DOI: 10.17803/1729-5920.2024.212.7.039-048

Д. К. Боков
Университет прокуратуры Российской Федерации
г. Москва, Российская Федерация

Цифровая инфраструктура терроризма: стратегия уголовно-правового противодействия

Резюме. Статья посвящена мало разработанной в теории уголовного права проблеме уголовно-правового противодействия деятельности, связанной с цифровой инфраструктурой терроризма. Автор формулирует понятие такой инфраструктуры, выделяет ее элементы. В статье аргументируется положение о необходимости принципиального разделения таких категорий, как кибертерроризм и цифровая инфраструктура терроризма. С опорой на концепцию проактивного противодействия преступности автор предлагает конкретные меры, направленные на установление ответственности за действия, связанные с поддержкой цифровой инфраструктуры терроризма. Обоснованы предложения о необходимости: 1) разработки механизма принятия решения о том, что деятельность иностранной или международной организации связана с поддержкой терроризма; 2) установления уголовной ответственности за участие в деятельности, а равно за установление или поддержание сотрудничества с иностранной либо международной организацией, в отношении которой принято решение о признании ее деятельности направленной на поддержку терроризма.

Ключевые слова: цифровая инфраструктура терроризма; терроризм; кибертерроризм; проактивная концепция противодействия терроризму; уголовное право; цифровизация
Для цитирования: Боков Д. А. Цифровая инфраструктура терроризма: стратегия уголовно-правового противодействия. *Lex russica*. 2024. Т. 77. № 7. С. 39–48. DOI: 10.17803/1729-5920.2024.212.7.039-048

Digital Infrastructure of Terrorism: A Strategy for Criminal Law Counteraction

Dmitry K. Bokov
University of the Prosecutor's Office of the Russian Federation
Moscow, Russian Federation

Abstract. The paper is devoted to the problem of criminal law counteraction to activities related to the digital infrastructure of terrorism, which has been insufficiently developed in the theory of criminal law. The author formulates the concept of such an infrastructure, highlights its elements. The paper argues for the need for a fundamental separation of such categories as cyberterrorism and the digital infrastructure of terrorism. Based on the concept of proactive crime prevention, the author proposes specific measures aimed at establishing responsibility for actions related to the support of the digital infrastructure of terrorism. The author makes the following proposals: 1) developing a mechanism for deciding that the activities of a foreign or international organization are related to the support of terrorism; 2) establishing criminal liability for participation in activities, as well as for establishing or maintaining cooperation with a foreign or international organization in respect of which a decision has been made to recognize its activities aimed at supporting terrorism.

Keywords: digital infrastructure of terrorism; terrorism; cyberterrorism; proactive concept of countering terrorism; criminal law; digitalization

© Боков Д. К., 2024

Cite as: Bokov DA. Digital Infrastructure of Terrorism: A Strategy for Criminal Law Counteraction *Lex russica.* 2024;77(7):39-48. (In Russ.). DOI: 10.17803/1729-5920.2024.212.7.039-048

Цифровизация оказывает существенное влияние на отдельного человека, общество и государство. В связи с внедрением информационно-телекоммуникационных технологий за прошедшие годы произошли значимые и зримые изменения в сфере государственного управления, экономики, здравоохранения, образования и др. Специалисты повсеместно и единодушно отмечают, что данный процесс является необратимым и обещает множество поистине революционных преобразований. Активно ведутся дискуссии относительно тех фундаментальных изменений, которые будут связаны с определенным уровнем развития и внедрения технологий искусственного интеллекта и робототехники[1]. Уже сегодня является практически неоспоримым, что будущее человечества так или иначе будет связано с «цифрой» и во многом предопределено ею.

