающие от традиционного внимания.

Прежде всего, интеллектуальные модули могут быть использованы для восстановления удалённой информации. В условиях, когда подозреваемый пытается удалить компрометирующие файлы с жёсткого диска, флеш-накопителя или смартфона, ИИ может анализировать низкоуровневую структуру файловой системы, определять наличие пустых секторов, фрагментов данных, ранее занимавших эти участки, и восстанавливать утерянные блоки информации. Такая реконструкция осуществляется за счёт алгоритмов машинного обучения, обученных на тысячах аналогичных ситуаций, где известна структура восстановления. Благодаря этому возможно воссоздание даже тех файлов, которые были подвергнуты нескольким циклам удаления и перезаписи.

Вторым значимым направлением является выявление скрытых или маскированных данных. Злоумышленники нередко используют специальные программы, позволяющие прятать файлы под видом других – например, изображение, содержащее в себе скрытый архив, исполняемый файл, спрятанный в системной библиотеке, или документ, внедрённый в структуру мультимедийного объекта. ИИ способен распознавать такие аномалии путём анализа статистических отклонений, сопоставления характеристик файлов с нормой и обнаружения несоответствий между заявленным и фактическим содержанием.

Ещё одна область – это анализ стеганографических объектов. Стеганография, в отличие от криптографии, направлена не на шифрование содержания, а на сокрытие самого факта передачи информации. ИИ может быть обучен выявлять закономерности, характерные для искусственно

изменённых изображений, аудиофайлов или видео. Например, алгоритм может заметить, что в определённой части изображения нарушена структура шума, что может свидетельствовать о наличии встроенного сообщения. При этом используется совокупность методов компьютерного зрения, сверточных нейросетей и анализа сигналов, что позволяет системам выходить за пределы возможностей человеческого восприятия.

В рамках гипотетического примера можно рассмотреть ситуацию, связанную с расследованием дела о вымогательстве в городе А. Подозреваемый утверждал, что не вел никакой переписки с жертвой и не имел отношения к угрозам. Однако интеллектуальная система, проанализировав временные файлы браузера, извлекла фрагменты удалённой переписки в зашифрованном чате, дополнительно идентифицировала электронные адреса и цифровые подписи, указывающие на участие конкретного пользователя в обсуждении преступных намерений. Такой подход позволил подтвердить наличие переписки, несмотря на попытки её уничтожения.

Ещё один гипотетический пример касается расследования трансграничного дела в городе К. о легализации денежных средств, полученных преступным путём. Используя ИИ-модуль, сотрудники экспертного учреждения смогли построить цепочку транзакций между 18 цифровыми кошельками, оформленными на вымышленные имена, с последующим выводом средств в офшорные зоны. Выявление этой цепочки стало возможным за счёт анализа метаданных транзакций, выявления повторяющихся паттернов в поведении аккаунтов и сопоставления информации из открытых и закрытых источников, включая утечки с теневых форумов и базы данных, размещённые в даркнете.

Применение интеллектуальных алгоритмов может быть полезным и при анализе устройств, подвергшихся преднамеренному уничтожению данных. Например, если при изъятии ноутбука выяснилось, что жёсткий диск был отформатирован, ИИ может использовать методы глубокой реконструкции данных с учётом фрагментации, анализа сигнатур и возможного восстановления структуры директорий. Подобные технологии также эффективны при работе с повреждёнными носителями информации – например, в случаях, когда диск был подвержен механическому воздействию или попыткам термического разрушения.

Интерес представляет и возможность применения ИИ в анализе мобильных устройств. В современных смартфонах значительное количество информации хранится в виде кэшированных данных, временных файлов приложений, журналов активности и даже системных логов. Интеллектуальная система может агрегировать эти данные, выявлять связи между действиями пользователя, анализировать временные метки и строить цифровой профиль, позволяющий судить о поведении подозреваемого в определённый период времени. Например, в деле о нападении в городе С. система зафиксировала, что мобильное устройство подозреваемого находилось вблизи места происшествия, а также использовалось для доступа к картам и маршрутному планированию в ночь совершения преступления. Эти

данные не хранились в явном виде и были выявлены лишь после глубокой интеллектуальной обработки системных логов устройства.

Важной задачей при внедрении ИИ в сферу криминалистики остаётся обеспечение допустимости полученных данных в судебном процессе. Для этого необходимо нормативное закрепление методик, описание используемых алгоритмов, процедуры аудита и экспертизы программных средств. Выводы, полученные с помощью интеллектуальных систем, должны быть воспроизводимыми, обоснованными и понятными как экспертам, так и участникам судебного разбирательства. Поэтому особое внимание следует уделять вопросам верифицируемости моделей, ограничениям их применения и корректной интерпретации результатов.

Кроме того, необходимо учитывать риски, связанные с ошибками алгоритмов. Переобучение, недостоверность обучающих данных, предвзятость выборок и иные технические особенности могут привести к ложноположительным результатам, что в условиях уголовного судопроизводства может иметь тяжёлые последствия. Именно поэтому решения, основанные на ИИ, должны рассматриваться исключительно как инструменты поддержки, а не как окончательные источники доказательств.

С этической точки зрения, применение ИИ в анализе скрытых данных должно соответствовать принципам справедливости, уважения к частной жизни и недопустимости произвольного вмешательства. Необходимо соблюдение принципа соразмерности, при котором глубина и объём анализа должны быть соотносимы с тяжестью и характером расследуемого правонарушения. Также важно обеспечить информирование сторон о факте использования интеллектуальных систем, особенно в случаях, когда это влияет на права и обязанности участников процесса.

В перспективе развитие ИИ в области анализа цифровых следов будет сопряжено с созданием гибридных систем, сочетающих машинное обучение, экспертные правила и элементы правовой логики. Такие платформы смогут не только выявлять данные, но и формировать гипотезы, сопоставлять их с нормами права и предлагать обоснованные выводы, основанные на совокупности цифровых и юридических фактов. Например, в автоматическом режиме можно будет составлять проект экспертного заключения с указанием обнаруженных цифровых следов, их трактовки и возможного значения в контексте дела.

Таким образом, технологии искусственного интеллекта открывают принципиально новые возможности для идентификации цифровых следов, ранее недоступных традиционным методам. Однако практическая реализация этих возможностей требует выверенного нормативного и этического сопровождения, строгого контроля над качеством алгоритмов и постоянного участия человека на всех ключевых этапах анализа. Только в этом случае интеллектуальные системы смогут стать надёжным инструментом в арсенале судебной экспертизы, способствуя укреплению доказательственной базы и повышению объективности уголовного судопроизводства.

В условиях усложнения методов сокрытия и искажения доказательственной информации в рамках уголовного судопроизводства особую актуальность приобретает разработка и внедрение интеллектуальных технологий, способных идентифицировать признаки фальсификации как самих объектов судебной экспертизы, так и заключений, представляемых экспертами. Технологии искусственного интеллекта, основанные на алгоритмах глубокого обучения, нейросетевых моделях и методах обработки цифровых следов, открывают принципиально новые возможности для детектирования аномалий, выходящих за рамки доступного восприятия даже высококвалифицированного эксперта-человека. Особенно перспективным представляется использование ИИ в тех случаях, когда фальсификация осуществляется с высокой степенью технической изощрённости – путём клонирования цифровых следов, внесения изменений в метаданные, подделки текстов заключений с использованием стилей подлинных экспертов и иных форм «цифровой мимикрии».

Гипотетический пример позволяет обрисовать возможный контур использования таких технологий. Допустим, в городе К. возникло подозрение относительно достоверности судебно-биологической экспертизы, проведённой по делу о причинении тяжкого вреда здоровью. Предметом экспертного анализа стали фрагменты одежды, на которых, согласно заключению, якобы были обнаружены следы крови подозреваемого. Однако защита заявила ходатайство о дополнительной проверке материалов, указывая на невозможность локализации обвиняемого в указанное время вблизи места происшествия. В рамках внутренней верификации экспертного заключения было задействовано интеллектуальное решение, способное анализировать совокупность данных, включая метаданные файлов микрофотографий, спектральные характеристики окрашенных пятен, а также лексико-стилистические особенности текстовой части заключения. ИИ выявил аномальное совпадение содержания ряда фраз с другими заключениями, ранее составленными и размещёнными в открытом доступе, а также обнаружил расхождение между заявленным временем анализа и временными метками, зафиксированными в EXIF-полях микроскопических изображений. На основании этих признаков было инициировано служебное расследование, в ходе которого подтвердились факты недобросовестного копирования заключения и манипуляций с визуальными доказательствами.

Потенциал интеллектуальных систем в таких ситуациях базируется, прежде всего, на их способности обрабатывать большие массивы структурированных и неструктурированных данных, сопоставлять их с эталонными базами экспертиз, идентифицировать повторяющиеся шаблоны и выявлять несоответствия, выходящие за пределы нормативных допусков. Например, анализ электронной структуры PDF-файла заключения может выявить следы редактирования, не фиксируемые стандартными средствами просмотра, либо фрагменты текста, вставленные из сторонних источников без соответствующей стилистической адаптации. Особенно значимыми являются случаи, когда в заключении используются специфические терминологические

конструкции, не характерные для практики конкретного учреждения, что может свидетельствовать о заимствовании или подмене документа.

В области криминалистики ИИ может также быть задействован для анализа изображений объектов экспертизы – следов на орудиях преступления, микрочастиц, биологических образцов – с целью установления признаков цифрового вмешательства, ретуширования или имитации структуры материала. К примеру, при визуализации повреждений на обуви, изъятой у подозреваемого, система может обнаружить дублирующиеся пиксельные шаблоны, указывающие на использование графического редактора. В других случаях алгоритмы машинного зрения способны установить несоответствие формы и угла падения предполагаемого пятна крови, сопоставляя его с базой траекторных моделей, что может указать на намеренную подделку.

