УДК 34.096; 341.1/8 DOI: 10.31249/iajpravo/2025.03.14

САЛЬНИКОВА А.К.[1] РЕЦЕНЗИЯ НА КНИГУ: МОНТАСАРИ Р. КИБЕРПРОСТРАНСТВО, КИБЕРТЕРРОРИЗМ И МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ: УГРОЗЫ, ОЦЕНКА И ОТВЕТНЫЕ МЕРЫ.
SALNIKOVA A.K. [Book review]. – Book review: Montasari R. Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses. – Cham: Springer NATURE Switzerland AG, 2024. – 270 p.

Ключевые слова: киберпространство; искусственный интеллект; кибертерроризм; терроризм; права человека; дипфейки.
Keywords: cyberspace; artificial intelligence; cyberterrorism; terrorism; human rights; deepfakes.

Для цитирования: Сальникова А.К. [Рецензия] // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. Государство и право. – 2025. – № 3. – С. 184–191. – Рецензия на книгу: Montasari R. [Монтасари Р.] Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses = Киберпространство, кибертерроризм и международная безопасность в условиях Четвертой промышленной революции: угрозы, оценка и ответные меры. – Cham: Springer NATURE Switzerland AG, 2024. – 270 p. – DOI: 10.31249/iajpravo/2025.03.14

Книга Резы Монтасари, старшего преподавателя кафедры криминологии Университета Суонси (Уэльс, Великобритания), имеющего докторскую степень в области цифровой криминалистики, представляет собой комплексное междисциплинарное ис-

[1] *Сальникова Анастасия Кирилловна*, младший научный сотрудник Центра междисциплинарных исследований ИНИОН РАН.

следование ключевых вопросов, связанных с кибертерроризмом, киберпространством, национальной и международной безопасностью. Как отмечает сам автор в аннотации к книге, в ней критически рассматриваются сложные взаимосвязи между киберпространством, кибертерроризмом, национальной и международной безопасностью и технологией ИИ. В этих целях раскрываются двойственная природа этих элементов, их потенциал как для полезного и конструктивного, так и для вредоносного применения в контексте современных киберугроз. Автор исследует мотивы, методы и последствия кибертерроризма, оценивает международные усилия по противодействию кибертерроризму, показывает прогресс в выработке единого подхода к реагированию и устранению сохраняющихся проблем и разногласий между государствами, представляет практические стратегии, направленные на выявление террористических атак и реагирование на них. Много внимания Р. Монтасари уделяет анализу эффективности, сильных и слабых сторон реагирования на кибератаки и векторы для совершенствования стратегий их предупреждения и борьбы с ними.

Книга состоит из введения и четырех разделов: раздел I – «Понятие терроризма и контртеррористические стратегии»; раздел II – «Пространство кибертерроризма», посвящен изучению современной природы кибертерроризма неизбежности его угрозы национальной безопасности; раздел III – «Противодействие терроризму с помощью технологических ресурсов»; раздел IV – «Искусственный интеллект и национальная и международная безопасность». Целями данного исследования является изучение различных вопросов, связанных с киберпространством и искусственным интеллектом: рассматриваются актуальные проблемы, связанные с темой исследования, вопросы трансформации терроризма ввиду массового распространения новых технологий и усилия международного сообщества по противодействию терроризму, обосновывается необходимость правовой регламентации регулирования новых технологий, а также представление практических рекомендаций специалистам.

Война в Ираке, которой посвящена глава 2 «Раскрытие государственных преступлений: критический анализ войны в Ираке и ее глобальных последствий» раздела I, служит, по словам автора, важнейшей отправной точкой данного исследования. В этой главе освещаются хитросплетения международной политики, вопросы ответственности государств и долгосрочные последствия военных вмешательств. Война в Ираке 2003 г. рассматривается как одно из

самых спорных политических решений за последние десятилетия (p. 19). В контексте общей темы данной работы в этой главе через анализ событий конкретного конфликта, его причин, действий мировых лидеров изучается само явление терроризма, обозначаются тенденция роста его масштаба, а также долгосрочные негативные последствия. Оценивая эти события, Р. Монтасари считает уместным дать понятие государственного преступления как действия или бездействия государства, которые нарушают внутреннее и международное законодательство, права человека или систематически наносят ущерб своему собственному населению или населению другого государства. Война в Ираке квалифицируется как агрессивная война, нарушающая Устав ООН.

