

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ КАЗАХСТАНА: ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И МЕХАНИЗМЫ ПРЕДОТВРАЩЕНИЯ ПОДРЫВА ОБЩЕСТВЕННОГО ДОВЕРИЯ

Д. УТЕГЕН, PhD докторант, Adjunct Assistant Professor Maqsut Narikbayev University (Республика Казахстан, г. Астана), e-mail: d_utegen@kazguu.kz

А. БАЛАХМЕТ, студентка 3 курса, Maqsut Narikbayev University (Республика Казахстан, г. Астана), e-mail: a.balakhmet@mail.ru

Актуальность исследования обусловлена ускоренной цифровой трансформацией государственного управления, в рамках которой государственные органы все чаще используют аналитические и генеративные системы искусственного интеллекта для подготовки проектов решений, обработки обращений граждан, сокращения времени принятия решений в рутинных административных процедурах и анализа больших массивов данных. Вместе с тем внедрение искусственного интеллекта в государственном секторе порождает значимые правовые риски, включая утечки персональных данных граждан и государственных служащих, раскрытие служебной информации ограниченного доступа, алгоритмическую предвзятость, а также ошибки и галлюцинации языковых моделей. Предметом исследования выступают законодательство Республики Казахстан в сфере цифрового права, искусственного интеллекта и персональных данных, а также право Европейского союза и стандарты Совета Европы, рассматриваемые в сравнительно-правовой перспективе. Цель статьи состоит в выявлении ключевых рисков применения искусственного интеллекта в государственном управлении Казахстана и в обосновании правовых и организационных инструментов, обеспечивающих баланс между эффективностью цифрового государства и гарантиями прав человека. Методологическую основу исследования составили формально-юридический и сравнительно-правовой методы, а также метод кейс-стади с опорой на зарубежный опыт и казахстанскую практику. Научная новизна работы заключается в комплексной оценке рисков цифровизации государственного управления через призму категории «правовое качество цифровизации» в условиях обновления цифрового законодательства Республики Казахстан. В качестве основного вывода обоснована необходимость перехода от абстрактных этических принципов к юридически обязательным процедурам, включая создание публичного реестра алгоритмических систем, используемых в государственном секторе.

Ключевые слова: общественное доверие, государственное управление, искусственный интеллект, персональные данные, конфиденциальность, служебная информация, алгоритмическая предвзятость, подотчетность, алгоритмические системы, Цифровой кодекс Республики Казахстан.

Введение

В Казахстане цифровая трансформация государственного управления в 2026 году получила дополнительный импульс – Указом Президента Республики Казахстан № 1151 от 6 января 2026 г. 2026 год объявлен Годом цифровизации и искусственного интеллекта [1]. В развитие данного решения Правительством утвержден План мероприятий по проведению Года цифровизации и искусственного интеллекта [2]. Одновременно принятие Цифрового кодекса Республики Казахстан [3] и профильного Закона Республики Казахстан «Об искусственном интеллекте» [4] переводит повестку внедрения интеллектуальных систем в плоскость юридически значимых обязанностей государственных органов и требований к подотчетности.

Еще в 1950 году А. Тьюринг задал дискуссионный вопрос: «Могут ли машины мыслить?» [5]. Э. Шмидт и соавторы утверждают, что искусственный интеллект становится фактором, формирующим социальную реальность и управленческие решения: «ИИ постепенно и незаметно становится автором нашей реальности» [6]. Для государственного управления это означает не только рост эффективности, но и усиление рисков для прав личности, прежде всего в части конфиденциальности данных и предсказуемости административных решений.

Практика передовых государств в сфере цифровизации государственных услуг демонстрирует, что инструменты искусственного интеллекта активно используются в различных формах в публичной сфере. Министерство юстиции Эстонии публично разъясняло, что не разрабатывает ИИ для замены судей, а сосредоточено на средствах снижения административной нагрузки и поддержке рабочих процессов [7; 8]. Также нашли широкое распространение процедурные модели управления рисками. Так, в Канаде действует Директива об автоматизированном принятии решений и обязательный инструмент предварительной оценки воздействия автоматизированных систем, проводимый до ее внедрения на права человека, оценка нацелена на выявление угроз для неприкосновенности частной жизни и защиты данных. [9; 24]. В Сингапуре государственное агентство цифровых технологий внедряет виртуальных помощников на сайтах государственных органов для помощи в навигации по услугам [10]. В Великобритании государственная цифровая служба запустила эксперимент с государственным чат-инструментом для упрощения доступа граждан к информации на государственном портале [11].

В международной практике цифровая зрелость государства оценивается через комплексные индексы и модели. Так, Индекс цифрового государства Организации экономического сотрудничества и развития использует измерения зрелости, включая цифровизацию, управление на основе данных, государство как платформу, открытость по умолчанию, ориентацию на пользователя и проактивность по части выявления уязвимостей и возникновения киберинцидентов [12]. Индекс зрелости государственных технологий Всемирного банка измеряет зрелость базовых государственных систем, цифровой инфраструктуры и электронных услуг, а также вовлечение граждан [13].

В Казахстане акцент на измеримости цифровой зрелости проявляется в переходе к цифровым метрикам результативности и прозрачности. Министерством финансов Республики Казахстан внедряется «цифровой профиль» государственного органа как совокупность данных об уровне цифровой зрелости и результативности ведомств, при этом отдельно подчеркивается необходимость экспертной верификации прогнозируемых данных, полученных с использованием интеллектуальных инструментов [14]. В отчете о реализации Концепции цифровой трансформации за 2023 год закреплены целевые показатели ускорения и автоматизации предоставления услуг [15].

Высокие позиции Казахстана в глобальных индексах электронного правительства по данным Обзора электронного правительства Организации Объединенных Наций 2024 г. отражают общую динамику цифрового развития [16], однако не исключают различия уровней зрелости между ведомствами и различий в качестве данных и процессов на уровне конкретных государственных органов.

