Политика и Общество
Правильная ссылка на статью:
Проскурина А.С., Цыганков А.Ю. Правовые аспекты использования искусственного интеллекта в задачах кибербезопасности // Политика и Общество. 2025. № 4. DOI: 10.7256/2454-0684.2025.4.72653 EDN: XGBIME URL: https://nbpublish.com/library_read_article.php?id=72653

Правовые аспекты использования искусственного интеллекта в задачах кибербезопасности

Проскурина Алина Сергеевна

ORCID: 0009-0006-8209-7310

бакалавр; юридический институт; Институт международного права и экономики им. Грибоедова

115598, Россия, г. Москва, ул. Липецкая 15, корпус 1

alina-muk@mail.ru

Цыганков Александр Юрьевич

кандидат юридических наук

доцент; кафедра "Гражданское право и гражданский процесс"; Московский университет им. А.С. Грибоедова, доцент, кафедра "Психолого-педагогических и правовых дисциплин", Московская академия предпринимательства

124365, Россия, москва область, г. Зеленоград, ул. квартал 2305, А

tsygan.alexandr2017@yandex.ru

Статья из рубрики "ОБЩЕСТВЕННАЯ БЕЗОПАСНОСТЬ"

DOI:

10.7256/2454-0684.2025.4.72653

EDN:

XGBIME

Дата направления статьи в редакцию:

09-12-2024

Аннотация: В статье исследуются правовые аспекты использования искусственного интеллекта в задачах кибербезопасности, включая анализ существующего законодательства Российской Федерации и международного опыта. Особое внимание уделяется ключевым вызовам, связанным с отсутствием унифицированных стандартов, необходимостью защиты персональных данных и предотвращением злоупотреблений при использовании ИИ. Рассматриваются стратегические инициативы, такие как

Национальная стратегия развития искусственного интеллекта и программа «Цифровая экономика Российской Федерации». Объектом исследования выступают общественные отношения, формирующиеся в процессе использования искусственного интеллекта в задачах кибербезопасности, включая взаимодействие между государственными и международными структурами, направленное на защиту данных, предотвращение кибератак и регулирование применения интеллектуальных технологий. Предметом исследования является комплекс норм, регулирующих данные отношения, включая национальное и международное законодательство, а также совокупность научных исследований и этических принципов, касающихся использования искусственного интеллекта в обеспечении кибербезопасности. Методологическую основу исследования составляют общенаучные и частнонаучные методы, обеспечивающие комплексный анализ правовых аспектов использования искусственного интеллекта в сфере кибербезопасности. Также применяются логические методы анализа, синтеза, дедукции и индукции, выявляющие закономерности правового регулирования и его влияние на цифровую безопасность. Важную роль играет сравнительно-правовой метод, используемый для анализа законодательства РФ. Делается вывод о необходимости комплексного подхода, включающего разработку стандартов, международное сотрудничество и создание прозрачных правоприменительных механизмов для обеспечения эффективного и безопасного использования ИИ в кибербезопасности. Одним из ключевых элементов решения этих проблем является выработка этических норм, регулирующих использование ИИ. Принятие Кодекса этики в сфере искусственного интеллекта свидетельствует о признании необходимости установления единых принципов для участников данного процесса. Однако действующий документ требует детализации и последующего закрепления в нормативно-правовых актах, регулирующих такие вопросы, как ответственность за действия автономных систем и использование ИИ в целях предотвращения кибератак. Этический кодекс ИИ должен стать основой для формирования национальных стандартов, способствуя созданию правового пространства, где балансируются интересы государства, бизнеса и общества. Без учета этих аспектов дальнейшее развитие ИИ будет сопровождаться увеличением рисков и утратой доверия к новым технологиям, что неизбежно отразится на национальной и международной безопасности.

Ключевые слова:

искусственный интеллект, кибербезопасность, правовое регулирование, защита данных, правоприменение, международное сотрудничество, национальная стратегия, цифровые технологии, киберпреступность, угроза

Киберпреступность — один из самых быстроразвивающихся видов экономической преступности [5, с. 20]. Постоянно совершенствуются информационные и цифровые технологии, растет квалификация злоумышленников. Возникает необходимость в создании современных методов защиты информации, обеспечивающих требуемый уровень защищенности от новых угроз. Для данных целей хорошо подходят методы защиты, основанные на использовании искусственного интеллекта (далее – ИИ).

