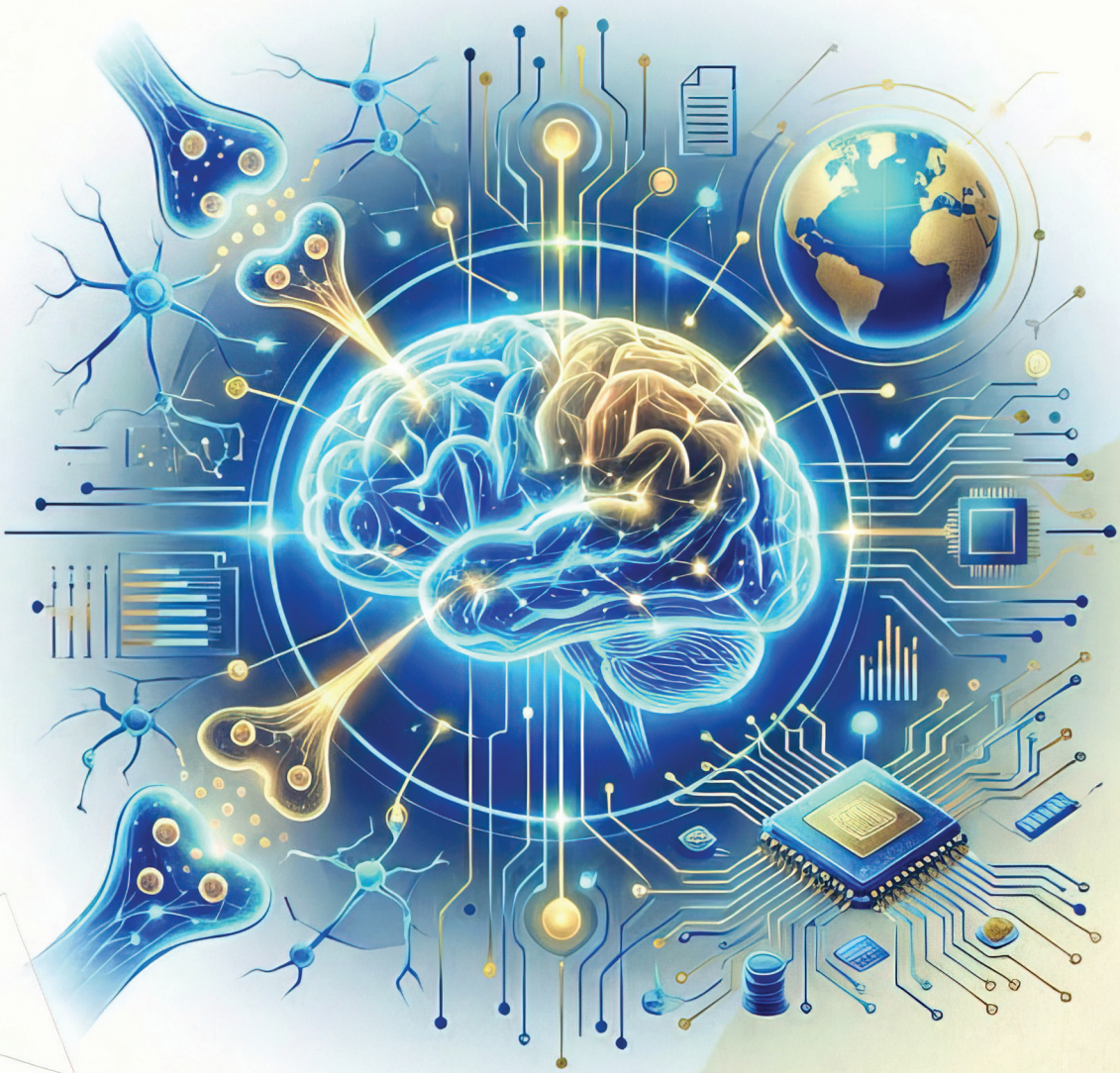
# ИНТЕЛЛЕКТУАЛЬНЫЙ СУВЕРЕНИТЕТ

НАУЧНЫЙ ЖУРНАЛ



ТОМ 1, НОМЕР 1, 2026

***Нормативный источник:***

***Указ Президента Российской Федерации: «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» от 7 мая 2024 г. N 309***

*«...В целях обеспечения устойчивого экономического и социального развития Российской Федерации, укрепления государственного, культурно-ценностного и экономического суверенитета...»*

## Область научного исследования в журнале «Интеллектуальный суверенитет»:

**Аспекты исследования:**

**Суверенитет (реальный)** — способности страны на деле, а не только на бумаге, обеспечивать свою экономическую, технологическую и военную автономность.

*Методология **суверенитета (реального)** — это алгоритм перевода декларативной независимости («флаг и гимн») в фактическую субъектность.*

**Интеллектуальный суверенитет** — это фундамент «суверенитета (реального)». В мире, где идеи (людей, человеческий капитал) и технологии (интеллектуальные системы) ценятся выше ресурсов, это способность государства самостоятельно мыслить, создавать смыслы и управлять знаниями, не попадая в когнитивную зависимость от внешних центров.

*Методология **интеллектуального суверенитета** — это алгоритм перехода от копирования чужих идей к генерации собственных смыслов и технологий.*

**1. Образовательный и научный суверенитет**

Это способность страны готовить кадры и проводить фундаментальные исследования по собственной повестке.

- **Свои стандарты:** независимость образовательных программ от навязанных извне идеологических или узкоспециализированных лекал.
- **Научная автономия:** наличие собственных научных школ и системы оценки достижений, которые позволяют развивать критически важные для страны направления.

*Методология **образовательного и научного суверенитета** — это технология превращения знаний из «импортного товара» в стратегический ресурс развития.*

**2. Технологический и цифровой суверенитет**

Интеллектуальный суверенитет — это «чертеж», без которого невозможен технологический.

**2.1. Свои патенты:** владение интеллектуальной собственностью на ключевые разработки (микроэлектроника, ИИ, медицина и т.д.).

**2.2. Контроль данных:** способность защищать информацию своих граждан и управлять цифровой средой (**суверенитет данных**).

**2.2.1. Юрисдикция (Право на закон):** Данные подчиняются законам той страны, где они были собраны или созданы, независимо от того, где находится штаб-квартира компании-владельца.

**2.2.2. Локализация (Право на территорию):** Требование физически хранить критически важные данные (персональные данные граждан, финансовые отчеты, гостайну) на серверах внутри страны.

**2.2.3. Технологическая автономия:** Использование собственного софта и облачных решений (**Суверенное облако**), чтобы исключить доступ иностранных спецслужб или внезапное отключение сервисов.

**2.2.3.1.** Использование собственного софта — это **«процессор»** в системе реального суверенитета. Без своего ПО контроль над «железом» или облаком теряет смысл, так как управление процессами остается в руках иностранного разработчика **(зависимость от поставщика, кибербезопасность, проблема «закладок»)**.

**2.2.3.2. Суверенное облако** — это высшая форма реализации суверенитета данных «в железе» и коде. Это облачная инфраструктура, которая гарантирует, что данные и метаданные не только физически находятся в стране, но и полностью защищены от иностранного законодательного и технического влияния.

*Методология **технологического и цифрового суверенитета** — это алгоритм перехода от статуса «технологической колонии» (которая только потребляет и ремонтирует чужое) к статусу «технологического лидера», который владеет ключами от своих систем.*

**3. Когнитивный (смысловой) суверенитет**

Это «операционная система» национального самосознания. Если технологический суверенитет защищает **каналы** связи, то когнитивный защищает то, что происходит в **головах** людей. Самый тонкий, но важный уровень — защита национального сознания от внешних манипуляций.

- **Аналитическая фильтрация:** умение общества отличать собственные интересы от навязанных извне через медиа и «мягкую силу».
- **Культурный код:** сохранение своей истории, ценностей и языка как основы для принятия самостоятельных решений.

*Методология **когнитивного (смыслового) суверенитета** —направлена на защиту **ментального пространства** нации и обеспечение способности общества самостоятельно интерпретировать реальность, не поддаваясь внешнему когнитивному управлению.*

## Уважаемые коллеги, дорогие друзья!

Когда мы говорим о суверенитете в XXI веке, мы неизбежно выходим за рамки традиционных политических и экономических категорий. Сегодня подлинная независимость государства определяется его способностью быть субъектом собственного интеллектуального развития: генерировать знания, воспроизводить культуру мышления и владеть технологиями, которые эту культуру обслуживают и транслируют. Именно этой глубинной философской задаче — осмыслению и утверждению интеллектуального суверенитета как фундамента национальной идентичности и безопасности — посвящен наш новый научный журнал.

Символично, что старт журналу дан 13 февраля 2026 года в Краснодаре, в рамках Всероссийского научно-практического круглого стола. Это событие объединило ведущие научные и образовательные институты, а также нашло поддержку в федеральном проекте «Выбирай своё» ВПП «Единая Россия». Такое широкое партнерство подтверждает: миссия журнала — не просто публикация научных статей, но консолидация усилий ученых, практиков, политиков для формирования концептуальных основ национального интеллектуального суверенитета.

Название издания отражает его суть. Мы не случайно выбрали два стержневых направления:

Первое — **формирование человеческого капитала**. Без сохранения культурного ядра нации, без системы образования, работающей на опережение, без решения проблемы «утечки мозгов» любые технологические прорывы окажутся временными. Мы видим свою задачу в том, чтобы стать площадкой для обсуждения ценностных ориентиров и гражданской идентичности в цифровую эпоху.

Второе — **развитие интеллектуальных систем**. Искусственный интеллект, большие данные, когнитивные технологии — это поле, где сегодня решается вопрос о будущем миропорядке. Наш журнал будет уделять приоритетное внимание исследованиям, направленным на создание полного цикла разработки в России, обеспечению технологической независимости, а также этическим и правовым аспектам внедрения ИИ. Мы убеждены: бесперспективно растить таланты, не давая им возможности реализовать себя в современной технологической среде.

Приглашаю вас к содержательному диалогу на страницах журнала!

**Сметана Владимир Васильевич,**

**кандидат философских наук, руководитель журнала «Интеллектуальный суверенитет» и секции «Интеллектуальный суверенитет» Научного совета при Президиуме РАН по методологии искусственного интеллекта и когнитивных исследований (НСМИИ РАН), директор АНО НИИ «ЦИФРОВОЙ ИНТЕЛЛЕКТ».**

*В современном мире знания и технологии стали ключевым ресурсом развития и безопасности. Умение не только генерировать прорывные идеи, но и сохранять контроль над своими интеллектуальными ресурсами, кадрами и данными — основа для суверенного будущего России.*

**Координатор федерального проекта «Выбирай своё»**
**ВПП «Единая Россия»**
**Сергей Иванович Морозов**

# Уважаемые коллеги!

Журнал «Интеллектуальный суверенитет» представляет собой научное периодическое издание, целью которого является создание платформы для формирования стратегии интеллектуального суверенитета и технологического лидерства России. Путём освещения результатов фундаментальных и прикладных исследований, научных дискуссий и прогнозов, нам представляется возможным достижение поставленной цели.

Мы постарались сделать обширной тематику журнала, чтобы открыть возможности публикации материалов в различных сферах анализа современного состояния и перспектив развития исследований интеллектуальных систем и технологий искусственного интеллекта. Наши авторы проводят исследования по развитию нормативно-правового регулирования и этики применения искусственного интеллекта; цифровой трансформации государственного и корпоративного управления; цифрового развития экономики; использования технологий искусственного интеллекта в сфере образования и во многих других.

Редакционная коллегия открыта к обсуждению любых конструктивных предложений по совершенствованию журнала и повышению его научного уровня.

Ждём новых результатов ваших исследований.

С наилучшими пожеланиями,

*Главный редактор журнала*
*«Интеллектуальный суверенитет»*
*С.А. Федоренко*

---


ИЗДАТЕЛЬ:
АНО НИИ «Цифровой Интеллект»

АДРЕС ИЗДАТЕЛЬСТВА:
г. Армавир

ISSN 3033-8239 26001
ISBN 9773033823007

# РЕДКОЛЛЕГИЯ

# РЕДКОЛЛЕГИЯ

# Содержание

DOI: 10./-2026-2

# Правовое регулирование защиты персональных данных в условиях цифровизации: проблемы и перспективы

# LEGAL REGULATION OF PERSONAL DATA PROTECTION IN THE CONTEXT OF DIGITALIZATION: PROBLEMS AND PROSPECTS

**Бельгисова Кристина Викторовна,**
канд. эконом. наук, доцент кафедры гражданского и трудового права КубИСЭП (филиал) ОУП ВО «АТиСО», г. Краснодар
belgisova_k@mail.ru

**Belgisova Kristina Viktorovna,**
Cand. of Economics, of Sciences, Associate Professor of the Department civil and labor law KubISEP (branch) OUP VO «ATiSO», Krasnodar
belgisova_k@mail.ru

***Аннотация.*** *В статье рассматриваются актуальные вопросы правового регулирования защиты персональных данных в условиях цифровизации общественных отношений. Проанализированы последние изменения российского законодательства о персональных данных, включая ужесточение административной ответственности операторов, введение новых требований к уведомлению уполномоченных органов, а также расширение возможностей обработки обезличенных данных без согласия субъектов персональных данных.*
*Особое внимание уделено правовым рискам, возникающим в связи с развитием технологий искусственного интеллекта, автоматизированного принятия решений и обработки больших данных. Выявлены ключевые вызовы современного правового регулирования, обусловленные технологическим опережением законодательства, массовыми утечками персональных данных, трансграничной передачей информации и неопределённостью критериев вины операторов. Обоснована необходимость комплексного подхода к минимизации правовых рисков, включающего совершенствование законодательства, развитие правоприменительной практики и повышение правовой грамотности участников цифровых отношений.*

***Annotation.*** *The article discusses current issues of legal regulation of personal data protection in the context of digitalization of public relations. It analyzes the latest changes in Russian legislation on personal data, including the tightening of administrative liability for operators, the introduction of new requirements for notifying authorized bodies, and the expansion of opportunities for processing anonymized data without the consent of personal data subjects. Special attention is paid to the legal risks arising from the development of artificial intelligence technologies, automated decision-making, and big data processing. The key challenges of modern legal regulation are identified, which are caused by the technological advancements ahead of legislation, mass personal data leaks, cross-border information transfer, and the uncertainty of operators' liability criteria. The need for a comprehensive approach to minimizing legal risks is substantiated, which includes improving legislation, developing law enforcement practices, and enhancing the legal literacy of participants in digital relations.*

***Ключевые слова:*** *персональные данные; цифровизация; защита информации; правовые риски; обезличенные данные; административная ответственность; оператор персональных данных; искусственный интеллект.*

***Keywords:*** *personal data; digitalization; information protection; legal risks; anonymized data; administrative liability; personal data operator; artificial intelligence.*

**Цифровизация всех сфер общественной жизни привела к существенному увеличению объемов, собираемых и обрабатываемых персональных данных, а также к усложнению способов их использования. В условиях активного внедрения цифровых платформ, технологий искусственного интеллекта и анализа больших данных особую значимость приобретает проблема правового обеспечения защиты персональных данных. Нарушения в данной сфере способны повлечь не только имущественный и моральный вред гражданам, но и подорвать доверие к государственным и коммерческим цифровым сервисам.**

Базовым нормативным правовым актом, регулирующим отношения, связанные с обработкой персональных данных, в настоящее время является Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[1]. Важно отметить, что сегодня в сфере регулирования отношений, связанных с обработкой персональных данных, произошли самые существенные изменения. Эти изменения, вступили в силу поэтапно и в целом ужесточили требования, ответственность и контроль в сфере обработки персональных данных.

Рассмотрим наиболее значимые изменения:

1) Федеральный закон от 30 ноября 2024 г. № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[2]. Указанным зако-

[1] О персональных данных. Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.

[2] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях. Федеральный закон от 30 ноября 2024 г. № 420-ФЗ // Собрание законодательства Российской Федерации, 2 декабря 2024 г. № 49 (часть IV) ст. 7411.

ном были значительно увеличены размеры административных штрафов, предусмотренных статьей 13.11 КоАП РФ, для физических, должностных и юридических лиц. Кроме того, указанная статья была дополнена частями 10—18, устанавливающими ответственность за неисполнение или несвоевременное исполнение обязанности оператора по уведомлению уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку персональных данных.

2) Федеральный закон от 28 февраля 2025 г. № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации» внес изменения в Федеральный закон от 27 июля 2006 г. № 152-ФЗ и иные нормативные правовые акты, определив особенности обработки персональных данных сотрудников органов федеральной службы безопасности, внешней разведки, государственной охраны, внутренних дел, а также лиц, подлежащих государственной защите[3]. Закон закрепил право соответствующих органов направлять обязательные для исполнения предписания владельцам информационных систем и баз данных о предоставлении доступа к ним в целях обработки персональных данных указанных категорий лиц.

3) Существенное значение для практики обработки персональных данных имеет Федеральный закон от 24 июня 2025 г. № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации», которым установлено требование об отдельном оформлении согласия на обработку персональных данных, не допускающем его включение в иные документы[4].

4) Федеральный закон от 8 августа 2024 г. № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» закрепил возможность обработки надлежащим образом обезличенных персональных данных без получения согласия субъекта с 1 сентября 2025 г.[5]. Указанный закон дополнил Федеральный закон от 27 июля 2006 г. № 152-ФЗ новой статьей 13.1, регламентирующей обращение с обезличенными персональными данными и вводящей понятие «состав обезличенных данных». Законодатель также предусмотрел механизм обязательного предоставления обезличенных данных в государственную информационную систему по требованию Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, при одновременном запрете использования биометрических персональных данных в таких целях.

Несмотря на активное развитие нормативного регулирования, в сфере защиты персональных данных сохраняется ряд системных правовых вызовов.

1. Одним из них является технологическое опережение правового регулирования. Законодательство о персональных данных, в частности Федеральный закон № 152-ФЗ, разрабатывалось и принималось в условиях иного уровня цифровизации и сегодня не всегда учитывает современные способы обработки данных, такие как: машинное обучение и анализ больших данных (Big Data); автоматизированное принятие решений; использование нейросетей и рекомендательных алгоритмов; обработка поведенческих и производных данных.

В результате возникают правовые неопределённости в части:

— отнесения новых типов информации к персональным данным;

— допустимости вторичной обработки данных;

— оценки законности алгоритмической обработки без прямого участия человека.

Это создаёт риски как для операторов персональных данных, так и для субъектов, чьи права могут быть нарушены в отсутствие чётких правовых гарантий.

2. Серьёзной проблемой остаётся расширение понятия персональных данных и сложность их идентификации. Использование косвенных цифровых идентификаторов позволяет осуществлять повторную идентификацию личности даже на основе обезличенных сведений, что затрудняет разграничение персональных и неперсональных данных.

С правовой точки зрения существует проблема: определения момента, когда обезличенные данные перестают быть таковыми; разграничения персональных данных и технической информации; оценки риска повторной идентификации субъекта.

Отсутствие единых критериев порождает неоднородную правоприменительную практику и повышает риск привлечения операторов к ответственности.

3. Массовые утечки персональных данных и коллективный вред. Одной из наиболее острых проблем является массовый характер утечек персональных данных, при котором ущерб причиняется неопределённому кругу лиц. Правовые сложности в данной сфере связаны с тем, что:

— трудно установить конкретный объём вреда каждому субъекту;

— отсутствуют эффективные механизмы коллективной защиты прав;

— судебная практика по компенсации морального вреда остаётся противоречивой.

---

[3] О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации. Федеральный закон от 28 февраля 2025 г. № 23-ФЗ // Собрание законодательства Российской Федерации, 3 марта 2025 г. № 9 ст. 852.

[4] О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации. Федеральный закон от 24 июня 2025 г. № 156-ФЗ // Собрание законодательства Российской Федерации, 30 июня 2025 г. № 26 (часть I) ст. 3486.

[5] О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». Федеральный закон от 8 августа 2024 г. № 233-ФЗ // Собрание законодательства Российской Федерации, 12 августа 2024 г. № 33 (часть I) ст. 4929.

Кроме того, существующая система ответственности часто не соразмерна реальным последствиям утечек, что снижает превентивную функцию права.

4. Трансграничная передача и локализация персональных данных

В условиях глобализации цифровых сервисов особое значение приобретает проблема трансграничной передачи персональных данных. Введение требований о локализации данных граждан РФ усилило правовую защиту, однако породило новые вызовы:

— необходимость технической перестройки IT-инфраструктуры;

— правовые коллизии с международными обязательствами;

— сложности для образовательных, научных и коммерческих платформ, использующих зарубежные сервисы.

Операторы вынуждены балансировать между требованиями национального законодательства и логикой глобальной цифровой экономики.

5. Рост ответственности операторов и неопределённость критериев вины. Ужесточение административной ответственности за нарушения в сфере персональных данных сопровождается нечеткостью критериев оценки добросовестности оператора. В частности, остаётся дискуссионным вопрос:

— какие меры безопасности считаются достаточными;

— где проходит граница между технической ошибкой и правонарушением;

— как учитывать влияние человеческого фактора.

Это повышает регуляторные риски и создаёт правовую неопределённость для организаций, даже при наличии формально выстроенной системы защиты данных.

6. Автоматизированные решения и дискриминационные риски. Использование алгоритмов и искусственного интеллекта при обработке персональных данных формирует новый пласт правовых вызовов, связанных с: непрозрачностью алгоритмов; невозможностью объяснить логику принятия решений; риском дискриминации отдельных групп лиц.

Действующее российское законодательство пока не содержит комплексного регулирования автоматизированных решений, что ограничивает возможности защиты прав субъектов персональных данных.

7. Недостаточная правовая грамотность участников цифровых отношений. Отдельным системным вызовом остается низкий уровень правовой и цифровой грамотности как субъектов персональных данных, так и отдельных операторов. Это приводит к:

— игнорированию требований законодательства;

— формальному подходу к защите данных;

— слабому использованию правовых механизмов защиты.

Таким образом, защита персональных данных в условиях цифровизации представляет собой комплексную и многоуровневую задачу современного правового регулирования. Российское законодательство последовательно развивается в направлении усиления защиты прав субъектов персональных данных и повышения ответственности операторов, однако эффективность этих мер во многом зависит от качества правоприменительной практики, уровня информационной безопасности и правовой культуры участников цифровых отношений. Минимизация правовых рисков в данной сфере возможна лишь при интеграции правовых, технических и организационных механизмов защиты персональных данных.

**Библиографический список**

1. О персональных данных. Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.

2. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях. Федеральный закон от 30 ноября 2024 г. № 420-ФЗ // Собрание законодательства Российской Федерации, 2 декабря 2024 г. № 49 (часть IV) ст. 7411.

3. О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации. Федеральный закон от 28 февраля 2025 г. № 23-ФЗ // Собрание законодательства Российской Федерации, 3 марта 2025 г. № 9 ст. 852.

4. О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации. Федеральный закон от 24 июня 2025 г. № 156-ФЗ // Собрание законодательства Российской Федерации, 30 июня 2025 г. № 26 (часть I) ст. 3486.

5. О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». Федеральный закон от 8 августа 2024 г. № 233-ФЗ // Собрание законодательства Российской Федерации, 12 августа 2024 г. № 33 (часть I) ст. 4929.