Несмотря на удобство и эффективность применения интеллектуальных инструментов в государственных услугах и судебной системе, существует ряд рисков, усиливающихся при недостаточной цифровой зрелости. Во-первых, возрастает риск утечек персональных данных и раскрытия служебной информации, особенно при использовании внешних сервисов без классификации данных, разграничения доступа и безопасной инфраструктуры, риски конфиденциальности и безопасности данных выделяются в рамках управления рисками искусственного интеллекта [16]. Во-вторых, алгоритмические решения могут воспроизводить структурную дискриминацию, если обучающие данные отражают недостоверные данные либо на входе языковая модель получила данные, основанные на предвзятом мнении [17; 18]. В-третьих, генеративные модели способны формировать правдоподобный, но фактически недостоверный контент, что критично при подготовке юридически значимых документов данный риск отдельно обозначен в профиле рисков генеративного искусственного интеллекта [20].

Отдельного внимания требуют биометрические технологии распознавания лиц, используемых правоохранительными органами, как зона повышенного риска, помимо того, в ЕС активно обсуж-

даются и иные формы биометрии, включая поведенческую, что обостряет вопросы определения правового режима, прозрачности и подотчетности при обработке таких данных [21]. Это подтверждает необходимость для госорганов заранее закреплять режимность биометрических данных и требования к проверке оснований обработки в ведомственных регламентах [21].

Указанные риски концентрируются в зоне управления данными, поскольку государственные органы одновременно выступают операторами обработки и пользователями персональных данных ограниченного доступа [22].

При этом для обеспечения доверия общества недостаточно этических деклараций и рекомендаций [23]. В научной статье Бегишева И. и Шутовой А. подчеркивается, что этические стандарты не заменяют правового регулирования и без нормативно закрепленных обязанностей и процедур формируется разрыв между этикой и исполнимыми механизмами ответственности, что особенно критично для публичного сектора [24].

По этой причине последующие разделы статьи фокусируются на правовых и организационных мерах предотвращения утечек и обеспечении сохранности данных при использовании ИИ. Для целей настоящей статьи ключевые понятия используются в значениях, закрепленных в национальном законодательстве и применимых международных стандартах.

Термины «искусственный интеллект», «система искусственного интеллекта» и «модель искусственного интеллекта» применяются в значении, установленном Законом Республики Казахстан «Об искусственном интеллекте» [4].

Под персональными данными понимаются сведения, относящиеся к определенному или определяемому субъекту; биометрические данные рассматриваются как персональные данные, характеризующие физиологические и биологические особенности, на основе которых можно установить личность [25].

Под служебной информацией ограниченного доступа в статье понимаются сведения, отнесенные к служебной информации ограниченного распространения и маркируемые пометкой «Для служебного пользования» в порядке, установленном Правительством Республики Казахстан [25]. Конфиденциальность данных понимается как режим недопущения несанкционированного доступа и раскрытия персональных данных и служебной информации, обеспечиваемый правовыми, организационными и техническими мерами защиты [25; 26].

Общественное доверие рассматривается как устойчивое ожидание законности, справедливости и предсказуемости действий государства, влияющее на легитимность управленческих решений. Оценка воздействия используется как обозначение предварительной процедуры выявления и снижения рисков для прав и свобод личности при внедрении и существенных изменениях цифровых решений повышенного риска, включая риски для частной жизни, конфиденциальности и недискриминации [9; 25; 28].

Индексирование неприкосновенности частной жизни применяется как авторский прикладной инструмент ведомственной самооценки на основе измеримых индикаторов конфиденциальности данных, подотчетности и безопасности.

Материалы и методы исследования

Исследование выполнено на основе формально-юридического анализа законодательства Республики Казахстан в сфере искусственного интеллекта, персональных данных и режима служебной информации [3; 4; 25; 26], а также сопоставления с правом Европейского союза и стандартами Совета Европы в части защиты данных и подотчетности цифровых решений [26; 27; 29].

Сравнительно-правовой анализ проводился путем выделения сопоставимых элементов регулирования цели обработки, минимизация данных, разграничение доступа, механизмов контроля и аудита и сопоставления того, как эти элементы закрепляются и реализуются на уровне законов и ведомственных процедур в Казахстане и на опыте стран участниц Европейского союза.

Метод анализа конкретных ситуаций применен для систематизации типовых инцидентов утечки данных, раскрытия служебной информации, ошибок и недостоверных выводов генеративных моделей, включая инцидент 2023 года сбоя генеративного сервиса [31]. На заключительном этапе выводы сформулированы в виде индикаторов индексирования неприкосновенности частной

жизни для каждого индикатора определены объект контроля, подтверждающий документ и ответственный субъект внутри государственного органа.

Основные положения

В соответствии со статьей 93 Цифрового кодекса Республики Казахстан цифровая трансформация государственного управления связана с повышением эффективности оказания государственных услуг, применения аналитики данных на основе принципа прозрачности и проактивности по рискам в целях соблюдения прав субъектов в цифровой среде [3]. По логике данного положения цифровая зрелость государственных органов должна оцениваться не только по скорости и удобству сервисов, но и по качеству архитектуры данных и соблюдению гарантий защиты неприкосновенности частной жизни и персональных данных.

Важный шаг в сторону измеримости закреплен в статье 95 Цифрового кодекса, где вводится индекс цифрового развития как комплексный показатель готовности государственных органов и организаций к процессам цифровизации [3]. Индекс определяется ежегодно в рамках оценки эффективности деятельности государственных органов, а методика его расчета утверждается уполномоченным органом по согласованию с Высшей аудиторской палатой [3]. Это положение создает нормативную основу для включения в оценку цифровой зрелости измеримых критериев доверия, основанных на режиме данных и подотчетности.

Для практической реализации принципа устойчивости общественного доверия представляется обоснованным дополнить оценку цифрового развития показателями «правового качества цифровизации», в том числе: наличием классификации данных и запретов на ввод служебной информации ограниченного доступа и специальных категорий персональных данных во внешние сервисы, управлением доступом, соблюдением обязанностей по уведомлению о нарушении безопасности персональных данных и наличием процедур человеческого контроля при пересмотре решений принятых на основе алгоритмов ИИ.