Достижения в области искусственного интеллекта, особенно в сегменте глубокого машинного обучения, стали катализатором технологического прогресса, создавая инструменты, которые превосходят человеческие возможности в таких областях, как распознавание изображений, анализ больших данных и обработка естественного языка.

Применение ИИ в задачах кибербезопасности позволяет оперативно выявлять сложные угрозы, автоматизировать мониторинг сетевой активности и защищать критически важные системы, такие как финансовые платформы и автономные транспортные средства. Однако такие технологии несут не только пользу, но и потенциальные риски. Расширение возможностей ИИ в корпоративной и государственной среде может приводить к манипуляциям и злоупотреблениям, создавая новые уязвимости для информационной безопасности [6, с. 710].

В условиях растущего влияния ИИ на сферу кибербезопасности возрастает потребность в четком и эффективном правовом регулировании его применения. Отсутствие унифицированных стандартов и механизмов контроля использования ИИ создает правовую неопределенность, которая может привести к правонарушениям, связанным с утратой данных, нарушением конфиденциальности и дискриминацией. Кроме того, важно учитывать аспекты правовой ответственности за действия автономных систем, решения которых оказывают непосредственное влияние на права и законные интересы граждан и организаций.

Сложность регулирования ИИ в сфере кибербезопасности усугубляется высокой скоростью технологического прогресса и глобальным характером цифровых угроз. В условиях, когда количество кибератак с применением машинного обучения и автоматизированных атакующих алгоритмов неуклонно растет, а злоумышленники используют ИИ для обхода традиционных систем защиты, становится очевидным необходимость разработки правовых механизмов, способных оперативно адаптироваться к новым вызовам. Отсутствие единых международных стандартов, регулирования ответственности за действия автономных систем и эффективных механизмов правоприменения создает неопределенность, которая может быть использована в ущерб интересам пользователей, бизнеса и государства. Поэтому выработка четкой нормативной базы, учитывающей этические и правовые аспекты использования ИИ, является не только задачей национального уровня, но и вопросом международного сотрудничества, направленного на обеспечение цифровой безопасности.

Вопросы правового регулирования искусственного интеллекта, его применения в сфере кибербезопасности, а также сопутствующие юридические, этические и технологические вызовы уже стали предметом научных исследований российских ученых. В отечественной юридической науке особое внимание уделяется таким аспектам, как правосубъектность искусственного интеллекта, защита персональных данных, регулирование автономных систем и правоприменительная практика в условиях цифровой трансформации. Важный вклад в изучение этих вопросов внесли такие исследователи, как Филипова И.А., Моисеев А.В., Морхат П.М., Ефхиев О.М.

Несмотря на существующие научные труды, тема правового регулирования использования искусственного интеллекта в сфере кибербезопасности остается актуальной и требует дальнейшего изучения. Это обусловлено динамичным развитием технологий, отсутствием единых международных стандартов, правовой неопределенностью в вопросах ответственности за действия автономных систем и увеличением числа киберугроз с применением ИИ. В современных условиях необходима выработка комплексного правового подхода, сочетающего национальные правовые нормы, международные соглашения и этические стандарты, обеспечивающие баланс между инновациями и защитой прав граждан. Таким образом, дальнейшее исследование данной темы необходимо для формирования эффективного законодательства, способного адаптироваться к стремительно изменяющейся цифровой среде.

Для успешного применения ИИ в кибербезопасности требуется разработка комплексной правовой базы, обеспечивающей баланс между инновациями и соблюдением прав человека. Ключевыми направлениями регулирования должны стать стандартизация использования ИИ, обеспечение прозрачности алгоритмов, защита персональных данных, а также формирование механизмов ответственности за ущерб, нанесенный в результате использования интеллектуальных систем. Кроме того, необходимо учитывать международный аспект регулирования, так как киберугрозы не знают государственных границ, что требует координации усилий на глобальном уровне. Этим обусловлена актуальность исследования правовых аспектов использования искусственного интеллекта в задачах кибербезопасности.

Объектом исследования выступают общественные отношения, формирующиеся в процессе использования искусственного интеллекта в задачах кибербезопасности, включая взаимодействие между государственными, корпоративными и международными структурами, направленное на защиту данных, предотвращение кибератак и регулирование применения интеллектуальных технологий. Предметом исследования является комплекс норм, регулирующих данные отношения, включая национальное и международное законодательство, правоприменительные механизмы, а также совокупность научных исследований и этических принципов, касающихся использования искусственного интеллекта в обеспечении кибербезопасности.

