

УДК [004.8+334.722-028.27]:351.824.1(476)

34. ПРАВОВЫЕ РИСКИ И МЕХАНИЗМЫ РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦИФРОВОМ БИЗНЕСЕ

Стецко А.А., студент гр. 374003, Спиридонова Е.Д., студент гр. 374003

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Горноста́й Л.Ч. – старший преподаватель кафедры Менеджмента

Аннотация. В статье рассматриваются правовые аспекты внедрения искусственного интеллекта в цифровых бизнес-моделях. Показано, что формирование эффективного регулирования ИИ требует не только адаптации национального законодательства, но и учета международных подходов. На основе анализа опыта Европейского союза и США выявлены ключевые векторы правового развития. Систематизированы основные риски использования ИИ в бизнесе и предложены механизмы их минимизации. Сформулированы прогнозные оценки изменения регуляторной среды Республики Беларусь с учетом существующей институциональной структуры.

Ключевые слова. Искусственный интеллект, цифровые платформы, правовое регулирование, риск-ориентированный подход, Республика Беларусь, международный опыт.

Введение. Технологии искусственного интеллекта становятся неотъемлемым элементом цифровой трансформации бизнеса, проникая в кредитование, страхование, кадровый отбор, генерацию контента и иные сферы, где требуется обработка больших массивов данных и автоматизация решений. В Республике Беларусь наблюдается активное внедрение ИИ-решений, прежде всего в резидентах Парка высоких технологий, однако правовая среда остается фрагментированной: отсутствует специализированный закон, регулирование осуществляется через разрозненные акты, что создает неопределенность для участников рынка. Актуальность исследования обусловлена необходимостью системного анализа существующих правовых рисков и выработки прогнозных механизмов регулирования, которые позволят, с одной стороны, снизить издержки бизнеса, связанные с правовой неопределенностью, а с другой – обеспечить защиту прав граждан и информационную безопасность.

Объектом исследования выступают общественные отношения, возникающие при разработке и использовании ИИ в цифровом бизнесе. Цель работы – на основе анализа национального законодательства и международных подходов выявить ключевые правовые риски и предложить регуляторные механизмы, адаптированные к условиям Республики Беларусь. Для достижения поставленной цели в исследовании использовались общенаучные и специально-юридические методы. Формально-юридический метод позволил проанализировать нормы действующего законодательства Республики Беларусь, регулирующие сферы, смежные с использованием ИИ (защита персональных данных, кибербезопасность, интеллектуальная собственность). Сравнительно-правовой метод применен для изучения моделей регулирования ИИ в Европейском союзе и США, что дало возможность выявить универсальные принципы и институциональные решения, адаптируемые к белорусской правовой системе. Системный анализ использован при классификации правовых рисков и обосновании взаимосвязи между пробелами в законодательстве и предлагаемыми механизмами их минимизации.

Основная часть. Правовая база Республики Беларусь, применимая к технологиям ИИ, формируется несколькими отраслевыми актами. Закон «О защите персональных данных» устанавливает требования к обработке личной информации, включая необходимость согласия субъекта и уведомления об инцидентах [1]; однако он не содержит норм об алгоритмической обработке как особой категории. Закон «Об информации, информатизации и защите информации» закрепляет общие принципы информационной политики, обеспечения конфиденциальности и целостности данных [2], но не учитывает специфику машинного обучения. Декрет Президента № 8 о развитии цифровой экономики создал льготный правовой режим для резидентов ПВТ [3], включив в перечень разрешенных видов деятельности разработку ИИ и допустив применение английского права в договорах. Указ № 40 о кибербезопасности относит ИИ-системы [4], обрабатывающие охраняемые сведения, к объектам критической информационной инфраструктуры, устанавливая обязательные требования к их защите. Закон об авторском праве и смежных правах не признает объекты, сгенерированные нейросетями, результатами творческого труда физического лица, что создает правовую неопределенность при их коммерциализации [5].

