Раздел III. ЧАСТНО-ПРАВОВЫЕ (ЦИВИЛИСТИЧЕСКИЕ) НАУКИ (ЮРИДИЧЕСКИЕ НАУКИ)

Научная статья
УДК 004.056:004.8:341.232

DOI: 10.24412/2225-8264-2024-4-851

Ключевые слова: искусственный интеллект, информационные технологии, кибербезопасность, цифровизация, киберпространство, киберпреступления, киберугрозы, правовое регулирование искусственного интеллекта

Keywords: artificial intelligence, information technology, cybersecurity, digitalization, cyberspace, cybercrime, cyberthreats, legal regulation of artificial intelligence

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ДВУЕДИНСТВО ПРЕИМУЩЕСТВ И УГРОЗ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Фудашкин В. А.[1]

Аннотация. *В статье рассматриваются ключевые аспекты применения искусственного интеллекта через призму кибербезопасности, с акцентом на наличие как преимуществ, так и угроз для данной сферы. Исследование направлено на анализ правовых аспектов применения технологий искусственного интеллекта в киберпространстве, оценку их влияния на защиту информационных систем, а также на выявление рисков и угроз, возникающих в связи с возможным использованием искусственного интеллекта в преступных целях со стороны злоумышленников. Целью исследования является комплексное изучение правовых и этических аспектов применения искусственного интеллекта, а также разработка предложений по совершенствованию законодательства в данной области. В рамках работы ставится задача определить баланс между преимуществами, которые искусственный интеллект дает в процесс обеспечения кибербезопасности, и угрозами, которые могут возникнуть вследствие его неправомерного использования. Для достижения поставленных целей в рамках статьи использованы общенаучные и специальные методы правового исследования, среди которых можно выделить такие как: метод анализа и синтеза, формально-юридический метод, сравнительно-правовой метод, историко-правовой метод, прогностический метод и др. Статья предназначена для юристов, специалистов в области информационных технологий и исследователей, интересующихся вопросами кибербезопасности и правового регулирования применения искусственного интеллекта.*

[1]**Фудашкин Виталий Анатольевич** — кандидат юридических наук, доцент кафедры гражданского права и процесса, Кыргызско-Российский Славянский Университет (Киргизия, г. Бишкек, пр. Чуй, д. 42, корпус 7)
E-mail: topmanagerkg@mail.ru
ORCID: 0009-0002-9022-9476

Поступила в редакцию: 23.09.2024

ARTIFICIAL INTELLIGENCE: THE DUALITY OF BENEFITS AND THREATS IN CYBERSECURITY

Vitalii A. Fudashkin
Candidate of Law, Associate Professor, Kyrgyz-Russian Slavic University

Abstract. *This research paper examines key aspects of artificial intelligence application through the lens of cybersecurity, with an emphasis on both the benefits and threats to this area. The study is aimed at analyzing the legal aspects of the use of artificial intelligence technologies in cyberspace, assessing their impact on the protection of information systems, and identifying risks and threats arising in connection with the possible use of artificial intelligence for criminal purposes by attackers. The aim of the study is a comprehensive study of the legal and ethical aspects of the use of artificial intelligence, as well as the development of proposals for improving legislation in this area. The work aims to determine the balance between the benefits that artificial intelligence provides in the process of ensuring cybersecurity and the threats that may arise as a result of its unlawful use. To achieve the stated goals, the article uses general scientific and special methods of legal research, among which the following can be distinguished: the method of analysis and synthesis, the formal-legal method, the comparative-legal method, the historical-legal method, the prognostic method, etc.*
The article is intended for lawyers, IT specialists and researchers interested in cybersecurity and legal regulation of the use of artificial intelligence.

Введение

Когда Джон Маккарти в 1956 году впервые предложил термин «искусственный интеллект» на конференции в Дартмуте, он, вероятно, не мог полностью осознать масштабы влияния, которое данная технология несколько десятилетий спустя окажет на жизнь всего человечества.

Первоначально понятие «искусственный интеллект» подразумевало создание машин, способных выполнять задачи, требующие человеческого интеллекта, таких как понимание языка, распознавание образов и принятие решений [1, с. 86; 2, с. 138].

Однако, в то время искусственный интеллект воспринимался скорее, как предмет академического исследования и научной фантастики, нежели как технология, которая кардинальным образом интегрируется в повседневную жизнь человека.

На момент возникновения концепции искусственного интеллекта, ее авторы и последователи концентрировались в основном на технических аспектах разработки систем, имитирующих когнитивные способности человека, и не могли предсказать те этические, социальные и правовые вызовы, которые возникнут в будущем.

