УДК 342, 343; 34.096 DOI: 10.31249/iajpravo/2025.03.08

ЗАХАРОВ Т.В.[1] ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА СИСТЕМУ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ВООРУЖЕННЫЕ КОНФЛИКТЫ (Обзор)

Аннотация. В обзоре представлены позиции российских и зарубежных ученых по отдельным вопросам международной информационной безопасности, в том числе различия в стратегиях США и России в этой области международного права. Рассматриваются вопросы применения технологий искусственного интеллекта в сфере национальной безопасности и в случае вооруженных конфликтов, проблемы злонамеренного использования искусственного интеллекта в целях изменения баланса сил в международной системе безопасности и юридической ответственности в области использования искусственного интеллекта в военных целях.

Ключевые слова: международное право; международная информационная безопасность; национальная безопасность; искусственный интеллект; автономные системы вооружения.

ZAKHAROV T.V. The Impact of the Artificial Intelligence on International Information Security System and Armed Conflicts (Review)

Abstract. The review presents the positions of Russian and foreign scientists on certain issues of international information security, including differences in the strategies of the United States and Russia in this area of international law. The issues of the use of artificial intelligence technologies in the field of national security and in the event of military conflicts, the problems of the malicious use of artificial intelligence in order to change the balance of power in the international secu-

[1] *Захаров Тимофей Владимирович* – научный сотрудник отдела правоведения ИНИОН РАН.

rity system and legal responsibility in the field of the use of artificial intelligence for military purposes are considered.

Keywords: international law; international information security; national security; artificial intelligence; autonomous weapons systems.

Для цитирования: Захаров Т.В. Влияние искусственного интеллекта на систему международной информационной безопасности и вооруженные конфликты (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 105–117. – DOI:10.31249/iajpravo/2025.03.08

Введение

На фоне стремительного развития информационно-коммуникационных технологий (ИКТ) и процессов глобализации актуальность вопросов информационной безопасности стала особенно очевидной, как и то, что практически каждая страна использует ИКТ в военно-политических и экономических целях. На наших глазах проходят противоборства стран в киберпространстве и информационные войны государств, которые включают проведение компьютерных атак на государственные ресурсы других стран, проведение в глобальном информационном пространстве действий, которые мешают стабильности, безопасности и поддержанию международного мира [1, с. 116].

Сегодня системы международной информационной безопасности подвергаются сложной проверке широким внедрением ИИ в экономическую и военную сферы. Использование ИИ, в частности, в военных целях зачастую опережает не только правовое регулирование, но и прогнозирование возможных последствий. В связи с этим внимание ученых сосредоточено на сложных вопросах юридической, международно-правовой ответственности.

В обзоре рассматриваются стратегии России и США в сфере международной информационной безопасности, влияние внедрения технологий ИИ на системы международной безопасности и их нормативные основы, предпосылки юридической ответственности за применение ИИ в военных целях.

Сходства и различия в стратегиях США и России в сфере международной информационной безопасности

Как показали результаты исследования, проведенные М.Р. Загайновым, доцентом кафедры правового регулирования экономи-

ческой деятельности юридического факультета Финансового университета при Правительстве РФ, США стремятся стать единственным лидером в глобальном информационном пространстве и подчинить себе другие страны, в то время как Россия организует международный диалог по информационной безопасности и сотрудничеству с другими странами, вовлекая их в качестве партнеров [1, с. 117].

После создания сети Интернет США локализовали управление этой Сетью преимущественно на своей территории. Придание ей глобального характера позволяет США использовать свое доминирование для решения собственных, в том числе силовых задач, как то: организация масштабных разведывательных операций и проведение компьютерных атак на критическую информационную инфраструктуру суверенных государств. Как отмечает М.Р. Загайнов, для сохранения своей лидирующей позиции США пытается принять всевозможные меры для изоляции информационного пространства от неугодных стран, меняя ранее установленные подходы. Чтобы противостоять этому, Россия неоднократно выступала за введение регулирования для обеспечения международной информационной безопасности [там же, с. 117].