Согласно требованиям статьи 43 права субъектов цифровой среды обеспечиваются при использовании алгоритмических систем и полностью автоматизированных решений, включая недопустимость применения дискриминационных мер, право на доступ к информации о порядке принятия алгоритмического решения [3]. Дополнительным инструментом подтверждения цифровой зрелости выступают предусмотренные Кодексом испытания и аудит цифровых объектов на соответствие требованиям кибербезопасности и аудит качества цифровых объектов, систем искусственного интеллекта с проверкой правомерности использования обучаемых данных и наличия запрещенных функциональных возможностей [3]. В качестве прикладного модуля для государственных органов может быть использовано индексирование неприкосновенности частной жизни, позволяющее фиксировать минимальный набор индикаторов конфиденциальности, безопасности и подотчетности при внедрении ИИ и иных цифровых решений.

Обеспечение общественного доверия в условиях повсеместной цифровизации государственных услуг требует предсказуемости режима обработки данных государственными органами, объяснимости процедур, периодического аудита и внедрения механизмов контроля.

Во-первых, в части конфиденциальности приоритет должен быть смещен от постфактум реагирования к превентивному управлению рисками на всех стадиях жизненного цикла ИИ. Рамочная модель управления рисками ИИ Национального института стандартов и технологий США исходит из необходимости непрерывного управления рисками, включая управление данными, тестирование, мониторинг уязвимостей [16]. Для госсектора Казахстана это означает закрепление обязательных правил безопасного использования ИИ государственными служащими путем классификации данных по уровню чувствительности, запрета на ввод служебной информации ограниченного распространения и специальных категорий персональных данных во внешние сервисы, а также применения технических и организационных средств предотвращения утечек данных. Данная логика коррелирует с публичной позицией депутата Мажилиса Е. Смышляевой о том, что в публичных и государственных процессах должны использоваться только цифровые решения, соблюдающие требования национального законодательства, поскольку применение непроверенных внешних платформ создает риски утраты контроля над персональными данными

и ограничивает возможности правовой защиты пользователей [32]. Дополнительно в парламентском обсуждении регулирования ИИ депутат Смышляева отдельно указывала на значимость защиты данных и ответственности за последствия применения ИИ [33]. Такой подход также соответствует принципам Организации экономического сотрудничества и развития по ИИ, где доверие связывается с уважением прав человека, прозрачностью, надежностью и подотчетностью цифровых систем [34].

В марте 2023 года произошел инцидент, связанный с генеративным сервисом ChatGPT, который был временно приостановлен из-за ошибки в программном компоненте с открытым исходным кодом. Компания OpenAI признала риск раскрытия ограниченных пользовательских данных у части пользователей, что демонстрирует возможность утечки даже при отсутствии умысла и при внешней зависимости от программных компонентов [31]. В Казахстане в соответствии с Законом Республики Казахстан «Об информатизации», Законом Республики Казахстан «О персональных данных и их защите» и подзаконными актами такие случаи должны рассматриваться не только как технический сбой, но и как юридически значимый инцидент. Собственник и (или) оператор при обнаружении нарушения безопасности персональных данных уведомляют уполномоченный орган в установленном порядке и сроке [25;35;36]. Уполномоченный орган, получив уведомление, в течение одного рабочего дня направляет оператору электронного правительства сведения, необходимые для оповещения субъектов персональных данных о нарушении безопасности персональных данных [36].

Во-вторых, для снижения дискриминационных эффектов и предотвращения непрогнозируемых последствий требуется закрепить обязательность предварительной оценки воздействия и процедур управления рисками до внедрения высокорисковых систем, а также при их существенных изменениях. В Европейском союзе статья 27 Регламента 2024/1689 предусматривает обязанность органов публичной власти и частных организаций, оказывающих публичные услуги, проводить оценку воздействия на фундаментальные права до первого использования высокорисковой системы ИИ, включая описание сценария применения, категорий затрагиваемых лиц и меры человеческого контроля [30]. Согласно статьям 10, 11, 14, 15 Регламент также устанавливает требования к управлению данными и наборами данных, к технической документации, к человеческому надзору, а также к точности, устойчивости и кибербезопасности на протяжении жизненного цикла [30].

Обсуждение

Практика ЕС подтверждает, что дискриминационный эффект может формироваться через данные и управленческие настройки. Так, в Нидерландах аналитика пособий по уходу за детьми показала, что риск-профилирование в целях выявления мошенничества может приводить к массовым ошибочным квалификациям заявителей как нарушителей [37; 38].

В Нидерландах также применялась система «Systeem Risico Indicatie» (далее – SyRI) – информационная система индикаторов риска для риск-профилирования в социальной сфере. Окружной суд Гааги в 2020 году признал использование SyRI несоразмерным вмешательством и указал на недостаточность гарантий, в том числе с учетом риска дискриминации и стигматизации, при непрозрачности критериев профилирования и отсутствии достаточного независимого контроля [39; 40].

Для Казахстана указанная процедурная модель соотносится с Цифровым кодексом Республики Казахстан, который закрепляет приоритет прав, свобод и законных интересов человека в цифровой среде как высшей ценности и ориентирует правоприменение на предотвращение дискриминации и злоупотреблений цифровыми технологиями [3]. Следовательно, требование предварительной оценки воздействия для высокорисковых систем, включая оценку рисков дискриминации и качества данных, может рассматриваться как инструмент практической реализации принципов цифрового законодательства, а не как дополнительная рекомендация.

При разработке ведомственных правил следует отдельно выделять биометрические системы как категорию повышенного риска и закреплять дополнительные гарантии их применения, путем ограничения целей, минимизации данных, независимого аудита, и процедур доступа. Сравнительные исследования по моделям регулирования распознавания лиц подчеркивают необходимость

риск-ориентированной категоризации биометрических систем и усиленных мер охраны биометрических данных как условия защиты права на неприкосновенность частной жизни [22].