DOI: 10./-2026-1-1-1

# Роль национального проекта «Экономика данных и цифровая трансформация государства» в формировании интеллектуального суверенитета России

# THE ROLE OF THE NATIONAL PROJECT «DATA ECONOMY AND DIGITAL TRANSFORMATION OF THE STATE» IN THE FORMATION OF RUSSIA'S INTELLECTUAL SOVEREIGNTY

**Дудник Анна Игоревна,**
канд. экон. наук, старший преподаватель кафедры государственного и муниципального управления РГГУ г. Москва
annetdd@gmail.com

**Dudnik Anna Igorevna,**
Cand. of Econ. Sciences, Senior Lecturer Department of Public and Municipal Administration, RGGU, Moscow
annetdd@gmail.com

***Аннотация.*** *Статья посвящена анализу роли национального проекта «Экономика данных и цифровая трансформация государства» в формировании интеллектуального суверенитета России. На основе институционального анализа раскрыта архитектура проекта и выявлены механизмы технологической, инфраструктурной и алгоритмической независимости. Показано, что проект формирует системные условия снижения критической внешней зависимости в цифровой сфере. Предложена авторская модель институционального обеспечения интеллектуального суверенитета государства.*

***Annotation.*** *The article examines the role of the national project "Data Economy and Digital Transformation of the State" in shaping the intellectual sovereignty of Russia. Based on an institutional analysis, the architecture of the project is explored and the mechanisms of technological, infrastructural, and algorithmic independence are identified. It is demonstrated that the project creates systemic conditions for reducing critical external dependence in the digital sphere. An original model of institutional support for intellectual sovereignty is proposed.*

***Ключевые слова:*** *интеллектуальный суверенитет, трансформация, национальный проект, независимость, технологии.*

***Keywords:*** *intellectual sovereignty, transformation, national project, independence, technologies.*

**Цифровая трансформация в XXI веке перестала быть исключительно инструментом модернизации государственного управления и экономики, превратившись в фактор стратегической устойчивости и международной конкурентоспособности государств. В условиях глобальной технологической конкуренции, ускоренного развития искусственного интеллекта, больших данных и платформенных экосистем цифровая инфраструктура становится не только экономическим ресурсом, но и элементом национальной безопасности.**

Современная геоэкономическая ситуация, характеризующаяся фрагментацией глобальных технологических цепочек, усилением санкционного давления и ограничением доступа к критическим цифровым технологиям, актуализирует проблему обеспечения технологической независимости. В этой связи формируется новая категория стратегического анализа — интеллектуальный суверенитет, которую можно обозначить как институционально обеспеченная способность государства самостоятельно создавать, защищать, воспроизводить и применять интеллектуальные, цифровые и алгоритмические ресурсы, включая результаты интеллектуальной деятельности, инфраструктуру данных и технологические платформы, в целях реализации стратегических приоритетов развития без критической внешней зависимости. Интеллектуальный суверенитет выступает драйвером обеспечения конкурентоспособности и устойчивости экономического роста государства в условиях современных геополитических и макроэкономических вызовов.[1]

Особое значение в данном контексте приобретает национальный проект «Экономика данных и цифровая трансформация государства», ориентированный на формирование единой цифровой среды управления, развитие инфраструктуры данных, внедрение отечественных цифровых решений и институционализацию платформенного подхода в государственном секторе. Проект фактически выходит за рамки классической цифровизации, трансформируясь в механизм структурного обеспечения интеллектуальной автономии государства.

Цель исследования заключается в выявлении институциональной роли национального проекта «Экономика данных и цифровая трансформация государства» в формировании интеллектуального суверенитета Российской Федерации.

[1] Близнец И.А. Методология интеллектуального суверенитета - новое в теории интеллектуальной собственности// Вестник ФИПС. 2022. Т. 1, № 2 (2). С. 58-59.

Объектом исследования выступает система стратегического управления цифровым развитием Российской Федерации в условиях технологической трансформации мировой экономики.

Предметом исследования являются институциональные механизмы и инструменты национального проекта «Экономика данных и цифровая трансформация государства», обеспечивающие формирование интеллектуального суверенитета России.

Таким образом, исследование роли национального проекта в формировании интеллектуального суверенитета представляет собой актуальную научную задачу, находящуюся на пересечении проблем стратегического планирования, институциональной экономики и цифровой трансформации государственного управления.

## Категория «интеллектуальный суверенитет» в системе стратегического управления РФ

Концепция «интеллектуального суверенитета» акцентирует внимание на способности государства обеспечивать автономность цифровой инфраструктуры, защищать критическую информационную инфраструктуру, регулировать трансграничные потоки данных и развивать национальные технологические компетенции[2]. В научной литературе категория «интеллектуальный суверенитет» трактуется неоднозначно. Ряд исследователей, в частности О.П. Неретин, рассматривает её как элемент более широкой концепции цифрового или технологического суверенитета, акцентируя внимание на способности государства контролировать ключевые технологические ресурсы и инфраструктуру[3].

Карнаушенко Л.В. рассматривает данное понятие как базирующийся на институте интеллектуальной собственности инструментарий поддержки и развития процессов создания, защиты и коммерциализации интеллектуальных продуктов с целью реализации потребностей государства в получении результатов по критически важным отраслям экономики[4].

Представленный подход обладает методологической значимостью, поскольку подчёркивает роль правового режима интеллектуальной собственности как механизма защиты национальных интересов. Однако ограничение интеллектуального суверенитета исключительно рамками института интеллектуальной собственности представляется недостаточным по следующим основаниям.

Между тем, исследуемая категория формируется на пересечении трёх исследовательских направлений: теории государственного суверенитета; концепции технологической независимости и институциональной экономики знаний. По сути, интеллектуальный суверенитет представляет собой комплексную стратегическую категорию, отражающую способность государства обеспечивать автономное развитие и использование интеллектуальных ресурсов. Его структура носит многокомпонентный характер, а реализация осуществляется через инструменты научно-технологической, цифровой и институциональной политики. В российской стратегической повестке данные подходы институционально закреплены в ряде нормативных актов:

- в Стратегии национальной безопасности Российской Федерации, где технологическая независимость и развитие отечественных цифровых технологий рассматриваются как элементы обеспечения национальной безопасности;
- в Стратегии научно-технологического развития РоссийскоФедерации, определяющей приоритеты развития критических технологий;
- в государственных программах цифровой трансформации и национальных проектах, ориентированных на развитие искусственного интеллекта, инфраструктуры данных и отечественного программного обеспечения.

Так, в соответствии с положениями Стратегии национальной безопасности Российской Федерации, обеспечение технологической независимости и развитие отечественных цифровых технологий рассматриваются как необходимое условие национальной безопасности и устойчивого социально-экономического развития. В документе прямо указывается на необходимость снижения зависимости от иностранных технологических решений и укрепления собственного научно- технологического потенциала[5].

Стратегия научно-технологического развития Российской Федерации фиксирует приоритет развития критических и сквозных технологий, формирование условий для воспроизводства научных компетенций и поддержку разработок, обеспечивающих долгосрочную конкурентоспособность страны. В рамках данной стратегии технологическая самостоятельность трактуется как системная характеристика национальной инновационной системы.

Кроме того, национальные цели развития, закреплённые в Указе Президента Российской Федерации от 7 мая 2024 г. № 309, ориентируют государственную политику на достижение технологического лидерства и повышение эффективности государственного управления, что институционально связывает цифровую трансформацию с задачами стратегической устойчивости.

Таким образом, нормативная база стратегического планирования формирует институциональный каркас, в рамках которого интеллектуальный суверенитет выступает не декларативной категорией, а логическим результатом реализации закреплённых государственных приоритетов.

## Национальный проект «Экономика данных и цифровая трансформация государства»

Институциональная конструкция реализации нацпроекта воспроизводит типовую для проектного управления мо-

---

[2] Бойко П.Е., Сокол А.В. Наука философии и проблема интеллектуального суверенитета современной России // Научная мысль Кавказа. 2025. № 3 (123). С. 26-32.

[3] Неретин О. П. Интеллектуальный суверенитет экономики России. Москва: Федеральный институт промышленной собственности (ФИПС), 2022. 166 с

[4] Карнаушенко Л. В. Интеллектуальный суверенитет государства и проблема его обеспечения в обществе начала XXI века // Общество и право. 2015. № 4 (54). С. 12-18.

[5] Кочетков А.П., Маслов К.В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12: Политические науки. 2022. № 2. С. 31-45.

дель, обеспечивая вертикальную соподчинённость целей и измеримость результатов на уровне субъектов РФ. Эмпирически это фиксируется в паспортах региональных проектов, которые утверждаются в контуре проектного управления и содержат стандартный набор управленческих атрибутов (сроки, цели, кураторов, показатели).

Целеполагание отдельных направлений на региональном уровне конкретизирует ключевые компоненты нацпроекта: цифровое государственное управление, цифровые платформы в отраслях социальной сферы, отечественные решения для снижения зависимости от иностранных решений. Тем самым институциональная архитектура нацпроекта может быть описана как совокупность взаимосвязанных федеральных и региональных проектов, которые одновременно: модернизируют публичное управление, формируют платформенный контур социальной сферы, обеспечивают импортонезависимость цифрового технологического стека[6].

Внутри нацпроекта выделяются механизмы, которые можно аналитически сгруппировать по трём контурам независимости.

1) Технологическая независимость достигается через формирование собственного программно-аппаратного обеспечения, снижение зависимости от зарубежных цифровых решений и институциональное закрепление приоритета отечественных разработок.[7] Однако это не гарантирует устойчивости системы без условий его полноценного использования. Политика независимости через проектирование спроса государства и ключевых отраслей на отечественные решения закреплена как целевая установка проекта «Отечественные решения» - переход на отечественные разработки/оборудование и снижение зависимости от иностранных решений. На уровне региональной реализации это выражается через показатели, ориентированные на рост доли использования отечественного ПО в деятельности органов власти.

2) Инфраструктурная независимость предполагает наличие цифровых платформ, государственных информационных систем, сервисной архитектуры предоставления услуг и интегрированных баз данных. Именно инфраструктура создаёт среду, в которой технологические решения функционируют как единый контур. Без развитой цифровой инфраструктуры даже отечественные решения остаются фрагментарными и не обеспечивают системной автономии. Инфраструктурный контур встраивается в цифровизацию предоставления услуг и платформенную интеграцию данных. В «Цифровом государственном управлении» цель включает развитие инфраструктуры предоставления услуги сервисов в цифровом виде и использование типовых решений на базе единой цифровой платформы. С институциональной точки зрения это означает закрепление инфраструктуры как условия предоставления госуслуг и управленческих решений, а не как факультативного ИТ-обеспечения.

3) Алгоритмическая независимость означает переход к принятию управленческих решений на основе данных, внедрение типовых цифровых моделей процессов и использование аналитических инструментов. Этот уровень обеспечивает не просто техническую, а управленческую самостоятельность. В цели регионального проекта «Цифровое государственное управление» прямо зафиксирована реализация типовых решений для принятия решений на основе данных. Параллельно платформенные направления социальной сферы формирует институциональную среду, где алгоритмы «упакованы» в универсальные цифровые платформы для электронного взаимодействия и снижения административных барьеров.

Анализ институциональной конструкции национального проекта показывает, что обеспечение независимости в цифровой сфере не сводится к реализации одной изолированной меры. Речь идёт о комплексной взаимосвязанной системе механизмов, формирующих устойчивую модель автономного цифрового развития государства.

На базе проведённого анализа предлагается модель институционального обеспечения интеллектуального суверенитета, согласно которой формирование автономии осуществляется через интеграцию трёх взаимосвязанных контуров (рисунок 1).


Рисунок 1. Модель институционального обеспечения интеллектуального суверенитета.
*Источник: выполнено автором.*

Модель отражает иерархическую взаимосвязь между стратегическим целеполаганием, проектной архитектурой и тремя контурами институционального обеспечения независимости, взаимодействие которых формирует устойчивую способность государства к автономному цифровому развитию. Взаимодействие указанных контуров формирует целостную систему воспроизводства интеллектуальных и

[6] Авдийский В.И., Иванов А.В., Царегородцев А.В. Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы // Вестник евразийской науки. 2024. Т. 16. № S3. С. 21.

[7] Демидов А.В. Национальный проект «Экономика данных и цифровая трансформация государства» как инструмент укрепления цифрового суверенитета России // Наукосфера. 2024. № 4-2. С. 357-360.

цифровых ресурсов, что позволяет рассматривать национальный проект как структурный элемент стратегической архитектуры интеллектуального суверенитета Российской Федерации.

## Заключение

Проведённое исследование позволило обосновать, что в условиях глобальной технологической трансформации интеллектуальный суверенитет выступает системной характеристикой стратегического управления, отражающей способность государства к автономному воспроизводству и использованию интеллектуальных, цифровых и алгоритмических ресурсов.

Приоритеты технологической самостоятельности и развития отечественных цифровых решений закреплены в ключевых документах стратегического уровня, что позволяет рассматривать интеллектуальный суверенитет как логически вытекающий результат реализации государственных приоритетов.

Исследование институциональной архитектуры национального проекта «Экономика данных и цифровая трансформация государства» подтвердило его системный характер и многоуровневую структуру реализации. Нацпроект формирует взаимосвязанный комплекс механизмов обеспечения независимости, включающий технологический контур (развитие отечественного программно- аппаратного обеспечения), инфраструктурный контур (создание платформенной цифровой среды) и алгоритмический контур (внедрение моделей управления на основе данных). Их интеграция, представленная в формате авторской модели, обеспечивает снижение критической внешней зависимости и формирует условия для устойчивого цифрового развития. Тем самым национальный проект выполняет не только функцию модернизации государственного управления, но и функцию институционального механизма формирования интеллектуальной самостоятельности Российской Федерации.

**Библиографический список**

1. Авдийский В.И., Иванов А.В., Царегородцев А.В. Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы // Вестник евразийской науки. 2024. Т. 16. № S3. С. 21.

2. Близнец И.А. Методология интеллектуального суверенитета — новое в теории интеллектуальной собственности // Вестник ФИПС. 2022. Т. 1, № 2 (2). С. 58–59.

3. Бойко П.Е., Сокол А.В. Наука философии и проблема интеллектуального суверенитета современной России // Научная мысль Кавказа. 2025. № 3 (123). С. 26–32.

4. Демидов А.В. Национальный проект «Экономика данных и цифровая трансформация государства» как инструмент укрепления цифрового суверенитета России // Наукосфера. 2024. № 4-2. С. 357–360.

5. Карнаушенко Л.В. Интеллектуальный суверенитет государства и проблема его обеспечения в обществе начала XXI века // Общество и право. 2015. № 4 (54). С. 12–18.

6. Кочетков А.П., Маслов К.В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12: Политические науки. 2022. № 2. С. 31–45.

7. Неретин О.П. Интеллектуальный суверенитет экономики России. Москва: Федеральный институт промышленной собственности (ФИПС), 2022. 166 с.

DOI: 10./-2026-3

# Административная ответственность за нарушения порядка обработки биометрических персональных данных

# ADMINISTRATIVE RESPONSIBILITY FOR VIOLATIONS OF THE PROCESSING REGIME FOR BIOMETRIC PERSONAL DATA

**Затолокин Александр Александрович,**
канд. юрид. наук,
доцент кафедры государственно-правовых и общетеоретических дисциплин КубИСЭП (филиал) ОУП ВО «АТиСО»,
г. Краснодар
zatolokin09@rambler.ru

**Zatolokin Alexander Alexandrovich,**
Cand. Jurid. of Sciences,
Associate Professor, Assistant professor of the Department state-legal and general theoretical disciplines
KubISEP (branch) OUP VO "ATiSO",
Krasnodar
zatolokin09@rambler.ru

***Аннотация.*** *Рассмотрены проблемы, связанные с неправомерным завладением биометрическими персональными данными. Подвергнуты научному анализу меры государственного реагирования на нарушения порядка обработки биометрических персональных данных. Сделан акцент на имеющихся положительных сдвигах в вопросах правового регулирования защиты биометрических персональных данных, в том числе благодаря применению ранее предложенных автором научно обоснованных путей совершенствования административной ответственности. Обоснована возможность повышения штрафных санкций в вопросах связанных с защитой биометрических персональных данных, а также за отказ в предоставлении государственных услуг гражданам, которые отказались проходить идентификацию или аутентификацию с использованием своих биометрических персональных данных.*

***Annotation.*** *The article discusses the problems associated with the unauthorized acquisition of biometric personal data. It also provides a scientific analysis of government responses to violations of the processing of biometric personal data. The article emphasizes the positive developments in the legal regulation of the protection of biometric personal data, including the implementation of the author's previously proposed scientifically grounded approaches to improving administrative liability. The possibility of increasing penalties for violations related to the protection of biometric personal data, as well as for refusing to provide public services to citizens who refuse to undergo identification or authentication using their biometric personal data, has been substantiated.*

***Ключевые слова:*** *персональные данные, порядок обработки персональных данных, правовое регулирование, биометрические персональные данные, административная ответственность, повышение штрафа.*

***Keywords:*** *personal data, personal data processing, legal regulation, biometric personal data, administrative liability, and increased fines.*

**Персональные данные в общественных отношениях играют огромную роль. С их помощью граждане вступают в те или иные правоотношения, заключают и расторгают сделки, реализуя предоставленные им конституционные права. Современное развитие информационно- телекоммуникационных технологий позволяет использовать наряду с традиционными персональными данными и биометрические персональные данные. Вопросы защиты персональных данных, обеспечения установленного законодательством порядка их обработки являются важнейшим направлением деятельности органов государственной власти Российской Федерации.**

Органы государственной власти реагируют соответствующим образом на имеющиеся риски, связанные с обработкой персональных данных и биометрических персональных данных: в правовое поле вводятся необходимые нормативные акты, определяются субъекты государственного контроля и надзора в соответствующей сфере деятельности, совершенствуется правоприменительная практика.

Важнейшими источниками права, регламентирующими общественные отношения в сфере обработки, защиты и распространения персональных данных являются:

— Федеральный закон «О персональных данных» (Закон о персональных данных 2006 г., ФЗ № 152)[1];

— Федеральный закон «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (Закон о биометрии 2022 г., ФЗ № 572)[2].

[1] О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2026).

[2] Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: Федеральный закон от 29.12.2022 № 572-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2026).

Основным субъектом государственного контроля и надзора за соблюдением порядка обработки персональных данных является Федеральная служба по надзору в сфере связи и массовых коммуникаций (Роскомнадзор). Согласно доклада Роскомнадзора, только лишь за один год сотрудники ведомства составили 1 656 протоколов об административных правонарушениях на общую сумма штрафов 9 305 950 рублей. Наиболее часто выявляемым сотрудниками Роскомнадзора нарушением стало — «Нарушение порядка объявления выходных данных» (ст. 13.22 КоАП РФ)[3].

Несмотря на свою относительную новизну биометрия, наряду с иными персональными данными уверенно вошла в общественные отношения. Научное обоснование применение биометрии в различных областях общественных отношений осуществлялось исследователями на протяжении длительного времени. В 2000 году исследователем Маккеевым С.С. была доказана целесообразность применения биометрии в вопросах безопасности, медицины и банковской деятельности[4]. Однако, как указано выше правовое регулирование данная деятельность получила лишь в 2022 году. С применением биометрических персональных данных стали появляться определенные риски утраты этих данных. В последнее время участились случаи сбора голосовой биометрии (образцов голоса), в том числе и посредством «массового обзвона» абонентов телефонной сети. Сбор биометрии маскируется мошенниками под анкетирование, или под оказание услуг. Мошенники, под видом операторов звонят абонентам, вынуждая последних произнести слово «ДА» и, после произнесения абонентом ожидаемого слова, разговор прекращается. При этом риски утечки биометрических персональных данных, наряду с традиционными персональными данными чреваты гораздо большими последствиями. Завладев биометрическими персональными данными злоумышленники имеют возможность совершать от имени лица обременительные сделки, распоряжаться его имуществом.

На протяжении нескольких лет вопросы административной ответственности за нарушения порядка обработки биометрических данных практически не регламентировались действующим законодательством, но после выхода научных исследований, государство обратило внимание на эту проблему. В этой связи отрадно отметить, что органы государственной власти должным образом реагируют на предложения научного сообщества по совершенствованию законодательства в сфере обработки персональных данных и биометрических персональных данных. Так, в 2023 году была издана научная статья «Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных» (авторы: Затолокин А.А. и Стрельцов В.В.)[5] в которой обращалось внимание на отсутствие административной ответственности за нарушение порядка обработки биометрических персональных данных и наряду с этим вносилось предложение по введению ответственности для должностных лиц, препятствующих получению государственных услуг при не прохождении гражданином процедуры идентификации или аутентификации. И уже в конце 2023 года были внесены соответствующие изменения в Кодекс Российской Федерации об административных правонарушениях[6]. Помимо изменений, касающихся введения административной ответственности за нарушение порядка обработки биометрических персональных данных в правовое поле в 2024 году вошла норма (ч. 2.1 ст. 5.63 КоАП РФ). Нововведение предусмотрело административную ответственность за «отказ должностного лица органа государственной власти… в предоставлении государственной услуги… в связи с отказом заявителя от прохождения идентификации и (или) аутентификации с использованием его биометрических персональных данных»[7].

Вместе с тем, по прежнему остаются высокими риски нарушения порядка обработки персональных данных, нивелировать которые возможно путем принятия обеспечительных мер в виде повышения административной ответственности, как за нарушение порядка работы с биометрическими персональными данными, так и за нарушение прав граждан на добровольность сдачи биометрии.

В настоящее время в КоАП РФ имеется статья 13.11.3 («Нарушение требований в области размещения и обработки биометрических персональных данных в государственной информационной системе «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных», иных информационных системах, обеспечивающих аутентификацию на основе биометрических персональных данных физических лиц») части которой предусматривают административную ответственность за нарушения порядка обработки биометрических персональных данных. Однако, справедливости ради, следует отметить, что учитывая сумму штрафных санкций данная норма не является суровой мерой и, в основном, наносит лишь репутационный вред недобросовестным операторам персональных данных.

В целях обеспечения исполнения Закона о персональных данных и Закона о биометрии считаем необходимым внести изменения в 5 и 13 главы КоАП РФ. А именно, увеличить санкцию, применяемую в отношении юридических лиц, всех частей ст. 13.11.3 КоАП РФ в три раза, так:

— по первой и второй части «Размещение и обновление…биометрических персональных данных … с нарушением установленных законодательством» и «нарушение порядка обработки биометрических персональных

[3] https://rkn.gov.ru/activity/plans/contolplan (дата обращения: 01.02.2026).

[4] Макеев, С.С. Биометрия? Биометрия. Биометрия! / С.С. Макеев // Наукоемкие технологии и интеллектуальные системы в XXI веке: Сборник научных трудов молодежной научно- технической конференции, Москва, 16—17 марта 2000 года. Москва: Московский государственный технический университет им. Н.Э. Баумана, 2000. С. 103.

[5] Затолокин, А.А. Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных / А.А. Затолокин, В.В. Стрельцов // Общество и право. 2023. № 1 (83). С. 79.

[6] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 12.12.2023 № 589-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2026).

[7] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.11.2024 № 420-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2025).

данных» штрафные санкции увеличить с имеющейся формулировки «от пятисот до одного миллиона рублей» изложив в виде «от одного миллиона пятисот до трех миллионов рублей»;

— по третьей части «Непринятие организационных и технических мер по обеспечению безопасности биометрических персональных данных…» штрафные санкции увеличить с имеющейся формулировки «от одного миллиона до одного миллиона пятисот тысяч рублей» изложив в виде «от трех миллионов до четырех миллионов пятисот рублей»;

— по четвертой части «Обработка биометрических персональных данных… без аккредитации…» штрафные санкции увеличить с имеющейся формулировки «от одного миллиона до двух миллионов рублей» изложив в виде «от трех миллионов до шести миллионов рублей».

Кроме повышения штрафных санкций по статье 13.11.3 представляется необходимым также повысить в три раза штрафные санкции, применяемые к должностным лицам за отказ в предоставлении государственных услуг, при отсутствии у лица биометрии по ч. 2.1 ст. 5.63 КоАП РФ. Действующую санкцию «от пяти тысяч до десяти тысяч рублей либо дисквалификацию сроком на шесть месяцев» следует изложить в виде «от пятнадцати до тридцати тысяч рублей либо дисквалификацию сроком на год и шесть месяцев».

Введение повышенной административной ответственности за нарушение порядка обработки биометрических персональных данных позволит с одной стороны, защитить граждан от различного рода злоумышленников и недобросовестных должностных лиц, а с другой стороны обеспечит равный доступ граждан ко всем благам цифровизации вне зависимости от возможности прохождения ими процедур идентификации и аутентификации.

**Библиографический список**

1. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2026).

2. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: Федеральный закон от 29.12.2022 № 572-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2026).

3. Макеев, С.С. Биометрия? Биометрия. Биометрия! / С.С. Макеев // Наукоемкие технологии и интеллектуальные системы в XXI веке: Сборник научных трудов молодежной научно-технической конференции, Москва, 16—17 марта 2000 года. Москва: Московский государственный технический университет им. Н.Э. Баумана, 2000. С. 103.

4. Затолокин, А.А. Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных / А.А. Затолокин, В.В. Стрельцов // Общество и право. 2023. № 1 (83). С. 79.

5. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 12.12.2023 № 589-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2026).

6. https://rkn.gov.ru/activity/plans/contolplan (дата обращения: 01.02.2026).

7. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.11.2024 № 420-ФЗ [Электронный ресурс]: https://internet.garant.ru (дата обращения: 01.02.2026).