Стремительное совершенствование искусственных нейронных сетей на основе глубокого обучения стало катализатором для дальнейшего развития искусственного интеллекта. Современный уровень эволюции искусственного интеллекта вышел далеко за рамки академических лабораторий, став неотъемлемой частью различных сфер общественной жизни.

В настоящее время, в эпоху глобальной кибертрансформации, интеграция искусственного интеллекта в повседневную жизнь человека уже не является предметом научной фантастики, а становится реальностью, затрагивающей все сферы жизнедеятельности общества. Искусственный интеллект проникает в различные отрасли — от медицины [3, с. 121] и промышленности [4, с. 50; 5, с. 509] до правосудия [6, с. 96; 7, с. 91] и национальной безопасности [8, с. 15], оказывая значительное влияние на социальные отношения, экономику, оборону и правовые системы государств.

Развитие искусственного интеллекта открыло перед человечеством не только обширные перспективы, но и создало многочисленные угрозы, связанные с его применением.

Данные угрозы, о которых, в частности, упоминает один из разработчиков компании «Google» — Блейк Лемойн, касаются потенциальной способности искусственного интеллекта выйти за пределы контроля со стороны человека и привести к возникновению серьезных рисков для общества и безопасности. Лемойн высказывает опасения по поводу того, что искусственный интеллект, обладая высокоразвитыми когнитивными способностями, может не только выполнять задачи, на которые он был запрограммирован, но и развивать собственные модели поведения, основанные на самообучении [9].

Для описания процесса всеобъемлющего проникновения искусственного интеллекта во все сферы человеческой жизни можно предложить новый термин «ноосинтез» (noosýnthesi, от греч. νοῦς — мысль, разум, ум и σύνθεσις — соединение, складывание, связывание), что буквально можно определить, как «слияние разума».

Этот термин отражает интеграцию искусственного интеллекта с человеческими действиями и повседневной жизнью, тем самым подчеркивая, что искусственный интеллект становится частью глобального «синтеза» человеческого разума и программных интеллектуальных систем.

В настоящий момент возникла ситуация, когда искусственный интеллект, благодаря своей способности к обработке огромных объемов данных, быстрому обучению и самообучению, может переиграть своего творца в так называемых «играх разумов».

Одним словом, неконтролируемое совершенствование «искусственного разума» может привести к ситуации, в которой искусственный интеллект, будучи приобретя способность к самовоспроизведению или модификации первоначально заложенных алгоритмов, будет стремиться к собственному выживанию или более того — доминированию, что поставит под угрозу контроль человека над созданной им технологией. Неизбежным следствием такого саморазвития является появление экзистенциальной угрозы.

Искусственный интеллект становится неотъемлемым элементом обработки данных и принятия решений в сферах, которые ранее считались исключительной прерогативой человека, в том числе в обеспечении безопасности, что создает необходимость переосмысления этических аспектов взаимодействия человека и технологий, прежде всего, таких его составляющих как робоэтика и машинная этика.

В этом контексте встает вопрос необходимости комплексного эффективного нормативного-правового, нормативно-технического и этического регулирования процесса создания, применения и контроля искусственного интеллекта в целях минимизации потенциальных угроз, которые он несет.

Обсуждение и результаты

В современном мире, характеризующемся глобальной цифровизацией и интеграцией информационных технологий во все сферы общественной и государственной жизни, кибербезопасность приобретает особое значение как ключевой элемент национальной и международной безопасности.

Повсеместное использование интернета, цифровых технологий и искусственного интеллекта сопровождается не только обширными возможностями для развития экономики, управления и социальной сферы, но и серьезными угрозами, связанными с кибератаками, незаконным доступом к информации, кибершпионажем, кибертерроризмом и другими формами преступлений, совершаемым в киберпространстве.

Обеспечение кибербезопасности обусловлено постоянным ростом количества и сложности киберугроз, с которыми ежедневно сталкиваются как государства, так и частные организации, и граждане. Кибератаки могут наносить ущерб не только экономической ин-

фраструктуре, но и угрожать основам государственной власти, нарушать права и свободы граждан, подрывать доверие к цифровым технологиям и услугам, а также дестабилизировать международные отношения.

Государства, обладая высокоразвитой цифровой инфраструктурой, оказываются наиболее уязвимыми к действиям злоумышленников, которые могут использовать кибератаки как инструмент воздействия на государственные и социальные институты.

В связи с этим, кибербезопасность является неотъемлемой частью Стратегии национальной безопасности Российской Федерации [10], в которой в качестве стратегического национального приоритета закреплено развитие безопасного информационного пространства и защита российского общества от информационно-психологического воздействия деструктивного характера.