Таким образом, национальное регулирование характеризуется фрагментарностью и отсутствием единой концепции. В то же время государственная программа «Цифровая Беларусь» на 2026–2030 годы в блоке обеспечения цифрового суверенитета ставит задачи развития ИИ-инфраструктуры, что свидетельствует о намерении перейти к более системной политике [6].

Анализ международного опыта регулирования ИИ необходим для выявления институциональных решений, которые могут быть адаптированы к национальной правовой системе с учетом ее сложившейся структуры и приоритетов развития. Изучение зарубежных подходов позволяет не только идентифицировать универсальные принципы (риск-ориентированность, прозрачность, человеческий контроль), но и оценить эффективность различных моделей с точки зрения баланса между стимулированием инноваций и защитой публичных интересов. Для Республики Беларусь, находящейся на этапе формирования системного регулирования, такое сравнение снижает издержки нормотворчества за счет использования апробированных решений.

В качестве объектов анализа выбраны две юрисдикции – Европейский союз и Соединенные Штаты Америки. Выбор обусловлен несколькими факторами. Во-первых, данные регионы формируют два основных вектора современного правового регулирования ИИ: унифицированный (ЕС) и секторально-децентрализованный (США). Во-вторых, именно эти модели оказывают наибольшее влияние на формирование международных стандартов и практик, что подтверждается активной имплементацией их подходов в документах ОЭСР, ЮНЕСКО и ISO [7]. В-третьих, для белорусского бизнеса, ориентированного на экспорт ИТ-услуг, соответствие требованиям этих юрисдикций является значимым конкурентным преимуществом.

Европейский союз реализовал модель жесткого правового регулирования, приняв Регламент об искусственном интеллекте (EU AI Act 2024/1689). Ключевым элементом выступает классификация ИИ-систем по уровням риска: от минимального до неприемлемого. Для систем высокого риска установлены обязательные требования к качеству обучающих данных, прозрачности, документированию, человеческому контролю и кибербезопасности. Аналитическая оценка данной модели позволяет выделить ее сильные стороны: создание единого правового поля для всех государств-членов, снижение транзакционных издержек для разработчиков за счет унификации требований, а также четкие механизмы ответственности, включая оборотные штрафы. Однако жесткая классификация и административная нагрузка на субъектов, особенно малых и средних предприятий, могут сдерживать инновации в новых сегментах, где уровень риска сложно определить на ранней стадии.

Соединенные Штаты Америки сохраняют секторальный подход, основанный на сочетании отраслевых нормативных актов (в сферах здравоохранения, финансов, гражданских прав) и добровольных фреймворков. Наиболее значимым инструментом является NIST AI Risk Management Framework (AI RMF 1.0), который предлагает рекомендации по идентификации, оценке и управлению рисками на всех этапах жизненного цикла ИИ, но не устанавливает юридически обязательных требований. Аналитическая оценка американской модели показывает, что ее преимущество – высокая гибкость, позволяющая адаптировать регулирование под отраслевые особенности и скорость технологического развития. Вместе с тем отсутствие единого законодательного акта порождает правовую неопределенность, особенно в сферах, не охваченных отраслевыми нормами, а также создает риски неравенства правоприменения между штатами.

Сравнительный анализ двух моделей позволяет сделать вывод, что выбор между унифицированным и секторальным регулированием зависит от институциональной зрелости правовой системы и приоритетов государственной политики. Для Беларуси, где специализированное законодательство об ИИ находится в стадии разработки, риск-ориентированная классификация из EU AI Act может служить основой для структурирования будущего закона, однако имплементация должна учитывать существующую фрагментарность регулирования и отсутствие специализированного надзорного органа. Одновременно рекомендательные стандарты NIST и ISO/IEC 42001 могут быть использованы для построения систем внутреннего контроля в организациях, что позволит гармонизировать практики с международными ожиданиями без немедленного введения жестких обязательных требований [8].