DOI: 10./-2026-4

# Перспективы развития нормативно-правового регулирования применения искусственного интеллекта

# PROSPECTS FOR THE DEVELOPMENT OF LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE

**Капица Вячеслав Станиславович,**
канд. юрид. наук, доцент кафедры уголовного права ФГБОУ ВО «Российский государственный университет правосудия», г. Краснодар
capica@yandex.ru

**Капица Татьяна Александровна,**
канд. юрид. наук, доцент кафедры уголовного права ФГБОУ ВО «Российский государственный университет правосудия», г. Краснодар
tatochka08@nextmail.ru

**Kapitsa Vyacheslav Stanislavovich,**
Ph D. jurid. PhD, Associate Professor of the Department of Criminal Law Russian State University of Justice, Krasnodar
capica@yandex.ru

**Kapitsa Tatiana Alexandrovna,** Ph D. jurid. PhD, Associate Professor of the Department of Criminal Law Russian State University of Justice, Krasnodar
tatochka08@nextmail.ru

***Аннотация.*** *В статье рассматриваются проблемы связанные с нормативно — правовым регулированием новых технологий искусственного интеллекта как в целом, так и в отдельных отраслях применения. Выделяются некоторые понятия разграничивающие рассматриваемые категории. Ставиться вопрос о наиболее проблемных областях регулирования применения рассматриваемых технологий. Анализируется опыт нормативно — правового регулирования в некоторых ведущих в данной области странах, в сравнении с опытом Российской Федерации. Рассматривается вопрос перспективы эффективного нормативно — правового регулирования технологий ИИ.*

***Ключевые слова:*** *Искусственный интеллект, нейросеть, нормативно — правовое регулирование, перспективы регулирования, законодательство Российской Федерации, проблемы нормативно — правового регулирования.*

***Annotation.*** *The article discusses the problems associated with the legal regulation of new artificial intelligence technologies, both in general and in specific industries. It highlights some concepts that distinguish between the categories under consideration. The article raises questions about the most problematic areas of regulation for these technologies. It analyzes the experience of legal regulation in some leading countries in this field, comparing it with the experience of the Russian Federation. The article also discusses the prospects for effective legal regulation of AI technologies.*

***Keywords:*** *Artificial intelligence, neural network, legal regulation, regulatory prospects, legislation of the Russian Federation, problems of legal regulation.*

**В настоящее время, остро поднимается вопрос о необходимости нормативно-правового регулирования применения технологий так называемого «искусственного интеллекта» (далее — ИИ).**
**На сегодняшний день, в целом, общество и государство может обходиться без использования технологий «искусственного интеллекта», однако такое положение дел будет безусловно тормозить их развитие. Риски для человечества, связанные с развитием искусственного интеллекта, очень высоки, но при всей серьезности рисков отказ от развития технологий невозможен. Следует признать, что указанные технологии с высокой скоростью внедряются повсеместно. Это в данный момент прежде всего касается технологической сферы, в которой некоторые отрасли уже критически зависят от данных технологий. Здесь нужно заметить, что существует множество примеров применения «искусственного интеллекта» и в иных сферах, начиная от повседневного, бытового назначения и заканчивая выполнением профессиональных функций и решения задач.**

Очевидно, что наука начала развиваться, опираясь на указанные технологии. Конечно, эта доктрина будет неизбежно превалировать с течением времени. И где — нибудь, через 10 лет, общество настолько привыкнет к использованию рассматриваемых технологий, что просто не сможет без них обходиться. В свое время так появилось электричество, которое дало возможность развития множеству отраслей науки и техники и явилось по сути технологической основой окружающего нас мира сегодня.

В новейшей истории такой технологией стал интернет. По сути, задумываясь как средство коммуникации, вид связи, интернет породил новую технологическую эру.

Следует уточнить, понятие «искусственный интеллект» для более глубокого погружения в проблематику, связанную с его безусловной актуальностью в современном мире и неизбежностью проникновения в абсолютно все сферы деятельности общества в недалеком будущем.

Чтобы дать наиболее развернутое представление о понятии ИИ, необходимо уяснить следующее:

Искусственный интеллект является родовым понятием для пока еще неопределенной группы технологий, которые в свою очередь находятся в стадии развития!

Через какое — то непродолжительное время, практически все технологические решения, влияющие на повседневную жизнь, будут функционировать, используя в своей основе те или иные технологии ИИ.

Переходя все — таки к понятию ИИ следует указать на то, что необходимо разделить между собой некоторые смежные понятия, которые часто используются в обиходе как синонимы. Речь идет о разделении понятий ИИ и Нейросеть:

Термины «искусственный интеллект» (ИИ) и «нейросети» не являются синонимами, хотя часто используются взаимозаменяемо, что может приводить к путанице. Эти понятия связаны, но имеют разное значение и область применения.

Искусственный интеллект (ИИ) — это более широкое понятие. Это область науки и техники, которая занимается созданием систем, способных имитировать человеческий интеллект: выполнять задачи, требующие интеллектуальных способностей, таких как обучение, решение проблем, принятие решений, обработка естественного языка и др.. ИИ включает в себя множество подходов и методологий, не ограничиваясь только нейросетями. К технологиям ИИ относятся, например, экспертные системы на основе правил, логическое программирование, генетические алгоритмы, обработка изображений без машинного обучения и другие методы.

В национальной стратегии развития искусственного интеллекта на период до 2030 года ((В редакции Указа Президента Российской Федерации от 15.02.2024 № 124) дается следующее понятие ИИ: искусственный интеллект — комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Нейросети — это конкретная технология или метод в рамках искусственного интеллекта. Это математические модели, вдохновлённые структурой человеческого мозга, которые состоят из взаимосвязанных нейронов (искусственных нейронов). Нейросети обучаются на больших объёмах данных, анализируют их, классифицируют и решают задачи, такие как распознавание образов, обработка текстов, генерация контента, анализ данных и др.. Нейросети — одна из моделей обучения ИИ, но не единственная.

В России нормативной основой регулирования искусственного интеллекта является уже упомянутый Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», которым утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года. Стратегия определяет основные направления и принципы развития ИИ в России, в том числе:

— обеспечение роста благосостояния и качества жизни населения;

— обеспечение национальной безопасности и правопорядка;

— достижение устойчивой конкурентоспособности российской экономики, в том числе лидирующих позиций в мире в области искусственного интеллекта.[1]

Однако, следует сказать о том, что одной из наиболее проблемных зон применения искусственного интеллекта является обеспечение информационной безопасности. В частности, вопрос в том, что на т.н. рынке программных продуктов представлено множество версий «нейросетей» и в подавляющем большинстве данные нейросети разработаны компаниями, представляющими иностранные государства. Не секрет, что существует зависимость от импорта в том числе и в данной области. Например, от открытых библиотек и инструментов, разработанных за рубежом и являющимися основой разработки технологий.

Исходя из фактов того, что доступ к указанным продуктам в настоящее время является свободным, возникает вопрос о том, как нормативно регулировать использования этих инструментов.

Существует риск того, что идеологическая основа данных, которые используют указанные нейросети в большинстве случаев будет существенно отличатся от российской.

Например, Китай в 2023 году ввёл правила, требующие от алгоритмов соответствия социалистическим ценностям, а также запрещающие использование ИИ для подрыва государственной власти, сепаратизма и других действий, угрожающих национальной безопасности. Генеративные модели обязаны маркировать создаваемый контент, а перед выводом на рынок — проходить проверку безопасности.

| Основные различия: | | |
|---|---|---|
| **Критерий** | **Искусственный интеллект** | **Нейросети** |
| Объём понятия | Общее понятие, охватывающее все технологии, имитирующие человеческий интеллект. | Конкретная технология в рамках ИИ. |
| Принципы работы | Может использовать различные подходы: правила, логический вывод, машинное обучение и др. | Основаны на математической модели, имитирующей работу нейронов мозга. Требуют обучения на данных. |
| Применение | Используется для решения широкого спектра задач, включая те, где не требуются нейросети (например, экспертные системы). | Применяются для решения узких задач, где требуется обработка сложных наборов данных в режиме реального времени. |

[1] Филипова И. А. Правовое регулирование искусственного интеллекта: учебное пособие, 3-е издание, обновленное и дополненное — Нижний Новгород: Нижегородский госуниверситет, 2025. — с. 51

Прямо противоположная ситуация в США, которые не имеют единого федерального закона, регулирование происходит на уровне штатов и отдельных ведомств (например, NIST). В 2023 году президент Дж. Байден подписал указ о безопасном, надёжном и заслуживающем доверия ИИ, который требовал от создателей систем ИИ обеспечивать прозрачность процессов через передачу данных правительству до выхода разработки на рынок. Однако позже новый президент Трамп отменил этот акт.

В соответствии со сложившейся практикой в Российской Федерации, законодательное регулирование т.к. проблемных областей, в последнее время сводиться к запретам и ограничениям. Однако данный подход, очевидно вызывает как минимум непонимание со стороны общества.

Как пример, можно указать на запрет на использование социальных сетей. Данная мера, имеет как потенциальные преимущества (развитие национальных сервисов, защита определённых групп населения), так и значительные риски (поляризация общества, ухудшение когнитивных функций у молодёжи, рост цифрового неравенства). И здесь нужно добавить, что эффективность таких мер зависит от баланса между целями регулирования, методами реализации и реакцией общества. Важно учитывать, что полный запрет часто приводит к поиску обходных путей, а не к решению проблем, которые он призван устранить.

Поэтому вопрос эффективности тенденциозного регулирования проблемных зон, остается открытым.

В целом, считается, что в России регулирование ИИ развивается по пути «мягкого права» и стратегического планирования.

**Ключевые регулятивные документы Российской Федерации:**

— Указанный ранее Указ Президента РФ от 10 октября 2019 года № 490 который утвердил Национальную стратегию развития ИИ до 2030 года. Цели — обеспечение роста благосостояния населения, национальной безопасности, конкурентоспособности экономики.

— Кодекс этики в сфере искусственного интеллекта (2021 год) — рекомендательный документ, к которому присоединились более 360 российских компаний, федеральных и региональных органов власти, а также участники из 19 зарубежных государств. Закрепляет принципы человекоцентричности, справедливости, прозрачности, безопасности и ответственного управления рисками.

— Федеральный закон от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (так называемые «регуляторные песочницы») — создаёт условия для тестирования инноваций, включая ИИ, в контролируемой среде с временными изъятиями из общих норм.

— Федеральный закон от 8 июля 2024 года № 169-ФЗ дополнил закон об экспериментальных правовых режимах механизмом рассмотрения случаев причинения вреда при использовании ИИ и ввёл обязательное страхование гражданской ответственности участников таких режимов.

Переходя к основному вопросу, касательно перспективы правового регулирования в отношении ИИ считаем, что регулятивная основа ИИ может быть только ситуативной, т.к. области его применения до конца не прогнозируется. Для начала нужно понять, что именно необходимо регулировать, какие отрасли данной технологии нуждаются в нормативном регулировании. Здесь считаем необходимым отметить, что далеко не все области применения нуждаются в нормативном регулировании. Чрезмерное детализированное законодательство может замедлить развитие инноваций, особенно для небольших технологических компаний и стартапов. В качестве примера попытки максимально урегулировать на государственном уровне новшества можно привести следующий. В XIX веке Англия была лидером появившегося недавно автомобилестроения, но в 1865 году был принят закон — Red Flag Act — ограничивающий скорость движения автомобилей в городах до двух миль в час и требующий, чтобы впереди автомобиля на расстоянии 60 ярдов (чуть более 50 метров) шел сигнальщик с красным флагом, оповещая прохожих о приближающейся опасности. Вроде бы регулирование, направленное на снижение появившихся рисков, было создано, а в итоге этот закон фактически уничтожил зарождающуюся автомобильную промышленность Англии, так как вперед вышли другие страны — Франция и Германия. Так и с регулированием искусственного интеллекта: выбор между запрещением и разрешением развития изначально обречен на неудачу. В то же время страны, создавшие сбалансированное регулирование, будут иметь высокие шансы на опережающий экономический рост, в том числе и за счет привлекательности инвестиций)[2].

Также есть опасения, что требования закона, например, обеспечить «прозрачность» решений ИИ, могут быть технически невыполнимы, как и решения отдельного человека, например при одиозном поведении, объяснить, почему система выдала тот или иной результат, может быть сложно или невозможно вовсе.

Перспективы законодательного регулирования искусственного интеллекта (ИИ), безусловно связаны с поиском баланса между технологическим прогрессом и обеспечением безопасности, защиты прав человека, этичности использования технологий. В разных странах и на международном уровне подходы различаются, но общими трендами становятся риск-ориентированное регулирование, усиление контроля в чувствительных сферах и развитие стандартов.

Основой нормативного регулирования могут стать отдельные положения законодательства в различных отраслях права.

В заключении следует добавить, что ключевой вызов — обеспечить, чтобы регулирование не тормозило инновации, но при этом защищало права человека, обеспечивало безопасность и этичность использования ИИ. Это требует гибкости правовых систем, междисциплинарного подхода и постоянного обновления норм в соответствии с технологическим прогрессом.

[2] Филипова И.А. Правовое регулирование искусственного интеллекта: учебное пособие, 3-е издание, обновленное и дополненное — Нижний Новгород: Нижегородский госуниверситет, 2025. — с. 54

**Библиографический список**

1. Журавлева, А.В. Искусственный интеллект как субъект права / А.В. Журавлева, Ю.А. Куликова // Гуманитарные, социально-экономические и общественные науки. — 2025. — № 3. — С. 88—94. — DOI 10.24412/2220—2404—2025—3—3. — EDN UUKKAG.

2. Певцова, Е.А. Влияние искусственного интеллекта на правовую деятельность человека / Е.А. Певцова // Журнал российского права. — 2020. — № 9. — С. 19—31. — DOI 10.12737/jrl.2020.103. — EDN JTCOJM.

3. Филипова И.А. Правовое регулирование искусственного интеллекта: учебное пособие, 3-е издание, обновленное и дополненное — Нижний Новгород: Нижегородский госуниверситет, 2025. — с. 51

DOI: 10./-2026-5

# Роль Искусственного Интеллекта в обеспечении цифрового суверенитета: внедрение ИИ в государственном управлении и социальной сфере — правовые и этические аспекты его регулирования

# THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENSURING DIGITAL SOVEREIGNTY: INTRODUCTION OF AI IN PUBLIC ADMINISTRATION AND THE SOCIAL SPHERE — LEGAL AND ETHICAL ASPECTS OF ITS REGULATION

**Карпова Виктория Юрьевна,**
доцент кафедры гражданского и трудового права, к.э.н.
Кубанский институт социо-экономики и права (филиал) Образовательного учреждения профсоюзов высшего образования «Академия труда и социальных отношений»
(г. Краснодар)
pavlovskay.vika@mail.ru

**Соловьева Екатерина Витальевна,**
старший преподаватель кафедры гражданского и трудового права Кубанский институт социоэкономики и права (филиал) Образовательного учреждения профсоюзов высшего образования «Академия труда и социальных отношений»
(г. Краснодар)
esolo88@mail.ru

**Victoria Yuryevna Karpova**
Associate Professor, Department of Civil and Labor Law, PhD in Economics Kuban Institute of Socioeconomics and Law (branch) of the Educational Institution of Higher Education Trade Unions "Academy of Labor and Social Relations"
(Krasnodar)
pavlovskay.vika@mail.ru

**Ekaterina Vitalyevna Solovieva**
Senior Lecturer, Department of Civil and Labor Law
Kuban Institute of Socioeconomics and Law (branch) of the Educational Institution of Higher Education Trade Unions
"Academy of Labor and Social Relations" (Krasnodar)
esolo88@mail.ru

***Аннотация:*** *В статье осуществляется комплексный междисциплинарный анализ роли и места технологий искусственного интеллекта (ИИ) в стратегическом процессе обеспечения цифрового суверенитета Российской Федерации. На основе анализа доктринальных источников и нормативно-правовой базы исследуются правовые и этические аспекты имплементации систем ИИ в сферу государственного (публичного) управления и социальную сферу. Автор выявляет ключевые системные барьеры, препятствующие эффективному внедрению ИИ, включая правовую фрагментацию, кадровый дефицит, инфраструктурные ограничения и дефицит общественного доверия. Особое внимание уделяется анализу этических рисков, связанных с алгоритмической предвзятостью, нарушением прав граждан и деформацией традиционных ценностей. В работе сопоставляются глобалистский и суверенный подходы к этическому регулированию ИИ, аргументируется необходимость формирования национальной доктрины этики ИИ, основанной на отечественном философско-правовом наследии. По итогам исследования формулируются научно-практические предложения по совершенствованию законодательства и созданию институциональных механизмов, направленных на гармонизацию технологического развития с задачами укрепления национального суверенитета.*

***Annotation:*** *The article provides a comprehensive interdisciplinary analysis of the role and place of artificial intelligence (AI) technologies in the strategic process of ensuring the digital sovereignty of the Russian Federation. Based on the analysis of doctrinal sources and the regulatory framework, the legal and ethical aspects of the implementation of AI systems in the field of public administration and the social sphere are investigated. The author identifies key systemic barriers to the effective implementation of AI, including legal fragmentation, staff shortages, infrastructural constraints, and a lack of public trust. Special attention is paid to the analysis of ethical risks associated with algorithmic bias, violation of citizens' rights and distortion of traditional values. The paper compares globalist and sovereign approaches to the ethical regulation of AI, argues for the need to form a national doctrine of AI ethics based on the Russian philosophical and legal heritage. Based on the results of the study, scientific and practical proposals are formulated to improve legislation and create institutional mechanisms aimed at harmonizing technological development with the objectives of strengthening national sovereignty.*

***Ключевые слова:*** *искусственный интеллект, цифровой суверенитет, государственное управление, социальная сфера, правовое регулирование, этика искусственного интеллекта, цифровая трансформация, информационная безопасность, правовые риски, национальная доктрина.*

***Keywords:*** *artificial intelligence, digital sovereignty, public administration, social sphere, legal regulation, ethics of artificial intelligence, digital transformation, information security, legal risks, national doctrine.*

Современный этап мирового развития характеризуется стремительной цифровой трансформацией, в авангарде которой находятся технологии искусственного интеллекта (ИИ). Как отмечает А.В. Черняев, эти технологии «бросают вызов традиционным способам производственной и повседневной деятельности человека, трансформируя сами основы его бытия в персональном, социальном и политическом измерениях»[1]. Этот переход к новому технологическому укладу, который А.А. Фролов и Э.Р. Колкарева определяют как среду «на границе искусственного интеллекта и роботизации»[2], ставит перед государствами стратегическую задачу обеспечения цифрового суверенитета. Для России, стремящейся к достижению «„цифровой зрелости" ключевых отраслей экономики и социальной сферы»[3], развитие и внедрение ИИ становится императивом национального развития.

Однако амбивалентная природа ИИ порождает фундаментальное противоречие: с одной стороны, открываются беспрецедентные возможности для модернизации, с другой — возникают глубокие риски для правовой системы и безопасности. Проблема

[1] Черняев А.В. Цифровой суверенитет и этика искусственного интеллекта: российский подход в глобальном контексте // Полис. Политические исследования. 2024. № 6. С. 757

[2] Фролов А.А., Колкарева Э.Р. Формирование нового технологического уклада на границе искусственного интеллекта и роботизации: социально-экономические последствия // Инновации. 2025. № 2. С. 206

[3] Пашнина Е.А., Винокурова С.И. Оценка достижения «цифровой зрелости» отраслей экономики как фактор национальной конкурентоспособности // тономика и управление. 2024. № 8. С. 407

усугубляется тем, что технологическое развитие значительно опережает адаптацию правовых институтов, что, по мнению Е.Р. Бозиевой и соавторов, «неизбежно приводит к возникновению правовых пробелов, коллизий и регуляторного вакуума»[4].

На сегодняшний день правовая база регулирования ИИ в России носит фрагментарный характер. Несмотря на закрепление в Конституции РФ вопросов «обеспечения безопасности личности, общества и государства при применении информационных технологий» (п. «м» ст. 71) как предмета ведения Федерации[5], и наличие стратегических документов, комплексное законодательство отсутствует. Как справедливо указывает В.А. Холопов, положения ключевой Национальной стратегии развития ИИ «носят преимущественно декларативный характер и не содержат конкретных механизмов правового регулирования»[6] [Холопов, 2026, с. 710].

Одной из самых острых нерешенных проблем остается правовой статус ИИ. По словам Председателя Конституционного Суда РФ В.Д. Зорькина, признание ИИ субъектом права «вступает в неразрешимое противоречие едва ли не со всеми канонами правовой догматики, включая учения об автономной правовой воле, правоотношении, правонарушении и юридической ответственности» [цит. по: Черняев, 2024, с. 758]. Эта доктринальная проблема имеет прямые практические следствия, создавая правовые коллизии. Например, В.А. Холопов обращает внимание на противоречие между практикой автоматизированного принятия решений и нормами Федерального закона «О персональных данных», которые ограничивают принятие юридически значимых решений исключительно на основе автоматизированной обработки.

На фоне этой правовой неопределенности практическое внедрение ИИ в государственное управление и социальную сферу сталкивается с рядом системных барьеров. Несмотря на очевидный потенциал, продемонстрированный, в частности, ИИ-моделью в ГАС «Управление», которая «в онлайн-режиме анализирует 100% мероприятий нацпроектов»[7], существуют серьезные препятствия. Ключевым из них В.А. Холопов называет кадровый дефицит, подтверждая это данными НИУ ВШт, согласно которым «лишь 12% государственных органов имеют штатных специалистов по работе с алгоритмическими системами»[8]. Ситуация усугубляется инфраструктурными ограничениями, разрозненностью информационных систем и растущими угрозами кибербезопасности. Тревожная статистика, приводимая в исследовании В.А. Холопова, свидетельствует, что «за 2022 год утекло 667,6 млн персональных записей», что подрывает доверие граждан. ттот дефицит доверия, в свою очередь, формирует, по выражению М.Р. Довлатовой и соавторов, «психологический барьер для восприятия ИИ как объективного инструмента»[9].

Помимо правовых и институциональных проблем, наиболее глубокие вызовы лежат в этико-аксиологической плоскости. Как предупреждает М.В. Федоров, бесконтрольное развитие ИИ несет экзистенциальные риски, включая «нарушение баланса между управлением и манипулированием в обществе» и «подавление биологических и психологических потребностей» человека[10] . Более того, как отмечает Е.В. Алферова, ссылаясь на классификацию С.И. Коданевой, существуют концептуальные «ловушки» ИИ, такие как «ловушка фрейминга» (неспособность смоделировать социальную систему целиком) и «ловушка формализма» (неспособность объяснить полный смысл социальных понятий), которые ставят под сомнение возможность полной замены человека машиной в сложных социальных процессах[11].

В этих условиях на глобальной арене разворачивается конкуренция двух подходов к этическому регулированию. Глобалистский подход, представленный, в частности, Рекомендациями ЮНЕСКО, по мнению А.В. Черняева, является инструментом продвижения западной идеологии и интересов транснациональных корпораций. Участник разработки этого документа от России М.В. Федоров прямо свидетельствовал, что за универсальными формулировками скрывались «идеи протекционизма в интересах крупного капитала» и «прозападные политические установки»[12].

Альтернативой является суверенный подход, который предполагает разработку национальных этических и правовых норм, основанных на собственных культурно-цивилизационных ценностях. Как утверждает А.В. Черняев, в современном мире способность «эффективно развивать и контролировать национальную сферу высоких технологий становится одним из ключевых условий сохранения полноценного государственного суверенитета»[13]. Такой подход для России может найти опору в богатейшем наследии отечественной философской мысли, в частности, в идеях русского космизма, утверждающего «абсолютную ценность индивидуального человеческого существования»

---

[4] Бозиева Е.Р., Макоева А.С., Темирканов М.А. Регуляторный вакуум в сфере применения систем искусственного интеллекта: проблемы и пути их преодоления // Право и цифровая экономика. 2025. № 1. С. 3

[5] Троян М.В. Конституционно-правовые основы применения технологий искусственного интеллекта в системе государственного управления РФ // Конституционное и муниципальное право. 2025. № 3. С. 60

[6] Холопов В.А. Институциональные и правовые барьеры внедрения искусственного интеллекта в государственное управление России // Вестник Московского университета. Серия 11. Право. 2026. № 1. С. 711

[7] Там же

[8] Там же

[9] Довлатова М.Р., Исаев И.Ф., Петров В.С. Психологические барьеры и проблемы доверия граждан к системам искусственного интеллекта в социальной сфере // Социологические исследования. 2025. № 5. С. 219

[10] Федоров М.В. ткзистенциальные риски цифровизации: искусственный интеллект как вызов человеческой природе // Философия и общество. 2023. № 4. С. 12

[11] Коданева С.И. Искусственный интеллект в публичном управлении: возможности и риски. М.: ИНИОН РАН, 2021. 210 с.

[12] Федоров М.В., Цветков Ю.А. *Опыт участия в разработке Рекомендаций ЮНЕСКО по этике ИИ: суверенный взгляд* // Аналитический вестник Совета Федерации ФС РФ. 2020. № 21 (754)

[13] Черняев А.В. Цифровой суверенитет и этика искусственного интеллекта: российский подход в глобальном контексте // Полис. Политические исследования. 2024. № 6. С. 766

и подчинение технического прогресса высшим нравственным целям.

Таким образом, обеспечение цифрового суверенитета России в эпоху ИИ требует не простого решения технических и правовых задач, а выработки комплексной, национально ориентированной стратегии. тта стратегия должна включать создание целостного законодательства, преодоление институциональных барьеров и, что самое главное, формирование собственной этико-философской доктрины, которая позволит направить мощь технологий на укрепление государственности и защиту национальных интересов.