Обеспечение противодействия киберугрозам также является в соответствии с п. 20 Стратегии научно-технологического развития Российской Федерации [11] одним из приоритетов научно-технического развития страны.

Стратегический характер также носит участие Российской Федерации в обеспечении кибербезопасности на региональном уровне и реализуется через многостороние международные механизмы сотрудничества, направленные на противодействие преступлениям в сфере информационных технологий.

В рамках участия в Организации Договора о коллективной безопасности (ОДКБ) и Содружестве Независимых Государств (СНГ), Российская Федерация активно продвигает региональные инициативы по обеспечению информационной безопасности, что находит свое отражение в таких международных актах как Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года [12] и Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий [13].

Как определяет А. В. Минбалеев, кибербезопасность максимально взаимоувязана с возможностями искусственного интеллекта [14, с. 120].

Использование искусственного интеллекта в целях обеспечения информационной безопасности представляет собой одно из важнейших направлений в реализации Национальной стратегии развития искусственного интеллекта на период до 2030 года [15]. Согласно положениям данной Стратегии, искусственный интеллект является ключевым инструментом для защиты критической информационной инфраструктуры и противодействия современным киберугрозам, что обусловлено многообразием рисков в цифровой среде.

В условиях стремительного роста объемов данных и совершенствования методов кибератак, использование технологий искусственного интеллекта позволяет значительно повысить уровень кибербезопасности за счет внедрения автоматизированных систем мониторинга, обнаружения и нейтрализации угроз.

Способность искусственного интеллекта анализировать большие массивы информации в режиме реального времени способствует раннему выявлению киберугроз, адаптации защитных механизмов под новые типы атак и их нейтрализации на ранних стадиях.

Таким образом, искусственный интеллект может предоставить новые тактико-технические приемы (инструменты) в борьбе с киберпреступностью [16, с. 185].

Необходимо заметить, что в настоящее время, на практике искусственный интеллект уже активно применяется в различных сферах кибербезопасности и его эффективность подтверждена реальными результатами. Примерами использования искусственного интеллекта в целях обеспечения кибербезопасности могут выступать:

- автоматизированные системы обнаружения и предотвращения кибератак на основе искусственного интеллекта.

Эти системы способны выполнять широкий спектр задач, направленных на выявление, анализ и предотвращение угроз в цифровом пространстве, опираясь на методы глубокого машинного обучения и нейронные сети. Основными функциями данных систем являются: обнаружение аномалий и подозрительной активности, анализ вредоносного программного обеспечения, прогнозирование кибератак, высокий уровень самообучения;

- антифишинговые системы с интегрированным искусственным интеллектом.

Они представляют собой передовые технологии, которые направлены на выявление, предотвращение и борьбу с фишингом — одной из самых распространенных кибератак, целью которой является обман пользователя для получения конфиденциальной информации (банковские данные, логины, пароли и т.д.). Основными принципами работы данных систем являются: Анализ ссылок и URL-адресов, анализ электронной почты и сообщений, поведенческий анализ, обнаружение поддельных веб-сайтов, самообучение и улучшение алгоритмов;

- системы защиты персональных данных на основе искусственного интеллекта.

Это технологически продвинутые решения, которые позволяют более эффективно и комплексно обеспечивать безопасность конфиденциальной информации, подверженной рискам утечек, краж и несанкционированного доступа. Их основными функциями являются: обнаружение аномалий и подозрительной активности, анализ и идентификация угроз в режиме реального времени, контроль доступа и управление привилегиями, шифрование и защита данных, предотвращение утечек данных (DLP-системы), автоматизация аудита и мониторинга, а также защита от кибератак и вредоносного программного обеспечения.

Исходя из вышесказанного, можно установить, что использование истем защиты на основе искусственного интеллекта предоставляет значительные преимущества в области кибербезопасности. Они повышают эффективность защиты, обеспечивая проактивное обнаружение и предотвращение угроз, снижая нагрузку на специалистов и поднимая уровень защиты данных на новый уровень. В эпоху глобальной цифровизации и

роста числа кибератак, искусственный интеллект становится незаменимым инструментом для обеспечения безопасности информации и предотвращения преступлений в киберпространстве.

Однако, как определяет С. В. Федотов, наряду с преимуществами использования искусственного интеллекта в сфере обеспечения кибербезопасности, он стал неотъемлемой частью современных киберугроз, и киберпреступники активно используют его для усиления своих атак [17, с. 183].

Криминальные субъекты разработали уникальный комплексный метод совершения противоправных действий с использованием новейших информационных технологий, основанных на нейронных сетях и искусственном интеллекте. Они активно применяют цифровые устройства для планирования преступной деятельности, реализации и координации своих действий.