Как и любое явление, цифровизация подчиняется законам диалектики, имея не только положительную, но и негативную сторону. Она привела к большей — пожалуй, невиданной ранее во всей истории — отчужденности человека. Казалось бы, говорить об изоляции человека в эпоху гиперсвязанного мира принципиально неверно, ведь никогда ранее человек не обладал технологиями, позволяющими ему без особого труда и материальных затрат из одной точки мира контактировать с разными людьми, находящимися от него на расстоянии нескольких тысяч километров. Вместе с тем цифровизация привела к прогрессирующей проблеме добровольного «бегства» личности от реальности в мир искусственных конструкций, акторов и фактов. В результате этого цифровая коммуникация стала всё больше замещать традиционную, обрекая человека эпохи Четвертой промышленной революции[2] на одиночество и изоляцию в реальном мире. Парадокс заключается в том, что при внимательном рассмотрении и анализе такого ежедневного цифрового общения довольно часто обнаруживается, что преобладающим источником получения информации, эмоций и впечатлений выступает отнюдь не живой человек, а искусственно созданная личность в социальной сети, медийный проект (блог), чат-бот и т.п. Этому есть конкретное объяснение, и современная наука в целом уже довольно обстоятельно описала содержание, а также перспективные последствия цифровизации в этом отношении.

Неудивительно, что с развитием информационных технологий невиданные возможности для расширения своего влияния на массовое сознание получила идеология терроризма. Как совершенно справедливо пишет Д. А. Ковлагина, непосредственное информационно-психологическое воздействие террористических групп осуществляется посредством создания такими образованиями своих веб-сайтов, СМИ, радио- и телевизионных частот[3].

Использование террористическими образованиями средств коммуникации для пропаганды — это только часть проблемы. Компоненты информационно-телекоммуникационной инфраструктуры стали использоваться при совершении самих террористических актов. Еще в 2008 г. при террористической атаке в Мумбаи злоумышленники как на стадии приготовления, так и в процессе своих преступных действий (в результате которых погибли 166 человек) активно использовали цифровые технологии: проводили разведку посредством сетевой картографической службы, координировали свои действия, получали информацию в режиме реального времени о международной реакции на их террористический акт и действиях силовых структур[4]. Процесс включения компонентов информационно-коммуникационной инфраструктуры в террористическую деятельность развился в то, что на настоящий момент можно именовать *цифровой инфраструктурой терроризма.* Так, в структуре террористической

---

1 См., например: *Бегишев И. Р., Хисамова З. И.* Искусственный интеллект и уголовный закон. М., 2024 ; *Бегишев И. Р.* Уголовно-правовое регулирование робототехники. М., 2022.

2 См.: *Шваб К.* Четвертая промышленная революция : пер. с англ. М., 2018. С. 119.

3 *Ковлагина Д. А.* Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия. М., 2017. С. 75–76.

4 Террористическая атака на индийский город Мумбаи в ноябре 2008 года // РИА «Новости». URL: https://ria.ru/20131126/979475607.html (дата обращения: 12.03.2024).

организации «Исламское государство»[5] функционируют полноценные медиа-агентства для производства на высоком профессиональном уровне продукции в целях последующего распространения в сети «Интернет». Кроме того, созданы специальные подразделения (например, Cyber Caliphate), которые разрабатывают и используют собственное программно-техническое обеспечение (вредоносные и иные компьютерные программы, мессенджеры и т.п.), а также проводят кибератаки на информационные ресурсы отдельных организаций и государств[6].

Здесь следует внести необходимую ясность в соотношение таких категорий, как *кибертерроризм* и *цифровая инфраструктура терроризма*. Задача осложняется тем, что в отношении первого в науке уголовного права нет общепринятого подхода. Считается, что в определении кибертерроризма доминируют два направления. Согласно первому из них, кибертерроризм представляет собой совершённую в террористических целях атаку на частные или общественные информационные системы, критическую информационную инфраструктуру государства и пр.[7] Как нетрудно заметить, выделяются два ключевых критерия: террористическая цель деяния и направленность посягательства именно на компоненты цифровой инфраструктуры.

Суть второго, более широкого подхода заключается в определении кибертерроризма как любого вида террористической деятельности, совершаемого с использованием компонентов информационных технологий. В этом отношении кибертерроризмом является и прохождение обучения с использованием сетевых технологий в целях дальнейшего совершения террористических актов.