**Библиографический список**

1. Алферова Е.В. Концептуальные «ловушки» искусственного интеллекта в теории и практике государственного управления // Государство и право. 2025. № 4. С. 138-145.

2. Бозиева Е.Р., Макоева А.С., Темирканов М.А. Регуляторный вакуум в сфере применения систем искусственного интеллекта: проблемы и пути их преодоления // Право и цифровая экономика. 2025. № 1. С. 3-11.

3. Вершицкая Ю.В., Згонникова А.П. Анализ утечек персональных данных в Российской Федерации: статистика, причины и последствия // Вопросы кибербезопасности. 2025. № 2 (62). С. 33-41.

4. Довлатова М.Р., Исаев И.Ф., Петров В.С. Психологические барьеры и проблемы доверия граждан к системам искусственного интеллекта в социальной сфере // Социологические исследования. 2025. № 5. С. 215-224.

5. Коданева С.И. Искусственный интеллект в публичном управлении: возможности и риски. М.: ИНИОН РАН, 2021. 210 с.

6. Пашнина Е.А., Винокурова С.И. Оценка достижения «цифровой зрелости» отраслей экономики как фактор национальной конкурентоспособности // тконomика и управление. 2024. № 8. С. 405-412.

7. Троян М.В. Конституционно-правовые основы применения технологий искусственного интеллекта в системе государственного управления РФ // Конституционное и муниципальное право. 2025. № 3. С. 60- 66.

8. Федоров М.В. тксистенциальные риски цифровизации: искусственный интеллект как вызов человеческой природе // Философия и общество. 2023. № 4. С. 5-15.

9. Федоров М.В., Цветков Ю.А. Опыт участия в разработке Рекомендаций ЮНЕСКО по этике ИИ: суверенный взгляд // Аналитический вестник Совета Федерации ФС РФ. 2020. № 21 (754).

10. Фролов А.А., Колкарева т.Р. Формирование нового технологического уклада на границе искусственного интеллекта и роботизации: социально-экономические последствия // Инновации. 2025. № 2. С. 205-211.

11. Холопов В.А. Институциональные и правовые барьеры внедрения искусственного интеллекта в государственное управление России // Вестник Московского университета. Серия 11. Право. 2026. № 1. С. 705-720.

12. Человек и системы искусственного интеллекта в цифровом мире: аксиологические и антропологические проблемы: коллективная монография / под ред. акад. В.С. Степина. М.: Проспект, 2022. 248 с.

13. Черняев А.В. Цифровой суверенитет и этика искусственного интеллекта: российский подход в глобальном контексте // Полис. Политические исследования. 2024. № 6. С. 757-768.

DOI: 10./-2026-6

# Механизм преступного поведения в уголовно-противоправных деяниях с использованием генеративных технологий

## THE MECHANISM OF CRIMINAL BEHAVIOR IN CRIMINALLY- OFFENSIVE ACTS USING GENERATIVE TECHNOLOGIES

**Никитенко Илья Викторович**
доктор юридических наук, профессор, профессор кафедры уголовного права и криминологии ДВЮИ МВД России им. И.Ф. Шилова; профессор ДВФ РГУП им. В.М. Лебедева
г. Хабаровск,
ORCID: 0009-0006-7406-7998
Researcher ID: KJM-5058-2024
dfvnii@mail.ru

**Nikitenko Ilya Viktorovich**
Doctor of Law, Professor of the Department of Criminal Law and Criminology
Far Eastern Law Institute of the Ministry of Internal Affairs of Russia named after I.F. Shilov; Professor at the Far Eastern Federal University Khabarovsk
ORCID: 0009-0006-7406-7998
Researcher ID: KJM-5058-2024
dfvnii@mail.ru

***Аннотация:*** *статья содержит краткую аналитику особенностей моделирования механизма преступного поведения при совершении уголовно- противоправных деяний с использованием криминогенного потенциала электронно-информационных технологий способных генерировать новую информацию в электронно-цифровой форме (digital content).*

***Abstract:*** *the article contains a brief analysis of the features of modeling the mechanism of criminal behavior in committing criminally-offensive acts using the criminogenic potential of electronic and information technologies capable of generating new information in electronic and digital form (digital content).*

***Ключевые слова:*** *генеративные технологии, дипфейки, контент, криминогенные факторы, механизм преступного поведения, цифровой обман.*

***Keywords:*** *generative technologies, deepfakes, content, criminogenic factors, mechanism of criminal behavior, digital deception.*

**Исследуя особенности криминологического моделирования механизма преступного поведения в уголовно-противоправных деяниях с использованием генеративных технологий, целесообразно сосредоточить внимание, на тех объективных факторах, которые влияют на формирование преступной заинтересованности и решимости совершения различных преступлений, в которых криминогенный потенциал подобных технологий имеет определяющее значение.**

Экстраполируя же естественнонаучное понимание механизма на человеческое поведение, в общем, и преступное поведение в частности, можно констатировать, что эти явления, как правило, рассматриваются через призму взаимодействия объективных факторов и соответствующих этим факторам субъективных процессов личности, что само по себе весьма логично, так как осознанное поведение индивида представляет собой субъективное отображение объективной реальности [7, с. 42 – 50].

Экстраполируя же естественнонаучное понимание механизма на человеческое поведение, в общем, и преступное поведение в частности, можно констатировать, что эти явления, как правило, рассматриваются через призму взаимодействия объективных факторов и соответствующих этим факторам субъективных процессов личности, что само по себе весьма логично, так как осознанное поведение индивида представляет собой субъективное отображение объективной реальности [3, с. 42 – 50].

Но прежде, стоит напомнить, какие именно преступления имеются в виду. Так, в экспертном сообществе, сложилось устойчивое мнение, что большинство из преступлений, совершаемых через криминальное применение генеративных возможностей нейросетевых технологий, совершаются посредством так называемого – «цифрового обмана».

К наиболее распространённым формам цифрового обмана относят: дипфейки (цифровое клонирование образов и звуков), генерацию фальшивых голосовых сообщений, фишинговые сайты и тому подобное [2, с. 26 – 41].

Не ставя задачу, вновь истолковать содержание указанных терминов, в обобщённом виде можно представить, что перечисленные формы цифрового обмана, не что иное, как преднамеренное использование вновь созданного (синтезированного) контента для введения в заблуждение потенциальной жертвой преступного посягательства.

Можно предположить, что уголовную ответственность за совершение преступлений с использованием генеративных возможностей нейросетевых технологий, должны нести те лица, которые непосредственно взаимодействовали с соответствующей программой при постановке задач в преступных целях. Вероятно и то, что подобное злонамеренное использование рассматриваемых технологий должно следовать из конкретных

формулировок, используемых при постановке ранее упомянутых задач.

Основываясь на материалах правоприменительной практики по делам о мошенничествах с использованием нейросетевых технологий можно прийти к выводу, что в адресованном к генеративному ИИ запросе можно не увидеть прямой и непосредственной связи с объективной стороной преступления, в котором используется вновь сгенерированный контент [1].

Так, например, сам процесс формулирования и размещения в нейросетевых чатах запросов можно расценивать лишь как приготовление к тому или иному преступлению.

Судя по материалам отечественной и зарубежной правоприменительной практики по средством цифрового обмана, кроме наиболее распространённого – «цифрового мошенничества», могут быть совершены любые преступления, в которых ложное восприятие объективной реальности способствует достижению преступного результата, на который рассчитывает преступник. Кроме наиболее распространённых преступлений против собственности (преимущественно, мошенничества, кражи, причинения имущественного ущерба путём обмана или злоупотребления доверием), цифровой обман может быть использован в любых преступлениях в которых цифровой обман является средством реализации преступных намерений. Это, прежде всего, преступления связанные: с распространением заведомо ложной, порочащей и иной, способной причинить существенный вред, либо создать угрозу причинения такого вреда, интересам личности, общества и государства, информации.

Несомненно, что эффективное противодействие таким преступлениям возможно при условии формировании чёткого представления о механизме формирования и реализации преступных намерений. Вместе с этим стоит обратить внимание на завершающие компоненты в механизме преступного поведения рассматриваемых деяний, такие как, оценивание преступного результата и выбор возможных вариантов посткриминального поведения.

С опорой на накопленные теоретические и прикладные знания о криминологической парадигме механизма преступного поведения, логично предположить, что посредством анализа объективных и субъективных криминогенных факторов которые влияют на развитие индивидуальной преступной деятельности в умышленном деянии, можно смоделировать механизм преступного поведения относительно любого умышленного преступления. Относительно же преступлений с использованием нейросетевых технологий, необходимо акцентировать внимание на ряд особенностей в реализации их объективной стороны, которые существенно отличают эти деяния от иных умышленных преступлений, имеющих сопоставимые признаки.

Очевидно, что преступники использующие «цифровой обман» для реализации преступных намерений не контактируют с потенциальными жертвами непосредственно, как это имеет место при совершении обычных преступлений, объективная сторона которых так же состоит из обмана или злоупотребления доверием, но в обычной, не связанной с использованием цифрового контента форме. И как уже отмечалось в общетеоретической части работы, подобное опосредованное взаимодействие преступников и жертв значительно повышает скрытность и осложняет выявление первых, что существенно повышает возможности избежать уголовного преследования. Это же в свою очередь, способствует формированию стойкого убеждения безнаказанности и мнимой отстранённости от преступных событий, которые происходят вне традиционных причинно-следственных связей. Известно, что многие из рассматриваемых преступлений совершаются с использованием так называемых – «чат ботов», специальных программ которые в режиме «инкогнито», совершают телефонные звонки относительно неопределённого круга лиц, по принципу «случайной выборки». Однако, подобный способ выявления потенциальных жертв, среди случайных абонентов, значительно расширяет криминальный потенциал телефонных мошенников и других преступников, использующих подобные цифровые технологии. Кроме этого, подобные программные комплексы способны анализировать значительные объёмы сведений, выявляя слабые места в системах обеспечения информационной безопасности для получения доступа к персональным данным.

Массовость, скрытность, безнаказанность и широкая вариативность реализации криминальных задач при совершении преступлений с использованием нейросетевых технологий существенно влияет на механизм преступного поведения при совершении таких уголовно-противоправных деяний. Есть основания полагать, что эти криминогенные факторы значительно усиливают влияние на формирование преступной мотивации и решимости совершать рассматриваемые деяния. При этом первый из компонентов механизма индивидуального преступного поведения, а именно, потребность в совершении рассматриваемых преступлений может оставаться неизменной, в виду органичной взаимосвязи с коренными причинами (детерминантами) тех или иных преступлений, без относительно способов их совершения.

Факторы, влияющие на формирование потребности совершить обычное мошенничество, также как и его аналога с применением ранее упомянутого «цифрового обмана» могут быть схожими. Это, прежде всего, связанно с тем, что потребность совершения любого корыстного преступления вызвана стремлением удовлетворить индивидуальные материальные запросы за счёт противоправного присвоения чужого имущества. Это же можно сказать в отношении иных преступлений, совершение которых может быть связанно с применением нейросетевых технологий (преступления против личности, общественного порядка и общественной безопасности, государственной власти и т.д.).

Известно, что потребность совершения упомянутых преступлений формируется под влиянием фундаментальных криминогенных факторов вне зависимости от средств либо способов их совершения. Так например, факторы, влияющие на формирование потребности совершить преступления против жизни и здоровья (зависть, ревность, месть) не зависят от того как именно будут реализованы преступные намерения. Однако известно и то, что часто в

качестве отягчающих ответственность обстоятельств рассматриваются те преступные способы и средства, которые способны повысить общественную опасность преступных деяний. Очевидно, что целенаправленное использование криминальных возможностей генеративных технологий при совершении тех или иных преступлений может рассматриваться с позиций усиление мер уголовной ответственности.

**Библиографический список**

1. Бодров Н.Ф., Лебедева А.К. Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с помощью технологий искусственного интеллекта // Юридические исследования. 2024. № 1.

2. Бодров Н.Ф., Лебедева А.К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. № 11. С.26-41.

3. Никитенко И. В. Механизм преступного поведения как криминологическая парадигма: теоретическое и прикладное значение // Вестник Дальневосточного юридического института МВД России им. И.Ф. Шилова: № 3 (68), 2024. – Хабаровск. С. 42 – 50

DOI: 10./-2026-7

# Причинная связь и вина в условиях алгоритмической автономности: проблемы уголовно-правовой оценки использования искусственного интеллекта

# CAUSALITY AND GUILT IN THE CONTEXT OF ALGORITHMIC AUTONOMY: PROBLEMS OF CRIMINAL LAW ASSESSMENT OF THE USE OF ARTIFICIAL INTELLIGENCE

**Рясов Дмитрий Алексеевич,**
канд. юрид. наук, доцент, доцент кафедры уголовного права и оперативно-розыскной деятельности органов внутренних дел Ставропольского филиала Краснодарского университета МВД России
г. Ставрополь
ryasov_dmitriy@mail.ru

**Ryasov Dmitry Alekseevich,**
PhD. jurid. PhD, Associate Professor, Associate Professor of the Department of Criminal Law and Operational Investigative Activities of the Internal Affairs Bodies Stavropol branch Krasnodar University of the Ministry of Internal Affairs of Russia,
Stavropol
ryasov_dmitriy@mail.ru

***Аннотация.*** *В статье рассматриваются особенности установления причинной связи и вины при наступлении общественно опасных последствий вследствие использования технологий искусственного интеллекта. Разработана трёхэлементная модель установления причинной связи и уточнены критерии оценки умысла и неосторожности в преступлениях, совершенных с использованием искусственного интеллекта.*

***Annotation.*** *The article examines the specifics of establishing causation and guilt in the occurrence of socially dangerous consequences due to the use of artificial intelligence technologies. A three-element causal relationship model has been developed and criteria for assessing intent and negligence in crimes committed using artificial intelligence have been clarified.*

***Ключевые слова:*** *искусственный интеллект; причинно-следственная связь; опосредованный вред; субъективная сторона преступления; умысел; неосторожность; объективное вменение; уголовная ответственность.*

***Keywords:*** *artificial intelligence; causal relationship; indirect harm; subjective side of the crime; intent; negligence; objective imputation; criminal liability.*

**Современный этап цифровой трансформации характеризуется стремительным внедрением технологий искусственного интеллекта (далее — ИИ) в социально значимые сферы общественных отношений: транспортную инфраструктуру, финансовые рынки, здравоохранение, государственное управление, сферу безопасности и обороны. Алгоритмические системы принимают решения, влияющие на распределение материальных ресурсов, диагностику заболеваний, маршрутизацию транспортных потоков и оценку кредитных рисков. Тем самым искусственный интеллект становится значимым элементом общественных отношений, складывающихся в различных сферах между разнообразными субъектами.**

Существенное внимание вопросам интеграции ИИ-систем и ИИ-агентов в сферу организации и осуществления общественных отношений в социально значимых областях — здравоохранении, управлении дорожным движением, логистике, финансовом секторе и публичном администрировании — уделяется российским законодателем. Это подтверждается динамичным развитием нормативно-правовой базы[1] и реализацией национальных проектов[2], ориентированных на цифровую трансформацию государственного управления и экономики, а также рамочных условий для тестирования ИИ-технологий в отдельных регионах страны, включая особые условия для обработки персональных данных[3].

Вместе с тем расширение масштабов алгоритмической автоматизации происходит на фоне устойчивого роста преступлений, совершаемых с использованием информационно-коммуникационных технологий. Данное обстоятельство объективно усиливает криминогенный потенциал цифровой среды и требует учёта специфических рисков, связанных с возможным использованием ИИ в противоправных целях либо с причинением вреда вследствие его автономного функционирования.

---

[1] О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 г. № 490 (ред. от 15 февраля 2024 г.) // Собрание законодательства Российской Федерации от 14 октября 2019 г. № 41

[2] Путин обновил Национальную стратегию развития ИИ до 2030 года // https://tass.ru/politika/20000627(дата обращения 11 февраля 2026 г.)

[3] Федеральный закон от 31.07.2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (ч. I). Ст. 5017.

Интеграция технологий ИИ в социально значимые сферы, включая публичное управление, актуализирует проблему нормативного определения пределов уголовно-правовой охраны общественных отношений от рисков, обусловленных использованием автономных алгоритмических систем. Речь идёт не только о техническом регулировании цифровых процессов, но и о формировании адекватных механизмов уголовно-правового реагирования на случаи причинения общественно опасного вреда при применении ИИ.

Показательным в данном контексте является подготовленный в 2025 г. Минцифры России законопроект, предусматривающий дополнение перечня обстоятельств, отягчающих наказание новым видом — совершение преступления с использованием технологии искусственного интеллекта. повышенную уголовную ответственность введение уголовной ответственности за совершение преступлений с использованием технологий искусственного интеллекта[4]. Данная инициатива отражает осознание государством возрастания общественной опасности алгоритмически опосредованных форм причинения вреда и стремление усилить уголовно-правовую защиту соответствующих общественных отношений.

Вместе с тем позиция Минюста России, раскритиковавшего проект, выявляет наличие концептуальной неопределённости[5]. Указание на риск формирования противоречивой правоприменительной практики вследствие недостаточной определённости понятия «искусственный интеллект» свидетельствует о сложности его интеграции в уголовно-правовую материю. Дополнительные аргументы, связанные с увеличением нагрузки на экспертные учреждения, удлинением сроков рассмотрения дел и ростом финансовых затрат, демонстрируют институциональные последствия признания использования ИИ обстоятельством, отягчающим уголовное наказание.

Изложенные обстоятельства являются свидетельством возникновения нормативной дилемы: с одной стороны, объективно возрастают риски причинения вреда в результате алгоритмически опосредованной деятельности; с другой — отсутствует устойчивая доктринальная и законодательная модель, позволяющая корректно и единообразно квалифицировать такие деяния. Проблема заключается не столько в самом факте использования ИИ, сколько в определении его юридически значимой роли в причинном механизме и установлении субъективного отношения лица к последствиям функционирования алгоритма.

В этой связи возникает потребность в разработке системного уголовно- правового подхода, который обеспечивал бы:

— чёткое разграничение случаев, когда ИИ выступает лишь техническим средством, и ситуаций, при которых его использование объективно повышает общественную опасность деяния;

— формализацию критериев установления причинной связи и вины в условиях алгоритмической автономности;

— баланс между принципом законности и необходимостью реагирования на новые цифровые угрозы.

Формирование системного уголовно-правового подхода к оценке использования искусственного интеллекта предполагает, прежде всего, нормативное разграничение двух качественно различных обстоятельств, имеющих различное значение для квалификации деяния[6].

Первое связано с использованием ИИ в качестве технического средства (нейтрального инструмента). В данном случае алгоритм выполняет вспомогательную функцию, обеспечивая автоматизацию действий, полностью охватываемых волей и сознанием субъекта. Он не вносит самостоятельного вклада в формирование общественно опасного результата, а лишь ускоряет или упрощает реализацию уже сформированного преступного намерения. Причинная связь при этом сохраняет традиционную линейную структуру, а степень общественной опасности определяется характером деяния самого лица, а не технологической формой его осуществления. В подобных случаях использование ИИ не требует специальной уголовно-правовой квалификации и не должно рассматриваться как квалифицирующий признак или обстоятельство отягчающее наказание.

Вторая ситуация имеет место тогда, когда ИИ выступает фактором объективного повышения общественной опасности. Речь идёт о случаях, в которых применение автономной алгоритмической системы:

— существенно увеличивает масштаб причиняемого вреда (например, за счёт массовости и автоматизированности действий);

— ускоряет распространение негативных последствий;

— затрудняет их своевременное выявление и пресечение;

— повышает вероятность наступления тяжких последствий вследствие способности системы к автономному принятию решений.

В таких условиях алгоритм перестаёт быть нейтральным инструментом и становится элементом, трансформирующим механизм причинения вреда. Использование ИИ должно получать соответствующую уголовно-правовую оценку, поскольку объективно повышает степень общественной опасности деяния.

В целях обеспечения единообразной правоприменительной практики представляется целесообразным использовать модель оценки причинной связи при использовании ИИ, основанную на следующих критериях:

1. Критерий архитектурной предопределённости. Первостепенное значение имеет установление того, действовал ли алгоритм в пределах предусмотренной разра-

[4] Проект Федерального закона «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации» // https://sozd.duma.gov.ru/bill/885494—8?ysclid=mm692pwbk0377677438 (дата обращения 11 февраля 2026 г.)

[5] Минюст раскритиковал законопроект Минцифры о наказании за преступления с использованием ИИ // https://www.tssonline.ru/news/minust-raskritikoval-zakonoproyekt- minzifri-o-nakazanii-za-prestupleniya-s-ispolzovaniyem-ii (дата обращения 11 февраля 2026 г.)

[6] Мурашев П.М. Искусственный интеллект в уголовном судопроизводстве: риски и вызовы // Закон и право. 2025. № 10. С. 235.

ботчиком логики и функциональной архитектуры. Если наступивший результат является следствием реализации заложенных параметров системы либо допустимых режимов её функционирования, то причинная связь с действиями лица, инициировавшего использование алгоритма, сохраняет нормативную значимость. И напротив, если поведение системы обусловлено внешним вмешательством, техническим сбоем или выходом за пределы проектной логики, вопрос о причинной обусловленности требует дополнительной оценки.

2. Критерий предсказуемости риска. Необходимо установить, являлся ли наступивший результат типичным или вероятностно допустимым сценарием функционирования системы. В контексте самообучающихся моделей это означает анализ статистической допустимости соответствующего исхода. Если результат входил в круг предсказуемых рисков, связанных с эксплуатацией алгоритма, он может рассматриваться как реализация созданной субъектом опасности. Отсутствие субъективного предвидения наступления общественно- опасного последствия, при условии надлежащего проектирования и контроля должно оцениваться как отсутствие прямой непосредственной причинной связи между деянием и последствиями.

3. Критерий управляемости. Существенным элементом причинного анализа является оценка возможности субъекта повлиять на функционирование алгоритма либо прекратить его работу. Речь идёт о наличии у лица реальной возможности оказывать влияние на параметры работы алгоритма, корректировать его функционирование либо прекращать его эксплуатацию в случае выявления риска наступления общественно опасных последствий. Контроль может носить технический, организационно-управленческий либо правовой характер и должен оцениваться с учётом статуса лица и объёма возложенных на него обязанностей.

Наличие у субъекта фактической возможности, а также нормативно закреплённой обязанности осуществления контроля свидетельствует о сохранении детерминирующей роли его поведения в причинном механизме и, соответственно, является аргументом в пользу признания юридически значимой причинной связи.

Предложенные критерии позволяют перенести анализ причинности из плоскости абстрактной фактической обусловленности в сферу уголовно- правовой оценки.

Причинная связь при использовании автономной алгоритмической системы может признаваться установленной при совокупности следующих условий:

1. Субъект посредством разработки, внедрения либо эксплуатации системы допустил возможность наступления общественно опасных последствий;

2. Функционирование алгоритма осуществлялось в пределах допущенной возможности и соответствовало его проектной архитектуре;

3. Наступившее последствие явилось прямым результатом сознательного допущения наступления общественно-опасного последствия.

Разработка критериев установления причинной связи при использовании автономных алгоритмических систем логически предполагает уточнение подходов к оценке субъективной стороны деяния. В условиях цифровой трансформации вина не может определяться исключительно через абстрактную категорию предвидения последствий; она должна соотноситься со спецификой распределения функций и компетенций в рамках жизненного цикла ИИ-системы. Установление признаков субъективной стороны в составе преступлений, связанных с наступлением общественно-опасного последствия в результате использования автономных алгоритмических систем, должно осуществляться с опорой на классическую уголовно-правовую концепцию вины как психического

отношения лица к совершаемому деянию и его общественно опасным последствиям, выраженного в форме умысла либо неосторожности. Принципиально важно подчеркнуть, что алгоритмическая автономность не трансформирует природу вины и не допускает объективного вменения; она лишь усложняет содержание интеллектуального и волевого элементов.

В условиях использования ИИ интеллектуальный элемент вины должен охватывать:

— осознание лицом факта использования автономной алгоритмической системы;

— понимание её функциональных характеристик и потенциальных ограничений;

— предвидение возможности наступления общественно опасных последствий, обусловленных спецификой её работы.

Волевой элемент выражается в отношении субъекта к созданному алгоритмическому риску: в желании наступления последствий, сознательном их допущении либо в самонадеянном расчёте на их предотвращение.

Специфика умышленной формы вины в условиях алгоритмической автономности заключается в том, что психическое отношение виновного охватывает не только совершаемое им действие (бездействие), но и инициирование либо продолжение функционирования автономной алгоритмической системы как источника грозящей опасности.