Однако при экстраполяции европейской и американской моделей на белорусскую правовую среду необходимо учитывать институциональные ограничения. В Республике Беларусь отсутствует специализированный орган по регулированию ИИ, а координация между Национальным центром защиты персональных данных, Оперативно-аналитическим центром и Наблюдательным советом ПБТ носит фрагментарный характер. Это делает невозможным прямое копирование жесткого механизма EU AI Act, который требует централизованного нотификации и надзора. С другой стороны, сугубо добровольный подход США, основанный на отраслевых фреймворках, в условиях отсутствия развитого регулирования в смежных сферах (например, в области алгоритмической дискриминации) может привести к правовой неопределенности и неравенству правоприменения. Таким образом, для Беларуси наиболее реалистичным представляется гибридный сценарий: закрепление на законодательном уровне риск-ориентированной классификации (по аналогии с ЕС) с одновременным наделением существующих институтов дополнительными полномочиями, а также внедрение добровольных стандартов (NIST AI RMF, ISO/IEC 42001) для внутреннего управления рисками на уровне компаний.

Проведенный анализ национального регулирования и международных подходов позволяет системно выделить правовые риски использования ИИ в цифровом бизнесе. Выявленные риски не являются абстрактными, а напрямую коррелируют с проблемами действующего законодательства (отсутствие специального закона, неопределенность в сфере интеллектуальной собственности,

фрагментарность требований к обработке данных) и одновременно учитывают те зоны ответственности, которые в международной практике уже признаны критическими (дискриминация, прозрачность, человеческий контроль).

Риск нарушения законодательства о персональных данных. Возникает из-за отсутствия в белорусском Законе «О защите персональных данных» специальных норм об автоматизированной обработке и алгоритмических решениях, что создает правовую неопределенность при использовании больших массивов данных для обучения ИИ. В ЕС данный риск системно минимизируется статьей 22 GDPR, запрещающей исключительно автоматизированные решения, а также требованиями EU AI Act о качестве обучающих данных и человеческом контроле. В США отсутствие единого федерального акта о данных порождает разнородные требования на уровне штатов, что затрудняет масштабирование ИИ-решений, но при этом гибкость позволяет адаптировать меры защиты под конкретную отрасль. Минимизация риска в белорусских условиях достигается проведением оценки воздействия на защиту данных (DPIA), применением обезличивания и обеспечением прозрачности уведомлений субъектов.

Риск кибербезопасности. Обусловлен отсутствием специализированных стандартов безопасности для ИИ в национальном законодательстве, при том что Указ № 40 относит ИИ-системы к объектам критической информационной инфраструктуры лишь при определенных условиях. В ЕС EU AI Act обязывает разработчиков систем высокого риска внедрять меры кибербезопасности на этапе проектирования (security by design). В США NIST AI RMF предлагает детальные рекомендации по управлению уязвимостями моделей, включая защиту от состязательных атак, однако эти меры не носят обязательного характера. Минимизация риска предполагает внедрение шифрования, контроля целостности моделей, регулярное тестирование на проникновение и применение принципов безопасной разработки.

Риск нарушения интеллектуальной собственности. Возникает из-за неопределенности правового статуса объектов, сгенерированных ИИ, и отсутствия в Законе об авторском праве норм о лицензировании обучающих данных. В ЕС и США данная проблема активно проявляется в судебных спорах (например, иски правообладателей к разработчикам генеративных моделей). EU AI Act требует документирования обучающих данных, что повышает прозрачность, но не решает вопрос лицензирования. В США отраслевой подход приводит к различным прецедентам в зависимости от юрисдикции, усиливая неопределенность. Минимизация риска достигается проверкой лицензионной чистоты обучающих выборок, фиксацией творческого вклада человека в итоговый результат и включением соответствующих гарантий в договоры с контрагентами.