Есть весьма серьезные основания к тому, чтобы согласиться с необходимостью принципиального разделения совершаемых в террористических целях компьютерных атак против объектов информационно-телекоммуникационной инфраструктуры (собственно кибертерроризма) и любой другой террористической деятельности (склонение, пропаганда, обучение, финансирование), реализуемой с использованием цифровых технологий. Все-таки природа кибертерроризма определяется не только и не столько средством воздействия, сколько направленностью самого общественно опасного деяния, то есть его объектом. И потому кибертерроризм следует понимать исключительно как компьютерную атаку на объекты, прежде всего критически значимые, информационно-телекоммуникационной (цифровой) инфраструктуры.

Проблема определения цифровой инфраструктуры терроризма в теории уголовного права по большому счету еще не была даже поставлена. Соответственно, говорить о ее разработанности на данный момент нельзя. Специалисты лишь обсуждают факты, когда те или иные цифровые технологии были использованы террористами для своих акций.

Полагаем, что в определении цифровой инфраструктуры терроризма нужно исходить из следующих критериев. Прежде всего, в уголовно-правовом контексте цифровая инфраструктура терроризма не может быть сведена к конкретным материальным объектам (серверам, сайтам, социальным сетям, программному обеспечению и т.п.). Такие средства и технологии в правовом смысле нейтральны. Соответственно, цифровая инфраструктура терроризма представляет собой не совокупность цифровых технологий и объектов (аппаратного обеспечения, средств связи и соединения (маршрутизаторы, кабели и т.п.), средств хранения данных и др.), а специфическую *деятельность*, направленную на их изготовление, приспособление, приобретение, предоставление и использование в целях совершения террористических преступлений.

Второй критерий выявляет террористическую составляющую такой деятельности, а именно ее направленность на формирование и развитие идеологической основы, кадрового резерва, организационно-управленческих структур, материально-технической и информационной базы терроризма.

С учетом изложенного можно сформулировать определение цифровой инфраструктуры

---

[5] Организация признана террористической и ее деятельность запрещена на территории РФ. См.: решение Верховного Суда РФ от 29.12.2014 по делу № АКПИ 14-1424С // СПС «КонсультантПлюс».

[6] Информационные ресурсы ИГИЛ // Новое восточное обозрение. URL: https://journal-neo.su/ru/2015/06/08/informatsionny-e-resursy-igil/ (дата обращения: 16.03.2024).

[7] См.: *Краинский В. В.*, *Машко В. В.* Кибертерроризм: криминологическая характеристика и квалификация // Государство и право. 2023. № 1. С. 79–91.

терроризма: это *умышленные общественно опасные деяния, направленные на создание и развитие технологий и построенных на их основе цифровых продуктов, обеспечивающих вычислительные, телекоммуникационные и сетевые мощности для осуществления террористической деятельности.*

Соответственно, предметом воздействия такой деятельности выступают:

— *аппаратное обеспечение* (персональные компьютеры, серверы, центры обработки данных (ЦОД), коммутаторы и т.п.);

— *программное обеспечение* (операционные системы, вредоносные компьютерные программы, веб-ресурсы и др.);

— *сетевое обеспечение* (технологии внутренней и внешней связи).

Возвращаясь к вопросу о соотношении кибертерроризма и цифровой инфраструктуры терроризма, важно указать на следующее. Цифровая инфраструктура терроризма является обязательной составляющей (необходимой предпосылкой) кибертерроризма. Вместе с тем цифровая инфраструктура терроризма как криминальная деятельность по своему масштабу значительно шире и направлена на обеспечение терроризма во всех возможных проявлениях.

Таким образом, можно заключить, что цифровая инфраструктура имманентна кибертерроризму и он невозможен без нее. В то же время инструментарий цифровой инфраструктуры терроризма этим не исчерпывается, поскольку обнаруживает себя во многих других видах террористической деятельности, не связанных с целевыми атаками на информационные сети, автоматизированные системы управления и т.п.