Методологическую основу исследования составляют общенаучные и частнонаучные методы, обеспечивающие комплексный анализ правовых аспектов использования искусственного интеллекта в сфере кибербезопасности. В работе применяются логические методы анализа, синтеза, дедукции и индукции, позволяющие выявить закономерности правового регулирования и его влияние на цифровую безопасность. Важную роль играет сравнительно-правовой метод, используемый для анализа законодательства Российской Федерации и международных правовых норм, регулирующих применение ИИ. Системный и системно-структурный методы позволяют рассмотреть правовые нормы в их взаимосвязи с технологическими и этическими аспектами кибербезопасности. Формально-юридический метод применяется для интерпретации нормативных правовых актов, регулирующих использование ИИ. Использование исторического метода позволяет проследить эволюцию правового регулирования ИИ, а статистический метод применяется для анализа данных о кибератаках и эффективности существующих правовых механизмов.

Современная мировая цифровая экосистема ежегодно пополняется сотнями миллионов устройств интернета вещей и миллиардами строк нового программного кода, формируя беспрецедентный объем данных и взаимосвязей. Цифровые технологии и интеллектуальные системы уже стали неотъемлемой частью развития бизнеса, обеспечивая его адаптивность и стимулируя инновации. Однако вместе с этими достижениями неизбежно увеличивается число уязвимых точек в цифровой инфраструктуре, что расширяет спектр киберугроз и разнообразие методов их реализации [2, с. 24].

Основные проблемы защиты корпоративной информации остаются критически актуальными на фоне стремительного развития технологий и увеличения количества кибератак. Одной из ключевых трудностей является недостаточный уровень защиты, предоставляемый региональными коммерческими и государственными инфраструктурами. Это обусловлено как ограниченностью ресурсов, так и отсутствием единых стандартов для обеспечения безопасности на различных уровнях. Такая фрагментированность

создает значительные пробелы в защите данных и упрощает злоумышленникам доступ к уязвимым точкам.

Еще одной важной проблемой является низкая квалификация IT-специалистов, что проявляется в отсутствии регулярного совершенствования используемых протоколов безопасности и недостатке актуальных знаний о современных угрозах. Нередко компании продолжают использовать устаревшие средства защиты и программное обеспечение, что становится катализатором для успешной реализации атак. Данные уязвимости возникают из-за как финансовых ограничений, так и отсутствия стратегического понимания важности своевременного обновления систем безопасности.

Ситуация осложняется слабой подготовкой рядового персонала, который нередко пренебрегает элементарными правилами кибергигиены. Отсутствие регулярного обучения и инструктажей способствует распространению фишинговых атак и других методов социальной инженерии, которые становятся эффективным инструментом для злоумышленников. Даже самая продвинутая технологическая защита может быть подорвана человеческим фактором, если сотрудники организации не осведомлены о базовых принципах безопасности.

Дополнительным вызовом является отсутствие координации и единой политики среди ведомств и организаций в вопросах противодействия киберугрозам. Без четко согласованных регламентов и распределения зон ответственности эффективная защита корпоративной информации становится практически невозможной. Необходима выработка комплексного подхода, охватывающего как технологические, так и организационные аспекты, с обязательным учетом постоянно меняющихся сценариев кибератак.

Искусственный интеллект демонстрирует значительный потенциал в обеспечении кибербезопасности, предлагая новые методы и инструменты для противодействия угрозам. Применение ИИ основано на принципе обучения систем на основе существующих данных, что позволяет эффективно адаптировать их к выявлению новых угроз. Данный подход сочетает машинное обучение и аналитические методы, обеспечивая комплексное решение задач в сфере информационной безопасности.

Одной из ключевых задач, решаемых с помощью ИИ, является обнаружение вторжений. Использование алгоритмов машинного обучения позволяет анализировать огромные объемы данных, выявлять аномалии и распознавать действия, характерные для кибератак. Такая автоматизация значительно повышает скорость обнаружения угроз и снижает вероятность их пропуска.

Также искусственный интеллект активно применяется для выявления уязвимостей в программном коде, что становится важным этапом в создании безопасных программных решений. Сканируя большие массивы данных, алгоритмы способны обнаруживать потенциальные ошибки и уязвимости, которые могут быть использованы злоумышленниками. Это направление все еще развивается, но уже показывает высокую эффективность.