В административных процедурах необходим минимальный стандарт объяснимости и права на оспаривание решений, поддержанных ИИ. Канадская Директива об автоматизированном принятии решений предусматривает обязательную предварительную оценку воздействия автоматизированных систем на права и интересы затрагиваемых лиц, а также меры прозрачности и механизмы обжалования [9; 28]. Для Казахстана подобная логика существенно важна, в тех случаях, где решения затрагивают доступ к услугам, социальным выплатам, контрольным и надзорным мерам. В практическом плане это требует закрепления обязанности указывать правовое основание и используемые данные, процедуры пересмотра результата человеком, понятного канала подачи жалобы и исправления ошибки, а также фиксации стадий принятия решения и ответственных лиц [3].

Инструментом укрепления доверия является публичный реестр алгоритмических систем, применяемых государственными органами в высокорисковых сферах, с описанием цели, правового основания, категории данных, ответственного оператора, процедуры проверки результатов и итогов оценки риска. Реестр снижает информационную асимметрию между государством и гражданами, создает основу для независимого аудита и повышает предсказуемость государственного управления.

В сентябре 2025 года правительство Албании объявило о назначении виртуального министра на основе ИИ под наименованием Diella с задачей повышения прозрачности и борьбы с коррупцией в государственных закупках [41]. В феврале 2026 года агентство Reuters сообщило о судебном споре, в рамках которого актриса заявила, что ее изображение и голос были использованы для создания аватара без надлежащего согласия, что актуализировало вопрос правового режима биометрических данных и ответственности публичных субъектов [42]. Параллельно отмечались случаи распространения сатирических и ложных сообщений вокруг кейса, что повышает значимость прозрачной коммуникации государства и верифицируемости фактов при внедрении ИИ в публичной сфере [43].

Наконец, важно учитывать, что применение ИИ в госсекторе затрагивает не только цифровые права граждан, но и служебную идеологию как систему ценностей публичной службы. Нарушение конфиденциальности служебной информации и персональных данных государственных служащих повышает уязвимость ведомств, снижает качество принятия решений и создает риски злоупотреблений. Следовательно, меры по защите данных в госсекторе должны рассматриваться как элемент укрепления доверия и профилактики коррупционных рисков.

Заключение

Таким образом, применение искусственного интеллекта в государственном управлении одновременно расширяет возможности цифрового государства и усиливает риски, способные подорвать устойчивость общественного доверия. К числу наиболее критичных относятся риски конфиденциальности персональных данных граждан и государственных служащих, раскрытия служебной информации ограниченного доступа, дискриминационных эффектов и ошибок генеративных моделей.

В Казахстане этап 2025-2026 годов характеризуется институционализацией искусственного интеллекта через принятие Цифрового кодекса и профильного закона. Вместе с тем доверие граждан зависит от того, насколько измеримо и проверяемо государство обеспечивает режим данных и подотчетность цифровых решений. В этой связи целесообразно использовать предусмотренный Цифровым кодексом индекс цифрового развития как инструмент оценки цифровой зрелости государственных органов и дополнить методику его расчета показателями правового качества цифровизации, включая управление данными, безопасность и гарантии прав субъекта при применении алгоритмических систем [3].

В качестве прикладных рекомендаций для государственных органов, в развитие экспертных предложений, представленных автором Даной Утеген на Совете по вопросам цифровизации и искусственного интеллекта при партии АМАНАТ в рамках Года цифровизации и искусственного интеллекта, предлагается:

- утвердить обязательную оценку воздействия на права человека и конфиденциальность для высокорисковых систем;
 - внедрить публичный реестр алгоритмических систем в госсекторе и единый стандарт информирования и пересмотра решений;
 - установить усиленные ограничения для применения биометрической идентификации и обработки данных детей;
 - закрепить ведомственные правила безопасного использования ИИ, включая запрет на ввод чувствительных данных во внешние сервисы и процедуры уведомления об инцидентах;
 - обеспечить независимый аудит качества и кибербезопасности цифровых объектов.
- Реализация указанных мер повысит предсказуемость цифровых процедур, снизит риски утечек данных и дискриминации, тем самым поддержит устойчивость общественного доверия.

Вклад авторов:

Балахмет А.Б. – разработка концепции статьи, сбор эмпирических материалов, подготовка первоначального текста;

Утеген Д. – методология исследования, правовой анализ, рекомендации, обсуждение и написание и утверждение окончательной версии.

Д. Утеген, PhD докторант, Adjunct Assistant Professor Maqсут Narikbayev University (Қазақстан Республикасы, Астана қ.); А. Балахмет, 3 курс студенті, Maqсут Narikbayev University (Қазақстан Республикасы, Астана қ.): Қазақстанның мемлекеттік басқаруындағы жасанды интеллект: дербес деректерді қорғау және қоғамдық сенімнің әлсіреуінің алдын алу тетіктері.