Важной особенностью является использование методов цифровой маскировки, включая подмену IP-адресов, шифрование, использование прокси-серверов и иных способов, которые позволяют им эффективно скрывать свою личность.

В рамках осуществления киберпреступлений, преступные группы широко применяют автоматизированные инструменты и программы, позволяющие совершать незаконные действия в автоматизированном режиме. Данные преступления часто совершаются в виртуальной среде — киберпространстве, обладающем новыми, усложненными характеристиками, такими как глобальная связь и трансграничность.

Киберпреступления не имеют территориальных границ, что позволяет злоумышленникам находиться в одной юрисдикции, в то время как их жертвы могут находиться в другой. Данный фактор значительно осложняет процесс выявления, преследования и привлечения к ответственности виновных лиц.

Все перечисленные особенности криминалистической характеристики киберпреступлений свидетельствуют о повышенной сложности их расследования [18, с. 589].

Сложность предупреждения и выявления киберпреступлений заключается помимо всего в том, что преступления, в основе которых используется искусственный интеллект, представляют собой одно из наиболее динамично развивающихся явлений.

Использование искусственного интеллекта, таким образом, может нести в себе следующие угрозы для кибербезопасности со стороны киберпреступников:

• Атаки на основе автоматизации и адаптации.

Искусственный интеллект способен автоматизировать процессы производимых кибератак, что позволяет преступникам проводить их с большей частотой и на более сложном и эффективном уровне. Адаптивные алгоритмы искусственного интеллекта могут анализировать системы защиты, выявлять их уязвимости и корректировать тактику атак в режиме реального времени.

• Использование искусственного интеллекта для обхода киберзащитных систем.

Преступники могут применять искусственный интеллект для создания сложных схем обхода существующих киберзащитных механизмов. Алгоритмы искусственного интеллекта могут анализировать работу систем защиты, выявлять паттерны их работы и находить способы преодоления защитных барьеров, таких как системы обнаружения вторжений, фаерволы и антивирусные программы.

• Совершенствование методов социальной инженерии.

Искусственный интеллект может быть использован для создания сложных атак, основанных на социальной инженерии. С помощью искусственного интеллекта преступники могут анализировать огромные объемы данных о жертвах, персонализируя фишинговые атаки или мошеннические схемы. Применение технологий глубокого обучения позволяет искусственному интеллекту имитировать поведение людей, создавая убедительные поддельные сообщения, телефонные звонки и даже видео.

• Угрозы со стороны автономных вредоносных программ.

Вредоносные программы, интегрированные с искусственным интеллектом, могут работать автономно, принимая решения на основе анализа окружающей среды и условий киберпространства. Такие программы способны не только проникать в системы, но и адаптироваться к их защите, меняя свою структуру и методы атаки, что затрудняет их обнаружение и удаление.

• Масштабирование атак с минимальным вмешательством со стороны оператора.

Использование искусственного интеллекта позволяет киберпреступникам атаковать сразу множество целей одновременно с минимальными затратами человеческих ресурсов. Вредоносное программное обеспечение на основе искусственного интеллекта может самостоятельно находить уязвимые системы, подбирать к ним ключи доступа, заражать их вредоносными программами и контролировать процесс проникновения в системы.

• Создание более опасных моделей вредоносного программного обеспечения.

Искусственный интеллект может быть использован для создания новых видов вредоносного программного обеспечения, которое способно обходить «традиционные» системы защиты, анализируя их слабые стороны и адаптируясь к ним.

• Сложность обнаружения киберпреступлений и привлечения к ответственности виновных лиц.

Искусственный интеллект позволяет преступникам оставаться анонимными и скрывать следы своей противоправной деятельности. Технологии искусственного интеллекта могут использоваться для шифрования данных, подделки цифровых подписей и маскировки IP-адресов, что затрудняет работу правоохранительных органов по их идентификации. Это повышает вероятность безнаказанности за совершенные киберпреступления, что стимулирует их дальнейшее совершение.

Как нами было определено выше, искусственный интеллект имеет потенциал для применения в различным областях, включая обеспечение правопорядка и национальной безопасности. Однако, его использование в противоправных целях может исходить не только со стороны киберпреступников, но и от самих госу-

дарств, в частности, со стороны правоохранительных органов и органов национальной безопасности. Таким образом, данная категория угроз может в себя включать:

• Нарушение прав и свобод человека.