Интерес представляет также исследование проблем, связанных с гуманитарной интервенцией, ее мотивами, которые в значительной степени обусловлены предполагаемой угрозой терроризма и оружия массового уничтожения в Ираке. Кроме того, обсуждаются общие итоги и долгосрочные последствия этого важного события (p. 19–26).

Следующая глава 3 раздела I – «Оценка эффективности контртеррористических стратегий Великобритании и альтернативных подходов» – содержит анализ положений законодательных актов Великобритании, принятых в целях противодействия терроризму. Великобритания сталкивается с постоянной проблемой противодействия терроризму. Объединенный центр анализа терроризма (JTAC), работающий под эгидой Службы безопасности MI5, присвоил текущему национальному уровню террористической угрозы наименование «существенный», что указывает на вероятную террористическую атаку. Понятие терроризма, как оно определено в Законе Великобритании о терроризме 2000 г., охватывает акты насилия или угрозы насилия, направленные на оказание влияния на правительство или запугивание широкой общественности с целью достижения конкретных политических, религиозных или идеологических целей. Такие действия могут быть связаны с угрозой или причинением серьезного насилия отдельным лицам, причинением существенного имущественного ущерба или выводом из строя электронных систем. Ученые также дают академическое определение терроризма, охарактеризовав его как тактику, которая вселяет страх и использует «принудительное политическое насилие». Это часто рассматривается как рассчитанная и демонстративная практика, включающая «прямые насильственные действия», лишенные «юридических или моральных ограничений» (p. 28).

Цель этой главы – изучение эффективности контртеррористических стратегий Великобритании и анализ альтернативных подходов, основанных на фактических данных, критическая оценка текущей практики борьбы с терроризмом, применяемой Соединенным Королевством, с учетом спорных вопросов, связанных с их эффективностью. В частности, основное внимание уделяется британскому механизму борьбы с терроризмом, известному как Антитеррористическая стратегия Соединенного Королевства, разработанная в 2003 г., последняя редакция которой была принята в 2023 г. Р. Монтасари раскрывает ключевые направления Стратегии – «предотвращать, преследовать, защищать и готовиться» (prevent, pursue, protect и prepare). Особой критике подвергается такое ее направление, как «предотвращать» (prevent) за стигматизацию мусульман, непрозрачность механизмов контроля, недостаток независимости. При этом на основе всестороннего изучения текущей практики в главе обозначены основные проблемы и предложены конкретные рекомендации, направленные на достижение баланса между жесткими мерами безопасности и защитой индивидуальных прав, подчеркивается необходимость увеличения прозрачности деятельности ответственных органов государственной власти, а также достижения большей открытости.

Отдельное внимание в главе 4 «Понимание и оценка роли женщин в борьбе с терроризмом» раздела I автор уделяет рассмотрению феномена женщин в терроризме. Р. Монтасари опровергает устоявшийся миф, заключающийся в понимании положения женщин в терроризме исключительно как жертв, а также утверждает, что традиционный подход, который делит женщин на «жертв» и «преступниц», слишком упрощает реальность. Чтобы глубже понять мотивы совершения ими определенных действий, необходимо отказаться от жестких категорий и рассматривать их участие в терроризме как многофакторное явление. Так, рассматривается устоявшийся стереотип, в соответствии с которым роль женщин в терроризме сводится лишь к пассивному участию: жены или матери террористов, принимающих участие лишь из-за мужей и сыновей, или женщины, неспособной к принятию решений самостоятельно. Далее автор, опираясь на пул современных исследований, описывает трансформированные модели участия женщин в террористических актах: они стали активными участницами и не только исполнительницами, а организаторами, идеологами и, в исключительных случаях, лидерами террористических группировок. В качестве практических примеров рассматривается практический

опыт нескольких террористических организаций. Резюмируя проведенный анализ, автор приходит к выводу о необходимости отказа от представления женщин в терроризме исключительно в качестве жертв, а также о необходимости изучения терроризма в целом, как многосубъектного состава преступления, принимая во внимание изменяющееся положение женщин и занятие ими более активных позиций.