Еще одним важным направлением является дополнение традиционной аналитики угроз методами машинного обучения. ИИ позволяет не только использовать базы данных с известными угрозами, но и выявлять ранее неизвестные атаки путем анализа поведения систем. Таким образом, создается более гибкая и адаптивная защита, способная реагировать на новые вызовы.

Наконец, применение ИИ для поиска аномалий в системах позволяет эффективно предотвращать мошеннические действия. Алгоритмы анализируют поведенческие паттерны и фиксируют отклонения от нормы, что помогает обнаруживать подозрительные действия в режиме реального времени. Это ускоряет реагирование на угрозы и минимизирует возможный ущерб [2, с. 26].

На сегодняшний день необходимость разработки правового регулирования использования искусственного интеллекта в сфере кибербезопасности стала очевидной. Государства, заинтересованные в повышении эффективности защиты информации и предотвращении киберугроз, активно работают над созданием нормативной базы, способствующей безопасному и ответственному применению ИИ в данной области. К апрелю 2021 года собственные стратегии и документы, посвященные развитию ИИ, включая его использование для кибербезопасности, разработали более 30 стран, включая Россию [8]. Великобритания, например, в сентябре 2021 года представила национальную стратегию, которая также охватывает аспекты применения ИИ в задачах защиты критически важной инфраструктуры и информационных систем [1, с. 90].

При этом наличие национальной стратегии в области искусственного интеллекта не является обязательным условием для разработки правового регулирования его применения в кибербезопасности. Некоторые страны предпочитают использовать точечные нормативные акты, регулирующие отдельные аспекты, такие как защита данных, ответственность за киберинциденты с участием автономных систем и правила эксплуатации алгоритмов анализа сетевой активности. Другие государства стремятся интегрировать стратегическое планирование с созданием нормативов прямого действия, что позволяет быстрее реагировать на конкретные угрозы и вызовы в киберсфере [4, с. 131].

Ведущие страны в области ИИ, включая США, Великобританию, Европейский Союз, Китай, Японию и Южную Корею, уже разработали нормативные акты, направленные на регулирование применения ИИ в кибербезопасности [10]. Данные документы охватывают широкий спектр вопросов — от стандартов разработки алгоритмов для обнаружения кибератак до механизмов предотвращения их использования злоумышленниками. Однако стремление к быстрому внедрению новых документов также подвергается критике. Увеличение числа нормативных актов, компетентных органов и экспертных групп, занимающихся этой сферой, приводит к усложнению правоприменительной практики и затрудняет мониторинг изменений и инициатив. Это особенно важно в условиях динамично развивающейся сферы киберугроз, требующей гибкости и координации на национальном и международном уровнях [7, с. 4].

В Российской Федерации правовое регулирование применения искусственного интеллекта в сфере кибербезопасности находится на стадии становления, что отражено в ряде стратегических документов. Одним из ключевых является Национальная стратегия развития искусственного интеллекта до 2030 года, утвержденная Указом Президента РФ от 10 октября 2019 года № 490[1]. Данный документ закладывает основы для развития технологий ИИ, подчеркивая необходимость обеспечения безопасности, защиты прав и свобод человека, прозрачности процессов, а также сохранения технологического суверенитета. Указанные принципы согласуются с международными подходами, включая стратегии США и Европейского Союза, что создает предпосылки для гармонизации правовых норм в глобальном масштабе.

Важным элементом государственной политики в области ИИ является Национальная программа «Цифровая экономика Российской Федерации» на 2019–2024 годы[2]. В рамках этой программы реализуется федеральный проект «Искусственный интеллект», курируемый Минцифры России. Проект направлен на поддержку научных исследований, разработку программного обеспечения, создание комплексной системы правового регулирования в сфере ИИ, повышение доступности и качества данных, а также обеспечение рынка квалифицированными кадрами. Особое внимание уделяется вопросам кибербезопасности, поскольку применение ИИ в этой сфере требует четкого нормативного регулирования для предотвращения потенциальных рисков.

Для апробации новых правовых механизмов в 2020 году был принят Федеральный закон № 123-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»[3]. Данный закон предоставляет возможность устанавливать специальные правовые режимы для тестирования инновационных технологий, включая ИИ, в различных областях, в том числе в кибербезопасности. Однако некоторые ключевые вопросы, такие как налоговые льготы и специальные режимы, остаются вне рамок экспериментальных правовых режимов, что ограничивает их потенциал в стимулировании развития технологий ИИ.