Особую категорию представляют так называемые текстовые фальсификации. С использованием моделей естественного языка, таких как GPT, возможно не только автоматическое составление экспертных заключений, но и генерация правдоподобных научных обоснований, ссылок на нормативные акты и прецеденты. Это обстоятельство требует от проверяющих инстанций задействования аналогичных ИИ-моделей для выявления признаков машинного происхождения текста: однообразие синтаксических структур, статистическая аномалия в частоте терминов, использование фразеологизмов, не характерных для профессионального сообщества экспертов. Подобная анализаторская функция может быть встроена в электронные системы регистрации заключений, автоматически маркируя подозрительные участки текста для последующей проверки.

Наряду с очевидными преимуществами, интеграция ИИ в сферу фальсификационной экспертизы сопряжена с рядом правовых и этических ограничений. Во-первых, существует риск «ложноположительных» срабатываний, когда система ошибочно интерпретирует допустимую профессиональную вариативность как фальсификацию. Во-вторых, алгоритмическая непрозрачность решений может затруднить оспаривание результатов такой проверки в судебном порядке, особенно если методика анализа не прошла научную валидацию и не имеет официального утверждения в рамках процессуального законодательства. Наконец, возникает вопрос конфиденциальности и безопасности баз данных, на которых обучаются такие системы, поскольку утечка или неправомерный доступ к ним может привести к компрометации экспертной деятельности в целом.

Таким образом, интеллектуальные системы представляют собой значительный ресурс в борьбе с фальсификацией экспертных заключений, но их использование требует выверенного сочетания научной валидности, правовой регламентации и профессионального контроля. Только в этих условиях возможно гармоничное внедрение ИИ в судебно-экспертную практику, способствующее укреплению доверия к правосудию, повышению объективности экспертных оценок и защите прав участников уголовного процесса.

ЗАКЛЮЧЕНИЕ

Монография посвящена изучению концептуальных, в том числе правовых и организационно-тактических аспектов внедрения и использования ИИ в правоохранительной деятельности. Объективной основой для проведения данной работы послужил тренд на цифровизацию государственного управления и правоохранительной системы, при этом особое внимание уделялось роли ИИ как технологического инструмента, обладающего потенциалом изменить подходы к осуществлению оперативно-розыскной, следственной, экспертной, надзорной и судебной деятельности.

В исследовании сформулирована авторская позиция относительно сущностных характеристик ИИ, выделены четыре ключевые группы свойств, на которых должно основываться правовое понимание данной технологии: объективные (формальные и технические признаки), функциональные (выполнение когнитивных задач), инструментальные (основанность на алгоритмах и математических моделях) и самореферентные (способность к обучению и самообучению). Такое комплексное понимание позволяет адекватно идентифицировать предмет правового регулирования, а также установить пределы допустимого вмешательства ИИ.

Исследование показало, что на текущем этапе развития правоохранительных органов Республики Казахстан существует определённый нормативный дефицит в сфере правового регулирования ИИ. Несмотря на наличие общих положений в Законе Республики Казахстан «Об информатизации», а также разрабатываемого проекта Закона Республики Казахстан «Об искусственном интеллекте», в целом законодательство не содержит специальных норм, регулирующих допустимость, процедуры верификации, формы и пределы применения ИИ в контексте уголовного преследования, прокурорского надзора или судебной экспертизы. В связи с этим в монографии обоснована необходимость разработки специализированного подзаконного регулирования, включающего положения об алгоритмической ответственности, верификации данных, нормативной допустимости ИИ в качестве источника доказательственной информации.

Особое внимание уделено параметризации применения ИИ в правоохранительной деятельности. Автором предложена классификация индикаторов эффективности, включающая количественные (время реакции, количество автоматизированных процедур), качественные (степень обоснованности решений, уровень доверия к системе), аналитические (глубина анализа, связность выводов) и индикаторы надежности (ошибочность, устойчивость к манипуляции данными). Такая параметризация позволяет не только оценивать эффективность внедрения ИИ, но и использовать данные показатели для внутреннего аудита, стратегического планирования и обеспечения прозрачности алгоритмов.

Систематизация направлений применения искусственного интеллекта в правоохранительной деятельности открывает широкие возможности для повышения качества правосудия на всех его этапах. В сфере судебной

деятельности ИИ способен служить эффективным инструментом контроля за соблюдением процессуальных стандартов, обеспечивая автоматизированный мониторинг отклонений от норм и регламентов работы судей и аппарата суда. Переводческое сопровождение и языковое обеспечение судебных процедур, реализуемое на базе нейросетевых моделей, создаёт предпосылки для ускорения рассмотрения дел с участием иностранных граждан и международных организаций, а административно-ресурсная поддержка снижает нагрузку на персонал за счёт оптимизации документооборота и распределения задач. Наконец, аналитическая обработка больших объёмов судебных данных позволяет выявлять тенденции в практике применения норм, прогнозировать возможные «узкие места» и разрабатывать превентивные меры для повышения эффективности правоприменения.

В области прокурорского надзора ключевым достижением становится автоматизация составления актов проверки и реагирования, что существенно ускоряет формирование официальных документов и повышает их стандартизированность. Инструменты ИИ для анализа состояния законности помогают выявлять системные нарушения и вырабатывать рекомендации по их устранению. Мониторинг данных о незаконном движении активов и анализ информации из различных источников (финансовых отчётов, баз данных, СМИ и интернет-ресурсов) способствуют своевременному выявлению схем вывода и легализации средств. При этом применение инструментов ИИ для установления оснований отмены или приостановления актов, а также для проверки материалов уголовных дел и формирования линии обвинения, создаёт предпосылки для более обоснованной и детализированной прокурорской позиции.

Следственная деятельность получает качественно новые инструменты для построения и проверки гипотез: автоматизированный анализ материалов уголовных дел на основе методов машинного обучения позволяет выявлять скрытые связи между эпизодами, предлагать приоритетные направления проверки и восстанавливать следовую картину событий при фрагментарности данных. Алгоритмы поиска признаков серийности и прогнозирования вероятности новых правонарушений обеспечивают проактивный подход к предупреждению преступлений. Кроме того, интеграция данных социальных сетей, интернет-архивов и других онлайн-ресурсов в следственный процесс расширяет информационную базу для уточнения фактических обстоятельств и повышения точности выводов.

В секторе судебно-экспертной деятельности применение ИИ позволяет существенно повысить результативность криминалистических исследований: технологии обработки изображений и компьютерного зрения ускоряют анализ материалов дела и объектов расследования, а специализированные модели выявляют файлы и цифровые данные, недоступные традиционным средствам. Использование алгоритмов для выявления фальсификаций экспертных заключений повышает надёжность экспертиз. Наконец, интеллектуальные системы поддержки принятия решений обеспечивают экспертам возможность эффективно работать с большими объёмами информации и принимать

взвешенные решения даже при фрагментарности или неопределённости данных, что в целом способствует укреплению доверия к судебно-экспертному процессу и повышению качества правосудия.

Также в монографии выделены направления тактического использования ИИ: поддержка при формировании линии обвинения, предварительный анализ массива цифровых улик, оценка достоверности цифровых доказательств, обработка оперативной информации. Отдельное внимание уделено международным практикам (КНР, ЕС, США), позволившим обосновать применимость гибридной модели, при которой ИИ используется как ограниченно автономный аналитический субъект, а решения остаются в сфере человеческого контроля.

Результаты проведенного исследования имеют теоретическое и практическое значение. Теоретически – они позволяют расширить понятийный аппарат юридической науки применительно к новым объектам регулирования, включая алгоритмы, цифровые следы, машинное обучение. Практически – они могут использоваться в качестве основы для разработки ведомственных инструкций, методических рекомендаций, образовательных программ по цифровому праву, прокурорскому и судебному надзору в условиях цифровой трансформации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» // https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-kazahstan-v-epohu-iskusstvennogo-intellekta-aktualnye-zadachi-i-ih-resheniya-cherez-cifrovuyu-transformaciyu-885145 (дата обращения: 10.10.2025).

2 В Казахстане появилось Министерство искусственного интеллекта и цифрового развития // https://www.gov.kz/memleket/entities/mfa-kishinev/press/news/details/1076132?lang=ru&ysclid=mhaw8tuj62806796317 (дата обращения: 01.10.2025).

3 Жаслан Мадиев назначен заместителем премьера-министром искусственного интеллекта и цифрового развития // https://tengrinews.kz/kazakhstan_news/jaslan-madiev-naznachen-zamestitelem-premera-ministrom-581068/?ysclid=mhawb9harx386533978 (дата обращения: 01.10.2025).

4 Госзакупками в Албании будет заниматься ИИ-министр Диэлла // https://forbes.kz/articles/goszakupkami-v-albanii-budet-zanimatsya-ii-ministr-diella-b3fbaa (дата обращения: 01.10.2025).

5 Казахстанским следователям поможет искусственный интеллект // https://ru.sputnik.kz/20250715/kazakhstanskim-sledovatelyam-pomozhet-iskusstvennyy-intellekt-55636405.html?ysclid=mhaxegglb955695593 (дата обращения: 15.08.2025).

6 U.S. Department of Justice Artificial Intelligence and Criminal Justice Final Report // https://www.justice.gov/olp/media/1381796/dl (дата обращения: 25.05.2024).

7 Modeling the global economic impact of AI // https://www.mckinsey.com/featured-insights/artificial-intelligence/notes (дата обращения: 25.05.2024).

8 Морхат П.М. К вопросу об определении понятия искусственного интеллекта // Право и государство: теория и практика. – 2017. – №12(156). – С. 25-32.