Для осуществления террористической деятельности лица используют вполне законные инструменты цифровой коммуникации (мессенджеры, социальные сети, многопользовательские онлайн-игры и т.п.). При этом применяются популярные и незапрещенные анонимайзеры — специальные программы, предназначенные для изменения или сокрытия сетевых идентификаторов пользователя. В связи с этим возникает вполне понятный вопрос о том, могут ли такие объекты выступать маркерами цифровой инфраструктуры терроризма. Полагаем, что для этого нет значимых препятствий. Весь вопрос заключается в том, чтобы разделить общедоступные цифровые продукты, фактически используемые террористами, и заведомо созданные или приспособленные для осуществления террористической деятельности. По аналогии можно указать, что не возникает сомнений относительно того, что используемые террористами объекты недвижимости и транспортные средства выступают частью их материально-технической базы (иначе — инфраструктуры). Хотя и дома, и автомобили являются вполне легитимными объектами гражданских прав. Также сто́ит поступать и с законными инструментами цифровой коммуникации.

С учетом изложенного следует сделать вывод, что орудия и средства цифровой инфраструктуры терроризма могут быть представлены двумя самостоятельными комплексами (типами):

— комплексом открытых (находящихся в свободном доступе) технологий и цифровых продуктов, используемых в целях осуществления террористической деятельности;

— комплексом специальных («закрытых») технологий и цифровых продуктов, заведомо созданных, распространяемых и используемых для осуществления террористической деятельности.

Иными словами, об орудиях и средствах цифровой инфраструктуры терроризма можно говорить в широком и узком смысле. Понятно, что наибольшую опасность и, соответственно, интерес представляют компоненты цифровой инфраструктуры закрытого типа. Наиболее наглядно они могут быть представлены вредоносными компьютерными программами, заведомо созданными для целевых атак на автоматизированные системы управления объектов транспорта, энергетики, здравоохранения и др. Вместе с тем закрытый тип инструментария цифровой инфраструктуры терроризма также представлен специальными ресурсами в закрытом («черном») сегменте сети «Интернет», так называемом Darknet; программным обеспечением для управления боевыми беспилотниками кустарного производства; специально разработанными мессенджерами; программами для шифрования данных; сетями и оборудованием для передачи данных; созданными для осуществления террористической деятельности центрами обработки данных и т.п.

Уникальной и непроявленной проблемой цифровой инфраструктуры терроризма является то, что один человек или малая группа, обладающие специальными знаниями и навыками, способны с использованием компонентов цифровой среды осуществлять террористическую деятельность, сопоставимую по своим масшта-

бам с аналогичной деятельностью многих лиц в составе террористического сообщества либо террористической организации.

На это обстоятельство обращает внимание В. С. Овчинский: «Ключевым фактором повышения могущества малых групп и индивидов является развитие ИКТ. С одной стороны, развитие этих технологий привело к широкому внедрению Интернета, а соответственно, и к возможности не только разрушить, но и взять под управление любые системы, связанные с Интернетом через киберпространство. С другой стороны, ИКТ резко удешевляют производственные процессы и делают доступными многие изделия, оборудование и т.п. для небольших групп… Соответственно, небольшие группы и даже отдельные граждане могут получить новейшие разработки критических технологий, например искусственного интеллекта, по сути, бесплатно»[8].

К этому же выводу приходит Е. А. Русскевич, обращая внимание на «гипертаргетированность» современной компьютерной преступности, то есть способность практически одномоментно вызывать колоссальные по своему масштабу последствия и причинять вред сразу сотням, тысячам и даже миллионам потерпевших[9].

Цифровая инфраструктура терроризма предназначена не только для террористической пропаганды и вербовки. Цифровые технологии и продукты используются террористами для атак на критическую информационную инфраструктуру государств, для хищения денежных средств у граждан и организаций в целях финансирования террористической деятельности, для атак в отношении отдельных пользователей, в том числе для их последующего шантажа и возможной вербовки.