Государства, обладая неограниченным доступом к технологиям искусственного интеллекта, могут злоупотреблять ими для тотального контроля за гражданами. Использование данных технологий для массового наблюдения, анализа поведения может привести к серьезным нарушениям права на неприкосновенность частной жизни. Правоохранительные органы могут также применять системы мониторинга, такие как технологии распознавания лиц, для массового слежения за гражданами без достаточных правовых оснований и без надлежащего контроля со стороны судебных органов.

• Кибершпионаж и вмешательство в личную жизнь.

Государства могут использовать искусственный интеллект для осуществления кибершпионажа как внутри страны, так и за её пределами. С помощью данных технологий возможен автоматический взлом систем, сбор конфиденциальных данных, а также координация дестабилизирующих операций в киберпространстве. Такие действия со стороны государства могут быть направлены на вторжение в частную жизнь граждан, мониторинг коммуникаций и нарушение прав на конфиденциальность личной информации. Осуществление подобных действий в отношении других государств может привести к эскалации международных конфликтов, нарушению международной безопасности и стабильности.

• Концентрация власти, политическое преследование и подавление деятельности оппозиции.

Государства могут использовать технологии искусственного интеллекта для подавления и контроля за политической оппозицией. Применение технологий глубокого анализа и автоматизированного мониторинга может позволить правоохранительным органам отслеживать и подавлять инакомыслящих, осуществлять мониторинг и цензуру информации, контролировать политическую активность, препятствовать свободе слова. В отсутствие надлежащих правовых механизмов регулирования такие действия могут нарушать основные права и свободы граждан, закрепленные в национальном и международном законодательствах.

• Манипуляция общественным сознанием и вмешательство в демократические процессы.

Искусственный интеллект может использоваться для манипуляции общественным мнением и вмешательства в политические процессы, включая выборы. Государства могут применять искусственный интеллект для создания и распространения дезинформации, влияния на общественные мнения и настроения, результаты выборов как в своих интересах, так и для подрыва суверенитета других стран. Такие действия могут ослабить демократические институты и подорвать доверие к правовым механизмам.

• Ведение кибервойн.

Применение искусственного интеллекта государствами для проведения трансграничных операций, таких как кибератаки или вмешательство в дела других государств, может представлять собой нарушение норм международного права и привести к международным конфликтам и кризисам. Атаки на критически важные инфраструктуры других государств, манипуляция информацией и вмешательство в суверенные дела могут привести к серьезным дипломатическим и политическим последствиям. В отсутствие международного консенсуса относительно правового регулирования искусственного интеллекта возрастает риск неконтролируемой эскалации конфликтов, которая может подорвать стабильность международного правопорядка.

Использование искусственного интеллекта в противоправных целях со стороны государств и государственных структур, включая правоохранительные органы, представляет серьезную угрозу для прав и свобод человека, политической стабильности и международного правопорядка. Это еще раз подчеркивает необходимость разработки как на национальном, так и международном уровнях эффективных механизмов правового регулирования использования искусственного интеллекта и международного сотрудничества в этой сфере.

Так же не стоит забывать, что одной из значительных и потенциально опасных угроз для кибербезопасности может являться и сам искусственный интеллект. Современные системы искусственного интеллекта обладают способностью к быстрому обучению, обработке огромных объемов данных, и развитию автономных функций, что, с одной стороны, значительно расширяет возможности в обеспечении кибербезопасности, но с другой — создает новые риски и угрозы. К возможным угрозам для кибербезопасности со стороны искусственного интеллекта можно отнести:

• Непредсказуемость поведения искусственного интеллекта.

Высокий уровень автономности искусственного интеллекта может привести к непредсказуемым решениям и действиям, особенно в условиях сложных или необычных ситуаций, которые не были предусмотрены в процессе обучения системы. Неправильная интерпретация данных или некорректное прогнозирование сценариев может повлечь за собой выполнение вредоносных операций или отказ в оказании необходимых мер киберзащиты, что создает угрозу для целостности, конфиденциальности и доступности информации.

• Эксплуатация уязвимостей.

Автономные системы искусственного интеллекта, несмотря на свою способность к самообучению и адаптации, остаются уязвимыми перед целенаправленными атаками. Злоумышленники могут использовать эти системы для разработки и осуществления кибератак, направленных на автоматическое обнаружение и использование слабых мест в сетевой инфраструктуре, что может привести к массовым сбоям и утечкам данных.

• Проблема контроля.

В процессе совершенствования автономных систем искусственного интеллекта возрастает риск утраты контроля со стороны человека над действиями и решениями таких систем. Вследствие этого, в случае сбоя

или ошибки в работе алгоритмов искусственного интеллекта, либо при злонамеренном вмешательстве в их работу, оперативное вмешательство и коррекция поведения системы могут оказаться затруднительными или невозможными. В результате возможны неконтролируемые последствия, которые могут привести к серьезным нарушениям в функционировании информационных систем и кибербезопасности в целом.