9 Тлембаева Ж.У. О некоторых подходах к правовому регулированию искусственного интеллекта // Вестник Института законодательства и правовой информации Республики Казахстан. – 2021. – №2(65). – С. 61-74.

10 Castro D., New J. The promise of artificial intelligence // Center for Data Innovation. – 2016. – Vol. 115, Issue 10. – P. 32-35.

11 Tesla's Musk predicts AI will be smarter than the smartest human next year // https://www.reuters.com/technology/teslas-musk-predicts-ai-will-be (дата обращения: 15.01.2025).

12 Siegel E. Elon Musk Predicts Artificial General Intelligence In 2 Years. Here’s Why That’s Hype // https://www.forbes.com/sites/ericsiege (дата обращения: 18.09.2024).

13 McCarthy J. What is artificial intelligence // http://jmc.stanford (дата обращения: 19.01.2025).

14 Kurzweil R. The Age of Intelligent Machines. – Cambridge, 1990. – 565 p.

15 Rich E., Knight K. Artificial Intelligence. – Ed. 2nd. – NY.: McGraw-Hill, 1991. – 621 p.

16 Dobrev D. A definition of Artificial Intelligence // https://archive.org/details/arxiv-1210.1568 (дата обращения: 19.01.2025).

17 Bellman R.E. An Introduction to Artificial Intelligence: Can Computers Think? – San Francisco, 1978. – 146 p.

18 Russell S.J. Artificial intelligence: a modern approach. – Upper Saddle River, NJ: Pearson Education, 2022. – 1166 p.

19 Бахтеев Д.В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений: дис. ... д-ра. юрид. наук: 5.1.4. – Екатеринбург, 2022. – 504 с.

20 Родзинский Д.Л. Антропологические аспекты бытия и небытия: автореф. ... канд. филос. наук: 09.00.13. – М., 2014. – 46 с.

21 Родзинский Д.Л. Мистические основания рационализма // Философия и общество. – 2023. – №4. – С. 90-103.

22 Mart'inez-Fern'andez S., Bogner J., Franch X. et al. Software Engineering for AI-Based Systems: A Survey // ACM Transactions on Software Engineering and Methodology (TOSEM). – 2021. – Vol. 31. – P. 1-59.

23 Jutel M., Zemelka-Wiącek M., Ordak M. et al. The artificial intelligence (AI) revolution: How important for scientific work and its reliable sharing // Allergy. – 2023. – Vol. 78, Issue 8. – P. 2085-2088.

24 Декарт Р. Сочинения в 2 т. / пер. с лат. и фр. – М.: Мысль, 1989. – Т. 1. – 654 с.

25 Bayley D.H. Law enforcement and the rule of law: Is there a tradeoff? // Criminology & Public Policy. – 2002. – Vol. 2, Issue 1. – P. 133-154.

26 Muzychuk O., Salmanova O., Khromov A. et al. Law enforcement agencies in the system of subjects of human rights protection and defence // Revista de Gestão e Secretariado (Management and Administrative Professional Review). – 2023. – Vol. 14, Issue 9. – P. 15004-15019.

27 Bysaga Y., Bielova M., Fridmanskyy R. Conceptual principles of defining tasks and functions of law enforcement bodies in the system of state power: theoretical and legal dimension // Analytical and Comparative Jurisprudence. – 2024. – Issue 6. – P. 81-86.

28 Soroka S., Skoropad T. Ensuring the implementation of human and citizen rights and freedoms through the prism of the activities of law enforcement bodies // Visnik Nacional’nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki. – 2023. – Issue 40. – P. 352-357.

29 Ермолаев К.А. Цели и задачи правоохранительной деятельности Министерства юстиции Российской Федерации // Закон и право. – 2020. – №2. – С. 140-143.

30 Sherman L.W., Gottfredson D., MacKenzie D.L. et al. Preventing crime: What works, what doesn't, what's promising. – Washington: National Institute of Justice, 1998. – 19 p.

31 Srinithi T. AI-Driven Crime Prevention: Balancing Predictive Policing with Individual Rights // International Journal of Legal Science and Innovation. – 2024. – Vol. 6, Issue 6. – P. 143-156.

32 Burton J., Janjeva A., Moseley S. et al. AI and Serious Online Crime // https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas_research_ (дата обращения: 01.04.2025).

33 London Underground Is Testing Real-Time AI Surveillance Tools to Spot Crime // https://www.wired.com/story/london-underground-ai (дата обращения: 18.03.2025).

34 Martínez-Mascorro G.A., Abreu-Pederzini J.R., Ortiz-Bayliss J.C. et al. Suspicious behavior detection on shoplifting cases for crime prevention by using 3D convolutional neural networks // arXiv preprint arXiv:2005.02142. – 2020.

35 Adithya P.R. et al. Crowd management, crime detection, work monitoring using AI/ML // https://arxiv.org/abs/2311.12621 (дата обращения: 10.05.2025).

36 IronYun. How AI Can Improve Local Policing Strategies // https://www.vaidio.ai/blog/how-ai-can-improve-local-policing (дата обращения: 18.01.2025).

37 Jackman S. AI in the Fight Against Crime: How San Francisco is Using Tech to Stay Safe // https://www.lvt.com/blog/ai-in-the-fight-against (дата обращения: 20.03.2025).

38 Meta to use facial recognition technology in fight against celebrity investment scam ads // https://www.theguardian.com/technology (дата обращения: 25.01.2025).

39 Как Sergek использует ИИ для борьбы с пробками, снижения смертности в ДТП и эвакуации при ЧС // https://kz.kursiv.media (дата обращения: 25.03.2025).

40 Ешназаров А.А. Применение искусственного интеллекта и технологий «блокчейн» в уголовном судопроизводстве // Права человека и судебная власть современного Казахстана: проблемы, тенденции и перспективы: сб. мат-лов. 2-го Евразийского форума по правам человека. – Нур-Султан, 2021. – С. 61-66.

41 AI can help police predict if someone is at risk of domestic abuse // https://www.thetimes.com/uk/crime/article/ai-can-help-police-predict (дата обращения: 18.02.2025).

42 Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations // https://www.rand.org/pubs/research_reports/RR233.html (дата обращения: 25.01.2025).

43 Egbert S., Leese M. Criminal Futures: Predictive Policing and Everyday Police Work. – London, 2021. – 242 с.

44 Ferguson A.G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. – NY., 2017. – 272 с.

45 Predictive Policing Software Terrible At Predicting Crimes // https://themarkup.org/prediction-bias/2023/10/02/predictive-policing (дата обращения: 05.12.2024).

46 Study Finds That Police “Crime Predicting” AI Fails Miserably at Predicting Crimes. Who could have seen this coming? // https://futurism.com/the-byte/predictive-policing-ai-fails (дата обращения: 19.12.2024).

47 Politicians Move to Limit Predictive Policing After Years of Controversial Failures // https://www.techpolicy.press/politicians-move-to-limit (дата обращения: 12.01.2025).

48 Predictive Policing Explained // https://www.brennancenter (дата обращения: 27.01.2025).

49 Partial ban on ‘predictive’ policing and crime prediction systems included in final EU AI Act // https://www.fairtrials.org/articles/news (дата обращения: 13.02.2025).

50 . Уголовно-процессуальный кодекс Республики Казахстан: принят 4 июля 2014 года, №231-V ЗРК // https://adilet.zan.kz/rus/docs (дата обращения: 10.04.2025).

51 Закон Республики Казахстан «О правоохранительной службе»: принят 6 января 2011 года, №380-IV // https://adilet.zan.kz/rus/docs (дата обращения: 10.04.2025).

52 Уголовный кодекс Республики Казахстан: принят 3 июля 2014 года, №226-V ЗРК // https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 11.04.2025).

53 Бахтеев Д.В. Оценка эффективности интеллектуальных систем в правоохранительной деятельности на примере проекта NSP-sigver // Искусственный интеллект и большие данные (Big data) в судебной и правоохранительной системе: реалии и требования времени: мат-лы международ. науч.-практ. конф. – Косшы, 2023. – С. 179-185.

54 Floridi L. The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. – Oxford, 2023. – 312 p.

55 Innes M. Investigation and Detection: Back to the Future // International Journal of Police Science & Management. – 2024. – Vol. 26, Issue 4. – P. 434-437.

56 Ekundayo F. Big Data and Machine Learning in Digital Forensics: Predictive Technology for Proactive Crime Prevention // World Journal of Advanced Research and Reviews. – 2024. – Vol. 24, Issue 02. – P. 2692-2709.

57 Crime prediction and forecasting using machine learning algorithms // https://www.researchgate.net/publication/355872171 (дата обращения: 10.02.2025).

58 Ensign D., Friedler S.A., Neville S. et al. Runaway feedback loops in predictive policing // PMLR. – 2018. – Vol. 81. – P. 160–171.

59 Rapid DNA // https://le.fbi.gov/science-and-lab (дата обращения: 17.02.2025).

60 Guide to All Things Rapid DNA // https://le.fbi.gov/file-repository/guide-to-all-things-rapid-dna-4-10-2024.pdf (дата обращения: 05.03.2025).

61 What’s Possible with Rapid DNA Technology // https://nij.ojp.gov/library/publications/whats-possible-rapid-dna (дата обращения: 10.03.2025).

62 Philly’s new AI cameras will catch drivers passing stopped school buses // https://www.axios.com/local/philadelphia/2025/04/22/ai-cameras-septa (дата обращения: 23.04.2025).

63 AI can help cities make roads safer by analyzing traffic accident data // https://www.uoc.edu/en/news/2021/059-ai-traffic-accidents-cities (дата обращения: 17.01.2025).