Россия, констатирует М.Р. Загайнов, последовательно реализует свой подход к ответственному поведению государств в цифровой среде, как на своей территории, так и во внешней политике. В частности, 26 мая 2021 г. на заседании ООН была принята предложенная Россией резолюция 75/282 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». В это же время была завершена деятельность рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ, созданной по российской инициативе еще в 2018 г. Ее итоговый доклад включает рекомендации о необходимости продолжить переговорный процесс по международной информационной безопасности под эгидой ООН в ближайшие пять лет.

Развивая идею объединения стран в сфере обеспечения международный информационной безопасности, Россия предложила создать реестр контактных пунктов, чтобы наладить прямую связь между компетентными органами стран. Это могло бы не только помочь своевременному реагированию на компьютерные атаки, но и значительно снизить напряженность в случае неправильного понимания киберинцидентов [там же, с. 119].

Американский подход к информационной безопасности в киберпространстве

Подход США к безопасности в киберпространстве, по мнению М.Р. Загайнова, кратко можно назвать: «лучшая форма защиты – нападение». Основная идея нормативно-правового регулирования в США вопросов кибербезопасности сводится к информационному господству [там же, с. 119–120].

В это же время Соединенные Штаты совместно с более чем 55 странами подписали в 2022 г. Декларацию о будущем Интернета, разработанную в США. Эти государства, согласно Декларации, выступают против подавления свободы выражения мнений, цензуры независимых новостных источников, продвижения дезинформации, вмешательства в выборы других стран. Как отмечает заместитель секретаря Совета безопасности РФ О.В. Храмов, «подписанты Декларации фактически делегировали Вашингтону свое суверенное право на обладание национальной информационной инфраструктурой, поскольку корпорация по управлению доменными именами и IP-адресами (ICANN), на которую возложены контрольные функции над глобальной сетью, на практике полностью подчинена американскому правительству» [цит. по: 1, с. 120]. По сути, считает Загайнов, данный документ наделяет США монополией в области регулирования и позволяет Вашингтону подмять под себя информационные инфраструктуры суверенных государств [там же, с. 120].

Одной из наиболее актуальных проблем в сфере международной информационной безопасности можно назвать односторонние киберсанкции США. Так, США ограничили импорт высокотехнологичной продукции в Россию и запретили участие России во Всемирном мобильном конгрессе. В июне 2022 г. Белый дом заявил, что сведет на нет сотрудничество в области технологий и науки с государственными российскими исследовательскими учреждениями и лицами, связанными с ними [там же, с. 122].

Искусственный интеллект как фактор изменения баланса сил в международной системе информационной безопасности

Одной из проблем в области мировой информационной безопасности нового поколения можно назвать злонамеренное использование искусственного интеллекта, например, для упрощения практик дезинформации с помощью создания фейковых

аудиоклипов и видеороликов. Также отмечается использование технологий ИИ для осуществления пропагандистской деятельности террористическими организациями [1, с. 122].

В связи с этим, именно ИИ рассматривается в качестве фактора изменения баланса сил в системе международной информационной безопасности. При этом решения алгоритма ИИ заранее предугадать невозможно [там же, с. 122].

При этом Госдеп США с 2022 г. уже использует ИИ и другие передовые ИТ-технологии для пропаганды против России и Китая. По заявлению Госсекретаря США Э. Блинкина, Соединенные Штаты используют ИИ для сбора доказанных фактов российской дезинформации, чтобы сообщить о ней партнерам по всему миру. В 2024 г. администрация президента Д. Байдена заявила о том, что рассматривается возможность по ограничению доступа к развитым моделям ИИ России, Китая и некоторых других стран. По сути, США открывает новый фронт с целью оградить ряд стран от американских технологий ИИ [там же, с. 122].

Способность разрабатывать и внедрять новейшие технологии, в том числе ИИ, рассматриваются М. Горовицем, профессором Пенсильванского университета (США), Ш. Пиндайк, исследователем в области технологий и международной безопасности Института глобальных конфликтов и сотрудничества Калифорнийского университета (США), Ливерморской и Лос-Аламосской национальных лабораторий (США) и К. Махони, докторантом факультета политических наук Пенсильванского университета, исследователем Вашингтонского центра новой американской безопасности (Center for a New American Security (CNAS)). Государства, стремящиеся быть на шаг впереди других, часто ищут стратегии, использующие новые технологии для усиления своей способности оказывать влияние на международной арене, подчеркивают они [2, p. 914].