В октябре 2021 года в рамках I Международного форума «Этика искусственного интеллекта: начало доверия» был подписан Кодекс этики в сфере искусственного интеллекта [9]. Данный документ, разработанный при участии Минэкономразвития и представителей крупнейших российских компаний, инвестирующих в технологии ИИ, устанавливает принципы человеко-ориентированного подхода, уважения автономии и свободы воли человека, соответствия закону и недискриминации. Присоединение к Кодексу является добровольным, однако его принятие свидетельствует о стремлении бизнеса и государства к ответственному использованию ИИ, включая его применение в кибербезопасности.

В феврале 2024 года Президент РФ подписал указ, обновляющий Национальную стратегию развития искусственного интеллекта на период до 2030 года. Обновленная стратегия акцентирует внимание на необходимости разработки правовых механизмов, обеспечивающих безопасное и эффективное использование ИИ в различных сферах, включая кибербезопасность. Это свидетельствует о признании государством важности правового регулирования ИИ для защиты информационных систем и предотвращения киберугроз.

Кроме того, в июне 2024 года были внесены поправки в Указ Президента РФ от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»[4]. Данные изменения направлены на усиление кибербезопасности страны, включая использование технологий ИИ для обнаружения и предотвращения кибератак. Поправки предусматривают разработку и внедрение нормативных актов, регулирующих применение ИИ в сфере информационной безопасности, что способствует созданию комплексной системы защиты от современных киберугроз.

В своей работе «Правосубъектность искусственного интеллекта в сфере права» П.М. Морхат утверждает, что признание искусственного интеллекта самостоятельным субъектом права способно упростить разрешение вопросов ответственности за действия автономных систем [3, с. 29]. Однако, представляется, что такой подход несет в себе серьезные риски и порождает больше вопросов, чем решает.

Во-первых, признание ИИ субъектом права нарушает основополагающие принципы правопорядка, основанные на способности субъекта нести моральную и юридическую ответственность. Искусственный интеллект, даже самый продвинутый, лишен сознания, воли и способности осознавать свои действия. Ответственность за действия ИИ, на мой взгляд, должна лежать на лицах, его создавших и использующих — разработчиках и владельцах. Такой подход не только сохраняет логику правоприменения, но и стимулирует заинтересованные стороны к разработке более безопасных и этически обоснованных технологий.

Кроме того, введение ИИ в категорию субъектов права может создать правовую неопределенность, осложняя процесс правоприменения и контроля. В условиях стремительного технологического развития требуется гибкое, но четкое регулирование, обеспечивающее баланс между инновациями и ответственностью, где центральное место отводится человеку как создателю и пользователю технологий.

Таким образом, современное правовое регулирование использования искусственного интеллекта в сфере кибербезопасности демонстрирует стремительное развитие как на национальном, так и на международном уровнях. Однако данный процесс сопряжен с рядом вызовов, связанных с необходимостью обеспечения технологической прозрачности, защиты персональных данных и предотвращения злоупотреблений. Российская Федерация предпринимает последовательные шаги для формирования эффективной нормативной базы, что отражается в стратегических документах, таких как Национальная стратегия развития искусственного интеллекта и программа «Цифровая экономика». Особое внимание уделяется вопросам кибербезопасности, поскольку применение ИИ требует не только научных и технологических разработок, но и четкого правового регулирования.

Ключевой проблемой остается отсутствие унифицированных стандартов, что приводит к правовой неопределенности и затрудняет оперативное реагирование на новые угрозы. Для устранения этого недостатка требуется комплексный подход, включающий стандартизацию алгоритмов ИИ, разработку международных соглашений и создание прозрачных механизмов правоприменения. Принятие Федерального закона № 123-ФЗ об экспериментальных правовых режимах стало важным шагом в этой области, однако недостаточное внимание к вопросам налоговых льгот и других стимулирующих механизмов ограничивает потенциал данного подхода.

Одним из ключевых элементов решения этих проблем является выработка этических норм, регулирующих использование ИИ. Принятие Кодекса этики в сфере искусственного интеллекта свидетельствует о признании необходимости установления единых принципов для участников данного процесса. Однако действующий документ требует детализации и последующего закрепления в нормативно-правовых актах, регулирующих такие вопросы, как ответственность за действия автономных систем и использование ИИ в целях предотвращения кибератак. Этический кодекс ИИ должен стать основой для формирования международных обязательств и национальных стандартов, способствуя созданию правового пространства, где балансируются интересы государства, бизнеса и общества. Без учета этих аспектов дальнейшее развитие ИИ будет сопровождаться увеличением рисков и утратой доверия к новым технологиям, что неизбежно отразится на национальной и международной безопасности.