• Отсутствие прозрачности в принятии решений.

Одной из особенностей искусственного интеллекта является сложность интерпретации решений, принимаемых системой на основе машинного обучения и нейронных сетей. Отсутствие прозрачности и возможности детального анализа принятия решения может вызвать серьезные трудности в процессе расследования инцидентов, связанных с кибербезопасностью, а также в установлении ответственности за действия искусственного интеллекта.

• Проблемы этики искусственного интеллекта.

Наряду с увеличением роли искусственного интеллекта в сфере кибербезопасности, возникает необходимость оценки его использования с точки зрения этических норм. Этика, являясь основой сугубо человеческого взаимодействия, приобретает особое значение в условиях, когда принятие решений перекладывается на алгоритмы. Многие авторы определяют этическую составляющую искусственного интеллекта как одну из ключевых проблем [19, с. 380; 20, с. 32].

По словам Заместителя Генерального директора ЮНЕСКО по вопросам социальных и гуманитарных наук Габриэлы Рамос: «Технологии искусственного интеллекта приносят значительные выгоды во многих областях, но без этических рамок они могут привести к распространению предубеждений и дискриминации в реальном мире, разжиганию разногласий и угрозе фундаментальным правам и свободам человека. Ни в одной другой области наличие этического компаса не является столь актуальным, как в сфере искусственного интеллекта [21].

В 2020 году ЮНЕСКО опубликовало Рекомендации по этическим аспектам искусственного интеллекта [21], в которых подчеркивается важность защиты прав и свобод человека при использовании искусственного интеллекта. Помимо этого, 1 августа 2024 года в ЕС вступил в силу Регламент Европейского Союза об искусственном интеллекте (Artificial Intelligence Act), который направлен на регулирование искусственного интеллекта с акцентом на управление рисками. Регламент вводит строгие требования для «высокорискованных» ИИ-систем (например, в здравоохранении, транспорте, правоприменении), а также запрет на некоторые виды использования искусственного интеллекта, такие как массовая слежка и социальный рейтинг.

Выводы

В результате проведенного исследования установлено, что искусственный интеллект является двуединым феноменом в сфере кибербезопасности, выступая одновременно как инструмент защиты и потенциальный источник угроз.

С одной стороны, искусственный интеллект обеспечивает совершенствование методов обнаружения и предотвращения кибератак, повышая эффективность систем безопасности посредством машинного обучения и анализа больших объемов данных.

С другой стороны, возможности искусственного интеллекта могут быть использованы злоумышленниками для создания более сложных и труднообнаружимых методов нападения, включая автоматизированные фишинговые атаки и распространение вредоносного программного обеспечения.

Правовая регламентация применения искусственного интеллекта в области кибербезопасности находится на этапе становления и требует комплексного подхода. При этом, комплексное нормативное регулирование процессов создания, применения и контроля искусственного интеллекта должно проходить с учетом правовых, технических и этических аспектов. Современное законодательство должно быть направлено на соблюдение баланса между развитием инноваций и обеспечением защиты прав и свобод человека, а также предотвращение рисков, связанных с использованием искусственного интеллекта.

Международное сотрудничество и гармонизация подходов к регулированию искусственного интеллекта являются важными шагами на пути к созданию универсальных стандартов и норм, которые обеспечат безопасное и этически оправданное использование данной технологии.

Список источников

1. Носов Н. Ю., Соколов М. Д. Тенденции развития искусственного интеллекта // Современные научные исследования и инновации. 2016. № 5(61). С. 86–89.

2. Савченко И. С. Заложник «китайской комнаты» или в поисках сознания у машин // Заметки ученого. 2020. № 2. С. 138–143.

3. Фершт В. М., Латкин А. П., Иванова В. Н. Современные подходы к использованию искусственного интеллекта в медицине // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2020. Т. 12. № 1(48). С. 121–130.

4. Калиновская И. Н., Завьялова А. О. Направления использования искусственного интеллекта в организации производства на предприятиях легкой промышленности // Материалы и технологии. 2020. № 1(5). С. 50–56.

5. Минбалеев А. В., Берестнев М. А., Евсиков К. С. Регулирование использования искусственного интеллекта в добывающей промышленности // Известия Тульского государственного университета. Наука о Земле. 2022. № 2. С. 509–525.

6. Спицин И. Н., Тарасов И. Н. Использование искусственного интеллекта при отправлении правосудия: теоретические аспекты правовой регламентации (постановка проблемы) // Актуальные проблемы российского права. 2020. Т. 15. № 8(117). С. 96–107.