64 How HSBC fights money launderers with artificial intelligence // https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights (дата обращения: 17.02.2025).

65 Real-World Examples of How Artificial Intelligence is Being Used in Financial Services // https://www.ciocoverage.com/real-world (дата обращения: 11.04.2025).

66 Clearview AI // https://www.clearview.ai (дата обращения: 01.01.2025).

67 ImageVision. Suspicious Activity Detection // https://imagevision.ai /suspicious-activity (дата обращения: 07.01.2025).

68 Facial recognition technology. Metropolitan Police // https://www.met.police.uk/advice/advice-and-information/fr/facial (дата обращения: 15.01.2025).

69 Facial Recognition // https://www.interpol.int/en (дата обращения: 01.02.2025).

70 Selvadurai N., Karim E. The effective governance of AI: Harmonising the regulation of face recognition technologies in the Asia-Pacific region // Journal of Internet Law. – 2020. – Vol. 24, Issue 2. – P. 3-14.

71 Artificial intelligence must be grounded in human rights – says High Commissioner // https://www.ohchr.org/en/statements (дата обращения: 12.02.2025).

72 Racism and AI bias: A past that leads to a biased future? // https://www.ohchr.org/en/stories/2024/07/racism-and-ai-bias-past (дата обращения: 09.03.2025).

73 Denmark: AI-powered welfare system fuels mass surveillance and risks discriminating against marginalized groups // https://www.amnesty.org (дата обращения: 28.03.2025).

74 Садыков М.Б., Бегалиев Е.Н., Бахтеев Д.В. и др. Применение искусственного интеллекта и чипирования человека в судебно-медицинской экспертизе: научный обзор // Судебная медицина. – 2024. – Т. 10, №1. – С. 88-98.

75 Баданова А.Н., Бегалиев Е.Н., Шабанов В.Б. и др. Медико-криминалистическая процедура дистанционного медицинского освидетельствования: научный обзор // Судебная медицина. – 2024. – Т. 10, №1. – С. 15-25.

76 Чонбаев Е.Г., Бегалиев Е.Н., Куаналиева Г.А. и др. Криминалистические аспекты пыток посредством использования системы

искусственного интеллекта: научный обзор // Судебная медицина. – 2024. – Т. 10, №1. – С. 37-46.

77 Biometric surveillance technology: facial recognition, iris and fingerprint scans // https://www.azosensors.com/article.aspx?ArticleID=3028 (дата обращения: 20.04.2025).

78 Biometrics and privacy: issues and challenges // https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics (дата обращения: 20.04.2025).

79 Muckenhirn H., Martino L., Magimai-Doss M. On the use of voice biometrics for person identification in noisy conditions // IEEE Transactions on Information Forensics and Security. – 2021. – Vol. 16. – P. 1125–1139.

80 Gupta B., Quamara M. Social media forensics: A review // Electronics. – 2024. – Vol. 13, Issue 9. – P. 1671.

81 How digital forensic tools recover data from compromised systems // https://medium.com/@bevijaygupta/how-do-digital-forensics (дата обращения: 20.04.2025).

82 Gupta B. et al. Role of artificial intelligence in digital forensics // International Journal of Scientific Research & Engineering Trends. – 2024. – Vol. 10, Issue 4. – P. 121-123.

83 The right to privacy in the digital age – Report A/HRC/48/31 // https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital (дата обращения: 19.04.2025).

84 Cracking crime with AI // https://www.iadb.org/en/blog (дата обращения: 04.02.2025).

85 Fighting organized crime by automatically detecting money laundering // https://dl.acm.org/doi/abs/10.1145/3465481.3469196 (дата обращения: 26.03.2025).

86 AI and crime: Transforming law enforcement strategies // https://www.cognyte.com/blog/ai-and-crime/ (дата обращения: 17.01.2025).

87 Using artificial intelligence to address criminal justice needs // https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address (дата обращения: 02.01.2025).

88 Dragon Law Enforcement // https://www.nuance.com (дата обращения: 18.03.2025).

89 Alternative response models and disparities in policing // https://www.rand.org/content/dam/rand/pubs/research_reports (дата обращения: 20.04.2025).

90 Case Service – AI-driven citizen engagement solution // https://www.versaterm.com/case-service (дата обращения: 01.02.2025).

91 Artificial intelligence for speech and language analysis in criminal justice // https://nij.ojp.gov/funding/awards/2019-r2-cx-0033 (дата обращения: 20.04.2025).

92 KazMMLU: Kazakh massive multitask language understanding benchmark // https://arxiv.org/abs/2502.12829 (дата обращения: 01.04.2025).

93 Neural named entity recognition for Kazakh // https://arxiv.org/abs/2007.13626 (дата обращения: 05.04.2025).

94 Первая открытая языковая модель на казахском языке IrbisGPT опубликована в открытом доступе // https://digitalbusiness.kz (дата обращения: 09.04.2025).

95 Llama-3.1-Sherkala-8B-Chat: A Kazakh and English instruction-tuned model // https://arxiv.org/html/2503.01493v1 (дата обращения: 13.04.2025).

96 KazParC: A parallel corpus for machine translation in Kazakh, English, Russian and Turkish // https://arxiv.org/abs/2403.19399 (дата обращения: 17.04.2025).

97 Dataminr for News launched // https://www.usatoday.com (дата обращения: 12.02.2025).

98 Cyabra – кейс-стадии // https://cyabra.com/case-studies/ (дата обращения: 15.02.2025).

99 Bolster – Dark Web Monitoring // https://bolster.ai/platform/dark-web-monitoring (дата обращения: 15.02.2025).

100 The Role of AI in Dark Web Monitoring // https://www.zerofox.com (дата обращения: 27.01.2025).

101 Advances in AI Increase Risks of Government Social Media Monitoring // https://www.brennancenter.org/our-work/analysis-opinion/advances-ai (дата обращения: 04.01.2024).

102 Dakalbab F., Abu Talib M., Abu Waraga O. et al. Artificial intelligence & crime prediction: A systematic literature review // Social Sciences & Humanities Open. – 2022. – Vol. 6, Issue 1. – P. 100342.

103 Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations // https://nij.ojp.gov/library/publications/predictive-policing (дата обращения: 12.02.2025).

104 Cekic E. The impact of artificial intelligence tools on criminal psychological profiling // International Journal of Academic Research in Psychology. – 2024. – Vol. 11, Issue 1. – P. 1-13.

105 Perry W.L., McInnis B., Price C.C. et al. Predictive policing: the role of crime forecasting in law enforcement operations. – Washington 2013. – 189 p.

106 Бессонов А.А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2021. – №2. – С. 45-53.

107 Бессонов А.А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – №1(35). – С. 94-100.

108 Alikhademi K., Drobina E., Prioleau D. et al. A review of predictive policing from the perspective of fairness // Artif. Intell. Law. – 2022. – Vol. 30. – P. 1-17.

109 Бертовский Л.В., Сембекова Б.Р. Высокотехнологичные преступления как угроза национальной безопасности // Новеллы

материального и процессуального права: мат-лы всеросс. науч.-практ. конф. – Красноярск, 2020. – С. 127-130.

110 AI is turbocharging organized crime, EU police agency warns // https://apnews.com/article (дата обращения: 18.03.2025).

111 Company worker in Hong Kong pays out £20m in deepfake video call scam // https://www.theguardian.com/world/2024/feb/05/hong-kong (дата обращения: 20.02.2025).

112 Dunsin D., Ghanem M.C., Ouazzane K. et al. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response // Forensic Sci. Int.: Digit. Investig. – 2024. – Vol. 48. – P. 301675.

113 Police bust Vietnam-based phishing ring in W10b scam // https://www.koreaherald.com/article/3478244 (дата обращения: 15.02.2025).

114 Ekambaranathan A. Using stylometry to track cybercriminals in darknet forums. – Enschede: University of Twente, 2018. – 12 p.

115 Revolutionizing AI and Fraud Detection: How Deutsche Bank Achieved A 60% Reduction in False Positives // https://www.toolify.ai/ai-news (дата обращения: 13.02.2025).

116 Mohamed N. Current trends in AI and ML for cybersecurity: a state-of-the-art survey // Cogent Eng. – 2023. – Vol. 10, Issue 2. – P. 1-30.

117 Costa D.B., Pinna F.C.A., Joiner A.P. et al. AI-based approach for transcribing and classifying unstructured emergency call data: a methodological proposal // PLOS Digit. Health. – 2023. – Vol. 2, Issue 12. – P. e0000406.

118 Wu W. et al. Integrating emotion recognition with speech recognition and speaker diarisation for conversations // https://arxiv.org/abs/2308.07145 (дата обращения: 15.11.2024).

119 Alhussein G., Ziogas I., Saleem S. et al. Speech emotion recognition in conversations using artificial intelligence: a systematic review and meta-analysis // Artif. Intell. Rev. – 2025. – Vol. 58. – P. 198-1-198-49.

120 2024 State of AI in the Speech Technology Industry: AI Is Revolutionizing Translation, Dubbing, and Subtitling // https://www.speechtechmag.com (дата обращения: 15.11.2024).

121 Sentiment Analysis Moves into Voice Interactions // https://www.speechtechmag.com/Articles/Editorial/Features/Sentiment (дата обращения: 19.03.2025).

122 Visual Analytics for Sense-making in CRiminal Intelligence analysis (VALCRI) // https://cordis.europa.eu/project/id/608142 (дата обращения: 04.10.2024).

123 Воеводкин Д.В., Рустемова Г.Р., Бегалиев Е.Н. и др. К вопросу выявления поддельных заключений судебно-медицинских экспертиз посредством применения технологии искусственного интеллекта по опыту Республики Казахстан: научный обзор // Судебная медицина. – 2023. – Т. 9, №3. – С. 287-298.