Нельзя не учитывать и ту роль, которую играют информационные технологии в кадровом обеспечении террористической деятельности. Компоненты цифровой инфраструктуры позволяют определять пользователей, которые с наибольшей вероятностью поддерживают либо проявляют интерес к идеологии и практике терроризма. Это существенным образом облегчает деятельность профессиональных вербовщиков, которые «по воле случая» оказываются на жизненном пути таких лиц.

Цифровые технологии предоставили террористическим образованиям возможность иметь свои средства массовой информации, социальные сети, средства обмена сообщениями (мессенджеры), сложно организованную и весьма защищенную финансовую систему, а также систему материально-технического и кадрового обеспечения. Например, в литературе справедливо отмечается, что появление виртуальных финансовых активов, в том числе криптовалюты, стало возможным благодаря технологии блокчейн. Известный факт, что криптовалюты широко используются для анонимного финансирования терроризма[10]. Всё это в совокупности дает представление о том, насколько высокотехнологичными могут быть современные формы террористической деятельности.

В международных документах подчеркивается важность воздействия именно на факторы, способствующие терроризму. Тем самым проводится идея проактивного правоприменения: «Действия по борьбе с терроризмом должны быть сосредоточены главным образом на предупреждении терроризма или предотвращении террористических актов… действия должны заключаться в разработке и осуществлении перспективных стратегий, а не на принятии мер в ответ на отдельные террористические акты… принять меры против планов террористов и подготовки террористических актов до их практической реализации. Задача состоит в том, чтобы проактивно интегрировать материально-правовые и процессуальные механизмы в целях сокращения случаев применения тер-

---

8 *Овчинский В. С.* Криминология цифрового мира. М., 2018. С. 60–61.

9 *Русскевич Е. А.* Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. С. 45.

Нельзя не отметить, что эти процессы спрогнозированы задолго до «цифровой революции». Еще в начале 60-х гг. XX в. Станислав Лем писал, что в XXI в. новая производственная революция создаст условия, когда не только криминальные группы, но и отдельные преступники смогут ставить под угрозу нормальное функционирование и жизнь населения мегаполисов и даже государств (см.: *Лем С.* Сумма технологий. М., 2021).

10 *Грачева Ю. В.*, *Маликов С. В.*, *Чучаев А. И.* Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал Высшей школы экономики. 2020. № 1. С. 209.

рористического насилия и их масштаба, не выходя за жесткие рамки ограничений и гарантий, предусмотренных гражданской системой уголовного правосудия и принципом верховенства закона»[11].

В документе по технической помощи, подготовленном Управлением ООН по наркотикам и преступности, подчеркивается, что «в борьбе с терроризмом вряд ли можно считать удовлетворительным, когда правовой предпосылкой для уголовного преследования является факт совершения нападения, имеющего целью гибель десятков или сотен людей, или покушение на его совершение… Для того чтобы снизить уровень террористического насилия, соответствующие органы должны переключить свое внимание на проактивные меры пресечения на стадии планирования и подготовки террористических актов»[12].

Противодействие цифровой инфраструктуре терроризма требует комплексного подхода. Прежде всего это предполагает симметричное технологическое противодействие правоохранительных органов и специальных служб, когда вредоносной технологии противопоставляется технология, ее нейтрализующая. Е. А. Антонян и И. И. Аминов по данному поводу обоснованно пишут: «Чтобы предотвратить террористические угрозы и радикализацию в киберпространстве, правоохранительные органы должны иметь возможность быть в технологическом отношении на шаг впереди киберкриминала. Изворотливость и профессионализм кибертеррористов, а также их фантастически возросшие технологические возможности требуют от правоохранительных органов всего мира разработки адекватных механизмов противодействия кибертерроризму, стратегия борьбы с которым должна быть направлена на предупреждение и минимизацию угроз и рисков, порождаемых глобальной цифровизацией»[13].

Вместе с тем это решение проблемы в тактическом смысле. Не менее важна проработка вопросов стратегического противодействия цифровой инфраструктуре терроризма. В этом плане на первое место выходят вопросы применимости и достаточности имеющегося механизма уголовно-правовой охраны.