Зерттеудің өзектілігі мемлекеттік басқарудың жедел цифрландырылуымен байланысты, соның аясында мемлекеттік органдар шешім жобаларын әзірлеуде, азаматтардың өтініштерін өңдеуде, күнделікті әкімшілік рәсімдерде шешім қабылдау уақытын қысқартуда және ауқымды деректерді талдауда жасанды интеллект жүйелерін барған сайын жиі қолдануда. Сонымен қатар, мемлекеттік секторда жасанды интеллектті енгізу азаматтар мен мемлекеттік қызметшілердің дербес деректерінің таралуы, қолжетімділігі шектеулі қызметтік ақпараттың жария болуы, алгоритмдік біржақтылық, сондай-ақ модельдердің қателері мен «галлюцинациялары» сияқты елеулі құқықтық тәуекелдерді туындатады. Зерттеу пәні ретінде Қазақстан Республикасының цифрлық құқық, жасанды интеллект және дербес деректер саласындағы заңнамасы, сондай-ақ салыстырмалы-құқықтық қырынан қарастырылған Еуропалық Одақ құқығы мен Еуропа Кеңесінің стандарттары алынады. Зерттеудің мақсаты – Қазақстанның мемлекеттік басқару жүйесінде жасанды интеллектті қолдануға байланысты негізгі тәуекелдерді айқындау және цифрлық мемлекеттің тиімділігі мен адам құқықтарының кепілдіктері арасындағы тепе-теңдікті сақтауға мүмкіндік беретін құқықтық әрі ұйымдастырушылық тетіктерді негіздеу. Әдіснамалық негізін формальды-құқықтық және салыстырмалы-құқықтық әдістер, сондай-ақ шет мемлекеттердің тәжірибесі мен Қазақстан практикасына сүйенетін кейс-стади әдісі құрайды. Ғылыми жаңалығы мемлекеттік басқаруды цифрландыру тәуекелдерін Қазақстанның жаңарып жатқан цифрлық заңнамасы жағдайында «цифрландырудың құқықтық сапасы» ұғымы арқылы кешенді талдаудан көрінеді. Негізгі қорытынды ретінде мемлекеттік секторда қолданылатын алгоритмдік жүйелердің жария тізілімін енгізу және реттеуді абстрактілі этикалық қағидалардан заңдық тұрғыдан міндетті рәсімдерге көшіру қажеттігі негізделеді.

Түйінді сөздер: қоғамдық сенім, мемлекеттік басқару, жасанды интеллект, дербес деректер, құпиялық, қызметтік ақпарат, алгоритмдік біржақтылық, есептілік, алгоритмдік жүйелер, Қазақстан Республикасының Цифрлық кодексі.

D. Utegen, PhD Doctoral Candidate, Adjunct Assistant Professor at Maqсут Narikbayev University (Republic of Kazakhstan, Astana); A. Balakhmet, 3rd-year student at Maqсут Narikbayev University (Republic of Kazakhstan, Astana): Artificial Intelligence in Kazakhstan's Public Administration: Personal Data Protection and Mechanisms to Prevent the Erosion of Public Trust.

The relevance of this study stems from the accelerated digital transformation of public administration, in which public authorities increasingly use analytical and generative artificial intelligence (AI) systems to prepare draft decisions, process citizens' requests, shorten decision-making time in routine administrative procedures, and analyze large datasets. At the same time, the use of AI in the public sector creates significant legal risks, including personal data breaches affecting both citizens and civil servants, disclosure of restricted official information, algorithmic bias, as well as model errors and hallucinations. The subject of the study is Kazakhstan's legislation on digital law, artificial intelligence, and personal data protection, as well as European Union law and Council of Europe standards examined from a comparative legal perspective. The aim of the article is to identify the key risks related to the use of AI in Kazakhstan's public administration and to substantiate legal and organizational instruments capable of preserving a balance between the efficiency of the digital state and the protection of human rights. The methodological framework combines the formal legal method, comparative legal analysis, and the case-study method drawing on foreign experience and Kazakhstan's practice. The novelty of the study lies in its comprehensive assessment of the risks of digitalization in public administration through the lens of the "legal quality of digitalization" in the context of the development of Kazakhstan's digital legislation. The main conclusion is that regulation should shift from abstract ethical principles to legally binding procedures, including the introduction of a public register of algorithmic systems used in the public sector.

Keywords: public trust, public administration, artificial intelligence, personal data, confidentiality, official information, algorithmic bias, accountability, algorithmic systems, Digital Code of the Republic of Kazakhstan.

Список литературы:

1. Указ Президента Республики Казахстан от 6 января 2026 года № 1151 «Об объявлении Года цифровизации и искусственного интеллекта». URL: <https://www.akorda.kz/ru/ob-obyavlenii-goda-cifrovizacii-i-iskusstvennogo-intellekta-601222> (01.03.2026).
2. Постановление Правительства Республики Казахстан от 31 января 2026 года № 60 «Об утверждении Плана мероприятий по проведению Года цифровизации и искусственного интеллекта». URL: https://prg.kz/lawyer/document/?doc_id=36242706 (01.03.2026).
3. Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗПК. URL: <https://adilet.zan.kz/rus/docs/K2600000255> (01.03.2026).
4. Закон Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII ЗПК. URL: <https://adilet.zan.kz/rus/docs/Z2500000230> (01.03.2026).
5. Turing A.M. Computing Machinery and Intelligence. *Mind*. 1950. Vol. 59, No. 236. P. 433-460.
6. Киссинджер Г., Шмидт Э., Хаттенлокер Д. Искусственный разум и новая эра человечества. М.: Альпина ПРО; 2022.
7. Can AI Be a Fair Judge in Court? Estonia Thinks So. *WIRED*. 25 March 2019. URL: <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/> (01.03.2026).
8. Estonian Ministry of Justice. Estonia does not develop AI Judge. 16 February 2022. URL: <https://www.justdigi.ee/en/news/estonia-does-not-develop-ai-judge> (01.03.2026).
9. Treasury Board of Canada Secretariat. Directive on Automated Decision-Making. URL: https://publications.gc.ca/collections/collection_2021/sct-tbs/BT48-31-2021-eng.pdf (01.03.2026).
10. GovInsider. Is it time to say goodbye to 'Ask Jamie'? Inside GovTech's refresh of government chatbots. 13 September 2023. URL: <https://govinsider.asia/intl-en/article/is-it-time-to-say-goodbye-to-ask-jamie-inside-govtechs-refresh-of-government-chatbots> (01.03.2026).
11. Government Digital Service (UK). GOV.UK has entered the Chat: our vision for GOV.UK Chat. 16 December 2025. URL: <https://insidegovuk.blog.gov.uk/2025/12/16/gov-uk-has-entered-the-chat-our-vision-for-gov-uk-chat/> (01.03.2026).
12. OECD. Digital Government Index: 2019 Results. OECD Working Papers on Public Governance. 2020. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/digital-government-index_cec25265/4de9f5bb-en.pdf (01.03.2026).
13. World Bank. GovTech Maturity Index (GTMI). URL: <https://www.worldbank.org/en/programs/govtech/gtmi> (01.03.2026).