124 FaceVACS Technology – Cognitec // https://www.cognitec.com/facevacs-technology.html (дата обращения: 14.03.2025).

125 AI Means Better, Faster and More for First Responders // https://www.dhs.gov/science-and-technology/news/2024/10/31/feature (дата обращения: 04.04.2025).

126 GPT-4 // https://openai.com/research/gpt-4 (дата обращения: 08.03.2025).

127 LLaMA – Meta AI // https://ai.meta.com/llama (дата обращения: 25.02.2025).

128 Yin Z., Wang Z., Xu W. et al. Digital forensics in the age of large language models // https://arxiv.org/abs/2504.02963 (дата обращения: 20.03.2025).

129 Gunshot Detection – Flock Safety // https://www.flocksafety (дата обращения: 20.03.2025).

130 Surden H. Artificial Intelligence and Law: An Overview // Georgia State University Law Review. – 2019. – Vol. 35. – P. 1305-1340.

131 Ashley K.D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. – Cambridge, 2017. – 421 p.

132 LexisNexis // https://www.lexisnexis.com (дата обращения: 12.02.2025).

133 Susskind R. Tomorrow's Lawyers: An Introduction to Your Future. – Ed. 2th. – Oxford, 2017. – 240 c.

134 Aletras N., Tsarapatsanis D., Preoţiuc-Pietro D., Lampos V. Predicting judicial decisions of the European Court of Human Rights: a natural language processing perspective // PeerJ Comput. Sci. – 2016. – Vol. 2. – P. e93-1-e93-20.

135 Wischmeyer T., Rademacher T. Regulating Artificial Intelligence. – Cham: Springer, 2020. – 388 p.

136 Katz D.M., Hartung D., Gerlach L. et al. Natural language processing in the legal domain // https://papers.ssrn.com/sol3/papers.cfm?abstract_ (дата обращения: 15.01.2025).

137 How to Extract and Analyze Legal Documents with Gen AI // https://www.lexisnexis.com/community/insights/legal/b/product (дата обращения: 15.01.2025).

138 Document Automation for Law Firms – Mitratech HotDocs // https://mitratech.com/industries/legal/document-automation-for-law (дата обращения: 15.01.2025).

139 Harper S.B., Weber E.S. Fiduciary responsibility: facilitating public trust in automated decision making // J. Soc. Comput. – 2022. – Vol. 3. – P. 345-362.

140 Katz D.M., Bommarito M.J., Blackman J. A general approach for predicting the behavior of the Supreme Court of the United States // PLoS One. – 2017. – Vol. 12, Issue 4. – P. e0174698.

141 Surden H. Machine learning and law // Wash. Law Rev. – 2014. – Vol. 89, Issue 1. – P. 87–115.

142 Blue J // https://www.bluej.com (дата обращения: 15.03.2025).

143 Zlatescu I.M., Zlatescu P.E. Implementation of the European ethical charter on the use of artificial intelligence in judicial systems and their environment // Int. J. Law Jurisprud. – 2019. – Vol. 10, Suppl. 1. – P. 237–242.

144 Искусственный интеллект помогает казахстанским судьям выносить приговоры // https://baigenews.kz/iskusstvennyy-intellekt-pomogaet (дата обращения: 15.03.2025).

145 Искусственный интеллект рассмотрел 665 тысяч судебных дел в Казахстане // https://kz.kursiv.media/2025-01-21/smrd-aisud/ (дата обращения: 21.02.2025).

146 Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks // https://www.propublica.org (дата обращения: 30.12.2024).

147 Как применяют информационные технологии в судебной системе // https://mail.kz/ru/news/kz-news/kak-primenyayut-informacionnye (дата обращения: 24.07.2024).

148 Case Center – Digital Evidence Management // https://legal.thomsonreuters.com/en/products/case-center (дата обращения: 11.01.2025).

149 Communication on Digitalisation of justice in the European Union and Proposal for e-CODEX Regulation // https://commission.europa.eu (дата обращения: 11.01.2025).

150 DoNotPay // https://donotpay.com (дата обращения: 15.03.2025).

151 Susskind R. Online courts and the future of justice. – Oxford, 2019. – 368 p.

152 Пусть впахивают роботы // https://time.kz/articles/zloba (дата обращения: 05.03.2025).

153 Assessment Tool for the Operationalisation of the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment // https://rm.coe.int/cepej-2023-16final-operationalisation (дата обращения: 15.03.2025).

154 Shi C., Sourdin T., Li B. The smart court – a new pathway to justice in China? // Int. J. Court Adm. – 2021. – Vol. 12. – P. 367-1-367-20.

155 Kazakh Audio to Text – Kazakh Transcription Online // https://www.rask.ai/tools/transcription/transcribe-kazakh (дата обращения: 09.02.2025).

156 В Казахстане тестируют интернет-суд с ИИ и распознаванием речи // https://turantimes.kz/obschestvo/59324-v-kazahstane-testirujut-internet (дата обращения: 16.04.2025).

157 European e-Justice Strategy 2024–2028 // https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AC_202500437 (дата обращения: 16.02.2025).

158 Shanghai Court Adopts New AI Assistant // https://www.sixthtone.com/news/1003496/shanghai-court-adopts-new (дата обращения: 25.01.2024).

159 Цветкова А.Д. Сведения о компьютерном почерке: проблемы поиска баланса между свободой личности и безопасностью государства // Вопросы безопасности. – 2023. – №3. – С. 71-83.

160 Content Authenticity Initiative // https://contentauthenticity (дата обращения: 08.02.2025).

161 Truepic's Technology Provides Authenticity and Content Verification via Tamper-Evident Imagery // https://www.truepic.com/blog/truepics (дата обращения: 09.02.2025).

162 Cognitec Systems – The Face Recognition Company // https://www.cognitec.com (дата обращения: 09.02.2025).

163 Pangea – Security Guardrails for AI Applications // https://pangea.cloud (дата обращения: 09.02.2025).

164 Искусственный интеллект внедрят в судебную систему Казахстана: юристы останутся без работы? // https://astanatv.kz/ru/news/139199/ (дата обращения: 28.02.2025).

165 Buddi – a go anywhere, anytime personal emergency response service // https://buddi.uk/security (дата обращения: 14.03.2025).

166 The Impact of Electronic Monitoring on Correctional Outcomes // https://www.canada.ca/en/correctional-service/corporate/library (дата обращения: 15.03.2025).

167 BI Incorporated – Solutions // https://bi.com/solutions/ (дата обращения: 15.03.2025).

168 Smart Prisons and Artificial Intelligence Systems Expand in Finland // https://justice-trends.press/smart-prisons-and-artificial-intelligence (дата обращения: 08.03.2025).

169 Ertl T., Taugerbeck S., Esau M. et al. The Social Mile – how (psychosocial) ICT can help to promote resocialization and to overcome prison // Proc. ACM Hum.-Comput. Interact. – 2019. – Vol. 3. – P. 1-31.

170 Fedorczyk F. Navigating the dichotomy of smart prisons: between surveillance and rehabilitation // Law Innov. Tech. – 2024. – Vol. 16. – P. 243-260.

171 Ollo V. Artificial intelligence (AI) – the penitentiary trajectory of the format of the social and creative // Bull. Postgrad. Educ. (Ser.). – 2025. – Vol. 31, Issue 60. – P. 203-218.

172 Oswald M., Grace J., Urwin S. et al. Algorithmic risk assessment policing models: lessons from the Durham HART model and 'experimental' proportionality // Inf. Commun. Technol. Law. – 2018. – Vol. 27, Issue 2. – P. 223-250.

173 Andrews D., Bonta J., Wormith J. Level of Service/Case Management Inventory (LS/CMI) // In book: The SAGE Encyclopedia of Criminal Psychology. – Thousand Oaks, 2019. – Vol. 2. – P. 972-974.

174 Atlas of Automation: Automated Decision-Making and Participation in Germany // https://atlas.algorithmwatch.org (дата обращения: 14.03.2025).

175 The Potential of AI to Enhance Mental Health in Correctional Facilities: Benefits for Staff and Incarcerated Individuals // https://emhicglobal.com (дата обращения: 10.03.2025).

176 The Times Crime and Justice Commission. Proposals by Times Crime and Justice Commission could become law // https://www.thetimes.co.uk (дата обращения: 15.03.2025).

177 Debt Collection AI Agent // https://beam.ai/agents/debt (дата обращения: 16.01.2025).

178 Beyond Automation: How AI is Revolutionizing Debt Recovery // https://thelevel.ai/blog/ai-debt-recovery/ (дата обращения: 12.02.2025).

179 AI in Collections: Transforming Debt Recovery Efficiency // https://convin.ai/blog/ai-in-collections-call-payments/ (дата обращения: 12.02.2025).

180 Machine Learning in Debt Collection: Transforming Recovery // https://convin.ai/blog/ai-in-collections-puabd/ (дата обращения: 13.02.2025).

181 FBI adds iris biometric to Next Generation Identification system // https://www.fbi.gov/news/stories/fbi-adds-iris-biometric-to-next (дата обращения: 15.03.2024).

182 Electronic Monitoring – Division of Adult Parole Operations (DAPO) // https://www.cdcr.ca.gov/parole/electronic-monitoring (дата обращения: 02.03.2025).

183 Social Media Screening – Probation – Parolee Monitoring // https://guardianalliancetechnologies.com/social-media-screening (дата обращения: 06.03.2025).

184 Ролз Дж. Теория справедливости / пер. с англ. – М., 2020. – 592 с.

185 Тайлер Т. Почему люди соблюдают закон / пер. с англ. – М., 2019. – 342 с.