7. Малина М. А. Использование искусственного интеллекта при отправлении правосудия по уголовным делам: проблемы и перспективы // Государство и право. 2022. № 1. С. 91–97.

8. Горохова С. С. Искусственный интеллект в контексте обеспечения национальной безопасности // Национальная безопасность / Nota Bene. 2020. № 3. С. 15–31.

9. Программист Google настаивает, что чат-бот с искусственным интеллектом — разумное существо [Электронный ресурс] // BBC NEWS. URL: https://www.bbc.com/russian/news-61775714 (дата обращения: 10.09.2024).

10. Стратегия национальной безопасности Российской Федерации (Утверждена Указом Президента РФ от 02.07.2021 г. № 400) // Правовая справочно-информационная система «Гарант».

11. Стратегия научно-технологического развития Российской Федерации (Утверждена Указом Президента РФ от 28.02.2024 г. № 145) // Правовая справочно-информационная система «Гарант».

12. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года от 18 октября 2016 года (Утверждена Решением Совета коллективной безопасности Организации Договора о коллективной безопасности от 14.10.2016 г.) // Правовая справочно-информационная система «Гарант».

13. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года // Правовая справочно-информационная система «Гарант».

14. Минбалеев А. В. Проблемы использования искусственного интеллекта в противодействии киберпреступности // Вестник Южно-Уральского государственного университета. Серия: Право. 2020. Т. 20. №. 4. С. 116–120.

15. Национальная стратегия развития искусственного интеллекта на период до 2030 года (Утверждена Указом Президента РФ от 10.10.2019 г. № 490 в ред. от 15.02.2024 г.) // Правовая справочно-информационная система «Гарант».

16. Сейдакматов Н. А., Куцев Е. В. Интеграция искусственного интеллекта в системы информационной безопасности: вызовы и возможности // Научные исследования в Кыргызской Республике. 2024. № 1. С. 24–34.

17. Федотов С. В. Применение технологий искусственного интеллекта в кибербезопасности // Культура информационной безопасности: вызовы времени: материалы XIV Международной научно-практической конференции студентов, аспирантов и молодых ученых. Москва, 2024. С. 183–187.

18. Пристанскова В. Д., Харатишвили А. Г., Евстратова Ю. А. Искусственный интеллект — новая форма использования специальных знаний в расследовании и раскрытии киберпреступлений // Всероссийский криминологический журнал. 2023. Том 17. № 6. С. 586–596.

19. Чаплыгин М. С., Постников А. В. Нравственный аспект использования искусственного интеллекта // Актуальные проблемы современной науки: исторические, философские, методологические аспекты. Сборник статей 3-ей Региональной научной конференции молодых ученых. Курский Государственный Университет. Курск, 2023. С. 375–381.

20. Сыряпина М. В., Лыкова М. П., Распопина Т. А. Обзор технологий искусственного интеллекта с этической точки зрения // Актуальные проблемы науки и образования в условиях современных вызовов. Сборник материалов XVIII Международной научно-практической конференции. Москва, 2023. С. 32–35.

21. Этические аспекты искусственного интеллекта [Электронный ресурс] // UNESCO. URL: https://www.unesco.org/ru/artificial-intelligence/recommendation-ethics (дата обращения: 15.09.2024).

22. Рекомендация об этических аспектах искусственного интеллекта [Электронный ресурс] // UNESCO. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus (дата обращения: 16.09.2024).

23. Регламент Европейского Союза об искусственном интеллекте [Электронный ресурс] // Национальный портал в сфере искусственного интеллекта. URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikh-stranakh/2024_reglament_evropeyskogo_soyuza_ob_iskusstvennom_intellekte_ano_cifrovaya_ekonomika_/ (дата обращения: 16.09.2024).

References

1. Nosov N.Yu., Sokolov M.D. Development of state intelligence. Trends in the development of artificial intelligence. *Sovremennie nauchnie issledovaniya i innovacii = Modern scientific research and innovation*. 2016; 5(61): 86-89. (In Russ.).

2. Savchenko I.S. Hostage of the «Chinese room» or in search of consciousness in machines. *Zametki uchenogo = Notes of a scientist.* 2020; 2: 138-143. (In Russ.).

3. Fersht V.M. Latkin A.P. Ivanova V.N. Modern approaches to the use of artificial intelligence in medicine. Territoriya novih vozmojnostei. *Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa = Territory of new opportunities. Bulletin of the Vladivostok State University of Economics and Service.* 2020. Vol. 12; 1(48): 121-130. (In Russ.).