14. Министерство финансов Республики Казахстан. Цифровой профиль – новый инструмент повышения прозрачности и эффективности государственных органов. URL: <https://www.gov.kz/memleket/entities/minfin/press/news/details/991210?lang=ru> (01.03.2026).

15. Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Отчет о реализации Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы (отчетный период: 2023 год). URL: https://prg.kz/document/?doc_id=37036172 (01.03.2026).

16. United Nations. E-Government Survey 2024. URL: <https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf> (01.03.2026).

17. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1; 2023. URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf> (01.03.2026).

18. Obermeyer Z., Powers B., Vogeli C., Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019. Vol. 366(6464). P. 447-453. DOI: 10.1126/science.aax2342.

19. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias // ProPublica. 23 May 2016. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (01.03.2026).

20. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1; 2024. URL: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf> (01.03.2026).

21. Рахметов Б., Хайзабеков К. Поведенческая биометрия в Европейском союзе: правовые вызовы и технологические перспективы. Journal of Digital Technologies and Law. 2025. Т. 3. № 1. С. 108–124. DOI: 10.21202/jdtl.2025.5. URL: <https://www.lawjournal.digital/jour/article/view/511> (01.03.2026).

22. Утеген Д., Рахметов Б.Ж. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования. Journal of Digital Technologies and Law. 2023. Т. 1. № 3. С. 825–844. DOI: 10.21202/jdtl.2023.36. URL: https://www.lawjournal.digital/jour/article/view/247?locale=ru_RU (01.03.2026).

23. Dempsey J.X. Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues. Berkeley: Berkeley Center for Law & Technology; 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2020/08/Artificial-Intelligence-An-Introduction-to-the-Legal-Policy-and-Ethical-Issues_JXD.pdf (01.03.2026).

24. Бегишев И.Р., Шутова А.А. Регулирование технологий искусственного интеллекта: столкновение этики и закона. Лоббирование в законодательстве. 2025. Т. 4. № 1. С. 21–28. DOI: 10.33693/2782-7372-2025-4-1-21-28. URL: <https://www.urvak.ru/articles/lo-6275-vypusk-1-regulirovanie-tekhnologiy-iskusst/> (01.03.2026).

25. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V. URL: <https://adilet.zan.kz/rus/docs/Z1300000094> (01.03.2026).

26. Постановление Правительства Республики Казахстан от 24 июня 2022 года № 429 «Об утверждении Правил отнесения сведений к служебной информации ограниченного распространения и работы с ней». URL: <https://adilet.zan.kz/rus/docs/P2200000429> (01.03.2026).

27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (01.03.2026).

28. Government of Canada. Algorithmic Impact Assessment tool. URL: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> (01.03.2026).

29. Council of Europe. Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law. Opened for signature 5 September 2024. URL: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> (01.03.2026).

30. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (01.03.2026).

31. OpenAI. March 20 ChatGPT outage: here's what happened. 24 March 2023. URL: <https://openai.com/index/march-20-chatgpt-outage/> (01.03.2026).

32. В Мажилисе презентовали законопроект об искусственном интеллекте // Zakon.kz. 03.03.2025. URL: <https://www.zakon.kz/obshestvo/6469053-v-mazhilise-prezentovali-zakon-proekt-ob-iskusstvennom-intellekte.html> (01.03.2026).

33. Аксенова Е. «Иностранные мессенджеры не исполняют закон» депутаты предложили навести порядок. Tengrinews.kz. 17.12.2025. Электронный ресурс. URL: https://tengrinews.kz/kazakhstan_news/inostrannyye-messendjeryi-ispolnyayut-zakon-deputaty-588223/ (01.03.2026).

34. OECD Principles on Artificial Intelligence. Adopted 2019 (updated). URL: <https://oecd.ai/en/ai-principles> (01.03.2026).

35. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V. URL: <https://adilet.zan.kz/rus/docs/Z1500000418> (01.03.2026).

36. Приказ и. о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 9 августа 2024 года № 481/НҚ «Об утверждении Правил осуществления уведомления субъектов персональных данных о нарушении безопасности персональных данных». URL: <https://adilet.zan.kz/rus/docs/V2400034919> (01.03.2026).

37. European Commission. ESPN Flash Report: Netherlands – Childcare Allowance Scandal (Toeslagenaffaire). PDF. URL: <https://ec.europa.eu/social/BlobServlet?docId=24723&langId=en> (01.03.2026).

38. Amnesty International. Xenophobic Machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal. 2021. PDF. URL: https://www.amnesty.nl/content/uploads/2021/10/20211014_FINAL_Xenophobic-Machines.pdf (01.03.2026).

39. Van Bekkum M., Zuiderveen Borgesius F. Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security. 2021. DOI: 10.1177/13882627211031257. URL: <https://journals.sagepub.com/doi/10.1177/13882627211031257> (01.03.2026).

40. Rechtbank Den Haag. (SyRI). 5 March 2020. URL: <https://uitspraken.rechtspraak.nl/details?id=ECLI%3ANL%3ARBDHA%3A2020%3A1878> (01.03.2026).

41. Albania appoints AI bot as minister to tackle corruption. Reuters. 11 September 2025. URL: <https://www.reuters.com/technology/albania-appoints-ai-bot-minister-tackle-corruption-2025-09-11/> (01.03.2026).

42. Albanian actor sues government for using her image as “AI minister”. Reuters. 13 February 2026. URL: <https://www.reuters.com/business/media-telecom/albanian-actor-sues-government-using-her-image-ai-minister-2026-02-13/> (01.03.2026).

43. BIRN: How “Diella” was used by the Russian Pravda network to spread disinformation. Balkanweb. 6 February 2026. URL: <https://www.balkanweb.com/en/birn-si-u-perdor-diella-nga-rjeti-rus-pravda-per-te-perhapur-dezinformim/> (01.03.2026).