В зависимости от того, как используются достижения ИИ в военной сфере, здравоохранении, образовании, производстве, финансах, социальных службах и других видах деятельности, зависит национальное могущество государства. Однако быстрые темпы внедрения ИИ во многих сферах затрудняют прогнозирование его влияния на глобальный баланс сил. Различия – в том, как национальные экономики и вооруженные силы используют ИИ сегодня. По мнению авторов, применение ИИ усугубляет неопределенность в отношении как возможностей, так и уязвимостей, которые ИИ создает для государств, стремящихся к власти [Ibid, p. 914].

Факторы, такие как внешняя и организационная среда, отношения между государством и обществом и идеологический дух, предопределяют то, насколько широко государства способны разрабатывать и применять системы ИИ. Риски и уязвимость, характерные для любой технологии, также влияют на то, как их внедрение меняет возможности государств по реализации своих интересов. Повсеместное использование алгоритмов для дополнения или замены ролей, ранее выполнявшихся людьми, может изменить ключевые особенности принятия решений в гражданской и военной сферах. Учитывая эти факторы, аналитики и практики могут наилучшим образом понять влияние ИИ на распределение международной власти, чтобы разработать оптимальные стратегии национальной безопасности [Ibid, p. 915].

В самом широком смысле международные нормы часто, как замечают авторы, разрабатываются и принимаются в результате процесса, в ходе которого ведутся активные дискуссии вокруг проектов «инициаторов-нормотворцев». Широкий круг участников, вовлеченных в дебаты о правильном использовании ИИ, в целом говорит о том, что в инициаторах создания нормы нет недостатка. Так, помимо промышленно развитых стран, которые лидируют в разработке ИИ, государства Глобального Юга взяли на себя ведущую роль в некоторых областях, особенно в дискуссиях об ограничениях на автономные системы вооружения [Ibid, p. 927]. Появление регулирующих норм, ограничивающих то, какие виды систем ИИ государства должны или не должны использовать в каких-либо (или в определенных) контекстах, обязательно будет зависеть от аргументированности позиции «инициаторов-норматворцев». До сих пор, как в демократических, так и в автократических государствах те, кто обладает наибольшими возможностями для применения ИИ в военных целях, не решались присоединиться к рядам призывающих к запрету автономных систем вооружения. Изменится ли это в будущем – вероятно, будет зависеть от изменений в контексте дискуссий, полагают авторы. Например, нормы, запрещающие автономное или другие классы оружия с поддержкой искусственного интеллекта, могут следовать по стопам табу ядерного оружия, возникшего в результате его катастрофического применения. Альтернативой могут быть аргументы в пользу более строгого регулирования военного ИИ, потенциально способного нарушать международное гуманитарное право. В то время как аргументы, основанные на международном гуманитарном праве, помогли разработать негативные нормы, запрещающие ослепляющие

лазеры и другое оружие неизбирательного действия, уникальные характеристики оружия, основанного на ИИ, позволяют вести дискуссии о возможности применения позитивных норм, предписывающих контроль со стороны человека [Ibid, p. 927].

Особое значение имеет вопрос о том, будут ли государства, внедряющие технологии ИИ в смертоносных целях, использовать такие технологии надлежащим образом. С точки зрения М. Горовица, Ш. Писайк и К. Махони, первые попытки Евросоюза ввести нормативные стандарты этичного ИИ в своем Общем регламенте по защите данных (General Data Protection Regulation (GDPR)) показывают, что государства склонны игнорировать значимость международных норм, когда речь заходит о защите основных интересов национальной безопасности. Права на поддающийся объяснению искусственный интеллект и защиту данных ограничены положениями ст. 23 Общего регламента о национальной безопасности, в соответствии с которыми государства – члены ЕС могут ограничивать права отдельных субъектов данных в целях национальной и общественной безопасности, обороны и связанных с ними целях [Ibid, p. 927].