[1] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (ред. от 15.02.2024) // Собрание законодательства РФ. – 2019. – № 41. – Ст. 5700.

[2] Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16). [Электронный ресурс]. – URL: https://base.garant.ru/72190282/ (дата обращения: 14.11.2024).

[3] Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (ред. от 08.08.2024) // Российская газета. – 2020. – 6 августа.

[4] Указ Президента Российской Федерации от 13 июня 2024 г. № 500 «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2024. – № 25. – Ст. 3465.

Библиография

1. Введенская Е.В. Актуальные проблемы робоэтики / Е.В. Введенская // Науковедческие исследования. – 2019. – № 9. – С. 88-101.
2. Кечеджиев, А. С. Искусственный интеллект в решении задач кибербезопасности / А. С. Кечеджиев, О. Л. Цветкова // Молодой исследователь Дона. – 2023. – Т. 8, № 2(41). – С. 23-27.
3. Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности : гражданско-правовые проблемы : дисс. ... доктора юрид. наук : 12.00.03 / Морхат П.М. – Москва, 2018. – 420 с.
4. Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники: история, современное состояние и перспективы развития: монография / В.В. Архипов и др.; под общ. ред. В.Б. Наумова – СПб.: НП-Принт, 2020. – 260 с.
5. Приходько Д. В. Киберпреступность как глобальная проблема современности / Д. В. Приходько, А. А. Белькова // Экономика и бизнес: теория и практика. – 2021. – № 4-2. – С. 19-26.
6. Яковлева Е. А. Роль технологий искусственного интеллекта в цифровой трансформации экономики / Е.А. Яковлева // Вопросы инновационной экономики. – 2023. – Т. 13. – № 2. – С. 707-726.
7. Veale M. A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence / M.A. Veale // European Journal of Risk Regulation. – № 11 (1). – E1. – P. 1-10.
8. Как развивается искусственный интеллект? [Электронный ресурс]. – URL: http://svop.ru/main/36999/ (дата обращения: 14.11.2024).
9. Кодекс этики в сфере ИИ. [Электронный ресурс]. – URL: https://ethics.a-ai.ru/ (дата обращения: 14.11.2024).
10. National AI policies & strategies [Электронный ресурс]. – URL: https://oecd.ai/en/dashboards (дата обращения: 14.11.2024).

Результаты процедуры рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье являются, как это следует из ее наименования, правовые аспекты использования искусственного интеллекта в задачах кибербезопасности. Заявленные границы исследования соблюдены ученым.

Методология исследования в тексте статьи не раскрывается.

Актуальность избранной автором темы исследования несомненна и обосновывается им следующим образом: "Киберпреступность — один из самых быстроразвивающихся видов экономической преступности [4, с. 20]. Постоянно совершенствуются информационные и цифровые технологии, растет квалификация злоумышленников. Возникает необходимость в создании современных методов защиты информации, обеспечивающих требуемый уровень защищенности от новых угроз. Для данных целей хорошо подходят методы защиты, основанные на использовании искусственного интеллекта (далее – ИИ). Достижения в области искусственного интеллекта, особенно в сегменте глубокого машинного обучения, стали катализатором технологического прогресса, создавая инструменты, которые превосходят человеческие возможности в таких областях, как распознавание изображений, анализ больших данных и обработка естественного языка. Применение ИИ в задачах кибербезопасности позволяет оперативно выявлять сложные угрозы, автоматизировать мониторинг сетевой активности и защищать критически важные системы, такие как финансовые платформы и автономные транспортные средства. Однако такие технологии несут не только пользу, но и потенциальные риски. Расширение возможностей ИИ в корпоративной и государственной среде может приводить к манипуляциям и злоупотреблениям, создавая новые уязвимости для информационной безопасности [5, с. 710]. В условиях растущего влияния ИИ на сферу кибербезопасности возрастает потребность в четком и эффективном правовом регулировании его применения. Отсутствие унифицированных стандартов и механизмов контроля использования ИИ создает правовую неопределенность, которая может привести к правонарушениям, связанным с утратой данных, нарушением конфиденциальности и дискриминацией. Кроме того, важно учитывать аспекты правовой ответственности за действия автономных систем, решения которых оказывают непосредственное влияние на права и законные интересы граждан и организаций" и др.

Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.

Научная новизна работы проявляется в ряде заключений автора: "Таким образом, современное правовое регулирование использования искусственного интеллекта в сфере кибербезопасности демонстрирует стремительное развитие как на национальном, так и на международном уровнях. Однако данный процесс сопряжен с рядом вызовов, связанных с необходимостью обеспечения технологической прозрачности, защиты персональных данных и предотвращения злоупотреблений. Российская Федерация предпринимает последовательные шаги для формирования эффективной нормативной базы, что отражается в стратегических документах, таких как Национальная стратегия развития искусственного интеллекта и программа «Цифровая экономика». Особое внимание уделяется вопросам кибербезопасности, поскольку применение ИИ требует не только научных и технологических разработок, но и четкого правового регулирования. Ключевой проблемой остается отсутствие унифицированных стандартов, что приводит к правовой неопределенности и затрудняет оперативное реагирование на новые угрозы. Для устранения этого недостатка требуется комплексный подход, включающий стандартизацию алгоритмов ИИ, разработку международных соглашений и создание прозрачных механизмов правоприменения. Принятие Федерального закона № 123-ФЗ об экспериментальных правовых режимах стало важным шагом в этой области, однако

недостаточное внимание к вопросам налоговых льгот и других стимулирующих механизмов ограничивает потенциал данного подхода"; "Одним из ключевых элементов решения этих проблем является выработка этических норм, регулирующих использование ИИ. Принятие Кодекса этики в сфере искусственного интеллекта свидетельствует о признании необходимости установления единых принципов для участников данного процесса. Однако действующий документ требует детализации и последующего закрепления в нормативно-правовых актах, регулирующих такие вопросы, как ответственность за действия автономных систем и использование ИИ в целях предотвращения кибератак. Этический кодекс ИИ должен стать основой для формирования международных обязательств и национальных стандартов, способствуя созданию правового пространства, где балансируются интересы государства, бизнеса и общества. Без учета этих аспектов дальнейшее развитие ИИ будет сопровождаться увеличением рисков и утратой доверия к новым технологиям, что неизбежно отразится на национальной и международной безопасности" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и, безусловно, заслуживает внимания потенциальных читателей.

Научный стиль исследования выдержан автором в полной мере.

Структура работы логична. Во вводной части статьи ученый обосновывает актуальность избранной им темы исследования. В основной части работы автор анализирует правовые аспекты использования искусственного интеллекта в задачах кибербезопасности, выявляет соответствующие проблемы правового регулирования и предлагает пути их решения. В заключительной части работы содержатся выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию и не вызывает особых нареканий.

Библиография исследования представлена 9 источниками (монографией, научными статьями, аналитическими данными, документом), в том числе на английском языке. С формальной точки зрения источников должно быть не менее 10. Следовательно, теоретическая база работы нуждается в расширении.

Апелляция к оппонентам имеется, но носит общий характер. В научную дискуссию с конкретными учеными автор не вступает, ссылаясь на ряд теоретических источников исключительно в обоснование своих суждений либо для иллюстрирования отдельных положений работы.

Выводы по результатам проведенного исследования имеются ("Таким образом, современное правовое регулирование использования искусственного интеллекта в сфере кибербезопасности демонстрирует стремительное развитие как на национальном, так и на международном уровнях. Однако данный процесс сопряжен с рядом вызовов, связанных с необходимостью обеспечения технологической прозрачности, защиты персональных данных и предотвращения злоупотреблений. Российская Федерация предпринимает последовательные шаги для формирования эффективной нормативной базы, что отражается в стратегических документах, таких как Национальная стратегия развития искусственного интеллекта и программа «Цифровая экономика». Особое внимание уделяется вопросам кибербезопасности, поскольку применение ИИ требует не только научных и технологических разработок, но и четкого правового регулирования. Ключевой проблемой остается отсутствие унифицированных стандартов, что приводит к правовой неопределенности и затрудняет оперативное реагирование на новые угрозы. Для устранения этого недостатка требуется комплексный подход, включающий стандартизацию алгоритмов ИИ, разработку международных соглашений и создание прозрачных механизмов правоприменения. Принятие Федерального закона № 123-ФЗ об экспериментальных правовых режимах стало важным шагом в этой области, однако недостаточное внимание к вопросам налоговых льгот и других стимулирующих

механизмов ограничивает потенциал данного подхода. Одним из ключевых элементов решения этих проблем является выработка этических норм, регулирующих использование ИИ" и др.), обладают свойствами достоверности, обоснованности и, несомненно, заслуживают внимания научного сообщества.
Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере информационного права, административного права при условии ее доработки: раскрытии методологии исследования, дополнительном обосновании актуальности его темы (в рамках сделанного замечания), расширении теоретической базы работы, введении дополнительных элементов дискуссионности.