References:

1. Ukaz Prezidenta Respubliki Kazakhstan ot 6 yanvarya 2026 goda No. 1151 «Ob ob»yavlenii Goda tsifrovizatsii i iskusstvennogo intellekta». URL: <https://www.akorda.kz/ru/ob-obyavlenii-goda-cifrovizatsii-i-iskusstvennogo-intellekta-601222> (01.03.2026).

2. Postanovlenie Pravitel'stva Respubliki Kazakhstan ot 31 yanvarya 2026 goda No. 60 «Ob utverzhdenii Plana meropriyatii po provedeniyu Goda tsifrovizatsii i iskusstvennogo intellekta». URL: https://prg.kz/lawyer/document/?doc_id=36242706 (01.03.2026).

3. Tsifrovoy kodeks Respubliki Kazakhstan ot 9 yanvarya 2026 goda No. 255-VIII ZRK. URL: <https://adilet.zan.kz/rus/docs/K2600000255> (01.03.2026).

4. Zakon Respubliki Kazakhstan «Ob iskusstvennom intellekte» ot 17 noyabrya 2025 goda No. 230-VIII ZRK. URL: <https://adilet.zan.kz/rus/docs/Z2500000230> (01.03.2026).

5. Turing A.M. Computing Machinery and Intelligence. Mind. 1950. Vol. 59, No. 236. P. 433-460.

6. Kissindzher G., Shmidt E., Khattenloker D. Iskusstvennyi razum i novaya era chelovechestva. M.: Alpina PRO; 2022.

7. Can AI Be a Fair Judge in Court? Estonia Thinks So // WIRED. 25 March 2019. URL: <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/> (01.03.2026).
8. Estonian Ministry of Justice. Estonia does not develop AI Judge. 16 February 2022. URL: <https://www.justdigi.ee/en/news/estonia-does-not-develop-ai-judge> (01.03.2026).
9. Treasury Board of Canada Secretariat. Directive on Automated Decision-Making. URL: https://publications.gc.ca/collections/collection_2021/sct-tbs/BT48-31-2021-eng.pdf (01.03.2026).
10. GovInsider. Is it time to say goodbye to 'Ask Jamie'? Inside GovTech's refresh of government chatbots. 13 September 2023. URL: <https://govinsider.asia/intl-en/article/is-it-time-to-say-goodbye-to-ask-jamie-inside-govtechs-refresh-of-government-chatbots> (01.03.2026).
11. Government Digital Service (UK). GOV.UK has entered the Chat: our vision for GOV.UK Chat. 16 December 2025. URL: <https://insidgovuk.blog.gov.uk/2025/12/16/gov-uk-has-entered-the-chat-our-vision-for-gov-uk-chat/> (01.03.2026).
12. OECD. Digital Government Index: 2019 Results. OECD Working Papers on Public Governance. 2020. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/digital-government-index_cec25265/4de9f5bb-en.pdf (01.03.2026).
13. World Bank. GovTech Maturity Index (GTMI). URL: <https://www.worldbank.org/en/programs/govtech/gtmi> (01.03.2026).
14. Ministerstvo finansov Respubliki Kazakhstan. Tsifrovoy profil' – novyi instrument povysheniya prozrachnosti i effektivnosti gosudarstvennykh organov. URL: <https://www.gov.kz/memleket/entities/minfin/press/news/details/991210?lang=ru> (01.03.2026).
15. Ministerstvo tsifrovogo razvitiya, innovatsii i aerokosmicheskoi promyshlennosti Respubliki Kazakhstan. Otchet o realizatsii Kontseptsii tsifrovoy transformatsii, razvitiya otrasli informatsionno-kommunikatsionnykh tekhnologii i kiberbezopasnosti na 2023-2029 gody (otchetnyi period: 2023 god). URL: https://prg.kz/document/?doc_id=37036172 (01.03.2026).
16. United Nations. E-Government Survey 2024. URL: <https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf> (01.03.2026).
17. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1; 2023. URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf> (01.03.2026).
18. Obermeyer Z., Powers B., Vogeli C., Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019. Vol. 366(6464). P. 447-453. DOI: 10.1126/science.aax2342.
19. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias. ProPublica. 23 May 2016. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (01.03.2026).
20. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1; 2024. URL: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf> (01.03.2026).
21. Rakhmetov B., Khaizabekov K. Povedencheskaya biometria v Evropeiskom soyuze: pravovye vyzovy i tekhnologicheskie perspektivy. Journal of Digital Technologies and Law. 2025. T. 3. No. 1. S. 108-124. DOI: 10.21202/jdtl.2025.5. URL: <https://www.lawjournal.digital/jour/article/view/511> (01.03.2026).
22. Utegen D., Rakhmetov B. Zh. Tekhnologiya raspoznavaniya lits i obespechenie bezopasnosti biometricheskikh dannykh: komparativnyi analiz modelei pravovogo regulirovaniya. Journal of Digital Technologies and Law. 2023. T. 1. No. 3. S. 825-844. DOI: 10.21202/jdtl.2023.36. URL: https://www.lawjournal.digital/jour/article/view/247?locale=ru_RU (01.03.2026).
23. Dempsey J.X. Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues. Berkeley: Berkeley Center for Law & Technology; 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2020/08/Artificial-Intelligence-An-Introduction-to-the-Legal-Policy-and-Ethical-Issues_JXD.pdf (01.03.2026).