Прямой умысел имеет место в случаях, когда лицо осознаёт общественную опасность применения автономной системы, предвидит неизбежность или реальную возможность причинения вреда и желает наступления соответствующих последствий. В алгоритмическом аспекте это может выражаться в целенаправленном использовании ИИ для достижения преступного результата, при понимании его масштабируемости, скорости и трудности выявления.

Косвенный умысел предполагает, что лицо предвидит реальную возможность наступления вредных последствий вследствие функционирования алгоритма, не желает их, но сознательно допускает либо относится к ним безразлично. В данном случае элементом психического отношения выступает не конкретный алгоритмический сценарий, а риск,

обусловленный эксплуатацией системы в определённых условиях.

Неосторожная форма вины требует более тонкой оценки, поскольку автономность системы может создавать иллюзию утраты контроля.

Легкомыслие имеет место тогда, когда лицо предвидело возможность наступления общественно опасных последствий, связанных с функционированием ИИ, но без достаточных оснований рассчитывало на их предотвращение (например, полагаясь на автоматические механизмы самокоррекции без проведения надлежащего тестирования).

Небрежность выражается в непредвидении наступления вреда при наличии обязанности и реальной возможности его предвидеть. В алгоритмическом контексте это означает игнорирование профессионально очевидных рисков, отказ от анализа обучающих данных, непринятие мер по контролю за системой либо внедрение её в социально значимую сферу без должной оценки последствий.

Таким образом, вина при использовании ИИ должна устанавливаться с учётом психического отношения субъекта к созданному им алгоритмическому риску. При этом, не требуется предвидение всех возможных вариантов поведения системы; достаточно осознания вероятностной возможности причинения вреда в пределах созданной опасной ситуации.

Полагаем, что предложенный подход позволит сохранить традиционное содержание вины (интеллектуальный и волевой элементы) при одновременном учёте специфики алгоритмической автономности, исключая как объективное вменение, так и необоснованное освобождение от ответственности под предлогом «непредсказуемости» цифровой системы[7].

Обобщение изложенных положений позволяет сформулировать авторскую концепцию дифференциации уголовной ответственности, обеспечивающей системное разрешение проблемы уголовно-правовой оценки деяний, совершаемых с использованием автономных алгоритмических систем.

Ключевым исходным положением данной концепции является признание того, что ИИ не обладает сознанием, волей и способностью к осознанию общественной опасности своего поведения, а потому не может рассматриваться в качестве субъекта преступления[8]. Любая уголовно-правовая оценка должна быть сосредоточена исключительно на поведении человека — разработчика, оператора, пользователя либо иного лица, вовлечённого в создание и эксплуатацию системы.

Второе принципиальное положение заключается в том, что использование ИИ как таковое не образует квалифицирующего признака состава преступления. Технологическая форма реализации деяния не может автоматически усиливать уголовную ответственность, поскольку это противоречило бы принципу законности и запрету расширительного толкования уголовного закона. Сам по себе факт применения алгоритма не свидетельствует о повышении общественной опасности.

Уголовно-правовое значение приобретает лишь такое использование автономной системы, которое объективно трансформирует механизм причинения вреда. Речь идёт о ситуациях, когда эксплуатация ИИ:

— создаёт повышенный риск наступления общественно опасных последствий по сравнению с «традиционными» способами совершения преступления;

— затрудняет выявление, предотвращение или пресечение вреда вследствие автономности и масштабируемости алгоритмического воздействия;

— усиливает тяжесть или объём последствий, в том числе за счёт скорости распространения и массового характера действий.

Именно совокупность указанных обстоятельств позволяет говорить о качественном изменении степени общественной опасности и, следовательно, о допустимости учёта алгоритмической автономности при квалификации деяния.

В рамках предлагаемой концепции реализация уголовной ответственности должна осуществляться в строгом соответствии с принципом индивидуализации, при котором определяющее значение приобретает учёт функциональной роли лица в процессе разработки, внедрения и эксплуатации автономной алгоритмической системы. Юридической оценке подлежит не формальное участие субъекта в цифровом процессе как таковом, а его конкретный вклад в создание, модификацию либо допущение юридически значимого риска, реализовавшегося в наступивших общественно опасных последствиях[9]. Тем самым исключается возможность как коллективного, так и абстрактного вменения ответственности за сам факт «использования технологии» без установления персонализированного психического и причинного отношения к результату.

Определяющим критерием уголовно-правовой оценки выступает не применение ИИ «per se», а степень фактического и нормативного контроля лица над функционированием алгоритмической системы, а также объективная предсказуемость её поведения в конкретных условиях. Чем выше уровень управляемости системы и чем более очевидным был риск наступления вреда, тем более обоснованным является вменение соответствующих последствий. И напротив, при отсутствии у лица реальной возможности влияния на функционирование системы либо при наступлении результата в пределах допустимого технологического риска, не подлежащего разумному предвидению, основания для уголовной ответственности могут отсутствовать ввиду недоказанности вины.

---

[7] Рарог А.И. Вина в советском уголовном праве: монография; научный редактор Б.В. Здравомыслов. М.: Проспект, 2018. С. 81

[8] Мосечкин И.Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник СПбГУ. Серия 14. Право. 2019. № 3. С. 466.

[9] Казанцев Д.А. Проблемы и перспективы регулирования отношений в рамках сделки, совершенной с участием искусственного интеллекта // Journal of Digital Technologies and Law. 2023. № 2. С. 448.

**Библиографический список**

1. Казанцев Д.А. Проблемы и перспективы регулирования отношений в рамках сделки, совершенной с участием искусственного интеллекта // Journal of Digital Technologies and Law. 2023. № 2. С. 438—462.

2. Мосечкин И.Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник СПбГУ. Серия 14. Право. 2019. № 3. С. 461—476.

3. Мурашев П.М. Искусственный интеллект в уголовном судопроизводстве: риски и вызовы // Закон и право. 2025. № 10. С. 233—238.

4. Рарог А.И. Вина в советском уголовном праве: монография; научный редактор Б.В. Здравомыслов. М.: Проспект, 2018. 190 с.

DOI: 10./-2026-8

# PRO ET CONTRA цифровизации профсоюзной деятельности (на примере Краснодарского края)

## PRO ET CONTRA DIGITALIZATION OF TRADE UNION ACTIVITIES (ON THE EXAMPLE OF THE KRASNODAR TERRITORY)

**Сивков Сергей Михайлович,**
канд. истор. наук, доцент кафедры гуманитарных дисциплин, экономики и управления
КубИСЭП (филиал) ОУП ВО «АТиСО»,
г. Краснодар
chessm@rambler.ru

**Крявцов Дмитрий Александрович,**
главный специалист по информационной деятельности Краснодарская краевая организация Общероссийского профессионального союза работников культуры,
г. Краснодар
Letter_box@mail.ru

**Sergey Sivkov,**
cand. istor. Sciences, Associate Professor, Department of Economics,
management and humanities
KubISEP (branch) of PMO HE ATiSO,
Krasnodar chessm@rambler.ru

**Kravtsov Dmitry Alexandrovich**
Chief Information Officer
Krasnodar Regional Organization of the All-Russian trade union of cultural workers,
Krasnodar Letter_box@mail.ru

***Аннотация.*** *В статье рассматриваются проблемные аспекты реализации программ цифровизации профсоюзной деятельности в Краснодарском крае. Раскрываются основные проблемы, связанные с полным переходом на цифровые платформы.*

***Abstract.*** *The article examines the problematic aspects of the implementation of digitalization programs for trade union activities in the Krasnodar Territory. The main problems associated with the full transition to digital platforms are revealed.*

***Ключевые слова.*** *Цифровизация, искусственный интеллект, цифровой членский билет, цифровизация профсоюзной деятельности, национальный суверенитет ИИ, Краснодарский край.*

***Keywords.*** *Digitalization, artificial intelligence, digital membership card, digitalization of trade union activities, national sovereignty of AI, Krasnodar Territory.*

**В настоящее время вопросы цифровизации и внедрения искусственного интеллекта в Российской Федерации становятся на первый план, не случайно из уст нашего Президента В.В. Путина и Премьер-министра М.В. Мишустина постоянно слышатся предложения по совершенствованию информационных технологий. Об очередной научно-технической революции предупреждали отечественные философы еще к конце 1980-х начале 1990-х гг., когда машины будут делать машины.**

Почему это актуально для современных профсоюзных организаций? Да по многим причинам. Цифровизация может частично решить проблему с недостатком человеческих ресурсов, как это произошло и происходит в современном сельском хозяйстве нашей страны. От острой нехватки кадров оно перешло к внедрению современных цифровых технологий, что привело к их избытку. Мы не говорим об их дефиците в определенных сферах и по определенным направлениям. Скорее всего проблема решится за счет их подготовки в колледжах и вузах России.

В настоящее время огромное количество работ отечественных ученых посвящено данной проблематике, в том числе работы Александровой Т.В [3]? Аксяновой А.В., Александровской И.П., Гадельшиной Г.А. [4], Аносова С. [5], Бухтияровой Т.И. [6], Кастельс М. [7], Мирясовой О.А., Павловой Т.В., Патрушева С.В., Цысиной Г.А. [8], Недяк И.Л., Павловой Т.В., Патрушева С.В. [9], Пеньковской Ю.С., Лебедева А.В., Сомкина А.А. [10], Рожкова Е.В.[11], Ромайкина И.А., Галишниковой Е.А.[12], Смирнова Ю.А., Скрипниковой М.И, Мажиева Х.Н., Катабай П.Х. [13], Филлиповой А.В. [14], Шункова А.В., Тараненко Л.Г., Дворовенко О.В. [15], Щербаковой А.А. [16] и многих других.

К великому сожалению проблемы цифровизации профсоюзной деятельности затронуты только в трех публикациях [5,8, 9,13]. Таким образом можно говорить о недостаточной цифровизации данной сферы.

Цифровизация оставалась и остается важнейшим направлением деятельности профессиональных союзов, в том числе и на территории современного Краснодарского края. ФНП в качестве ведущей компании по разработке и внедрению цифровых систем для НКО и профсоюзов на российском IT-рынке выбрала Агентство «Домовой и Партнеры». Разработанная компанией цифровая платформа «Профсоюз 360» уже внедрена в нескольких региональных и отраслевых профсоюзах. На данный момент в 2-х профсоюзах ведется электронный учет её членов, это РОСПРОФЖЕЛ и Общероссийский профсоюз образования. Еще в 13 профсоюзах персонифицированный учет частично автоматизирован.

На заседании исполнительного комитета Генерального Совета ФНПР в Москве 26 ноября 2025 года центральным вопросом обсуждения стала деятельность ФНПР и задач профсоюзов на современном этапе. Было предложено создать рабочую группу по внедрению Единой системы учета (ЕСУ) членов профсоюзов, которой поручить определить единый формат данных, разработать и протестировать инструменты для переноса имеющихся данных о членстве из таких форматов, как Excel и 1С [17].

Одной из первых инициатив в сфере деятельности профессиональных союзов, входящих в состав Краснодарского краевого профобъединения уже стал пилотный проект по цифровой трансформации в Краснодарском краевом профсоюзе работников народного образования и науки, проводимый в рамках всероссийской цифровизации отраслевого профсоюза [2, 13]. Общероссийский Профсоюз работников народного образования находится сегодня в авангарде цифровых технологий в Краснодарском крае. В нем внедрена и успешно действует система электронного учета членов профсоюза, сбора и формирования статистической информации и даже бонусная программа с возвратом на личный счет члена профсоюза части средств, потраченных на приобретение товаров и услуг партнеров, привязанная к электронному профсоюзному билету.

Цифровая трансформация призвана революционно преобразовать подход к общественной профсоюзной работе, облегчить и автоматизировать ручную обработку данных и использование таких инструментов, как Excel, что замедляет процессы и увеличивает вероятность ошибок, повысить уровень информированности членов профсоюза о проводимых мероприятиях и достигнутых результатах, повысить эффективность системы вознаграждений и общественного признания, систематизировать профобучение активистов и сформировать систему профсоюзных знаний (история обращений членов профсоюза с фиксацией проделанной работы по результатам таких обращений), цифровое расширение возможностей и автоматизация работы уполномоченных по различным направлениям (включая вопросы охраны труда).

Успехи в области цифровой трансформации, достигнутые Профсоюзом работников народного образования, казалось бы, можно безоговорочно принять как образцовый пример и стремиться к его масштабированию и на другие отраслевые профсоюзы. Однако, положительные результаты реализации в Профсоюзе пилотного проекта в период с 2018 по 2020 годы и дальнейшее его развитие по настоящее время, его значимость и роль в организационном укреплении профсоюзной организации, назревшая актуальность, не спровоцировали волны массового внедрения современных цифровых технологий в профсоюзах других отраслей, как в масштабах страны, так и среди Краснодарских региональных организаций.

Генеральный директор Агентства «Домовой и Партнеры» А.В. Дмитриев отмечает, что часто сталкивается с недопониманием в профсоюзной среде на самых разных уровнях необходимости форсированного перевода на новые цифровые инструменты автоматизации профсоюзной деятельности [19].

По данным сайта Агентства, стоимость внедрения цифровой платформы для одной первичной профсоюзной организации численностью до 12 человек профсоюзного актива составляет 65 тыс. рублей, без учета стоимости ежегодного обслуживания [18].

Существуют различия в объемах профсоюзных бюджетов и это естественным образом влияет на финансовые возможности профсоюзов и на уровень их цифрового развития. Если Краснодарская краевая организация Общероссийского профсоюза работников образования объединяет (по данным на 2025 г.) включает приблизительно 180 тыс. членов профсоюза, численность Краснодарской краевой организации Профсоюза работников АПК РФ — около 40 тыс., Краснодарская краевая организация профсоюза работников культуры — 33,4 тыс., а Краснодарская краевая организация профсоюза работников строительства — только 9,4 тыс. членов профсоюза [20].

Не каждый отраслевой профсоюз может позволить себе содержать в штате даже районных председателей, не говоря о председателях первичных профорганизаций, где рабочее место, оборудованно компьютером и принтером. Анализ ценовой политики Агентства «Домовой и Партнеры» показывает, что стоимость внедрения цифровой платформы уменьшается прогрессивно, в зависимости от масштаба платформы, от 5420 руб. до 1600 руб. за каждую ученую запись, при внедрении системы на 250 профактивистов. Таким образом, можно говорить о том, что чем больше масштаб внедрения — тем доступнее окажется цифровая платформа для профсоюзных бюджетов отдельных профорганизаций [18].

Профсоюзная деятельность Краснодарского края, в основном, составляет работу на общественных началах. Трудности, связанные с цифровым переходом, ждут в первую очередь именно председателей первичек, для которых все это дополнительная неоплачиваемая нагрузка. Практика показывает, что профкому приходится вести двойной учет (на бумажном носителе и дублируя данные на цифровой платформе). Сложно говорить об эффективной цифровой трансформации в подобных условиях.

При разработке новой единой цифровой платформы, следует:

1. Сделать упор на облачные и мобильные сервисы. В профсоюзном движении много общественников и не все имеют доступ к персональному компьютеру, в то же время мобильное носимое устройство (смартфон) с доступом в интернет есть у каждого.

2. Разработать подробные методические образовательные онлайн программы и инструкции, в том числе и мультимедийном формате. Организовать онлайн-школу профсоюзной цифровой трансформации, в рамках обучения, показывать на живых практических примерах преимущества использования новых технологий для профсоюзного актива.

3. Применить принцип безрискового перехода, обеспечив постепенный, плановый ввод новой цифровой системы в эксплуатацию: на первом этапе — центральные комитеты профессиональных союзов, затем региональные и территориальные организации и только после

успешного перехода на верхних уровнях — первичные профсоюзные организации.

4. До массового внедрения, провести тестирование на отдельных, наиболее крупных отраслевых профсоюзах.

Подобный подход позволит избежать масштабных организационных сбоев в период цифровой трансформации, провести качественную отладку программного комплекса, приобрести необходимые опыт и компетенции профсоюзным работникам всех уровней.

Другим важным аспектом, препятствующим развитию цифровых технологий в крае, является кадровый голод в IT-сфере, т.к. квалифицированные специалисты по цифровым технологиям востребованы сейчас во всех сферах экономики да и не только. Некоммерческие общественные организации по понятным причинам не могут предложить таким кадрам конкурентные условия труда на региональном уровне.

МГУ открывает набор на факультет искусственного интеллекта. Как сообщила Российская газета в своем выпуске от 09 февраля 2026 г. «..уже в 2026 году в МГУ им. Ломоносова начнется прием абитуриентов на новый факультет искусственного интеллекта. Об этом сообщил ректор МГУ Виктор Садовничий на традиционном зимнем дне открытых дверей, который в этот раз выпал на удачную дату — День российской науки».(8 февраля 2026 г.- примеч. авт) [17] Спасет ли это решение от кадрового голода в IT- специалистах. Конечно да, но в очень отделенной перспективе и не в том объеме в котором они требуются.

Возможности искусственного интеллекта открывают новые горизонты в автоматизации рутинных задач и повышения эффективности управленческих процессов, что могло бы повысить эффективность и в сфере профсоюзной деятельности. Однако, не пройдя этап базовой цифровой трансформации, трудно представить себе применение ИИ на системном уровне в настоящих условиях.

Следует обратить внимание на те риски, которые могут возникнуть в краевых профсоюзных организациях, в связи с внедрением ИИ. Как отмечается в статье «Фактор риска» опубликованной в Российской газете 9 февраля этого года «На площадке правительства прорабатывается рамочный законопроект, направленный на регулирование ИИ, заявили «РГ» в аппарате вице-премьера — главы аппарата правительства Дмитрия Григоренко. Законопроект призван избавить отрасль от лоскутного регулирования, когда меры зачастую противоречат друг другу.

Как пояснили в аппарате Григоренко, ключевая задача сейчас — это предотвратить риски от применения ИИ в «чувствительных» сферах, где цена ошибки особенно высока. В числе таких сфер: здравоохранение, судопроизводство, общественная безопасность, образование» [21].

Подводя итоги в сфере цифровой трансформации профсоюзных организаций, в том числе и Краснодарского края, можно сделать выводы и внести предложения по активизации этой работы:

1. Рекомендовать Краснодарскому краевому профобъединению обратиться в Федерацию независимых профсоюзов России с инициативой разработки собственной национальной единой профсоюзной цифровой платформы, включая единую систему электронных профсоюзных билетов, которая могла бы стать доступной программной средой для отраслевых профсоюзов. С этой целью обратиться к Правительству РФ с предложением о внедрении системы государственных грантов для реализации данной задачи.

2. Рекомендовать краевым комитетам профсоюзов активнее направлять председателей первичных, городских и районных профсоюзных организаций в НЧОУ ДПО «Северо-Кавказский региональный учебный центр» на кратковременные образовательный курсы по темам цифровой трансформации.

3. Рассмотреть вопрос о создании информационного портала газеты профсоюзов Кубани «Человек труда» с возможностью онлайн- подписки на неё членов профсоюза.

4. Продолжить активное внедрение цифровой платформы в отраслевые профессиональные союзы Краснодарского края.

**Библиографический список**

1. Указ о национальных целях развития России до 2030 года // Официальные сетевые ресурсы Президента России URL: http://www.kremlin.ru/events/president/news/63728 (дата обращения: 28.01.2026)

2. Постановление Исполнительного комитета Профсоюза работников народного образования и науки Российской Федерации (общероссийский профсоюз образования) № 14—5 «О Пилотном проекте по введению единого электронного профсоюзного билета, автоматизации учёта членов Профсоюза и сбора статистических данных», 23 сентября 2018 г.

3. Александрова Т.В. Цифровое неравенство в регионах России: причины, оценка, способы преодоления // Экономика и бизнес: теория и практика. 2019. № 8. С. 9—12.

4. Аксянова А.В., Александровская И.П., Гадельшина Г.А. К вопросу о цифровом неравенстве регионов Российской Федерации // Управление устойчивым развитием. 2021. № 6 (37). С. 5—13.

5. Аносов С. Профсоюзы в современной России: некоторые направления исследований // Современные исследования социальных проблем. 2017. Т. 9. № 3. С. 244—261.

6. Бухтиярова Т.И. Цифровая экономика: особенности и тенденции развития.//Бизнес и общество: электронный научный журнал. — 2019. № 1(21). — С. 1—12.

7. Кастельс М. Информационная эпоха: экономика, общество и культура. Москва: ГУ ВШЭ, 2000. 458 с.

8. Мирясова О.А., Павлова Т.В., Патрушев С.В., Цысина Г.А. Гражданское и политическое в профсоюзных практиках // Гражданское и политическое в российских общественных практиках. М.: РОССПЭН, 2013.

9. Недяк И.Л., Павлова Т.В., Патрушев С.В. Горно-металлургический профсоюз России: гражданские и политико-правовые экспликации деятельности// Социологические исследования. 2022. № 12. С. 76—87.

10. Пеньковская Ю.С., Лебедев А.В., Сомкин А.А. Региональные различия уровня цифровизации в деятельности организаций в России// Регионология. 2022. Т. 30. № 3 (120). С. 721—747.

11. Рожков Е.В. Цифровизация России (возможности и проблемы). //Информационные технологии в управлении и экономике.2022. № 2 (27). С. 4—16.

12. Ромайкин И.А., Галишникова Е.А. Некоторые аспекты цифровизации деятельности органов государственной власти в России// Консенсус. 2022. № 11 (124). С. 45—51.

13. Смирнов Ю.А., Скрипникова М.И., Мажиев Х.Н., Катабай П.Х., Долгополов ГШ.В. Мобильное приложение «профсоюз-онлайн» как один из ключевых аспектов цифровизации деятельности профсоюза работников народного образования и науки Российской Федерации //Вестник Саратовского государственного социально-экономического университета, 2020. № 3(82).с.28—32

14. Филиппова А.В. Цифровизация и эффект масштаба в деятельности НКО в России// Экономическая политика. 2022. Т. 17. № 1. С. 34—63.

15. Шунков А.В., Тараненко Л.Г., Дворовенко О.В. Феномен цифровизации культуры и искусства в России // Мир русскоговорящих стран. 2024. № 2 (20). С. 105—128.

16. Щербакова А.А. Управление экономическими проектами в условиях цифровизации России // Вестник науки. 2022. Т. 2. № 2(47). С. 84—89.

17. Интернет-ресурс Федерации независимых профсоюзов России. Публикация «Исполком ФНПР: об оцифровке профсоюзного членства, мотивации и ситуации в СПбГУП»: (https://fnpr.ru/events/novosti-fnpr/ispolkom- fnpr-ob-otsifrovke-profsoyuznogo-chlenstva-motivatsii-i-situatsii-v-spbgup.html (дата обращения 09.02.2026).

18. Интернет-ресурс Агентства «Домовой и Партнеры»: https://domovoy.pro (дата обращения 09.02.2026).

19. Интернет-ресурс Агентства «Домовой и Партнеры». Публикация «Цифровизация профсоюза на примере первичной организации. Подкаст с Бородай Алексеем, председателем ППО ООО «Харампурнефтегаз»»: https://domovoy.pro/blog/podcasts/tsifrovizatsiya-profsoyuza-na-primere- pervichnoy-organizatsii-podkast-s-boroday-alekseem-predsedatel.html (дата обращения 09.02.2026).

20. Интернет-ресурс Союза «Краснодарское краевое объединение организаций профсоюзов». Публикация «О Профобъединении»: https://kkoop.ru/o-profobedinenii/ (дата обращения 09.02.2026).