186 Giddens A. The Consequences of Modernity. – Stanford, 1990. – 186 p.

187 Hood C., Rothstein H., Baldwin R. The Government of Risk: Understanding Risk Regulation Regimes. – Oxford, 2001. – 256 p.

188 Степаненко Д.А., Бахтеев Д.В., Евстратова Ю.А. Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. – 2020. – Т. 14, №2. – С. 206-214.

189 Garoupa N. The theory of optimal law enforcement // J. Econ. Surv. – 1997. – Vol. 11, Issue 3. – P. 267-295.

190 Bharati R.K. Ethical implications of AI in criminal justice: balancing efficiency and due process // Res. Rev. Int. J. Multidiscip. – 2024. – Vol. 9, Issue 7. – P. 93-105.

191 Бахтеев Д.В. Оценка эффективности интеллектуальных систем в правоохранительной деятельности на примере проекта NSP-SIGVER // Искусственный интеллект и большие данные (Big Data) в судебной и правоохранительной системе: реалии и требование времени: мат-лы международ. науч.-практ. конф. – Косшы, 2023. – С. 179-185.

192 Chiao V. Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice // Int. J. Law Context. – 2019. – Vol. 15, Issue 2. – P. 126-139.

193 Harcourt B.E. Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age. – Chicago: University of Chicago Press, 2007. – 336 p.

194 Sadykov M., Karim M.E., Tynyshbayeva A. et al. Properties of artificial intelligence systems in the context of their use in legal activities // Procced. 12th internat. Legal conf. (UUMILC 2023). – Sintok: Atlantis Press, 2024. – P. 156-169.

195 Курочкин С.А. Цифровые технологии и эффективность правосудия // Lex Russica. – 2022. – №10(191). – P. 152-163.

196 Садыков М.Б., Тынышбаева А.А. Принцип справедливости при использовании искусственного интеллекта и автоматизированных систем принятия решений в уголовном правосудии на примере преодоления расовой предвзятости // Вестник Карагандинской академии МВД РК им. Б. Бейсенова. – 2023. – №4(82). – С. 319-325.

197 Ardabili B., Pazho A., Noghre G. et al. Understanding policy and technical aspects of AI-enabled smart video surveillance to address public safety // Comput. Urban Sci. – 2023. – Vol. 3. – P. 21-1-21-17.

198 Ahmed A., Echi M. Hawk-Eye: an AI-powered threat detector for intelligent surveillance cameras // IEEE Access. – 2021. – Vol. 9. – P. 63283-63293.

199 Doshi K., Yilmaz Y. Online anomaly detection in surveillance videos with asymptotic bounds on false alarm rate // Pattern Recognit. – 2021. – Vol. 117. – P. 107865.

200 Khan R., Bajwa U., Raza R. et al. Anwar M. Beyond boundaries: advancements in fire and smoke detection for indoor and outdoor surveillance feeds // Eng. Appl. Artif. Intell. – 2025. – Vol. 142. – P. 109855.

201 Chen X. Efficient learning video surveillance and tracking based on deep learning algorithms // Procced. 4th internat. conf. Mobile Netw. Wireless Commun. (ICMNWC). – Bangalore, 2024. – P. 1-5.

202 Balti M., Somrani G., Jemai A. et al. AI-based video and image analytics // Procced. internat. conf. on Innovations in Intelligent Systems and Applications (INISTA). – Hammamet, – P. 1-6.

203 Lunhol O., Torhalo P. Artificial intelligence in law enforcement: current state and development prospects // Proceedings of Socratic Lectures. – 2024. – Vol. 10. – P. 120-124.

204 Sadykov M.B., Gajanayaka S.Ch. The use of artificial intelligence in law enforcement activity // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – 2023. – №1(31). – С. 175-183.

205 Kaplow L., Shavell S. Accuracy in the determination of liability // J. Law Econ. – 1992. – Vol. 37. – P. 1-15.

206 Sadykov M.B., Abzalbekova M.T., Gajanayaka S.C. Use of artificial intelligence in criminal investigation // Учёные труды Алматинской академии МВД РК им. М. Есбулатова. – 2024. – №1(78). – С. 402-409.

207 Scott K., Tredoux C., Nortje A. Evaluating the utility of facial identification information: accuracy versus precision // South Afr. J. Sci. – 2023. – Vol. 119, Issue 1/4. – P. 12067-1-12067-9.

208 Миронюк Р.В., Кобко Є.В. Оцінка громадськістю ефективності діяльності правоохоронного органу як форма громадського контролю // Аналітично-порівняльне правознавство. – 2024. – №6. – С. 618-625.

209 Hand D., Christen P., Kirielle N. F: an interpretable transformation of the F-measure // Mach. Learn. – 2020. – Vol. 110. – P. 451-456.

210 Lienig J., Bruemmer H. Reliability analysis // In book: Fundamentals of Electronic Systems Design. – Cham: Springer, 2017. – P. 45-73.

211 Hazra A. Using the confidence interval confidently // J. Thorac. Dis. – 2017. – Vol. 9, Issue 10. – P. 4124-4129.

212 Confidence Interval – GeeksforGeeks // https://www.geeksforgeeks (дата обращения: 18.03.2025).

213 Bostrom N. The control problem. Excerpts from Superintelligence: Paths, dangers, strategies // In book: Science Fiction and Philosophy: From Time Travel to Superintelligence. – Hoboken, 2016. – P. 308-330.

214 What does resource efficiency mean? // https://www.thecorporategovernanceinstitute.com/insights/lexicon/what (дата обращения: 18.03.2025).

215 Модернизация правоохранительных органов: индекс доверия // https://online.zakon.kz/Document/?doc_id=31400674&pos=12;-31 (дата обращения: 12.03.2025).

216 Игнатьев А.Г. Этика в области искусственного интеллекта в фокусе междисциплинарных исследований и развития национальных подходов: доклад. – М., 2022. – 28 с.

217 Сейтенов К.К., Садыков М.Б. Эпоха ChatGPT: к вопросу об этике и правовом регулировании генеративного искусственного интеллекта // Искусственный интеллект и большие данные (Big Data) в судебной и правоохранительной системе: реалии и требование времени: мат-лы международ. науч.-практ. конф. – Косшы, 2023. – С. 76-83.

218 Qualitative Usability Testing Tips // https://www.netizenexperience.com (дата обращения: 17.02.2025).

219 Садыков М.Б., Жилкайдаров Р.Р. Искусственный интеллект в правоохранительной деятельности: возможности и риски // Охрана, безопасность, связь. – 2024. – №9-1. – С. 238-249.

220 Харитонова Ю.С., Савина В.С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник Пермского университета. Юридические науки. – 2021. – №53. – С. 488-515.

221 Жарова А.К. Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы // J. Digital Technol. Law. – 2023. – Vol. 1, Issue 4. – P. 973-993.

222 Стэнфордские учёные представили индекс прозрачности ИИ-моделей: результаты удивляют // https://www.securitylab.ru/news (дата обращения: 19.11.2024).

223 Syrbu A.V., Sadykov M.B. Artificial intelligence in criminal investigation: opportunities and risks // Вестник Карагандинской академии МВД РК им. Б. Бейсенова. – 2024. – №2(84). – С. 181–188.

224 Algorithmic Complexity // https://devopedia.org/algorithmic (дата обращения: 19.03.2025).

225 Как провести аудит данных и оценить их качество: практическое руководство // https://apptask.ru/blog/audit-dannyx-i-ocenka (дата обращения: 19.03.2025).

226 How to Measure Data Quality // https://cellularnews.com (дата обращения: 14.02.2025).

227 Масштабируемость // https://piter-soft.ru/knowledge (дата обращения: 19.03.2025).

228 Lee Z.Y., Karim M.E., Ngui K. Deep learning artificial intelligence and the law of causation: application, challenges and solutions // Inf. Commun. Technol. Law. – 2021. – Vol. 30, Issue 3. – P. 255-282.

229 Nurkeeva D.R., Sadykov M.B. The usage of artificial intelligence to ensure the principle of legality in criminal proceedings: opportunities and risks // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – 2024. – №3(33). – С. 101-108.

230 Мохоря Е. Проблема соотношения права и закона в философии И. Канта и Г. Радбруха // Traditie şi inovare în cercetarea ştiinţifică: mater. conf. – Bălți, 2018. – P. 310-316.

231 Радбрух Г. Философия права / пер. с нем. – М., 2004. – 366 с.

232 Иеринг Р. Борьба за право / пер. с нем. – М., 2007. – 176 с.

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

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

235 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.

236 Artificial Intelligence and Criminal Justice. Final Report, December 3, 2024 // https://www.justice.gov/olp/media/1381796/dl (дата обращения: 10.01.2025).

237 AI Watch: Global regulatory tracker – United States // https://www.whitecase.com/insight-alert/ai-watch-global-regulatory (дата обращения: 20.01.2025).

238 Global AI Law and Policy Tracker // https://iapp.org (дата обращения: 31.01.2025).

239 Global AI Regulations Tracker: Europe, Americas & Asia-Pacific Overview // https://legalnodes.com/global-ai-regulations-tracker (дата обращения: 18.02.2025).

240 Five takeaways from UK’s AI safety summit at Bletchley Park // https://www.theguardian.com/technology/2023/nov/02/uk-ai-summit (дата обращения: 03.03.2025).

241 Мажилис принял закон об искусственном интеллекте // https://forbes.kz/articles/mazhilis-prinyal-zakon-ob-iskusstvennom-intellekte-17fd9f?ysclid=mh6mp1o25330322706 (дата обращения: 26.09.2025).