С другой стороны, некоторые государства – лидеры в области ИИ предприняли шаги, которые являются реакцией на общественное давление по соблюдению норм применения ИИ в военных целях. В сентябре 2020 г. США учредили Партнерство по искусственному интеллекту в интересах обороны (AI Partnership for Defense (PfD) между государствами-единомышленниками (like-minded states), внедряющими ИИ в военных целях, для укрепления практического сотрудничества по обмену данными, взаимодействия в других областях. По мнению авторов, политические рамки, разработанные государствами с наиболее мощными вооруженными силами, включая США и Китай, в соответствии с международными стандартами и этическими соображениями дают основания полагать, что международные нормы и практика государств будут продолжать развиваться параллельно, в диалоге друг с другом [Ibid, p. 928].

Возможные пути создания системы международной безопасности с помощью искусственного интеллекта

Один из вопросов, рассматриваемых М. Горовицом, Ш. Писайк и К. Махони, – направления наибольшего сосредоточения усилий государств на создании системы международной безопасности, все более насыщаемой средствами ИИ. Здесь авторы отмечают следующие проблемы:

1) большинство государств по-прежнему находятся на ранних стадиях обдумывания того, как ИИ будет интегрирован в гражданскую и военную сферы, и как можно использовать такие изменения, особенно в долгосрочной перспективе, для повышения своей способности достигать национальных целей. Целый ряд новых организаций и многосторонних форумов обсуждают риски, связанные с «милитаризацией» ИИ, и тем самым помогают формировать у государств представление не только о затратах и выгодах, связанных с обеспечением безопасности, но и о том, как это может повлиять на восприятие законности и целесообразности использования таких технологий;

2) помимо усилий государств, сосредоточенных на прогнозировании и разработке стратегии на десятилетия вперед, государства также осуществляют краткосрочные инвестиции в целях застраховаться от возможных преимуществ «первопроходцев», которые такие государства, как Соединенные Штаты и Китай, могли бы получить от ИИ;

3) стремление государств прогнозировать развитие ИИ и управлять ИИ влияет на их интересы в области безопасности и, по мнению авторов, будет по-прежнему осложняться скоростью, с которой новаторы в частном секторе опережают возможности регулирующих органов [2, p. 928–929].

Гиперглобализация продолжает способствовать быстрому распространению технологий и разработке новых инструментов, выходящих за рамки государственных исследований и разработок. То, как государства решат организовать свою внутреннюю политическую экономику в сфере применения ИИ, также будет иметь последствия для их успеха или неспособности сохранить возможность влиять на условия, в которых они конкурируют с другими в вопросах безопасности. Таким образом, заключают М. Горовиц, Ш. Писайк и К. Махони, во многих отношениях реакция государств на внутриполитические вызовы, связанные с инновациями в области ИИ, сыграет решающую роль в их позиционировании на международной арене [Ibid, p. 929].

К вопросу юридической ответственности в случае применения искусственного интеллекта в военных операциях и системах вооружений

На этой теме сосредоточен И. Нвагбара, исследователь из Канадского института международно-правовой экспертизы. В цен-

тре его внимания следующие вопросы: в какой степени системы ИИ надлежит использовать в конфликтных ситуациях; должны ли они использоваться для ведения боевых действий или должны ограничиваться разведкой, наблюдением и рекогносцировкой? Главный юридический вопрос в связи с применением ИИ в военных целях, волнующий автора и других ученых: кто несет ответственность за ущерб и жертвы, возникшие в результате автономных решений систем ИИ [3, p. 18–19].

Если системы оружия с искусственным интеллектом, такие как робототехника или смертоносные автономные системы вооружения (lethal autonomous weapons systems (LAWS)), используются для ведения физического боя, возникает вопрос, могут ли системы ИИ адекватно различать комбатантов и гражданских лиц? Ожидается, что в эти системы могут быть введены опознавательные знаки различных национальных вооруженных сил. Таким образом, у систем ИИ не могло бы возникнуть проблем с идентификацией и различением комбатантов в международных вооруженных конфликтах. Однако в категории немеждународных вооруженных конфликтов, которые составляют в современных конфликтах основную часть, возникает затруднение, когда для существующих и потенциальных негосударственных вооруженных группировок не существует установленных знаков отличия. В соответствии с международным гуманитарным правом, негосударственные вооруженные группы в немеждународных вооруженных конфликтах не имеют статуса комбатантов, как и члены организованных вооруженных групп, принимающие активные отличия [Ibid, p. 19].