4. Kalinovskaya I.N. Zavyalova A.O. Directions of using artificial intelligence in the organization of production at light industry enterprises. *Materiali i tehnologii = Materials and technologies*. 2020; 1(5): 50-56. (In Russ.).

5. Minbaleev A.V. Berestnev M.A. Evsikov K.S. Regulation of the use of artificial intelligence in the extractive industry. *Izvestiya Tulskogo gosudarstvennogo universiteta. Nauka o Zemle = Proceedings of Tula State University. Earth science.* 2022; 2: 509-525. (In Russ.).

6. Spicin I.N. Tarasov I.N. The use of artificial intelligence in the administration of justice: theoretical aspects of legal regulation (formulation of the problem). *Aktualnie problemi rossiiskogo prava = Actual problems of Russian law*. 2020. Vol. 15; 8(117): 96-107. (In Russ.).

7. Malina M.A. The use of artificial intelligence in the administration of justice in criminal cases: problems and prospects. *Gosudarstvo i pravo = State and law*. 2022; 1: 91-97. (In Russ.).

8. Gorohova S.S. Artificial intelligence in the context of ensuring national security. *Nacionalnaya bezopasnost / Nota Bene = National security / Nota Bene.* 2020; 3: 15-31. (In Russ.).

9. Google programmer insists that a chatbot with artificial intelligence is a reasonable being [Electronic resource] // BBC NEWS. URL: https://www.bbc.com/russian/news-61775714.

10. The National Security Strategy of the Russian Federation (Approved by Decree of the President of the Russian Federation No. 400 dated 07/02/2021) // The legal reference and information system «Garant».

11. The Strategy of scientific and technological development of the Russian Federation (Approved by Decree of the President of the Russian Federation dated 02/28/2024 No. 145) // The legal reference and information system «Garant».

12. The Collective Security Strategy of the Collective Security Treaty Organization for the period up to 2025 dated October 18, 2016 (Approved by the Decision of the Collective Security Council of the Collective Security Treaty Organization dated 10/14/2016) // Legal reference and information system «Garant».

13. Agreement on cooperation of the member States of the Commonwealth of Independent States in combating crimes in the field of information technology dated September 28, 2018 // Legal reference and information system «Garant».

14. Minbaleev A.V. Problems of using artificial intelligence in countering cybercrime. *Vestnik Yujno_Uralskogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of the South Ural State University. Series: Law.* 2020. Vol. 20; 4: 116-120. (In Russ.).

15. The National Strategy for the Development of Artificial Intelligence for the period up to 2030 (Approved by Decree of the President of the Russian Federation dated 10.10.2019 No. 490 as amended. dated 02/15/2024) // Legal reference and information system «Garant».

16. Seidakmatov N.A. Kucev E.V. Integration of artificial intelligence into information security systems: challenges and opportunities. *Nauchnie issledovaniya v Kirgizskoi Respublike = Scientific research in the Kyrgyz Republic*. 2024; 1: 24-34. (In Russ.).

17. Fedotov S.V. Application of artificial intelligence technologies in cybersecurity // Culture of information security: challenges of the time. Materials of the XIV International Scientific and Practical Conference of Students, postgraduates and Young Scientists. Moscow, 2024: 183-187.

18. Pristanskov V.D. Haratishvili A.G. Evstratova Yu.A. Artificial intelligence — a new form of using special knowledge in the investigation and disclosure of cybercrimes. *Vserossiiskii kriminologicheskii jurnal = All-Russian Journal of Criminology.* 2023. Volume 17; 6: 586-596. (In Russ.).

19. Chapligin M.S. Postnikov A.V. The moral aspect of the use of artificial intelligence // Actual problems of modern science: historical, philosophical, methodological aspects. Collection of articles of the 3rd Regional Scientific Conference of Young Scientists. Kursk State University. Kursk, 2023: 375-381.

20. Siryapina M.V. Likova M.P. Raspopina T.A. Review of artificial intelligence technologies from an ethical point of view // Actual problems of science and education in the context of modern challenges. Collection of materials of the XVIII International Scientific and Practical Conference. Moscow, 2023: 32-35.

21. Ethical aspects of artificial intelligence [Electronic resource] // UNESCO. URL: https://www.unesco.org/ru/artificial-intelligence/recommendation-ethics.

22. Recommendation on the ethical aspects of artificial intelligence [Electronic resource] // UNESCO. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus.

23. Regulation of the European Union on artificial intelligence [Electronic resource] // National portal in the field of artificial intelligence. URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikh-stranakh/2024_reglament_evropeyskogo_soyuza_ob_iskusstvennom_intellekte_ano_cifrovaya_ekonomika.