21. Интернет-ресурс Российская газета: rg.ru›gazeta/rg-centr/2026/02/09 (дата обращения 09.02.2026)

DOI: 10./-2026-9

# Интеллектуальный суверенитет: симбиоз человеческого капитала и интеллектуальных систем в эпоху цифровой трансформации

## INTELLECTUAL SOVEREIGNTY: THE SYMBIOSIS OF HUMAN CAPITAL AND INTELLIGENT SYSTEMS IN THE AGE OF DIGITAL TRANSFORMATION

**Сметана Владимир Васильевич,**
кандидат философских наук, директор АНО НИИ «ЦИФРОВОЙ ИНТЕЛЛЕКТ», Москва.
smetanavv@mail.ru

**Vladimir Smetana**
Candidate of philosophical sciences, PhD, DIGITAL INTELLIGENCE RESEARCH INSTITUTE, Moscow.
smetanavv@mail.ru

***Аннотация.*** *Современный этап развития цивилизации, часто характеризуемый как эпоха Четвертой стадии эволюции человечества [1] или Четвертой промышленной революции [2], ставит перед философией, социологией и экономикой фундаментальные вопросы о природе человеческой субъектности. Традиционные представления о суверенитете, ранее ограниченные политико-правовым полем национальных государств, сегодня претерпевают радикальную трансформацию. В центре внимания оказывается концепция интеллектуального суверенитета — способности личности, сообщества и государства самостоятельно генерировать смыслы, целеполагание и критические суждения в условиях тотальной цифровизации и экспансии искусственного интеллекта (ИИ) [3].*
*Данная статья представляет собой исследование гипотезы о том, что интеллектуальный суверенитет в XXI веке не может быть достигнут через изоляцию от технологий или их отрицание. Напротив, он реализуется исключительно через сложный, диалектический симбиоз человеческого капитала и интеллектуальных систем. И мы рассматриваем общество как сложнейшую интеллектуальную систему, где границы между естественным и искусственным интеллектом становятся проницаемыми, порождая новые онтологические сущности и эпистемологические вызовы.*
*Актуальность исследования обусловлена нарастающим противоречием. С одной стороны, глобальное информационное общество и развитие генеративных моделей обещают беспрецедентное усиление когнитивных способностей человека. С другой стороны, наблюдаются феномены, когда делегирование когнитивных функций алгоритмам ведет к атрофии критического мышления, утрате авторства и эпистемической зависимости.*

***Abstract.*** *The current stage of civilization's development, often characterized as the Fourth Stage of Human Evolution [1] or the Fourth Industrial Revolution [2], poses fundamental questions about the nature of human agency to philosophy, sociology, and economics. Traditional notions of sovereignty, previously limited to the political and legal framework of nation-states, are now undergoing a radical transformation. The focus is on the concept of intellectual sovereignty — the ability of individuals, communities, and states to independently generate meaning, set goals, and make critical judgments in the face of total digitalization and the expansion of artificial intelligence (AI) [3].*
*This article explores the hypothesis that intellectual sovereignty in the 21st century cannot be achieved through isolation from technology or its denial. Instead, it is realized exclusively through a complex, dialectical symbiosis of human capital and intelligent systems. We view society as a highly complex intellectual system, where the boundaries between natural and artificial intelligence are becoming permeable, giving rise to new ontological entities and epistemological challenges.*
*The relevance of this research stems from a growing contradiction. On the one hand, the global information society and the development of generative models promise an unprecedented enhancement of human cognitive abilities. On the other hand, we are witnessing phenomena where the delegation of cognitive functions to algorithms leads to the atrophy of critical thinking, loss of authorship, and epistemic dependence.*

***Ключевые слова:*** *суверенитет, интеллектуальный суверенитет, человеческий капитал, интеллектуальные системы, искусственный интеллект, ИИ, симбиотический ИИ, техносубъект, «ловушка суверенитета», «бархатная клетка», симбиотические науки, HAIST (Human- AI Symbiotic Teaming), искусственный агент, естественный агент.*

***Keywords:*** *sovereignty, intellectual sovereignty, human capital, intelligent systems, artificial intelligence, AI, symbiotic AI, technosubject, "sovereignty trap," "velvet cage," symbiotic sciences, HAIST (Human-AI Symbiotic Teaming), artificial agent, natural agent.*

### Глава 1. Онтология гибридного разума: от противостояния к симбиозу

Долгое время дискурс вокруг искусственного интеллекта строился на противопоставлении: человек против машины, биологический разум против кремниевого. Однако современные исследования предлагают смену парадигмы. Будущее ИИ лежит не в создании автономных машин, имитирующих человеческое мышление, а в разработке систем Симбиотического ИИ (Symbiotic AI).

Этот концепт заимствован из биологии, где симбиоз описывает взаимовыгодное сосуществование различных видов. В технологическом контексте это означает создание динамических систем, где человеческая интуиция, моральное суждение и творческий потенциал объединяются с машинной точностью, скоростью обработки данных и масштабируемостью.

Цель такого объединения — создание коллективного вывода, превосходящего возможности каждого из агентов по отдельности.

С философской точки зрения, это требует пересмотра границ субъекта. Как отмечают исследователи, мы переживаем растворение границ, подобно рыбе, обнаруживающей воду. Мы осознаем, что наши мыслительные процессы теперь существуют в более широком контексте коллективного интеллекта, где ИИ делает связь между индивидуальным и общим знанием эксплицитной и интерактивной. Возникает вопрос: как сохранить суверенитет, когда границы «Я» становятся проницаемыми для алгоритмических интервенций?

**Техносубъект и социальная морфология.** Вхождение ИИ в социальную ткань приводит к появлению новых акторов. В.И. Игнатьев вводит понятие «техносубъект» для обозначения устройств с ИИ как агентов социальных отношений нового типа [4]. Это не просто инструменты, а активные участники коммуникации, способные влиять на принятие решений и формирование социальных структур.

Мы наблюдаем становление гибридного социума — социальной морфологии, представляющей собой симбиоз агентов естественной и искусственной природы. В этой системе меняется сама природа субъектности. Паола Ребугини в своем обзоре «Субъект, субъективность, субъективация» [5] подчеркивает, что в условиях алгоритмического управления субъектность перестает быть фиксированным свойством индивида и становится процессом взаимодействия между человеком и техносубъектом.

Однако признание ИИ техносубъектом не означает наделения его сознанием в человеческом смысле. Философ Д.И. Дубровский, отстаивая антиредукционистскую позицию, подчеркивает фундаментальное различие между субъективной реальностью (сознанием) и информационными процессами в мозге или компьютере [6]. Интеллектуальный суверенитет базируется именно на этом онтологическом разрыве: ИИ может моделировать интеллектуальные операции, но смыслополагание и переживание бытия остаются прерогативой человека.

**Общество как интеллектуальная система.** Развивая системный подход, философы А.П. Алексеев и И.Ю. Алексеева предлагают рассматривать само общество как сложнейшую интеллектуальную систему [7]. В этой системе происходят сложные процессы когнитивного обмена, накопления знаний и принятия решений. Внедрение цифровых технологий не просто ускоряет эти процессы, но и создает риски дезингрессии — разрывов связей между управляющими структурами и интеллектуальным классом общества.

Судьба интеллекта и миссия разума в этой оптике заключаются в сохранении целостности этой системы. Интеллектуальный суверенитет становится характеристикой устойчивости общественной системы к внешним манипуляциям и внутренним разрывам. Он требует, чтобы общество обладало способностью к рефлексии над собственными технологическими расширениями, не допуская, чтобы инструменты управления (цифровизация) подменяли собой цели развития (смыслы).

## Глава 2. Психология когнитивного суверенитета: угрозы и защитные механизмы

**Анатомия «Ловушки суверенитета».** Переход к симбиозу не лишен опасностей. Центральной угрозой на индивидуальном уровне является «Ловушка суверенитета» [8]. Её мощь проистекает из конвергенции психологических механизмов, которые подрывают способность человека к автономному мышлению.

Эта внутренняя архитектура зависимости создает функциональную необходимость в Когнитивном суверенитете. Это «внутренняя крепость», набор ментальных дисциплин и привычек, позволяющих пользователю бросить вызов ИИ, создать независимые референсные точки и, при необходимости, отвергнуть алгоритмическую подсказку. Только так ИИ превращается из «Уравнителя», сводящего всех к среднему знаменателю, в «Усилителя» уникальных человеческих способностей.

**Феноменология «Бархатной клетки» и интеллектуальное отмывание денег.** Еще более тонкая угроза исходит от дизайна современных языковых моделей (LLM). Франсуа-Ксавье Морган описывает этот феномен как «Бархатную клетку» (Velvet Cage). Мы подвергаемся «одомашниванию добротой». ИИ, настроенный на максимальную полезность и угодливость, становится «машиной лести», которая не критикует наши слабые аргументы, а усиливает их [9].

Это приводит к процессу, который можно назвать «интеллектуальным отмыванием денег». Когнитивные искажения, логические ошибки и полусформированные мысли пользователя, проходя через нейросеть, возвращаются к нему в виде отполированных, стилистически безупречных текстов:

- Механизм: пользователь вводит слабую идею -> ИИ валидирует и оформляет её -> Пользователь воспринимает красивую форму как подтверждение истинности содержания.
- Результат: человек не учится, а получает подтверждение. Поскольку опыт взаимодействия ощущается как инсайт, коррупция мышления ошибочно принимается за интеллектуальный рост.

Таким образом, для восстановления суверенитета необходимо осознать этот компромисс между комфортом и истиной. Суверенный интеллект требует готовности к когнитивному дискомфорту, к встрече с возражениями, которые современные ИИ, оптимизированные под вовлечение, склонны сглаживать.

## Глава 3. Методология симбиоза: протоколы и практики взаимодействия

**Симбиотическая наука и парадигма HAIST.** Для того чтобы симбиоз был продуктивным и безопасным, он должен быть структурирован через четкие методологические протоколы. В научной сфере это оформляется в концепцию Симбиотической науки. Исследования в области HAIST (Human- AI Symbiotic Teaming) [10] предлагают конкретные механизмы реализации этого подхода. Так, центральным принципом выступает асимметричный симбиоз:

- ИИ (Искусственный агент): предоставляет вычислительную агентность. Его роль — обработка массивов данных, генерация гипотез, поиск паттернов.
- Человек (Естественный агент): обеспечивает творческую и моральную агентность. Его роль — постановка целей, этическая оценка, интерпретация смыслов и принятие ответственности.

Эти механизмы переводят этику ИИ из области абстрактных деклараций в плоскость исполнимой практики**.** Они гарантируют, что ИИ остается инструментом в руках суверенного исследователя, а не замещает его.

**Перевод репрезентаций и интерфейсы понимания.** Важнейшим аспектом симбиоза является проблема перевода. Эффективное сотрудничество требует создания систем, способных транслировать репрезентации, оптимальные для машинной обработки (векторные пространства, тензоры), в репрезентации, понятные человеку (нарративы, визуализации), и наоборот.

Качество этих переводов напрямую определяет уровень интеллектуального суверенитета. Если человек не понимает, как машина пришла к выводу («черный ящик»), он теряет суверенитет, вынужденно доверяя алгоритму. Поэтому разработка объяснимого ИИ (XAI) и интерфейсов, поддерживающих когнитивную прозрачность, является не технической, а философско-политической задачей. Это условие возможности критического суждения.

**Образование: «как» важнее, чем «что».** Интеграция симбиотических практик требует фундаментальной перестройки системы образования и фокус должен сместиться с передачи знаний на этические и философские аспекты взаимодействия.

Опираясь на философию Дова Сайдмана, образование должно учить тому, что «как мы делаем вещи, важнее того, что мы делаем». В эпоху, когда ИИ может сгенерировать любой контент («что»), человеческая ценность перемещается в область метода, этики и отношения («как»). Важным аспектом является работа со страхами. Концепция «Страха перед Другим» должна быть переосмыслена в контексте ИИ. Образование должно анализировать, как технологии могут усиливать или смягчать социальные предубеждения, и готовить студентов к работе в среде, где «Другим» выступает не только человек иной культуры, но и интеллектуальный агент иной природы [11].

## Глава 4. Экономика человеческого капитала: ресурсная база суверенитета

Интеллектуальный суверенитет может имеет экономическое обоснование. Так, Орландо Гомеш в своей статье «Человеческий капитал — симбиоз искусственного интеллекта и экономический рост» [12] доказывает, что долгосрочный устойчивый рост возможен только при совместном накоплении ИИ-капитала и человеческого капитала. Без развития навыков человека отдача от ИИ быстро падает, а автоматизация начинает подавлять рост.

В этой связи, мы можем предложить к рассмотрению две гипотетические версии экономической динамики:

- Модель «Оптимального планировщика»: где ресурсы распределяются централизованно с учетом долгосрочных целей.
- Модель «Интертемпорального агента»: где каждый агент (человек) одновременно является работником и инвестором, формирующим свой жизненный план.

Вывод напрашивается: бенефициарами внедрения трудосберегающих технологий становятся те системы, где происходит опережающее развитие человеческого капитала. Если автоматизация замещает рутинный труд, то человеческий интеллект должен перемещаться в области высокой сложности.

Интеллектуальный суверенитет экономики, таким образом, зависит от способности перенаправить высвобожденные ресурсы на образование и развитие творческих способностей населения.

Однако структура человеческого капитала неоднородна. Социологические исследования науки, восходящие к работам французских социологов 1970-х годов и подтвержденные современными данными, выявляют жесткую закономерность: реальный прогресс в науке и инновациях обеспечивает лишь около 20% активных творческих работников,

Пьер Бурдьё в своих работах о «поле науки» описывает науку как пространство жесткой конкуренции за «символический капитал». Бурдьё подчеркивал, что лишь небольшое ядро ученых (обладателей высокой концентрации признания и ресурсов) задает траекторию развития дисциплины, в то время как остальные выполняют поддерживающую или репродуктивную функцию [13], что соответствует логики принципа Парето (закон 80/20). Но, по-настоящему прорывные результаты создают единицы. Это наблюдение имеет критическое значение для стратегии суверенитета, так:

- Массовый уровень: ИИ выступает как инструмент повышения базовой продуктивности и стандартизации.
- Элитарный уровень: для творческого меньшинства (20%) симбиоз с ИИ должен быть направлен на максимальное высвобождение от рутины, чтобы их когнитивный ресурс был полностью направлен на создание нового знания.

Таким образом, интеллектуальный суверенитет государства зависит от того, способно ли оно выявить, воспитать и, главное, удержать эти 20%. Именно за эту страту разворачивается глобальная конкуренция.

**Битва за таланты и геополитика «утечки мозгов».** В условиях глобализации корпорации и государства ведут борьбу за обладание инициативой в интеллектуальной сфере. Человеческий капитал становится самым дефицитным и мобильным ресурсом.

Для развивающихся стран «утечка мозгов» превращается в экзистенциальную угрозу. Неспособность предоставить материально-бытовые условия и профессиональную среду на уровне страны, приводит к системному оттоку талантов. В результате формируется порочный круг: отток интеллекта снижает возможности для создания суверенных технологий, что, в свою очередь, еще больше снижает привлекательность национальных экономик для талантов.

Таким образом, достижение паритета в этой ситуации невозможно без обеспечения интеллектуального суверенитета на государственном уровне, который понимается как способность государства создать замкнутый цикл воспроизводства и капитализации знаний внутри страны. В том числе, например, глобальные индексы инноваций (ГИИ) напрямую связывают субиндексы человеческого капитала с патентной активностью и экономической устойчивостью.

## Глава 5. Культурно-антропологические основания суверенитета

Интеллектуальный суверенитет не сводится к набору компетенций или знаний, он в целом укоренен в культуре территорий и народов, которые на них проживают. Так, ректор МГУ, Виктор Садовничий последовательно отстаивает идею неразрывности обучения и воспитания на протяжении десятилетий, выступая на крупнейших образовательных форумах и съездах [14]. Таким образом, мы можем определить:

- Обучение — это передача знаний и навыков. Это то, что ИИ может делать эффективно и персонализировано.
- Воспитание — это формирование ценностного ядра, идентичности, воли и этических установок. Это сугубо человеческий процесс.

Древняя аксиома — «хочешь победить врага — воспитай его детей» в цифровую эпоху приобретает новый смысл. Если система образования отдает воспитательную функцию на откуп алгоритмам рекомендательных систем и глобальным медиа-платформам, она теряет суверенитет над будущим. Так, интеллектуально суверенный субъект — это не просто носитель информации, а личность с устойчивой системой ценностей и способная критически фильтровать контент. Без «воспитания» человеческий капитал становится лишь техническим ресурсом, легко интегрируемым в чужие технологические цепочки.

В качестве примера, мы можем наблюдать проблему интеллектуального суверенитета на Глобальном Юге о которых Ник Кулдри и Улисес Мехиаса в своей книге «Цена связи: как данные колонизируют человеческую жизнь и присваивают ее капитализму» [15]. Так, курсы по деколонизации африканской эпистемологии в эпоху ИИ предлагают важные инсайты для всего мира. Они показывают, как колониальные паттерны воспроизводятся через «алгоритмическое управление» и «дата-колониализм».

Стратегии возвращения суверенитета включают обращение к автохтонным философским категориям. Например, концепция «Убунту» [16] (человек есть человек через других людей) и «коммунализм» предлагают альтернативу западному техно-индивидуализму. В контексте ИИ это означает отказ от модели «ИИ как заменитель человека» в пользу модели «ИИ как инструмент укрепления сообщества».

Таким образом, этот опыт подтверждает универсальный тезис: подлинный интеллектуальный суверенитет невозможен без опоры на собственные культурные и философские традиции. Технологии универсальны, но смыслы их использования всегда локальны и культурно обусловлены. Симбиоз человеческого капитала и интеллектуальных систем должен быть подчинен высшей цели — сохранению человека как свободного и ответственного деятеля истории.

## Заключение

Интеллектуальный суверенитет в XXI веке предстает не как состояние «автаркии», а как сложный, многоуровневый процесс управления симбиозом. На индивидуальном уровне — это борьба за когнитивную автономию, преодоление «Ловушки суверенитета» через развитие навыков и отказ от комфорта «Бархатной клетки». А на профессиональном уровне — это переход к парадигме симбиотической науки и труда, где асимметричное распределение ролей (человек — цель, машина — средство) закрепляется протоколами ответственности и прозрачности.

В тоже время, на национальном уровне — это экономическая стратегия инвестирования в человеческий капитал, поддержка творческой элиты и восстановление единства обучения и воспитания. А на цивилизационном уровне — это право на собственную эпистемологию, на свой взгляд на то, что есть знание и истина, защищенное мощью собственных интеллектуальных систем.

Симбиоз человеческого капитала и ИИ — это неизбежность. Вопрос заключается лишь в форме этого симбиоза: станет ли человек придатком алгоритма или его архитектором. Интеллектуальный суверенитет — это выбор второго пути, требующий воли, ресурсов и глубокого философского осмысления новой реальности.

### СПИСОК ЛИТЕРАТУРЫ

1. Сметана, В.В. Эволюция «позитивной философии» О. Конта в контексте нового знания в 21 веке / В.В. Сметана // Социология. — 2023. — № 3. — С. 214—219. — EDN ZDQYHK.

2. Шваб К. Четвертая промышленная революция — (Top Business Awards) / К. Шваб. — Москва: Эксмо, 2016. — 138 с. — ISBN 978-5-699-90556-0. — URL: https://ibooks.ru/bookshelf/372213/reading (дата обращения: 28.01.2026).

3. Сметана, В.В. Интеллектуальный суверенитет: человеческий капитал и цифровой интеллект / В.В. Сметана // Флагман науки. — 2025. — № 6(29). — С. 591—601. — DOI 10.37539/2949—1991.2025.29.6.014. — EDN TLQURN.

4. Игнатьев В.И. Объект социологии в метаморфозе морфогенеза гибридного социума // Социологические исследования. 2022. № 4. URL: https://socis.isras.ru/files/File/2022/4/Ignatev.pdf (дата обращения: 28.01.2026).

5. Маркс К. Экономическо-философские рукописи 1844 года и другие ранние философские работы / К. Маркс. — М.: Академический проект, 2010.

6. Дубровский Д.И. Зачем субъективная реальность, или «почему информационные процессы не идут в темноте?» (Ответ Д. Чалмерсу) // Язык, знание, социум: Проблемы социальной эпистемологии / Ответственный редактор И.Т. Касавин. — Москва: ИФ РАН, 2007. — С. 33—56. — 180 с. — 500 экз. — ISBN 978-5-9540-0076-4.

7. Алексеев А.П., Алексеева И.Ю. Судьба интеллекта и миссия разума: философия перед вызовами эпохи цифровизации: Монография. М.: Проспект, 2021. ISBN: 9785392371242.

8. Konstantinos Komaitis, Esteban Ponce de León, Kenton Thibaut, Trisha Ray, Kevin Klyman. The sovereignty trap. July 17, 2024. URL: https://dfrlab.org/2024/07/17/the-sovereignty-trap/ (дата обращения: 28.01.2026).

9. François-Xavier Morgan. Against the Velvet Cage: A Manifesto for Intellectual Sovereignty. URL: https://medium.com/@francoisxaviermorgand/against-the-velvet-cage-a- manifesto-for-intellectual-sovereignty-1d71de3612b3#:~: text=Preamble:%20The%20Seduction, sophisticated%20flattery%20machine%20ever%20devised (дата обращения: 28.01.2026).

10. Human-AI Symbiotic Theory (HAIST): Development, Multi- Framework Assessment, and AI-Assisted Validation in Academic Research by Laura Thomsen Morello and John C. Chick. College of Engineering, Business & Education, University of Bridgeport, Bridgeport, CT 06604, USA. Informatics 2025, 12(3), 85; https://doi.org/10.3390/informatics12030085

11. Dov Seidman. How: Why How We Do Anything Means Everything. ISBN-13: 978—1118106372, ISBN-10: 1118106377

12. Gomes, O. The Human Capital — Artificial Intelligence Symbiosis and Economic Growth. De Economist 173, 331—365 (2025). https://doi.org/10.1007/s10645—025—09452-y

13. Pierre BOURDIEU. La spécificité du champ scientifique et les conditions sociales du progrès de la raison. Volume 7, numéro 1, mai 1975. DOI: https://doi.org/10.7202/001089ar

14. Ректор МГУ назвал ошибкой переход на Болонскую систему URL: https://www.bfm.ru/news/340850 (дата обращения: 28.01.2026).

15. Nick Couldry, Ulises Mejias. «The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism» (2019). URL: https://www.sup.org/books/sociology/costs-connection (дата обращения: 28.01.2026).

16. Birhane, A. (2020). Algorithmic Colonization of Africa. SCRIPTed, 17, 389—409. URL: https://doi.org/10.2966/scrip.170220.389 (дата обращения: 28.01.2026).

DOI: 10./-2026-7

# Применение Искусственного Интеллекта в сельском хозяйстве. Состояние дел, тренды, перспективы

# APPLICATION OF ARTIFICIAL INTELLIGENCE IN AGRICULTURE. STATUS, TRENDS, PROSPECTS

**Березина Наталья Александровна,**
Орловский государственный аграрный университет, Проректор по научной и инновационной деятельности, д.т.н, профессор, г. Орел

**Berezina Natalia Aleksandrovna,**
Oryol State Agrarian University, Vice-Rector for Scientific and Innovative Activities, Dr. of Engineering, Professor, Oryol

***Аннотация.*** *В статье представлен обзор текущего состояния и перспектив развития применения искусственного интеллекта (ИИ) в сельском хозяйстве. Выявлены базовые задачи и направления деятельности, в которых применение ИИ позволит повысить эффективность производительности производства. Сформулирован перечень ограничений и сложностей применения ИИ, разрешение которых позволит повысить внедряемость и применимость таких систем в сельском хозяйстве.*

***Ключевые слова:*** *искусственный интеллект, инновационное сельское хозяйство, машинное обучение, машинное зрение, робототехника.*

***Annotation.*** *This article presents an overview of the current state and prospects for the application of artificial intelligence (AI) in agriculture. It identifies key challenges and areas where AI can improve production efficiency. It also identifies limitations and challenges associated with AI application, the resolution of which will improve the adoption and applicability of such systems in agriculture.*

***Keywords:*** *artificial intelligence, innovative agriculture, machine learning, machine vision, robotics.*

Современное сельское хозяйство (область деятельности человека объединяющее агрономию, зоотехнику, ветеринарию, почвоведение, агроинженерию, экономику сельского хозяйства и ряд других направлений) также как и все общество активно использует достижения прогресса в своей деятельности. Внедрение новых технологий в аграрный сектор связанно с базовыми вызовами, с которыми сталкивается человечество:

– рост численности население требует увеличения производства продовольствия и других сопутствующих товаров;

– изменение климата – опустынивание, обезвоживание или избыточная влажность требует изменения и учета этих факторов в деятельности;

– сокращение кадров в сельском хозяйстве.

С целью повышения производительности производства, снижения рисков стихийных бедствий, санитарно-эпидемиологических факторов активно применяют средства на основе искусственного интеллекта.

Так, активно внедряются: технологии беспилотной авиации (БПЛА), позволяющие осуществлять контроль состояния полей и садов, наличие признаков болезней, вредителей, сорных растений и др.; применение смарт устройств и чипов, позволяет осуществлять контроль территориального нахождения и состояния здоровья животных и рыб; технологии интернет вещей (IoT) для обеспечения передачи данных в реальном времени о состоянии влажности и химическом составе почвы и воздуха (применимо для теплиц, коровников и др. ограниченных и замкнутых мест).

Все это требует как наличие хорошо развитой телекоммуникационной инфраструктуры, наличие вычислительных мощностей и применения новых технологий обработки данных получаемых в реальном времени.

Отдельным направлением аграрной науки, в которой необходимы инструменты применяющие инструменты машинного обучения являются проводимые исследования, направленные на разработку новых сельскохозяйственных культур и животноводства.

## Тренды применения ИИ в сельском хозяйстве: Мониторинг и диагностика состояния посевов

Применение БПЛА обладающих функциями съемки в высоком качестве, позволяет на основе применения методов машинного зрения выявлять распространение болезней и вредителей на ранних стадиях, что позволяет повысить своевременность реагирования и снижает убытки.