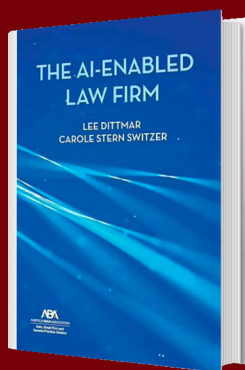
24. Begishev I.R., Shutova A.A. Regulirovanie tekhnologii iskusstvennogo intellekta: stolknovenie etikizakona. Lobbirovanie v zakonodatel'stve. 2025. T. 4. No. 1. S. 21-28. DOI: 10.33693/2782-7372-2025-4-1-21-28. URL: <https://www.urvak.ru/articles/lo-6275-vypusk-1-regulirovanie-tekhnologiy-iskusst/> (01.03.2026).
25. Zakon Respubliki Kazakhstan «O personal'nykh dannykh i ikh zashchite» ot 21 maya 2013 goda No. 94-V. URL: <https://adilet.zan.kz/rus/docs/Z1300000094> (d01.03.2026).
26. Postanovlenie Pravitel'stva Respubliki Kazakhstan ot 24 iyunya 2022 goda No. 429 «Ob utverzhdenii Pravil otneseniya svedenii k sluzhebnoi informatsii ogranichenного rasprostraneniya i raboty s nei». URL: <https://adilet.zan.kz/rus/docs/P2200000429> (01.03.2026).
27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (01.03.2026).
28. Government of Canada. Algorithmic Impact Assessment tool. URL: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> (01.03.2026).
29. Council of Europe. Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law. Opened for signature 5 September 2024. URL: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> (01.03.2026).
30. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (01.03.2026).
31. Open AI. March 20 ChatGPT outage: here's what happened. 24 March 2023. URL: <https://openai.com/index/march-20-chatgpt-outage/> (01.03.2026).
32. V Mazhilise prezentovali zakonoproekt ob iskusstvennom intellekte. Zakon.kz. 03.03.2025. URL: <https://www.zakon.kz/obshestvo/6469053-v-mazhilise-prezentovali-zakonoproekt-ob-iskusstvennom-intellekte.html> (01.03.2026).
33. Aksenova E. «Inostrannye messendzhery ne ispolnyayut zakon» – deputaty predlozhili navesti poryadok. Tengrinews.kz. 17.12.2025. URL: https://tengrinews.kz/kazakhstan_news/inostrannye-messendzhery-ispolnyayut-zakon-deputaty-588223/ (01.03.2026).
34. OECD Principles on Artificial Intelligence. Adopted 2019 (updated). URL: <https://oecd.ai/en/ai-principles> (01.03.2026).
35. Zakon Respubliki Kazakhstan «Ob informatizatsii» ot 24 noyabrya 2015 goda No. 418-V. URL: <https://adilet.zan.kz/rus/docs/Z1500000418> (01.03.2026).
36. Prikaz i.o. Ministra tsifrovogo razvitiya, innovatsii i aerokosmicheskoi promyshlennosti Respubliki Kazakhstan ot 9 avgusta 2024 goda No. 481/NK «Ob utverzhdenii Pravil osushchestvleniya uvedomleniya subektov personal'nykh dannykh o narushenii bezopasnosti personal'nykh dannykh». URL: <https://adilet.zan.kz/rus/docs/V2400034919> (01.03.2026).
37. European Commission. ESPN Flash Report: Netherlands – Childcare Allowance Scandal (Toeslagenaffaire). PDF. URL: <https://ec.europa.eu/social/BlobServlet?docId=24723&langId=en> (01.03.2026).
38. Amnesty International. Xenophobic Machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal. 2021. PDF. URL: https://www.amnesty.nl/content/uploads/2021/10/20211014_FINAL_Xenophobic-Machines.pdf (01.03.2026).
39. Van Bekkum M., Zuiderveen Borgesius F. Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security. 2021. DOI: 10.1177/13882627211031257. URL: <https://journals.sagepub.com/doi/10.1177/13882627211031257> (accessed: 01.03.2026).
40. Rechtbank Den Haag (SyRI). 5 March 2020. URL: <https://uitspraken.rechtspraak.nl/details?id=ECLI%3ANL%3ARBDHA%3A2020%3A1878> (01.03.2026).
41. Albania appoints AI bot as minister to tackle corruption. Reuters. 11 September 2025. URL: <https://www.reuters.com/technology/albania-appoints-ai-bot-minister-tackle-corruption-2025-09-11/> (01.03.2026).

42. Albanian actor sues government for using her image as «AI minister». Reuters. 13 February 2026. URL: <https://www.reuters.com/business/media-telecom/albanian-actor-sues-government-using-her-image-ai-minister-2026-02-13/> (01.03.2026).

43. BIRN: How “Diella” was used by the Russian Pravda network to spread disinformation. Balkanweb. 6 February 2026. URL: <https://www.balkanweb.com/en/birn-si-u-perdor-diella-nga-rrjetir-rus-pravda-per-te-perhapur-dezinformim/> (01.03.2026).

Для цитирования и библиографии: Утеген Д., Балахмет А. Искусственный интеллект в государственном управлении Казахстана: защита персональных данных и механизмы предотвращения подрыва общественного доверия // Право и государство. № 3(112), 2026. – С. 6-18. DOI: 10.51634/2307-5201_2026_3_6

Материал поступил в редакцию 14.03.2026



НОВЫЕ КНИГИ

Lee Dittmar, Carole Stern Switzer. The AI-Enabled Law Firm. American Bar Association. 2026. – 328 p.

ISBN-13: 978-1639057160

Planning for the effective integration and management of AI within a global law firm or corporate legal department represents a significant commitment – one that will undoubtedly consume substantial time, resources, and ongoing attention from leadership. This investment may initially appear as an unwelcome expansion of non-billable overhead, leading some to question its value proposition against traditional legal service delivery models. However, this planning process is not merely advisable but essential in a legal landscape where technological

adaptation has become a competitive necessity rather than a discretionary advantage.

The considered implementation of AI governance frameworks, training programs, and ethical guidelines serves multiple critical functions: It mitigates potentially severe regulatory, liability, and reputational risks that could arise from unstructured AI adoption; it creates the foundation for more efficient legal operations that will ultimately enhance client value; and it positions the organization to thrive amid unprecedented technological disruption that is already transforming client expectations, competitor capabilities, and the fundamental economics of legal practice. What may seem like an administrative burden today represents the scaffolding upon which tomorrow's successful legal enterprises will be built.