242 Сенат вернул в Мажилис законопроект об искусственном интеллекте // https://www.inform.kz/ru/senat-vernul-v-mazhilis-zakonoproekt-ob-iskusstvennom-intellekte-de173e?ysclid=mh6mkq1f3290396706 (дата обращения: 26.10.2025).

243 Темирбулатов С. Обсуждение продолжается: какой Цифровой кодекс мы примем? // https://online.zakon.kz/Document/?doc_id=36613095&ysclid=mh6n67kuoe32115389&pos=12;-10#pos=12;-10 (дата обращения: 26.10.2025).

244 ИИ под прицелом закона // https://kazpravda.kz/n/ii-pod-pritselom-zakona/?ysclid=mh6n41ylyo886193223 (дата обращения: 26.10.2025).

245 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on artificial intelligence and amending certain Union legislative acts (AI Act) // https://eur-lex.europa.eu/legal-content (дата обращения: 26.01.2025).

246 Thierer A. Evasive Entrepreneurs and the Future of Governance: How Innovation Improves Economies and Governments. – Washington, 2020. – 250 p.

247 AI Watch: Global regulatory tracker – United States // https://www.whitecase.com/insight-our-thinking/ai-watch-global (дата обращения: 01.04.2025).

248 В США заявили, что авторские права не распространяются на произведения, созданные ИИ // https://inbusiness.kz/ru/last/v-ssha (дата обращения: 19.03.2024).

249 The Take It Down Act and the Future of Platform Accountability // https://www.identity.com/the-take-it-down-act-and-the-future-of-platform-accountability/ (дата обращения: 26.10.2025).

250 Girl, 15, calls for criminal penalties after classmate made deepfake nudes of her and posted on social media // https://www.independent.co.uk/news/world/americas/elliston-berry-deepfakes-social-media-b2566806.html (дата обращения: 26.10.2025).

251 S.146 - TAKE IT DOWN Act // https://www.congress.gov/bill/119th-congress/senate-bill/146 (дата обращения: 26.10.2025).

252 AI Watch: Global regulatory tracker – China // https://www.whitecase.com/insight-alert/ai-watch-global-regulatory (дата обращения: 01.04.2025).

253 Shape of China’s AI regulations and prospects // https://law.asia/shape-of-china-ai-regulations-and-prospects/ (дата обращения: 25.02.2025).

254 Морозов Е. Дилемма Коллинриджа // https://educ.wikireading.ru (дата обращения: 03.07.2024).

255 Collingridge D. The Social Control of Technology. – NY., 1982. – 200 p.

256 China Enforces New AI Content Labeling Law in September 2025 // https://marketingtrending.asoworld.com/en/news/china-enforces-new-ai-content-labeling-law-in-september-2025/ (дата обращения: 25.10.2025).

257 Developments in the regulation of artificial intelligence // https://www.kwm.com/global/en/insights/latest-thinking/developments (дата обращения: 20.05.2024).

258 MCI Response to PQ on Regulatory Framework for Artificial Intelligence Governance in Singapore // https://www.mci.gov.sg/pressroom (дата обращения: 22.05.2024).

259 Указ Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации»: утв. 10 ноября 2019 года, №490 // http://publication.pravo.gov.ru/Document/View/0001201910110003 (дата обращения: 28.02.2024).

260 Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. – М.: Проспект, 2021. – 816 с.

261 Бахтеев Д.В. Искусственный интеллект: этико-правовые основы: монография. – М.: Проспект, 2023. – 176 с.

262 Skeem J.L., Lowenkamp C.T. Risk, race, & recidivism: predictive bias and disparate impact // Criminology. – 2016. – Vol. 54, Issue 4. – P. 680-712.

263 Конституционный закон Республики Казахстан «О прокуратуре»: принят 5 ноября 2022 года, № 155-VII ЗРК // https://adilet.zan.kz/rus (дата обращения: 19.01.2025).

264 China Unveils Artificial Intelligence ‘Prosecutor’ That Can Identify Dissent Against Regime, And Suggest Sentences // https://legalinsurrection.com (дата обращения: 02.06.2023).

265 Chinese scientists develop AI ‘prosecutor’ that can press its own charges // https://www.scmp.com/news/china/science/article/3160997/chinese (дата обращения: 02.06.2023).

ПРИЛОЖЕНИЕ А

Анкета для опроса сотрудников правоохранительных органов

Уважаемые коллеги!

Данный опрос проводится в рамках исследования на соискание степени доктора PhD докторанта Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан Садыкова Мухтара Бейбутовича на тему «Искусственный интеллект в правоохранительной деятельности: правовые и организационно-тактические аспекты».

Анкета является анонимной, в этой связи не требуется
указания Вашего имени.

1. В каком правоохранительном органе Вы служите?
А. Органы внутренних дел.
Б. Антикоррупционная служба.
В. Служба экономических расследований.
Г. Органы прокуратуры.

2. Стаж правоохранительной службы?
А. До года.
Б. От года до трех лет.
В. От трех до пяти лет.
Г. От пяти до семи лет.
Д. От семи до десяти лет.
Е. Свыше десяти лет.

3. В какой должности Вы проходите службу?
А. Оперативный сотрудник.
Б. Дознаватель.
В. Следователь.
Г. Прокурор.

4. Насколько хорошо Вы знакомы с технологиями искусственного интеллекта?

А. Имею незначительное представление о технологиях искусственного интеллекта и не интересуюсь вопросами повышения своей осведомленности по этой теме.

Б. Несмотря на ограниченные знания о технологиях искусственного интеллекта, в настоящее время нахожусь на стадии изучения данной темы.

В. Имею базовые знания о технологиях искусственного интеллекта и отслеживаю их развитие.

Г. Имею хорошие знания о технологиях искусственного интеллекта и отслеживаю их развитие.

5. Ваше отношение к технологиям искусственного интеллекта?

А. Крайне негативное.

Б. Негативное.

В. Нейтральное.

Г. Позитивное.

Д. Крайне позитивное.

6. Ваши навыки работы с системами на основе искусственного интеллекта:

А. Не имею навыков работы с системами на основе искусственного интеллекта;

Б. Имею минимальный опыт работы с системами на основе искусственного интеллекта.

В. Имею ограниченный опыт.

Г. Базовые навыки, имею опыт работы с некоторыми приложениями на основе искусственного интеллекта (ChatGPT, MidJourney).

Д. Имею навыки программирования и обучения систем искусственного интеллекта.

7. Считаете ли Вы, что система искусственного интеллекта способна заменить оперативного работника?

А. Да, способна заменить полностью.

Б. Да, но способна заменить лишь частично.

В. Нет, не способна заменить.

8. Считаете ли Вы, что система искусственного интеллекта способна заменить следователя?

А. Да, способна заменить полностью.

Б. Да, но способна заменить лишь частично.

В. Нет, не способна заменить.

9. Считаете ли Вы, что система искусственного интеллекта способна заменить прокурора?

А. Да, способна заменить полностью.

Б. Да, но способна заменить лишь частично.

В. Нет, не способна заменить.

10. Оцените степень Вашей готовности использовать технологии искусственного интеллекта при раскрытии уголовных правонарушений (по шкале от 1 до 5)?

А. 1.

Б. 2.

В. 3.
Г. 4.
Д. 5.

11. Оцените степень Вашей готовности использовать информацию от систем искусственного интеллекта при расследовании уголовных правонарушений (по шкале от 1 до 5)?

А. 1.
Б. 2.
В. 3.
Г. 4.
Д. 5.

12. Какой из вариантов соответствует Вашему видению роли искусственного интеллекта в правоохранительной деятельности?

А. Искусственный интеллект в роли следователя.

Б. Искусственный интеллект в роли помощника следователя.

В. Искусственный интеллект в роли судебного эксперта.

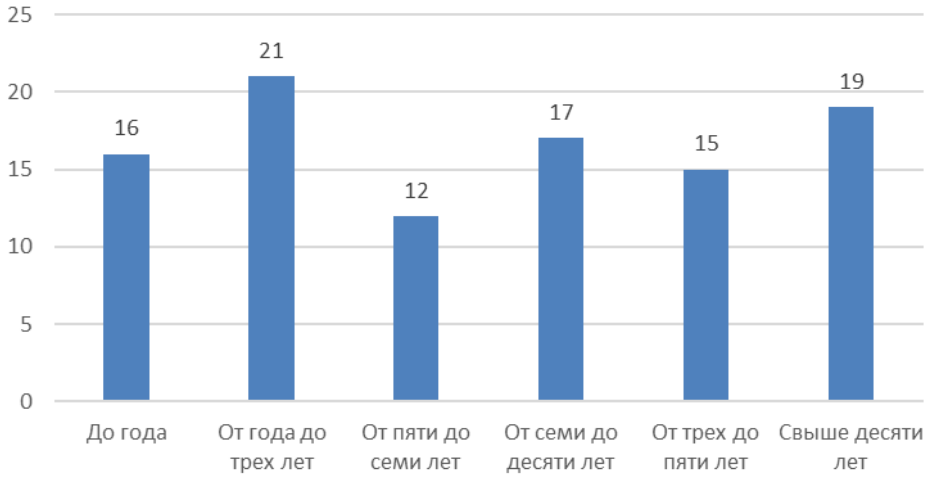
Г. Искусственный интеллект для сбора и обработки информации (прогноз преступности, выявление серийности, подготовка досье и т.д.).

Д. Не вижу перспектив использования искусственного интеллекта в правоохранительной деятельности.

Е. Иное (заполните текстовое поле).