Возникают следующие вопросы: как системы вооружения с ИИ, развернутые для ведения боевых действий в немеждународных вооруженных конфликтах, могут отграничивать тех, кто активно участвует в боевых действиях, от тех, кто не принимает активного участия в боевых действиях, в отсутствие знаков отличия? Будут ли системы ИИ, такие как роботы, обучены реагировать только в случае первоначального нападения со стороны людей? Если так, то системы ИИ будут лишены возможности самостоятельно наносить упреждающие удары в целях самообороны, что может лишить сторону военного преимущества, которое она стремится получить, применяя ИИ. Что представляет собой «атака» со стороны людей, и какой ответ системы ИИ дадут на такую «атаку» [Ibid, p. 20]?

Вместе с тем усовершенствованные технологии, включая системы ИИ с улучшенными возможностями наведения на цель, мо-

гут способствовать дальнейшему проведению различий между комбатантами и не комбатантами во время вооруженного конфликта [Ibid, p. 20].

Возникает спор о том, должны ли такие боевые роботы быть способны самостоятельно принимать решение о нанесении удара как система ИИ, или же это должны быть люди-операторы, наблюдающие за ситуацией с помощью монитора и принимающие это решение. Смогут ли системы ИИ применять сложные решения? Понимают ли они вообще концепцию сопутствующего ущерба и принцип пропорциональности, которые могли бы служить оправданием жертв среди гражданского населения пропорционально законному военному преимуществу [Ibid, p. 21]?

Несмотря на неопределенность, так или иначе, все сформулированные выше И. Нвагбаром вопросы касаются юридической и социальной ответственности за применение систем вооружения с использованием ИИ. С одной стороны, оспаривается ответственность государств за серьезные нарушения международного гуманитарного права. С другой стороны, международное уголовное право регулирует индивидуальную уголовную ответственность. Учитывая, что до сих пор исследовательские усилия, направленные на разработку смертоносных автономных систем вооружения, инициировались и финансировались государствами, – вопрос об ответственности начинается с государств [Ibid, p. 21].

Международное гуманитарное право, считает автор, должно применяться ко всем системам вооружений и, таким образом, ответственность государства за нарушение принципов международного гуманитарного права при применении смертоносных автономных систем вооружения возможна. Личная ответственность человека за решения о применении систем вооружений также должна сохраняться, поскольку ответственность не может быть передана машинам [Ibid, p. 22].

Однако практическое применение ответственности является запутанным и рискованным. Для установления индивидуальной уголовной ответственности требуется психологический элемент в той же мере, что и материальные элементы преступления.

Двумя факторами, определяющими психологический элемент преступления, являются «намерение» и «знание». Могут ли смертоносные автономные системы вооружения учитывать знание об основных международных преступлениях и действиях, лежащих в их основе? Могут ли они оценивать и разграничивать ситуации, которые представляют собой международные преступле-

ния, и отличать их от ситуаций, которые таковыми не являются? Если смертоносные автономные системы вооружения не могут понять знание о международных преступлениях, то по умолчанию у них определенно не может быть намерения их совершать. Возникает еще одна философская загадка, которая заключается в том, что если смертоносные автономные системы вооружения могут учитывать сложные знания о международных преступлениях и могут выбирать, иметь намерение их совершать, можно ли действительно говорить, что такие системы вооружений являются автономными или просто предварительно запрограммированными (специалистами-людьми) на то, чтобы иметь возможность оценить основные правовые аспекты международных преступлений? Покажет только время, полагает автор [Ibid, p. 23].

Ряд конкретных вопросов, касающихся юридической ответственности в случае применения систем ИИ в вооруженных конфликтах, продолжают занимать И. Нвагбара: если станет возможным, что смертоносные автономные системы вооружения будут иметь знания о международных преступлениях благодаря своим собственным когнитивным процессам, какие лица возьмут на себя ответственность за их преступления? Специалисты, создавшие такие системы (аппаратное и программное обеспечение)? Несут ли люди ответственность за физическое обслуживание таких систем, а также за разработку и применение таких систем отвечают военные и политические лидеры? [3, p. 23].