Риск алгоритмической дискриминации. Связан с тем, что обучающие выборки могут воспроизводить социальные предубеждения, а белорусское законодательство не содержит специальных норм о недискриминации в алгоритмах. В ЕС EU AI Act прямо запрещает системы, использующие вредоносные манипуляции или социальную оценку (неприемлемый риск), и требует тестирования на предвзятость для систем высокого риска. В США NIST AI RMF выделяет управление смещениями (bias management) в качестве ключевой области, однако отсутствие единого регулирования ведет к неравномерной защите прав граждан. Минимизация риска обеспечивается тестированием моделей на предмет смещений, обеспечением человеческого контроля за критически значимыми решениями и внедрением процедур объяснимости результатов.

Риск непрозрачности и неопределенности ответственности. Вытекает из сложности интерпретации решений ИИ-моделей и отсутствия в белорусском законодательстве требований к прозрачности и распределению ответственности между разработчиком, поставщиком данных и пользователем. В ЕС EU AI Act вводит обязательство информировать пользователей о взаимодействии с ИИ (требование прозрачности) и требует документирования для систем высокого риска. В США подходы к объяснимости развиваются в рамках рекомендательных фреймворков, но юридическая ответственность за решения ИИ остается неопределенной, что подтверждается отсутствием единой судебной практики. Минимизация риска достигается ведением журналов решений, детальной регламентацией ответственности в договорах и внедрением систем управления ИИ (AI Governance), включая внутренние процедуры аудита.

Актуальность выявленных правовых рисков подтверждается практикой белорусских компаний, резидентов Парка высоких технологий. Согласно анализу рынка труда, проведенному Секретариатом Наблюдательного совета ПБТ в 2025 году, внедрение ИИ привело к структурным изменениям спроса на специалистов: растёт потребность в экспертах, способных контролировать качество и безопасность ИИ-систем, интерпретировать их результаты и управлять рисками. Сохраняются также проблемы с качеством ИИ-генерируемого кода, сложностью отладки и наличием уязвимостей, что требует дополнительного человеческого контроля. В сфере финансовых технологий, где белорусские компании (в том числе резиденты ПБТ) разрабатывают скоринговые модели на основе ИИ, вопросы объяснимости алгоритмов и защиты прав потребителей приобретают критическое значение, особенно при ориентации на экспорт в юрисдикции с развитым регулированием (ЕС, США). Таким образом, недостаточная нормативная определённость в национальном законодательстве создаёт для белорусского ИИ-бизнеса как правовые, так и репутационные риски, влияющие на конкурентоспособность.

Формирование эффективного регулирования требует не только устранения пробелов, но и создания институциональных механизмов.

В настоящее время контроль в смежных сферах распределен между Национальным центром защиты персональных данных, Оперативно-аналитическим центром и Наблюдательным советом ПВТ; специализированный орган по регулированию ИИ отсутствует. С учетом Государственной программы «Цифровая Беларусь» на 2026-2030 годы и планов разработки закона «О технологиях искусственного интеллекта» прогнозируется переход к риск-ориентированному регулированию по аналогии с EU AI Act. Эффектами такого перехода станут снижение правовой неопределенности для бизнеса, создание легальных оснований для коммерциализации ИИ-продуктов и повышение защиты прав граждан через требования прозрачности и человеческого контроля. Дополнительным механизмом выступает использование международных стандартов ISO/IEC 42001 и NIST AI RMF для построения систем внутреннего управления рисками, что позволяет гармонизировать практики с глобальными требованиями и снизить издержки при выходе на внешние рынки. Комплексное применение обязательных и добровольных инструментов обеспечивает баланс между инновационным развитием и правовой определенностью [9].