Уголовное законодательство России в отношении цифровой инфраструктуры терроризма может быть реализовано следующим образом:

1) в порядке применения ч. 5 ст. 33 УК РФ об ответственности за пособничество в совершении любого преступления террористической направленности;

2) путем применения п. «р» ч. 1 ст. 63 УК РФ по признаку совершения преступления в целях поддержки терроризма;

3) в рамках ч. 1.1 или 3 ст. 205.1 УК РФ об ответственности за финансирование терроризма и пособничество в совершении преступлений, предусмотренных статьей 205, частью 3 ст. 206 и частью 1 ст. 208 УК РФ;

4) в порядке применения ст. 205.4 и 205.5 УК РФ, когда соответствующая деятельность являлась формой участия лица в террористическом сообществе либо организации;

5) посредством применения уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации (гл. 28 УК РФ).

В целом приведенный выше перечень возможных алгоритмов квалификации позволяет говорить о наличии определенной базы для уголовно-правового противодействия цифровой инфраструктуре терроризма. Вместе с тем вряд ли можно сделать вывод о том, что проблема решена полностью.

Во многом это связано с тем, что в российском уголовном законодательстве обстоятельно не решен вопрос об ответственности за саму *поддержку терроризма*. Предусмотренная уголовным законом ответственность за пособнические действия (в рамках Общей части) предполагает известную степень осведомленности лица о том, что соответствующие орудия или

---

[11] Предотвращение террористических актов: стратегия в области уголовного правосудия, интегрирующая нормы верховенства закона в осуществление положений документов Организации Объединенных Наций по борьбе с терроризмом. Рабочий документ по технической помощи, подготовленный Управлением Организации Объединенных Наций по наркотикам и преступности. ООН. Вена, 2006. С. 1–2.

[12] Предотвращение террористических актов: стратегия в области уголовного правосудия, интегрирующая нормы верховенства закона в осуществление положений документов Организации Объединенных Наций по борьбе с терроризмом. Рабочий документ по технической помощи, подготовленный Управлением ООН по наркотикам и преступности. Вена, 2006. С. 8, 10.

[13] *Антонян Е. А.*, *Аминов И. И.* Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6. С. 175.

средства разрабатываются и передаются именно для совершения конкретных преступлений террористической направленности.

А. А. Докуев, возможно, и прав, когда пишет, что включение ст. 205.1 УК РФ в российское уголовное законодательство позволило существенно расширить арсенал уголовно-правовых средств противодействия террористической деятельности, создать нормативную основу для раннего уголовно-правового реагирования на факты содействия террористической деятельности даже при отсутствии признаков соучастия в совершении террористического преступления[14].

Однако идея определения самостоятельного основания ответственности за содействие терроризму оказалась реализована, можно сказать, половинчато и в целом весьма неудачно. Начать с того, что толкование пособничества по ст. 205.1 УК РФ со временем было сведено всё к той же общей норме об ответственности за пособничество в рамках ч. 5 ст. 33 УК РФ: «Поскольку в деле отсутствуют данные о совершении (приготовлении, покушении) А. указанных преступлений, а Х. не содействовал ему либо другому лицу в совершении (приготовлении, покушении) какого-либо конкретного террористического акта и не оказывал помощь в создании, руководстве и финансировании незаконного вооруженного формирования, то оснований для осуждения его по ч. 3 ст. 205.1 УК РФ не имеется. Что касается осознания Х. того, что переданная им информация может быть использована для совершения преступлений террористической направленности, то данного обстоятельства недостаточно для осуждения по ч. 3 ст. 205.1 УК РФ»[15].

Аналогичный подход, по сути, реализован и в отношении финансирования терроризма. При применении ч. 1.1 ст. 205.1 УК РФ должна быть установлена прямая осведомленность лица о том, что передаваемые средства предназначены для обеспечения деятельности конкретной террористической организации либо совершения хотя бы одного из преступлений террористической направленности[16]. Следует указать еще и на то, что на уровне судов финансированию терроризма придано крайне расширительное толкование, включившее в содержание данного деяния также предоставление технических или иных материальных средств, в том числе на возмездной основе (что весьма сомнительно).