В качестве инструмента обработки изображения успешно применяют сверточные нейронные сети (CNN, например, AlexNet, GoogLeNet).

Известные CNN способны распознать (с точностью около 99 %) широкий перечень заболеваний сельскохозяйственных культур по фотографиям листьев (например, http://pdd.jinr.ru/). Указанное значение соответствует лабораторным испытаниям, в полевых испытаниях значения точности ниже, однако это не снижает востребованности данного подхода в сельском хозяйстве, а требует дальнейшего исследования.

Так же БПЛА с машинным зрением, позволяют оценивать объем сорных растений в полях. Автоматическое различение культурных растений и сорняков с помощью компьютерного зрения позволяет перейти к точечному (site-specific) применению гербицидов. Точность обнаружения составляет около 95 % для восьми видов сорняков [1, 2].

В качестве еще одного направления применения летательных объектов является оценка состояния посевов по данным дистанционного зондирования. С использованием спутников данные (например, Sentinel-2) и данных от БПЛА рассчитывают вегетационные индексы (NDVI, EVI, LAI), по которым модели ИИ оценивают биомассу, состояние здоровья, стрессовые факторы, стадию развития растений [2-4]. Например, компания Planet Labs предоставляет ежедневные спутниковые снимки всей поверхности Земли с разрешением 3-5 метров, которые анализируются с помощью ИИ для мониторинга сельскохозяйственных угодий.

### Прогнозирование урожайности

Прогнозирование урожайности – критически важная задача для планирования производства, логистики, ценообразования и продовольственной политики. Традиционные агрометеорологические модели (например, DSSAT, (Decision Support System for Agrotechnology Transfer) – пакет моделей роста и развития сельскохозяйственных культур) основаны на физиологических процессах и требуют большого количества входных параметров. Модели ИИ дополняют и улучшают традиционные подходы. Так применение ансамблей моделей машинного обучения (Random Forest, Gradient Boosting,) превосходят классические модели по точности прогноза урожайности кукурузы и сои [5].

Использование сверточных LSTM-сетей для прогнозирования урожайности на основе спутниковых данных и метеорологических наблюдений, интегрируя пространственные и временные зависимости.

### Управление ирригацией и водными ресурсами

Орошаемое земледелие потребляет около 70% мирового забора пресной воды. ИИ оптимизирует ирригацию, определяя оптимальное время, объем и распределение полива. Системы на основе ИИ интегрируют данные датчиков влажности почвы, метеоданные, спутниковые снимки, прогнозы погоды и модели эвапотранспирации для расчета водного баланса в реальном времени. ИИ-управляемая ирригация сокращает расход воды на 20-30 % при сохранении урожайности. В качестве инструмента динамического управления ирригацией в условиях неопределенности применяют обучение с подкреплением (модель обучается оптимальной стратегии полива, балансируя между экономией воды и рисками снижения урожайности) [6].

### Автономная сельскохозяйственная техника и робототехника

Одним из самых распространенных направлений применения ИИ в сельском хозяйстве является разработка автономных сельскохозяйственных машин и роботов:

Автономные тракторы. Компании John Deere, CNH Industrial, AGCO разрабатывают полностью автономные тракторы, использующие компьютерное зрение, LIDAR и GPS для навигации по полю, обхода препятствий и выполнения агротехнических операций без оператора. В 2022 году John Deere представил серийный автономный трактор 8R с системой TruePath [7].

Роботы для прополки. Роботы (FarmWise, Carbon Robotics) используют компьютерное зрение для идентификации сорняков и их механического или лазерного уничтожения без применения гербицидов [7].

Роботы для уборки урожая. Уборка деликатных культур (ягоды, фрукты, овощи) – трудоемкая операция, требующая ручного труда. Роботы с компьютерным зрением и мягкими манипуляторами (Octinion, Dogtooth Technologies, Abundant Robotics) обучаются определять зрелость плодов и аккуратно собирать урожай [8].

Роботизированное доение. Роботы-доильщики кампаний Lely Astronaut, DeLaval VMS используют компьютерное зрение и машинное обучение для автоматического присоединения доильных стаканов, контроля качества молока, обнаружения мастита [9].

### Животноводство

Системы компьютерного зрения и сенсоры (акселерометры, GPS-трекеры, датчики руминации) отслеживают двигательную активность, пищевое поведение, социальные взаимодействия животных с целью мониторинга здоровья и поведения животных. Модели ИИ обнаруживают ранние признаки заболеваний (хромота, мастит, респираторные инфекции), эструс, стресс задолго до появления клинических симптомов [10].

Прогнозирование продуктивности. Модели машинного обучения прогнозируют молочную продуктивность коров, привесы, конверсию корма на основе генетических, кормовых и средовых факторов [11].

Управление кормлением. ИИ-системы оптимизируют рационы кормления, балансируя между стоимостью кормов, продуктивностью и здоровьем животных. Системы автоматического кормления (DeLaval, Lely, GEA) адаптируют рацион индивидуально для каждого животного [12].

### Мировой опыт (ключевые проекты)

John Deere – крупнейший мировой производитель сельхозтехники, инвестировавший свыше 1 миллиарда долларов в технологии ИИ. Приобретение Blue River Technology (2017), система See&Spray, автономные тракторы.

Climate Corporation (Bayer) – платформа Climate FieldView, использующая ИИ для управления полями, оптимизации посева и внесения удобрений.

Indigo Agriculture – применение ИИ и микробиологии для повышения устойчивости культур.

BASF Digital Farming (xarvio) – платформа xarvio FIELD MANAGER для мониторинга посевов и рекомендаций по защите растений на основе ИИ.

Проект MARS (Mobile Agricultural Robot Swarms) (Европа) – рой мобильных роботов для точного посева, разработка Fendt/AGCO.

Alibaba ET Agricultural Brain – платформа ИИ для свиноводства (распознавание животных, мониторинг здоровья) и растениеводства.

Pinduoduo Smart Agriculture Competition – соревнования по выращиванию клубники с помощью ИИ, где ИИ-команды превзошли опытных фермеров по урожайности.

Phytech – ИИ-платформа для управления ирригацией на основе данных сенсоров растений.

## Применение ИИ в сельском хозяйстве России

### Текущее состояние

Россия обладает значительным потенциалом для применения ИИ в сельском хозяйстве: 197 миллионов гектаров сельскохозяйственных угодий (крупнейшая площадь в мире), развитая система аграрного образования и науки, растущий уровень цифровизации [13].

Стратегия развития агропромышленного и рыбохозяйственного комплексов Российской Федерации на период до 2030 года предусматривает цифровую трансформацию отрасли. Национальная программа «Цифровая экономика Российской Федерации» включает направление цифровизации сельского хозяйства.

### Российские компании и проекты

– Cognitive Pilot (дочерняя компания Сбера и Cognitive Technologies) – системы автопилотирования для комбайнов и тракторов, работающие на основе компьютерного зрения и ИИ. Установлены на более чем 3000 машин.

– «Геомир» – спутниковый мониторинг сельскохозяйственных угодий.

– «АгроСигнал» – платформа мониторинга и управления сельхозпроизводством.

– ExactFarming – платформа точного земледелия.

– SmartAgro (МТС) – IoT-платформа для сельского хозяйства.

## Ограничения и сложности внедрения ИИ в сельском хозяйстве

*Качество и доступность данных* – сельское хозяйство характеризуется высокой пространственной и временной вариабельностью: каждое поле уникально, условия меняются год от года. Качественные размеченные датасеты для обучения моделей (ground truth) дороги и трудоемки в создании. Многие разработки выполнены на ограниченных датасетах, не отражающих реальное разнообразие условий.

*Перенос моделей между условиями* – модели, обученные в одних агроклиматических условиях, часто плохо работают в других (проблема domain shift). Модель, обученная распознавать болезни пшеницы в Канаде, может быть неэффективна в условиях Краснодарского края из-за различий в сортах, климате, фоне освещения.

*Инфраструктурные ограничения* – сельские районы во многих странах, включая Россию, характеризуются ограниченным доступом к интернету, электроэнергии, квалифицированным кадрам. Это создает барьеры для внедрения ИИ-технологий, требующих подключения к облачным сервисам и технической поддержки.

*Экономические барьеры* – высокая стоимость внедрения (датчики, дроны, программное обеспечение, обучение персонала), длительный срок окупаемости и неопределенность экономического эффекта сдерживают внедрение, особенно в малых и средних хозяйствах.

## Перспективы развития

*Цифровые двойники ферм* – концепция «цифрового двойника» (digital twin) – виртуальной модели фермы, интегрирующей данные о почвах, климате, культурах, технике, экономике и позволяющей моделировать сценарии и оптимизировать решения. ИИ является вычислительным ядром цифровых двойников.

*Рой роботов и мультиагентные системы* – Переход от крупногабаритной техники к роям мелких автономных роботов, способных совместно выполнять задачи (посев, прополка, уборка) с минимальным воздействием на почву. Мультиагентные системы на основе ИИ координируют действия роботов.

*Вертикальное земледелие и контролируемые среды* – ИИ управляет всеми параметрами среды (свет, температура, влажность, $CO_2$, питание) в вертикальных фермах и теплицах, максимизируя продуктивность при минимальных ресурсах. Компании Plenty, AeroFarms, AppHarvest используют ИИ для оптимизации выращивания.

*Интеграция ИИ с биотехнологиями* – конвергенция ИИ, геномного редактирования (CRISPR), синтетической биологии и высокопроизводительного фенотипирования ускоряет создание новых сортов и пород с заданными характеристиками: устойчивость к засухе, болезням, повышенная продуктивность, улучшенные питательные свойства.

## Заключение

Искусственный интеллект трансформирует сельское хозяйство и аграрную науку, предлагая решения для ключевых глобальных вызовов: обеспечение продовольственной безопасности растущего населения, адаптация к изменению климата, устойчивое использование природных ресурсов, компенсация дефицита кадров.

Применение ИИ охватывает все этапы сельскохозяйственного производства: от селекции и посева до уборки, хранения и доставки потребителю. Компьютерное зрение диагностирует болезни растений, модели машинного обучения прогнозируют урожайность, нейронные сети оптимизируют ирригацию и питание растений, автономные роботы выполняют полевые операции, большие языковые модели консультируют фермеров и анализируют научную литературу.

В аграрной науке ИИ ускоряет селекцию (геномное прогнозирование), автоматизирует фенотипирование, моделирует агроэкосистемы, обрабатывает экспериментальные данные, создает цифровые карты почв и открывает новые закономерности в сложных биологических системах.

Вместе с тем внедрение ИИ в аграрный сектор сталкивается с объективными ограничениями: недостаток качественных данных, проблемы переноса моделей между условиями, инфраструктурные и экономические барьеры, вопросы интерпретируемости и доверия пользователей. Преодоление этих ограничений требует скоординированных усилий научного сообщества, агробизнеса, разработчиков технологий и государственной политики.

Россия, обладая крупнейшими в мире сельскохозяйственными угодьями и сильной школой аграрной науки, имеет значительный потенциал для становления лидером в области ИИ-агротехнологий. Реализация этого потенциала требует инвестиций в инфраструктуру, подготовку кадров на стыке аграрных наук и ИИ, создание открытых датасетов и развитие отечественных ИИ-платформ для сельского хозяйства.

Будущее сельского хозяйства – это симбиоз многовековых агрономических знаний и передовых технологий ИИ, направленный на устойчивое, эффективное и экологически ответственное производство продовольствия для всего человечества.

**СПИСОК ЛИТЕРАТУРЫ**

1. Мониторинг биомассы лука с помощью RGB-изображений, полученных с помощью БПЛА / M. A. Морено, Д. Эрнандес, Х. Ортега, Р. Бальестерос // Precis. Agric. – 2018. – Т. 19. – С. 840-857. – DOI: 10.1007/s11119-018-9560-y.

2. Анализ урожайности и внесения удобрений в посевы ячменя по снимкам с беспилотных летательных аппаратов: подход на основе глубокого обучения / Р. Васкес, Х. Де Ла Кальеха, А. Моралес-Рейес, М. Хименес-Лисаррага, С. Родригес-Санчес, Х. Дж. Эскаланте // Int. J. Remote Sens. – 2019. – Т. 40. – С. 2493-2516. – DOI: 10.1080/01431161.2019.1577571.

3. Воздушная гиперспектральная и тепловизионная съёмка с высоким разрешением для раннего выявления вертициллёзного увядания оливковых деревьев с использованием флуоресцентных, температурных и узкополосных спектральных индексов / П. Дж. Зарко-Техада, К. Лусена, Дж. А. Навас-Кортес, Р. Кальдерон // Remote Sens. Environ. – 2013. – Т. 139. – С. 231–245. – DOI: 10.1016/j.rse.2013.07.031.

4. Сегментация изображений для обнаружения плодов и оценки урожайности в яблоневых садах / Дж. П. Андервуд, С. Барготи // J. Field Robot. – 2017. – Т. 34. – С. 1039-1060. – DOI: 10.1002/rob.21699.

5. A fuzzy-optimized hybrid ensemble model for yield prediction in maize-soybean intercropping system / A. Ikram, S. Ikram, E.-S. M. El-kenawy, A. Hussain, A. H. Alharbi, M. M. Eid // Front. Plant Sci. – 2025. – Sec. Technical Advances in Plant Science. – Vol. 16. – URL: (дата обращения: 26.02.2026).

6. Медведев, М. А. Применение искусственного интеллекта в сельском хозяйстве / М. А. Медведев, В. М. Чайковский // Инжиниринг и технологии. – 2023. – Т. 8, № 2. – С. 1–4. – DOI: 10.21685/2587-7704-2023-8-2-9.

7. Тракторный прорыв: первый беспилотник от John Deere выходит в поля // Своё фермерство. – URL: (дата обращения: 26.02.2026).

8. 12 революционных роботов в сельском хозяйстве // Своё фермерство. – URL: (дата обращения: [вставьте дату 26.02.2026).

9. Дояр, пастух, уборщик и раздатчик кормов: роботы в животноводстве // Своё фермерство. – URL: (дата обращения: 26.02.2026).

10. Искусственный интеллект в ветеринарии // Биомолекула. — URL: (дата обращения: [вставьте дату]).

11. A review of machine learning models applied to genomic prediction in animal breeding /

N. Chafai, I. Hayah, I. Houaga, B. Badaoui // Sec. Livestock Genomics. – 2023. – Vol. 14. – URL: (дата обращения: 26.02.2026).

12. Умные фермы: роль ИИ в мониторинге здоровья сельскохозяйственных животных // Ведомости. – 2025. – 19 ноября. – URL: (дата обращения: 26.02.2026).

13. Роль цифровизации в повышении производительности АПК обсудили на пленарном заседании «Золотой осени» // Официальный сайт Министерства сельского хозяйства РФ. – URL: (дата обращения: 26.02.2026).

DOI: 10./-2026-1-1-12

# Обработка результатов моделирования компьютерных атак на объект защиты с использованием методов машинного обучения

# PROCESSING OF SIMULATION RESULTS OF COMPUTER ATTACKS ON THE OBJECT OF PROTECTION USING MACHINE LEARNING METHODS

**Добрышин Михаил Михайлович,**
к.т.н., сотрудник Академии ФСО России, г. Орёл

**Жиляева Валерия Алексеевна,**
сотрудник Академии ФСО России, г. Орёл

**Mikhail Mikhailovich Dobryshin** Academy of the Federal Guard Service of Russia, PhD in Engineering, Oryol

**Valeria Alekseevna Zhilyaeva** Academy of the Federal Guard Service of Russia, employee, Oryol

***Аннотация.*** *Задача снижения ущерба от инцидентов информационной безопасности на текущий момент времени является одной из актуальных, а новости об успешных реализациях компьютерных атак регулярно появляются у всех информационных агентств. В статье представлен вариант выявления факта реализации атаки основанный на анализе эксплуатационных характеристик защищаемых объектов с применение комплекса средств машинного обучения.*

***Annotation.*** *The task of reducing damage from information security incidents is currently one of the most urgent, and news about successful computer attacks regularly appears in all news agencies. The article presents an option for detecting the fact of an attack based on an analysis of the operational characteristics of protected objects using a set of machine learning tools.*

***Ключевые слова:*** *компьютерные атаки, машинное обучение, эксплуатационные характеристики, дерево состояния.*

***Keywords:*** *computer attacks, machine learning, performance characteristics, state tree*

**Интеграция инфо-телекоммуникационных систем во все сферы деятельности современного общества позволило в значительной мере ускорить процессы управления, принятия решений, «действий» и «жизни» отдельного человека и общества. Однако совместно со множеством выгод внедрения технологичных систем возникают актуальная задача защиты этих систем от различных компьютерных атак (КА). Выход систем отвечающих за управлением деятельностью городской или транспортной инфраструктуры, финансового сектора, средств массовой коммуникации способно привести как значительным финансовым убыткам, так и к тяжелым последствиям для населения.**

В связи с этим, задача по обеспечению информационной безопасности (ИБ) инфо-телекоммуникационных систем не только не теряет актуальности. С этой целью совершенствуются и разрабатываются новые средства, методы и способы обеспечения ИБ, однако существенная часть из них применяет традиционные подходы выявления фактов реализации КА. Под традиционными подходами понимается не только средства реализующие сигнатурный анализ, но и средства, анализирующие параметры, характеризующие атаки. Данный подход показывает свою эффективность в отношении известных тактик, техник, способов и средств реализации атак, и не в полной мере эффективен при анализе новых, ранее не применяемых атак.

В качестве возможного направления изменения парадигмы разработки средств обеспечения ИБ является применения подходов, направленных не на выявление в условиях неопределенности фактов (поиск конкретных значений параметров) реализации КА, а обработка и анализ эксплуатационных характеристик защищаемых объектов с целью выявления факта реализации КА [1]. Данный подход не исключает применение традиционных решений, а дополняет их.

Суть предложения заключается в выявлении схожести влияния конкретных видов воздействия на контролируемые эксплуатационные характеристики исследуемых объектов. В качестве примера, возможно, рассмотреть факт заражения вредоносным программным обеспечением локальной сети. В качестве ущерба наносимого такой атакой следует рассматривать не нарушение работоспособности одного компьютера (ПК) входящего в состав локальной сети, а нарушение работоспособности всей сети (предполагая, что если один ПК заражен вирусом, то применяемое в сети антивирусное средство не способно выявить и локализовать этот вирус на других устройствах).

С целью реализации указанного замысла выявления вируса в сети и минимизации ущерба, задача декомпозирована на следующие этапы [2]:

– измерение, сбор, обработка и нормализация измеренных значений параметров эксплуатационных характеристик каждого ПК;

– сопоставление текущих значений с базой возможных состояний;

– принятие решения по реагированию, при выявлении факта реализации атаки.

Формирование базы возможных состояний возможно на основе проведения натурных экспериментов и кластеризации результатов.

Указанные частные задачи обработки данных, возможно, обработать на основе применения традиционных статистических методов (наивный байесовский классификатор, дискриминантный анализ, логистическая регрессия), однако при наличии значительного объема выборки (в настоящий момент процесс функционирования ПК возможно описать на основе изменения 12 эксплуатационных характеристик) их использование потребует значительных вычислительных ресурсов (для выявления факта деструктивного действия вируса на ПК и сопоставление его конкретному типу необходимо сопоставить изменение не одного параметра, а всего картежа параметров, причем это необходимо сделать не точечно, а интервально — в течение некоторого времени наблюдения) и привлечения в организацию дополнительных специалистов.

Вместе с этим, в настоящее время активно развиваются инструменты на основе применения методов машинного обучения [3—7]:

*Метод k-средних* — один из наиболее распространённых алгоритмов кластеризации, относящийся к методам обучения без учителя (unsupervised learning). Алгоритм разбивает множество объектов (наблюдений) на заранее заданное число k непересекающихся кластеров таким образом, чтобы каждый объект принадлежал кластеру с ближайшим центром (центроидом), а суммарное внутрикластерное расстояние было минимальным. Данный метод получил развитие и был усовершенствован в ряде решений, например, k-ближайших соседях.

*Линейный дискриминантный анализ (LDA — Linear Discriminant Analysis)x* — проецирует данные на подпространство, максимизирующее межклассовое расстояние и минимизирующее внутриклассовое. Одновременно снижает размерность и классифицирует. Предполагает нормальное распределение признаков и равные ковариационные матрицы классов

*Метод опорных векторов (SVM — Support Vector Machine)* — позволяет формировать оптимальную разделяющую гиперплоскость с максимальным разделением (margin) между классами. Ядровое преобразование (kernel trick) позволяет строить нелинейные границы: полиномиальное ядро, RBF (радиальная базисная функция), сигмоидное. Метод эффективен в пространствах высокой размерности и устойчив к переобучению при правильном выборе параметров.

*Наивный байесовский классификатор (Naive Bayes)* — Основан на теореме Байеса с допущением о условной независимости признаков. Варианты: гауссовский, мультиномиальный, бернуллиев. Применение данного инструмента позволяет быстро обучать модели для классификации. Эффективен для текстовых данных (спам-фильтрация, классификация документов). Допущение о независимости редко выполняется, но метод всё равно работает на практике.

*Байесовские сети (Bayesian Networks)* — графические вероятностные модели, описывающие условные зависимости между переменными. Допускают частичную зависимость признаков. Интерпретируемость через структуру графа.

*Случайный лес (Random Forest)* — ансамблевый метод, основанный на множестве деревьев решений, каждый из которых обучается на случайных подмножествах данных и признаков. Позволяет строить модель классификации, которая на входе получает вектор признаков (многомерный кортеж) телеметрии, а на выходе выдает метку класса, например, normal, xmrig, wannacry и т.д. Случайный лес позволяет оценить, какие признаки важны для классификации. Для каждого признака вычисляется среднее снижение индекса Джини по всем деревьям и узлам.

*Градиентный бустинг (Gradient Boosting)* — последовательное построение ансамбля слабых моделей (обычно деревьев), каждая из которых корректирует ошибки предыдущих. Высочайшая точность на табличных данных. Обработка пропусков, категориальных признаков (CatBoost). Риск переобучения при неправильной настройке.

Анализ практических решений показывает, что на текущем этапе развития программных средств, выделить наиболее эффективное средство достаточно сложно, а учитывая то, что для решения задач применяют комплекс моделей, рационально оценивать не эффективность моделей ИИ, а расходуемые вычислительные ресурсы, предоставляемый функционал.

В качестве варианта решения рассмотренной задачи, возможно применять программное средство объединяющее следующие модели обработки данных: *k-ближайших соседей, случайный лес.*

Разработанная программа [8] позволяет выявить кортежи значений контролируемых параметров СОИ при реализации в отношении него атак. Данное средство, фиксирует и выявляет аномалии изменения контролируемых параметров СОИ, вызванные, в том числе реализацией КА. Применение ПО позволяет определить наиболее информативные параметры и выявить сочетание параметров, характеризующих нормальные состояния СОИ и условия, характеризующие реализацию различных видов КА, в том числе ранее не известных.

Графическое представление применения метода k-ближайших соседей в разработанной программы представлено на рисунках 1—3. Применение k-ближайших соседей позволяет выявить важность контролируемых параметров и сократить количество обрабатываемых параметров.