ПРИЛОЖЕНИЕ Б

а



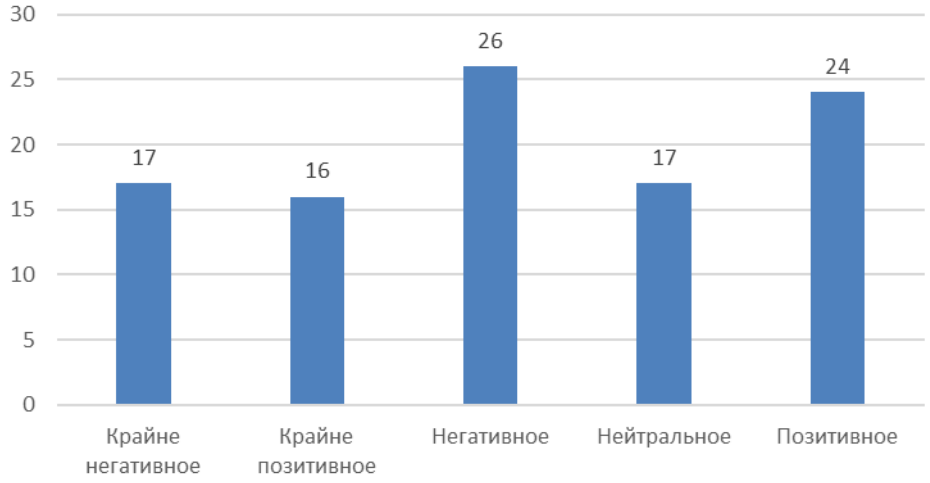
б

в

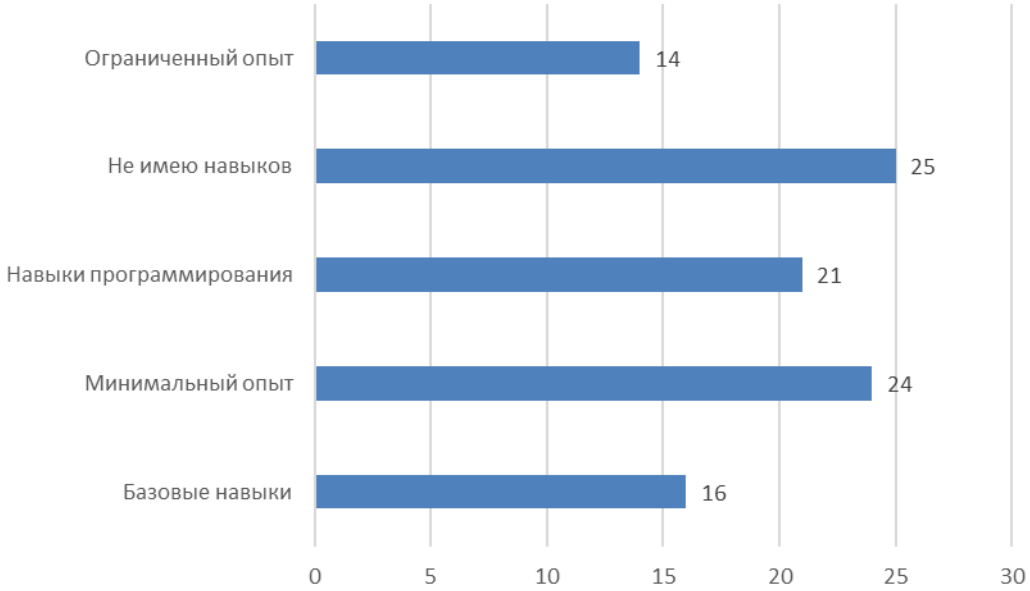
а – В каком правоохранительном органе Вы служите?; б – Стаж правоохранительной службы; в – В какой должности Вы проходите службу?

Рисунок Г.1 – Результаты анкетирования, лист 1

г



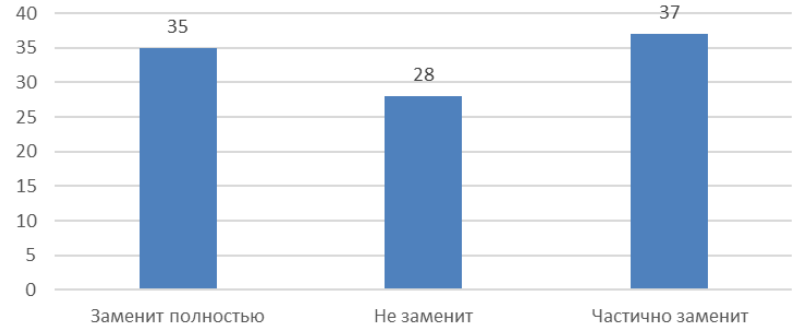
д



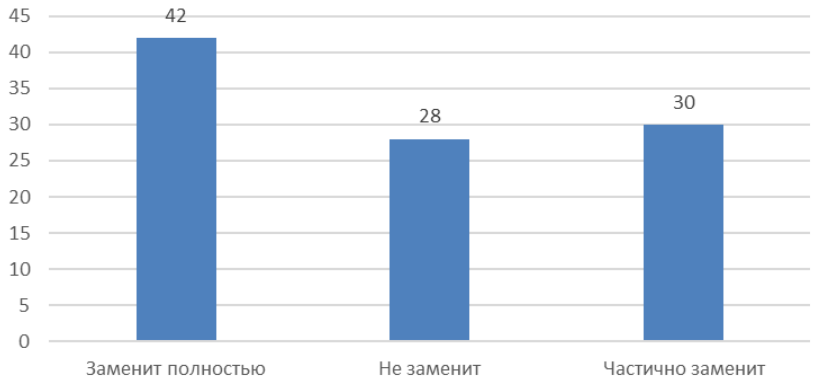
е

г – насколько хорошо Вы знакомы с технологиями искусственного интеллекта?; д – Ваше отношение к технологиям искусственного интеллекта; е – Ваши навыки работы с системами на основе искусственного интеллекта

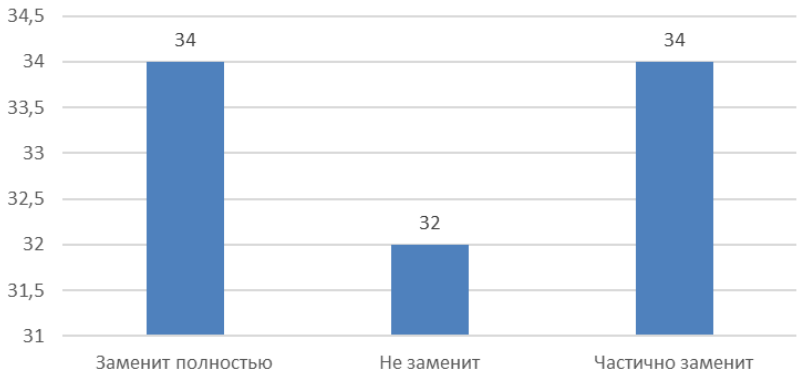
Рисунок Г.1, лист 2



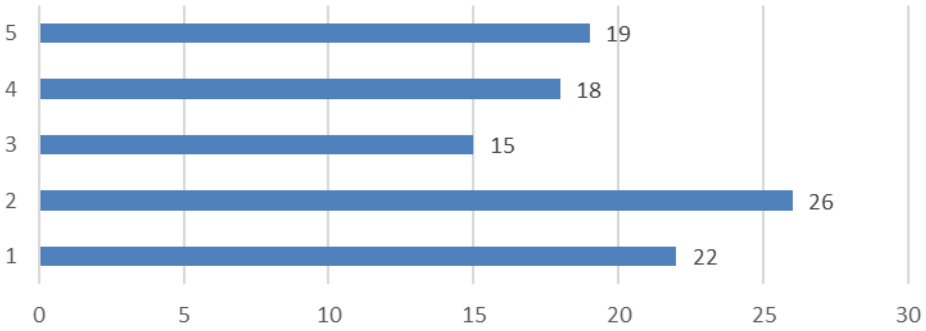
ж



и



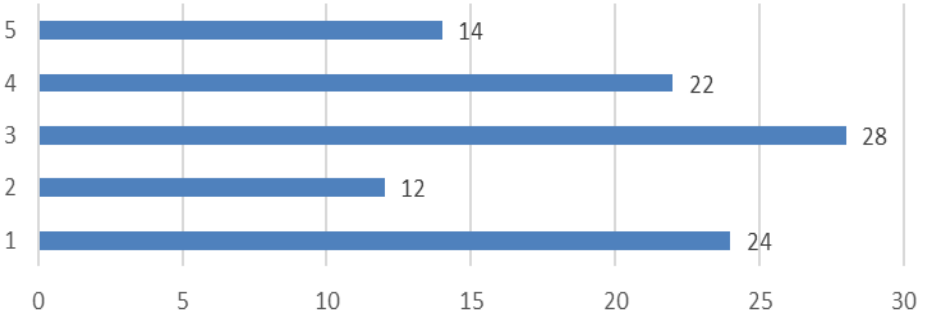
к



л

ж – Считаете ли Вы, что система искусственного интеллекта способна заменить оперативного работника?; и – Считаете ли Вы, что система искусственного интеллекта способна заменить следователя?; к – Считаете ли Вы, что система искусственного интеллекта способна заменить прокурора?; л – Оцените степень Вашей готовности использовать технологии искусственного интеллекта при раскрытии уголовных правонарушений (по шкале от 1 до 5)

Рисунок Г.1, лист 3



м

н

м – Оцените степень Вашей готовности использовать информацию от систем искусственного интеллекта при расследовании уголовных правонарушений (по шкале от 1 до 5); н – Какой из вариантов соответствует Вашему видению роли искусственного интеллекта в правоохранительной деятельности?

Рисунок Г.1, лист 4

Садыков М.Б.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Монография

Подписано в печать _____2026.
Формат 60×84 1/16.
Уч.изд.л. 25.80

Отпечатано в типографии Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан
010078, Акмолинская область,
г. Косшы, ул. Республики, строение 94