Результаты процедуры повторного рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Предмет исследования. В рецензируемой статье «Правовые аспекты использования искусственного интеллекта в задачах кибербезопасности» предметом исследования являются нормы права, регулирующие общественные отношения в сфере использования искусственного интеллекта в борьбе с киберпреступностью и ее профилактикой.
Методология исследования. Методологический аппарат составили следующие диалектические приемы и способы научного познания: анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, типология, классификация, систематизация и обобщение. Применение современных научных методов, таких как формально-логический, историко-правовой, сравнительно-правовой, статистический, социологический и др., позволило сформировать собственную авторскую позицию по заявленной проблематике.
Актуальность исследования. Актуальность темы исследования не вызывает сомнения. Автор правильно отмечает, что «несмотря на существующие научные труды, тема правового регулирования использования искусственного интеллекта в сфере кибербезопасности остается актуальной и требует дальнейшего изучения. Это обусловлено динамичным развитием технологий, отсутствием единых международных стандартов, правовой неопределенностью в вопросах ответственности за действия автономных систем и увеличением числа киберугроз с применением ИИ. В современных условиях необходима выработка комплексного правового подхода, сочетающего национальные правовые нормы, международные соглашения и этические стандарты, обеспечивающие баланс между инновациями и защитой прав граждан. Таким образом, дальнейшее исследование данной темы необходимо для формирования эффективного законодательства, способного адаптироваться к стремительно изменяющейся цифровой среде». Данные обстоятельства действительно обуславливают необходимость доктринальных разработок в сфере правового обеспечения использования искусственного интеллекта в борьбе с киберпреступностью.
Научная новизна.Не подвергая сомнению важность проведенных ранее научных исследований, послуживших теоретической базой для данной работы, тем не менее, можно отметить, что в этой статье сформулированы заслуживающие внимания

положения, которые указывают на важность этого исследования для юридической науки и его практическую значимость, например: «Ключевой проблемой остается отсутствие унифицированных стандартов, что приводит к правовой неопределенности и затрудняет оперативное реагирование на новые угрозы. Для устранения этого недостатка требуется комплексный подход, включающий стандартизацию алгоритмов ИИ, разработку международных соглашений и создание прозрачных механизмов правоприменения». В статье содержатся и другие положения, отличающиеся научной новизной и имеющие практическую значимость, которые можно расценить как вклад в отечественную юридическую науку.

Стиль, структура, содержание. Содержание статьи соответствует ее названию. Тема раскрыта. Соблюдены автором требования по объему материала. Материал изложен последовательно и ясно. Статья написана научным стилем, использована специальная юридическая терминология. Автором предпринята попытка структурировать статью. Статья состоит из введения, в котором обоснована актуальность темы исследования, основной части и заключения, содержащего итоги проделанной автором работы. Замечаний по содержанию нет.

Библиография. Автором использовано достаточное количество доктринальных источников, включая публикации последних лет. Ссылки на имеющиеся источники оформлены с соблюдением требований библиографического ГОСТа.

Апелляция к оппонентам. По спорным вопросам заявленной тематики представлена научная дискуссия, обращения к оппонентам корректные. Все заимствования оформлены ссылками на автора и источник опубликования. Анализируя разные точки зрения, автор высказывает собственное аргументированное мнение.

Выводы, интерес читательской аудитории. Статья «Правовые аспекты использования искусственного интеллекта в задачах кибербезопасности» рекомендуется к опубликованию. Статья соответствует тематике журнала «Политика и Общество». Статья написана на актуальную тему, отличается научной новизной и имеет практическую значимость. Данная статья может представлять интерес для широкой читательской аудитории, прежде всего, специалистов в области информационного права, уголовного права, а также, будет полезна для преподавателей и обучающихся юридических вузов и факультетов.