Еще один вопрос, касающийся индивидуальной уголовной ответственности за действия смертоносных автономных систем вооружения, заключается в том, какой вид ответственности применяется. Поскольку автономная система принимает решения совершить действие посредством своих автономных когнитивных процессов, она является непосредственным исполнителем. Поскольку люди не принимали участия в принятии автономного решения и не имели полного контроля над этим решением и последующими действиями, юридически было бы невозможно считать людей соисполнителями, косвенными исполнителями или косвенными соисполнителями. Таким образом, ответственность вышестоящего командования (superior responsibility) может стать следующим важным моментом в отношении режима ответственности [Ibid, p. 23].

Первый фактор, который необходимо определить в режиме ответственности вышестоящего командования, заключается в том, обладают ли военные командиры или лица, фактически выпол-

няющие функции военных командиров, эффективным управлением и контролем над силами, совершающими преступление. Это в полной мере касается и смертоносных автономных систем вооружения. В то же время, возможно ли обеспечить эффективное управление автономной системой вооружений? Есть ли в такой автономной системе вооружений компонент, который позволяет осуществлять управление человеком? Если да, то делает ли это такую систему по-настоящему автономной или полуавтономной?

Вторым фактором, связанным с ответственностью такого уровня командования, является осведомленность о совершении преступления. Учитывая автономный и рекурсивный характер смертоносных автономных систем вооружения, следует подчеркнуть, что их внутренний когнитивный процесс, а также процесс принятия решений не только не поддаются точному прогнозированию, но и не открыты для обсуждения с внешними силами [Ibid, p. 24].

Хотя, считает И. Нвагбара, можно установить факт совершения преступления автономной системой, шансы на то, что военное командование должно было знать, что система собирается его совершить, невелики, особенно когда в этот момент военный командир больше не может предотвратить их совершение. И предлагает сконструировать особый режим индивидуальной уголовной ответственности. Такой режим, по его мнению, может логично привести к ответственности политических и военных лидеров, ответственных за разработку и применение смертоносных автономных систем вооружения и стать тяжелым бременем для политических и военных элит стран, показывая им, что именно они будут нести ответственность за авантюры в области военных технологий [3, p. 24].

Заключение

Учитывая, что появление ИИ только начинает открывать новые возможности в военной сфере и сфере международной безопасности, остается неясным, каким образом субъекты международной системы придут к пониманию законности использования ИИ в условиях (военных) конфликтов. Насущная задача сейчас – заложить прочную теоретическую основу, способную максимально охватить практические проблемы, которые провоцирует повсеместное распространение технологий ИИ [2, p. 915, 926].

Государства осознают грозящую ИИ опасность и, тем не менее, не прекращают своих усилий по разработке смертоносных автономных систем вооружения. Более того, они объединяются

для выработки принципов разработки и применения ИИ в военных целях. Так, Франция и Германия подготовили в 2019 г. политическую декларацию «11 руководящих принципов, регулирующих разработку и использование автономных систем вооружения». Хотя такая декларация не является юридически обязательной или окончательным решением – ибо не наносит ущерб будущим обсуждениям, она явно показывает направленность политики – решать вопросы морального, юридического и оперативного плана, препятствующие появлению новых технологий, в том числе в информационной и военной сферах [3, p. 21–22].

Список литературы

1. Загайнов М.Р. Вопросы развития сотрудничества США и России в сфере международной информационной безопасности // Социально-политические науки. – 2024. – Т. 14, № 3. – С. 115–124.
2. Horowitz M., Pindyck Sh., Mahoney C. AI, the International Balance of Power, and National Security Strategy // The Oxford Handbook of AI governance / ed. by Justin B. Bullock, Yu- Che Chen, et. – Oxford: Oxford Univ. Press, 2024. – P. 914–936.
3. Nwagbara I. Artificial Intelligence and International Criminal Law // Artificial Intelligence and the Future of International Law Bridging Rights, Trade, and Arbitration / ed. by A. Poorhashemi. – London: Springer, 2024. – P. 16–27.