Заключение. Искусственный интеллект в цифровом бизнесе выступает инструментом развития электронной экономики, эффективность которого напрямую зависит от качества правовой среды. Для Республики Беларусь приоритетом является переход от фрагментарного регулирования, основанного на разрозненных отраслевых актах, к системному подходу, включающему риск-ориентированную классификацию ИИ-систем, создание специализированного надзорного механизма и имплементацию международных стандартов управления рисками. Предложенный анализ правовых рисков, подкрепленный опытом ЕС и США, позволяет сформулировать основу для нормотворческой деятельности и формирования внутренних политик управления ИИ в организациях. Реализация этих мер будет способствовать снижению правовых издержек бизнеса, повышению инвестиционной привлекательности ИТ-сектора и укреплению цифрового суверенитета страны.

Список использованных источников:

1. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [Электронный ресурс]. – Режим доступа: <https://etalonline.by/document/?regnum=h12100099>. – Дата доступа: 17.03.2026..
2. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (ред. 2024) [Электронный ресурс]. – Режим доступа: https://www.brsu.by/sites/default/files/ovr/docs/zakon_respubliki_bielarus_ob_informatsii_informatizatsii_i_izaschite.pdf. – Дата доступа: 17.03.2026.
3. Декрет Президента Республики Беларусь № 8 от 21 декабря 2017 г. «О развитии цифровой экономики» [Электронный ресурс]. – Режим доступа: <https://economy.gov.by/uploads/files/sanacija-i-bankrotstvo/Dekret-Prezidenta-Respubliki-Bielarus-ot-21-12-2017-N-8-O-r.pdf>. – Дата доступа: 17.03.2026..
4. Указ Президента Республики Беларусь № 40 от 14 февраля 2023 г. «О кибербезопасности» [Электронный ресурс]. – Режим доступа: <https://etalonline.by/document/?regnum=P32300040>. – Дата доступа: 17.03.2026.
5. Закон Республики Беларусь от 17 мая 2011 г. № 262-З «Об авторском праве и смежных правах» [Электронный ресурс]. – Режим доступа: <https://etalonline.by/document/?regnum=h11100262>. – Дата доступа: 17.03.2026..
6. Постановление Совмина РБ № 793 от 30 декабря 2025 г. «О государственной программе „Цифровая Беларусь“ на 2026–2030 годы» [Электронный ресурс]. – Режим доступа: https://government.by/sites/default/files/resolution/2026-01/793%2825990934_793_30_12_2025%29.pdf. – Дата доступа: 17.03.2026..
7. Князькова, В.С. Состояние и тенденции мирового развития информационно-коммуникационных технологий / В.С. Князькова // Бизнес. Образование. Экономика : Междунар. науч.-практ. конф., Минск, 7–8 апр. 2022 г. : сб. ст. – Минск : Институт бизнеса БГУ, 2022. – С. 153-156.
8. Князькова, В.С. Оценка эффективности повышения цифровой грамотности персонала в условиях цифровой трансформации / В.С. Князькова // Цифровая трансформация. – 2023. – Т. 29, № 1. – С. 23-31.
9. Бебяцкая, Т.Н. Электронная экономика: теория, методология, системный анализ / Т.Н. Бебяцкая. – Минск : Право и экономика, 2017. – 284 с.

УДК [004.8+334.722-028.27]:351.824.1(476)

LEGAL RISKS AND MECHANISMS FOR REGULATING THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN DIGITAL BUSINESS

Stetsko A.A., Spiridonova K.D.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Harnastai L.Ch. – Senior Lecturer, Department of Management

Annotation. This article examines the legal aspects of implementing artificial intelligence in digital business models. It demonstrates that effective AI regulation requires not only adapting national legislation but also taking into account international approaches. Key areas of legal development are identified through an analysis of the experience of the European Union and the United States. The main risks of using AI in business are systematized and mechanisms for mitigating them are proposed. Projections of changes in the regulatory environment of the Republic of Belarus are formulated, taking into account the existing institutional structure.

Keywords. Artificial intelligence, digital platforms, legal regulation, risk-based approach, Republic of Belarus, international experience.