В следующем разделе II – «Пространство кибертерроризма» – содержится две главы: «Современный кибертерроризм: тенденции, методы противодействия и последствия пандемии» (гл. 5) и «Изучение неизбежности угрозы национальной безопасности со стороны кибертерроризма» (гл. 6). В данных главах Р. Монтасари рассматривает феномен кибертерроризма и его потенциальные последствия как новой формы террористической деятельности в условиях быстро меняющегося технологического ландшафта. В рамках исследования автор оценивает «привлекательность» кибертерроризма, а именно: высокую анонимность, низкий порог входа, а также широкое распространение цифровых технологий. Данные аспекты являются серьезным вызовом для органов национальной безопасности. Так, значительный массив преступлений и на сегодняшний день остается нераскрытым ввиду невозможности деанонимизировать лицо, совершившее преступление или способствовавшее его совершению. В рамках исследования автор достигает одной из поставленных задач – оценки реального уровня угрозы кибертерроризма для национальной безопасности. Автор приходит к выводу о том, что наличествует сложная взаимосвязь между технологическим прогрессом, уязвимостями систем и воспринимаемой угрозой кибертерроризма, а также вероятность становления кибертерроризма в качестве наиболее эффективного способа совершения преступлений и насильственных актов.

Раздел III анализируемой монографии «Использование технологий для противодействия кибертерроризму» состоит из четырех глав, 7–10, в которых рассматриваются следующие вопросы: 1) влияние интернет-технологий на радикализацию терроризма и трансформацию его привычных форм. Так, медиапространство и Интернет в целом создали благоприятную среду для распространения, вербовки и организации террористической деятельности; 2) машинное обучение и методы глубокого обучения в борьбе с кибертерроризмом; 3) этические, юридические, технические и операционные проблемы, связанные с применением машинного обучения в борьбе с кибертерроризмом; 4) решение этических,

юридических, технических и оперативных проблем в борьбе с терроризмом с помощью машинного обучения: рекомендации и стратегии (p. 109–220).

Показательно то, что в этом разделе Р. Монтасари раскрывает содержание понятия «новый терроризм», ключевыми характеристиками которого, по его мнению, выступают: высокая степень технологичности, децентрализованность, идеологическая гибкость, массовое психологическое воздействие. «Новый терроризм» для реализации целей деятельности активно использует новые технологии и цифровые платформы, в первую очередь для пропаганды и вербовки, а также социальные сети, блокчейн-технологии, технологии шифрования.

Кроме того, в этом разделе рассматриваются вопросы: 1) баланса интересов: обеспечение безопасности в обществе посредством технологий распознавания лиц и умных камер и соблюдение прав человека, в том числе на частную жизнь; 2) ответственности. С точки зрения современного уровня научно-технологического развития, как уже было отмечено выше, в большинстве случаев нет возможности деанонимизировать лицо, совершившее преступное посягательство. В связи с этим вопрос несения уголовной или административной ответственности в части субъектного состава, остается неразрешенным; 3) юрисдикция. Кибертерроризм представляет наибольшую опасность, в первую очередь за счет «удаленного» формата совершения преступления: объект и субъект преступления зачастую находятся на территории разных государств. Поэтому так актуальна консолидация усилий мирового сообщества и сотрудничество государств, в том числе в вопросе раскрытия и расследования преступлений, а также выдачи информации о совершенном акте. Систематическое рассмотрение технических, операционных, этических и правовых барьеров создает основу для разработки сбалансированных стратегий, обеспечивающих как повышение уровня безопасности, так и защиту фундаментальных прав человека.