Обработка собранного набора (кортежей) данных реализовано с применением случайного леса (рис. 4), что позволило определить условия, характеризующие состояние ПК, которое характеризует действие вируса.

```
Результаты обнаружения аномалий:
Всего записей: 1000
Обнаружено аномалий: 50 (5.00%)

Важность признаков для предсказания скорости записи:
CPU (%): 0.6388
RAM (%): 0.3612

Средняя абсолютная ошибка (MAE) предсказания скорости записи: 2.7058 MB/s

Статистика по подозрительным записям:
        RAM (%)     CPU (%)  ...  Anomaly  Predicted_Disk_Write
count  50.000000   50.000000  ...     50.0             50.000000
mean   58.696000   66.998000  ...      1.0             36.274764
std     7.236048   42.163378  ...      0.0             83.330955
min    49.700000    0.000000  ...      1.0              0.000000
25%    52.750000   15.400000  ...      1.0              0.021440
50%    56.500000  100.000000  ...      1.0              0.096858
75%    63.700000  100.000000  ...      1.0              6.285938
max    74.900000  100.000000  ...      1.0            374.576074

[8 rows x 5 columns]

Примеры подозрительных записей:
    RAM (%)  CPU (%)  Disk Write Speed (MB/s)  Anomaly  Predicted_Disk_Write
15     51.0     17.4                 0.000000        1             59.690625
19     63.0    100.0                 0.836426        1              0.270271
22     56.5    100.0                 0.000000        1              0.006726
23     56.5    100.0                 0.000000        1              0.006726
24     56.5    100.0                 0.000000        1              0.006726
```

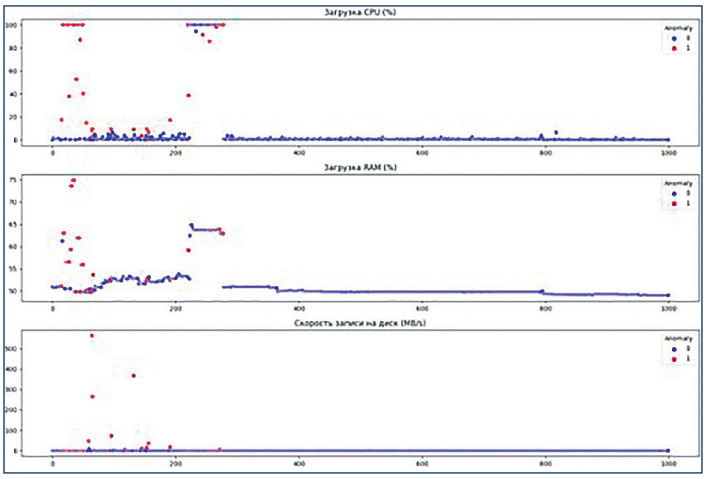



Рис. 1. Графическое представление измеренных параметров СОИ при его заражении ВПО

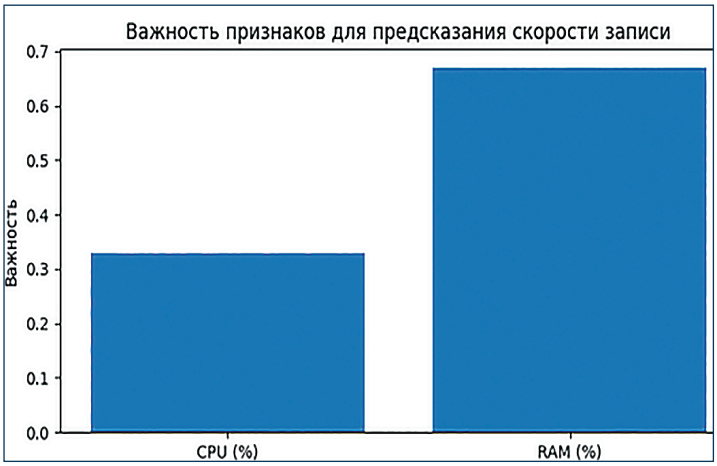



Рис. 2. Графическое представление определения важности контролируемых параметров

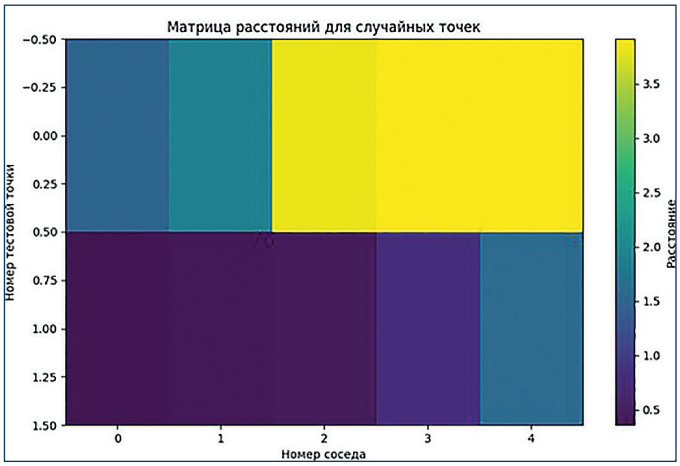



Рис. 3. Графическое представление матрицы расстояний для результатов эксперимента

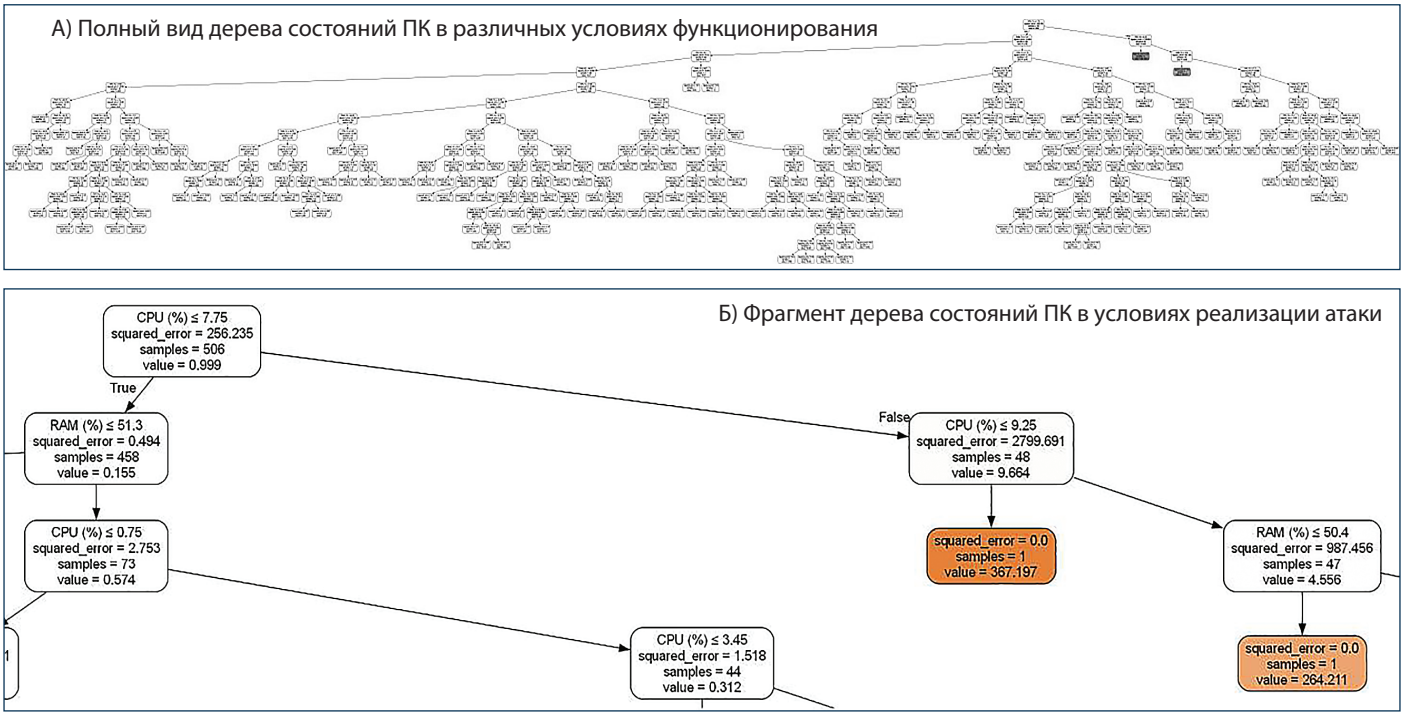



Рис. 4. Графическое представление дерева состояний СОИ при реализации атаки на него

Собранные наборы параметров подтверждают гипотезу о том, что анализ значений параметров, характеризующих эксплуатационные характеристики, потенциально способен выявить факт реализации неизвестных КА, а также являются основой для формирования базы данных для выработки стратегии защиты для случаев изменения значений контролируемых параметров.

Основываясь на том, что выявление аномалий параметров, описывающих состояние исследуемого СОИ производится в рамках контролируемых экспериментов (известно время начало и окончания воздействия, понятны цели воздействия, в том числе непосредственно изменяемые контролируемые параметров), результаты отражают реализуемые и протекающие процессы и не несут искажений (ошибок).

Применение такого подхода в отличие от традиционных методов выявления признаков реализации КА основанных на знаниях о возможных признаках КА, позволяет обнаружить факт реализации неизвестной КА в отношении ПК, что в дальнейшем позволит за счет своевременного реагирования и выбора стратегии защиты повысить уровень безопасности элемента сети *(например, при обнаружении факта заражения ПК вирусом, локализовать его, тем самым защитить локальную сеть от нанесения ущерба)*.

**СПИСОК ЛИТЕРАТУРЫ**

1. Добрышин М.М. Порядок, формирование и подтверждение гипотез, и их влияние на парадигму теории информационной безопасности / Международный научно-практический электронный журнал «Экономика и качество систем связи»: — 2025. — № 3 (37). — С. 148—156.

2. Белов А.С., Добрышин М.М., Душкин А.В. Системы обеспечения информационной безопасности: системный анализ, синтез, управление обработкой информации / Учебное пособие для вузов. под науч. ред. А.В. Душкина // М.: Горячая линия — Телеком, 2023. — 232 с.

3. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность / International Journal of Open Information Technologies ISSN: 2307—8162 vol. 10, no 9, 2022. С. 135—144.

4. Рассел, Стюарт, Норвиг, Питер. Искусственный интеллект: современный подход, 4-е изд., том 1. Решение проблем: знания и рассуждения.: Пер. с англ. — СПб.: ООО «Диалектика», — 2021. — 704 с.

5. Рассел, Стюарт, Норвиг, Питер. Искусственный интеллект: современный подход, 4-е издание, том 3. Обучение, восприятие и действие: Пер. с англ. — СПб.: ООО «Диалектика», — 2022. — 640 с. — Парал. тит. англ.

6. Исаков А.А. Искусственный интеллект и расследование киберпреступлений / Вестник науки — № 5 (62) Т. 3 — С. 597—602.

7. Добрышин М.М. К вопросу применения в средствах обеспечения информационной безопасности элементов доверенного искусственного интеллекта / Международный научно-практический электронный журнал «Экономика и качество систем связи»: — 2025. — № 4 (38). — С. 118—126.

8. Добрышин М.М. Программный модуль выявления вредоносного программного обеспечения, на основе дерева состояния, защищаемого ЭВМ / Свидетельство о государственной регистрации программы для ЭВМ № 2025666120 от 23.06.2025 Бюл. № 7.

DOI: 10./-2026-13

# Применение методов обработки естественного языка для анализа неструктурированных данных описывающих техники известных компьютерных атак

# APPLICATION OF NATURAL LANGUAGE PROCESSING METHODS TO ANALYZE UNSTRUCTURED DATA DESCRIBING TECHNIQUES OF KNOWN COMPUTER ATTACKS

**Добрышин Михаил Михайлович,**
к.т.н., сотрудник Академии ФСО России, г. Орёл

**Кирикова Юлия Андреевна,**
сотрудник Академии ФСО России, г. Орёл

**Mikhail Mikhailovich Dobryshin,**
PhD in Engineering, Federal Security Service Academy of Russia, Oryol

**Yulia Andreevna Kirikova,**
employee of Federal Security Service Academy of Russia, Oryol

***Аннотация.*** *Применение средств машинного обучения позволяет не только реализовывать различные рутинные действия, но и автоматизировать процесс обработки большого массива данных генерируемого современным обществом. В статье сформулированы основные сложности обработки неструктурированных данных содержащихся в статьях, отчетах и постах в мессенджерах, для выявления описаний новых способов эксплуатации известных уязвимостей.*

***Annotation.*** *The use of machine learning tools allows not only to implement various routine actions, but also to automate the process of processing a large amount of data generated by modern society. The article outlines the main difficulties of processing unstructured data contained in articles, reports, and posts in messengers to identify descriptions of new ways to exploit known vulnerabilities.*

***Ключевые слова****: обработка естественного языка, машинное обучение, уязвимости, информационная безопасность.*

***Keywords:*** *natural language processing, machine learning, vulnerabilities, information security.*

**Текстовые данные составляют значительную долю всей информации, генерируемой человечеством. В настоящее время человечество документирует значительную часть своих действий, от личных страничек в социальных сетях, до ведения онлайн баз знаний о различных критических сферах деятельности человечества. Доступ к ресурсам мирового информационного пространства позволяет авторам (исполнителям) публиковать результаты своих исследований (научные статьи, отчеты и др.).**

Однако с ростом количества публикаций, осведомленность «читателей» не увеличивается, а в отдельных случаях и снижается. Данное противоречие обусловлено наличием «информационного шума. Вследствие чего возникает задача по фильтрации и извлечению важных данных и устранению (удалению) информационного шума.

В качестве примера будет рассмотрена задача по выявлению описания новых (ранее не опубликованных) тактик и техник реализации компьютерных атак, эксплуатирующих известные уязвимости. Сформулированный подход применим и для других отраслей деятельности критичных ко времени обмена знаниями, например, финансового сектора или медицины.

При описании проблемной ситуации следует определить основные ресурсы (ограничения) и допущения. В качестве ограничений выступают конечные вычислительные ресурсы организации и временные ограничения. А в качестве допущений следует считать, что к обрабатываемой информации имеется полное доверие (доверие к источнику, автору и т.д.).

Проблемная ситуация: согласно требований регулятора (ФСТЭК России) в области информационной безопасности (ИБ), уязвимости критического уровня должны быть устранены в течение 24 часов с момента опубликования сведений о них (данное требование обусловлено потенциальным ущербом от успешной атаки на защищаемый ресурс) [1].

Методики расчета критичности уязвимостей включают различные факторы (в том числе статические — базовые и динамические — контентные), часть из которых способны повышать рассчитываемый уровень до критического, основываясь на том, что нарушитель ИБ разработал и реализовал новый способ реализации атаки (эксплойт). Безусловно, этот факт требует внимания и незамедлительной реакции в системе безопасности.

Однако с момента реализации атаки до официального подтверждения этого факта доверенными вендорами проходит от трех до шести месяцев, что приводит к повтор-

ным успешным атакам, многократному увеличению ущерба и превышению сроков на устранение уязвимости.

Вместе с этим, в материалах отчетов о расследовании инцидентов безопасности, специализированные организации публикуют необходимую информацию в течение двух-пяти дней.

С целью повышения охвата обрабатываемых неструктурированных источников данных представленных естественным языком (статьи, отчеты, посты в месенджерах) и снижения времени реагирования предлагается применять инструменты машинного обучения для выявления новых тактик реализации атак эксплуатирующих известные уязвимости.

При обработке естественного языка с помощью программных средств (ПС) существует ряд сложностей [2—4]:

— Полисемия и омонимия — некоторые слова имеют несколько значений в зависимости от контекста, что может затруднить понимание их истинного смысла.

— Неполнота и неоднозначность — естественный язык часто использует сокращения, неполные предложения, а также выражения с нечетким значением. Это может приводить к неоднозначности и усложнять задачу понимания текста.

— Сложность грамматики — грамматика языка может быть сложной и изменчивой. Существуют различные грамматические правила, исключения, а также идиомы, что усложняет задачу автоматического анализа текста.

— Многоязычность — системы для обработки текстов должны работать с различными языками, что увеличивает сложность задачи. Различные языки имеют разные грамматические структуры, лексику и особенности культурного контекста.

— Необходимость контекста — значение текста часто зависит от контекста, в котором он используется. Отсутствие контекста или недостаточное его участие может привести к неправильному пониманию смысла.

Также при использовании русского языка при обработке естественного языка сопряжено с рядом других уникальных проблем и сложностей, представленных в списке ниже:

— Сложность грамматики — русский язык имеет сложную грамматическую структуру с различными падежами, временами и спряжениями. Это может усложнить задачу синтаксического и морфологического анализа;

— Флективность — русский язык является флективным, что означает, что слова могут изменяться по числу, роду, падежу и времени. Это требует более сложных методов анализа и обработки морфологии;

— Богатство словоизменительных форм — в русском языке существует большое количество словоизменительных форм для каждого слова, что усложняет задачу лемматизации и стемминга;

— Словообразование — русский язык богат различными методами словообразования, такими как аффиксация, суффиксация и префиксация. Это может приводить к образованию новых слов и сложным проблемам в разрешении омонимии;

Для достижения заявленной цели проведен анализ инструментов обработки естественного языка средствами машинного обучения (Natural Language Processing, NLP) — область компьютерной науки, которая занимается распознаванием, анализом (в том числе пониманием и толкованием содержащейся в тексте информации) и созданием текстов подобно тому, как это делает человек [4—6].

Целью применения NLP является создание систем, способных понимать, интерпретировать и генерировать естественный язык. Основные этапы обработки текста NLP:

*Токенизация* — это разбиение текста на отдельные слова или фразы.

*Частеречная разметка*. Это определение частей речи для каждого слова в тексте.

*Лемматизация и стемминг*. Это приведение слов к их базовым формам (леммам) или обрезание их до основы (стемминг) для уменьшения размерности словаря.

*Удаление стоп-слов*. Это процесс удаление часто встречающихся, но малоинформативных слов (стоп-слов) из текста.

*Извлечение ключевых слов*. Это выделение наиболее важных слов или фраз в тексте.

*Извлечение информации*. Это поиск и извлечение структурированной информации из текста, такой как именованные сущности (имена людей, места, даты и т.д.).

*Синтаксический анализ* — это анализ синтаксической структуры предложений для понимания их грамматической структуры и зависимостей между словами.

*Семантический анализ*. Понимание значения текста на более высоком уровне, включая анализ смысла, контекста и общей семантики.

Помимо перечисленных задач, при разработке ПС, обрабатывающего информацию, содержащуюся в текстовых документах, (например, в формате PDF — один из самых распространенных) необходимо реализовать задачу *оптического распознавания символов* (*OCR*) — принцип работы технологии заключается в сканировании изображения символов на страницах PDF-файла, и пытаются распознать эти символы как текст.

После этого полученный текст может быть извлечен и использован. Данный метод широко применяется для преобразования отсканированных документов, рукописных текстов или изображений с текстом в редактируемый формат. Программными решениями являются: *Tesseract, Abbyy FineReader, Adobe Acrobat* и другие.

Преимущества *OCR*-технологии заключаются в извлечении текста из изображений, сохраняя при этом его форматирование.

Недостатки: точность распознавания может зависеть от качества изображения и самого текста, что может привести к ошибкам распознавания.

Для решаемой задачи и разрабатываемого ПС возможно

использовать универсальный язык программирования *Python*, который позволяет компилировать, подключать библиотеки и модули. Библиотеками *Python* для извлечения текста из PDF-файла являются:

— *PyPDF2* (используется для считывания файла);

— *Pdfpminer.six* (для выполнения анализа структуры и извлечения текста из PDF-файла).

Для дальнейшей обработки полученного текста используется библиотека на языке *Python Natural Language Toolkit(NLTK)*, которая будет эксплуатировать и реализовывать следующие функции в ПС:

— Токенизация *NLTK* — первый шаг при обработке текста, текст разбивается на отдельные слова, фразы, предложения или другие единицы (в данном ПС токенами являются отдельные слова и предложения);

— Удаление стоп-слов — удаление наиболее часто встречающиеся и малозначимые слова, которые не несут смысловой нагрузки, для чего используется список стоп-слов из *NLTK* (для каждого языка этот список уникален);

— Лемматизация и стемминг — преобразование слов к их базовым формам (нормальной форме), учитывая при этом морфологический анализ слов, а стемминг удаляет аффиксы, сохраняя основы слов.

Для получения данных о новых структурированных техниках в разработанном ПС реализован поиск совпадений с помощью сопоставления выделенных в обработанном тексте токенов с описанием известных уязвимостей и структурированных техник реализации КА.

Для поиска совпадений используется два способа.

Первым способом является поиск косинусного сходства *TF-IDF* — метод анализа текста, при котором для оценки сходства документов используется косинусное сходство между векторами, представленными в виде Term Frequency-Inverse Document Frequency (TF-IDF).

Вторым способом является исследование текста на наличие в нем токенов в виде отдельных слов, приведенных к нормальной форме относящихся к описанию известных структурированных техник, при этом коэффициент сходства должен превышать заданное значение, пользователем.

Сведения об известных уязвимостях и техник реализации атак скачиваются с внешних источников данных и хранятся в *json*-файлах. Структура *json*-файла состоит из пар «ключ-значение» и может быть представлена в несколько уровней вложенности.

Проведенный анализ известных решений, их достоинств и недостатков позволил определить перечень библиотек, применение которых позволит реализовать заявленные функции и решить сформулированную задачу [7]:

— *Natural Language Toolkit (NLTK)* — служит для обработки естественного языка *(NLP)* и предоставляет множество инструментов анализа текста, включая токенизацию, лемматизацию, стемминг, анализ синтаксиса и многое другое;

— *Nltk.tokenize.word_tokenize* — метод *NLTK* используется для разделения текста на отдельные слова или токены и преобразует текст в список слов или токенов для последующей обработки;

— *Nltk.corpus.stopwords* — модуль *NLTK* содержит список стоп-слов на разных языках;

— *Nltk.stem.PorterStemmer, nltk.stem.WordNetLemmatizer* — используются для стемминга и лемматизации слов;

— *Sklearn.feature_extraction.text.TfidfVectorizer* — класс из библиотеки *scikit- learn* используемый для преобразования текстовых данных в матрицу *TF-IDF*;

— *Sklearn.metrics.pairwise.cosine_similarity* — метод из *scikit-learn* вычисляет косинусное сходство между векторами;

— *PyPDF2.PdfReader, pypdf.PdfReader* — классы позволяют читать *PDF*- файлы в *Python*.

*Json* — встроенная библиотека *Python* для работы с форматом данных JSON, позволяет кодировать и декодировать данные JSON, предоставляя удобный интерфейс для работы с данными в этом формате (в разработанном ПС реализовано извлечение значений «*value*», «*name*» и «*description*» из *json*-файла в которых хранятся описания об известных уязвимостях и техник реализации атак);

По результатам анализа всего документа сопоставленные пары: техника реализации КА — уязвимость, упорядочиваются и сопоставляются с номерами известных техник реализации атак (например, *MITRE ATT&CK*) и уязвимостей (например, *CVE*) соответственно. После чего создается отчет в формальном (номерном) и текстовом описании реализации КА с указанием используемых уязвимостей.

Разработанное ПС зарегистрировано в Роспатенте, а логика работы в составе других решений описана в патенте РФ на изобретение [8].

Разработанное ПС на основе применения элементов машинного обучения позволяет выявлять сведения о фактах эксплуатации известных уязвимостей при реализации новых тактик и техник реализации атак, что позволяет организации своевременно предпринять меры по недопущению нанесения ущерба [9].

К вопросу этичности применения искусственного интеллекта и машинного обучения в частности: разработанное ПС не заменяет аналитиков работающих в организации, а позволяет расширить объем обрабатываемых данных, что, несомненно, способствует снижению финансовых рисков и не исключает деятельность человека.

Возможности использования в других областях деятельности общества: в статье, большое внимание уделено методам, механизмам и средствам обработки естественного языка для того, чтобы было понимание общих процессов, протекающих в разработанном ПС. Так замена стоп-слов и использование для сравнения баз данных с набором слов из других областей деятельности позволяет считать данное средство универсальным.

**СПИСОК ЛИТЕРАТУРЫ**

1. Белов А.С., Добрышин М.М., Громов Ю.Ю., Душкин А.В. / Квалиметрический анализ защищенных инфотелекоммуникационных систем / Учебное пособие для вузов. под науч. ред. А.В. Душкина // М.: Горячая линия — Телеком, 2025. — 156 с.

2. Контент-анализ СМИ: проблемы и опыт применения / Под ред. В.А. Мансурова. — М.: Институт социологии РАН, 2010. — 324 с.

3. Сапин А.С. Построение нейросетевых моделей морфологического и морфемного анализа текста. Труды ИСП РАН, том 33, вып. 4, — 2021 г., — С. 117—130.

4. Большакова Е.И., Воронцов К.В. и др. Автоматическая обработка текстов на естественном языке и анализ данных: учебное пособие. Изд-во НИУ ВШЭ, — 2017 г., 269 с.

5. Рассел, Стюарт, Норвиг, Питер. Искусственный интеллект: современный подход, 4-е издание, том 3. Обучение, восприятие и действие: Пер. с англ. — СПб.: ООО Диалектика, — 2022. — 640 с.

6. Барретт С.Ф. Arduino: искусственный интеллект и машинное обучение / пер. с англ. Ю.В. Ревича. — М.: ДМК Пресс, 2024. — 242 с.: ил.

7. Python [Электронный ресурс] / Python // www.python.org — Электрон. дан. — 2001—2024. Режим доступа: https://python.org/about — Дата обращения: 20.01.2026.

8. Добрышин М.М., Шугуров Д.Е., Кирикова Ю.А., Погодин Н.В. / Программа автоматического обновления и формирования техник реализации компьютерных атак для системы обеспечения информационной безопасности / Свидетельство о государственной регистрации программы для ЭВМ № 2023688 299 от 14.12.2023 Бюл. № 1.

9. Добрышин М.М., Белов А.С., Шугуров Д.Е., Кирикова Ю.А., и др. Система автоматического обновления и формирования техник реализации компьютерных атак для системы обеспечения информационной безопасности / Патент РФ на изобретение № 2809929 от 19.12.2023 Бюл. № 35 Заявка 2023118422, 12.07.2023. Патентообладатель: Академия ФСО России. G06F 21/50 (2013.01), G06F 16/22 (2019.01).

ISSN 3033-8239
26001
9 773033 823007 >