С. М. Кочои, обращаясь к анализу ст. 205.1 УК РФ, справедливо указывает и на другой значимый недостаток — возможность более строгого наказания организатора и пособника в сравнении с исполнителем террористического акта. По мнению автора, подобные конструкции в Особенной части оказывают негативное воздействие в целом на единый институт соучастия в Общей части[17].

В УК РФ поддержка терроризма упоминается лишь при определении цели, выступающей отягчающим обстоятельством, в п. «р» ч. 1 ст. 63 и аналогичной цели в диспозиции ст. 205.4. Получается, что иные формы поддержки (оказание услуг администрирования компьютерной системы и т.п.) могут преследоваться только через их оценку как пособнических, что не всегда возможно. Так, обычное предоставление услуг центра обработки данных не всегда может быть напрямую расценено как пособничество в террористической деятельности. Такая деятельность является вполне законной. Вместе с тем владельцы дата-центра могут быть осведомлены, что их отдельные клиенты аффилированы с террористическими организациями. Ведение бизнеса в рамках модели предоставления цифровых услуг всем желающим, в том числе тем, в отношении которых лица были проинформированы государственными органами о связи с террористической деятельностью, не образует пособничества.

Любая инфраструктура предполагает наличие людей, которые на постоянной основе осуществляют ее обслуживание и занимаются развитием. Это в полной мере применимо и к цифровой инфраструктуре терроризма. Разветвленная сеть технических устройств и программных продуктов требует привлечения специалистов самого разного профиля (системные

[14] *Докуев А. А.* Уголовная ответственность за содействие террористической деятельности : монография. М. : Юрлитинформ, 2016. С. 47.

[15] Обзор судебной практики Верховного Суда РФ № 3 (2019) (утв. Президиумом Верховного Суда РФ 27.11.2019) // СПС «КонсультантПлюс».

[16] Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда РФ от 25.09.2019 № 201-АПУ19-44 // СПС «КонсультантПлюс».

[17] *Кочои С. М.* Антитеррористическое уголовное право : монография. М., 2023. С. 59.

администраторы, программисты, веб-дизайнеры, контент-менеджеры и др.). Кроме того, инфраструктура требует постоянного технологического обеспечения и обновления. Это предполагает взаимодействие с поставщиками программного обеспечения и телекоммуникационного оборудования.

Оказание таких услуг и реализация соответствующих цифровых продуктов на постоянной основе субъектам, аффилированным с террористическими организациями либо сообществами, не позволяет говорить о наличии оснований для уголовной ответственности по действующему УК РФ. С учетом этого можно сделать вывод о наличии значимого пробела в уголовно-правовом противодействии деятельности, связанной с созданием и обеспечением цифровой инфраструктуры терроризма.

Признавая правильность именно проактивного противодействия терроризму, представляется необходимым реализовать следующий комплекс мер, направленных на купирование угроз от деятельности, связанной с цифровой инфраструктурой терроризма:

— прежде всего сто́ит разработать механизм принятия официального решения о том, что конкретная организация — иностранная либо международная — осуществляет деятельность, направленную на поддержку терроризма. Данный механизм может быть построен по типу процедуры признания нежелательной деятельности на территории Российской Федерации иностранной или международной организации в соответствии с Федеральным законом от 28.12.2012 № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации»;

— с учетом внедрения указанного выше механизма необходимо установить уголовную ответственность за участие в деятельности, а равно установление или поддержание сотрудничества с иностранной либо международной организацией, в отношении которой принято решение о признании ее деятельности направленной на поддержку терроризма;