Заключительный раздел IV – «Искусственный интеллект и национальная и международная безопасность» – охватывает три главы (гл. 11–13). В главе 11 – «Двойная роль искусственного интеллекта в онлайн-дезинформации: критический анализ» – раскрывается многогранная роль ИИ в сфере онлайн-дезинформации. В частности, рассматривается потенциал методов ИИ для создания высокореалистичной дезинформации и эффективного ее распространения среди широкой аудитории на платформах социальных

сетей. Более того, автор, характеризуя использование ИИ как средства борьбы с таким пагубным явлением, одновременно анализирует связанные с этим проблемы и этические затруднения. Для решения этих сложных проблем Р. Монтасари предлагает комплексный набор рекомендаций, направленных на их устранение и подчеркивает, что этические соображения должны быть неотъемлемой частью разработки и внедрения инструментов искусственного интеллекта, принимая во внимание непреднамеренные негативные последствия, которые могут возникнуть в результате их использования. Рассматривая многогранные проблемы, связанные с дезинформацией, генерируемой искусственным интеллектом, автор вносит значительный вклад в академическую дискуссию, а за счет формулирования практико-ориентированных рекомендаций создает основу для разработки эффективных правительственных стратегий.

В главе 12 – «Решение проблем, связанных с подделкой документов в Соединенном Королевстве: юридические и технические выводы с рекомендациями» – Р. Монтасари подчеркивает, что быстрое развитие технологий глубокого машинного обучения (DML) и ИИ за последнее десятилетие ознаменовало начало новой эры – эры цифровых инноваций. Ярким последствием стало возникновение «дипфейк-эры», рост дезинформационных рисков и угроз, превращающихся в механизм влияния и на обыденную жизнь граждан, и на политическую арену. В контексте Великобритании констатируется отсутствие комплексного законодательства, регулирующего «дипфейк-контент», а также непредвиденность скорых политических изменений в этой сфере.

Интерес у читателя может вызвать углубленный анализ этических и юридических проблем, связанных с подделкой порнографических материалов. Кроме того, в главе рассматриваются далеко идущие последствия подобной дезинформации и та роль, которую технология подделки может сыграть в усилении ее разрушительного и вредоносного воздействия. В конце главы Р. Монтасари призывает объединить усилия ученых и законодателей по реформированию законодательства в условиях внедрения ИИ и повышению цифровой грамотности для эффективного устранения потенциальных угроз, создаваемых новыми технологиями.

В завершающей главе 13 – «Влияние технологии распознавания лиц на фундаментальное право на неприкосновенность частной жизни и соответствующие рекомендации» – дается критический анализ влияния распознавания лиц на такое фундаментальное

право человека, как неприкосновенность частной жизни. С этой целью автор описывает многомерные аспекты технологии распознавания лиц (FRT), оценивает ее достоинства и присущие ей ограничения. Признавая многочисленные преимущества FRT, Р. Монтасари подчеркивает важность сбалансированного подхода, его потенциал для повышения безопасности и обеспечения гарантий соблюдения права на неприкосновенность частной жизни. По итогам этого всестороннего анализа автор предлагает ряд рекомендаций, направленных на защиту фундаментального права на неприкосновенность частной жизни в контексте внедрения системы распознавания лиц. Результаты исследования показывают, что по мере дальнейшего развития сферы применения биометрических технологий на первый план выходят такие требования, как повышение точности, прозрачности и создание надежной правовой базы. Кроме того, полученные результаты подчеркивают необходимость тщательной интеграции технологий и этики, что имеет первостепенное значение для обеспечения конфиденциальности личности.

Таким образом, можно заключить, что монография Р. Монтасари «Киберпространство, кибертерроризм и международная безопасность в эпоху Четвертой промышленной революции» представляет собой важный вклад в изучение киберугроз, кибертерроризма и роли технологий – особенно искусственного интеллекта – в обеспечении национальной и международной безопасности в эпоху Четвертой промышленной революции. Значение данной книги также состоит в ее междисциплинарном подходе, выявлении новых вызовов в сфере кибербезопасности и терроризма, а также практических рекомендациях и примерах противодействия современным угрозам. Благодаря этому данный труд становится настольным руководством для специалистов и государственных деятелей, стремящихся обеспечить безопасность в эпоху цифровой трансформации.