— реализация указанных мер исключительно на национальном уровне вряд ли обеспечит желаемый (наиболее эффективный) результат в решении проблемы цифровой инфраструктуры терроризма. Практика уголовного преследования лиц, поставляющих оборудование и (или) оказывающих IT-услуги субъектам, деятельность которых напрямую или опосредованно направлена на поддержку терроризма, должна приобрести статус международного стандарта. Понятно, что сегодня довольно сложно говорить о возможности достижения такого консенсуса на международном уровне. Хотя на уровне ООН данная проблема обсуждается весьма детально. Так, отмечается, что «государства-члены выражают всё большую обеспокоенность по поводу злонамеренного использования террористическими группами информационно-коммуникационных технологий, в том числе Интернета, социальных сетей и связанных с ними онлайн-пространств, таких как игровые платформы, для распространения недостоверной и заведомо ложной информации и пропаганды, а также для разжигания ненависти и насилия, создания сетей, вербовки, подготовки новобранцев, финансирования деятельности и приобретения оружия»[18]. Вполне достижимым и значимым шагом в этом отношении могло бы стать внесение дополнений в Шанхайскую конвенцию о борьбе с терроризмом, сепаратизмом и экстремизмом.

Как нетрудно заметить, общий смысл вышеизложенных инициатив сводится к тому, чтобы, объективно оценив риски цифровизации, расширить пределы уголовно наказуемого содействия терроризму, при этом упростив стандарт вменения. В рамках такой модели деятельность лица может быть признана преступлением уже на том основании, что, будучи осведомленным о статусе соответствующих субъектов как поддерживающих терроризм, оно продолжило осуществлять экономическую деятельность по оказанию услуг, поставке оборудования, программного обеспечения и др.

И наконец, нельзя не признать, что предлагаемый комплекс мер по изменению регулятивного и охранительного законодательства самым существенным образом вторгается в отношения, связанные с оборотом IT-услуг и цифровых продуктов. Необходимо учитывать, что на поставщиков услуг не могут быть возложены обязательства по мониторингу информа-

[18] Доклад Генерального секретаря ООН «Деятельность системы Организации Объединенных Наций по осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций» (Семьдесят седьмая сессия, 02.02.2023, A/77/718) // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/033/33/PDF/N2303333.pdf?OpenElement (дата обращения: 17.03.2024).

ции, которую они передают или хранят, а также обязательства по активному выявлению фактов или обстоятельств, указывающих на незаконную деятельность. Более того, поставщики услуг хостинга не должны привлекаться к ответственности, если у них отсутствуют фактические данные о незаконной деятельности или соответствующей информации, а также если им неизвестны факты или обстоятельства, свидетельствующие о незаконном характере деятельности или информации[19]. Соответственно, реализация предлагаемой модели должна предполагать самое внимательное отношение к обеспечению основополагающих прав и свобод личности.

СПИСОК ЛИТЕРАТУРЫ

Антонян Е. А., *Аминов И. И.* Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6 (103). С. 167–177.

Бегишев И. Р. Уголовно-правовое регулирование робототехники. М. : Проспект, 2022. 320 с.

Бегишев И. Р., *Хисамова З. И.* Искусственный интеллект и уголовный закон. М. : Проспект, 2024. 192 с.

Грачева Ю. В., *Маликов С. В.*, *Чучаев А. И.* Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал Высшей школы экономики. 2020. № 1. С. 189–211.

Докуев А. А. Уголовная ответственность за содействие террористической деятельности. М. : Юрлитинформ, 2016. 192 с.

Ковлагина Д. А. Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия. М. : Юрлитинформ, 2017. 168 с.

Кочои С. М. Антитеррористическое уголовное право : монография. М. : Проспект, 2023. 112 с.

Краинский В. В., *Машко В. В.* Кибертерроризм: криминологическая характеристика и квалификация // Государство и право. 2023. № 1. С. 79–91.

Лем С. Сумма технологий. М. : АСТ, 2021. 800 с.

Овчинский В. С. Криминология цифрового мира. М. : Норма : Инфра-М, 2018. 352 с.

Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. 521 с.

Шваб К. Четвертая промышленная революция : пер. с англ. М. : Издательство «Э», 2018. 208 с.

REFERENCES

Antonyan EA, Aminov II. Blockchain technologies in countering cyberterrorism. *Aktual'nye problemy rossijskogo prava*. 2019;6(103):167-177. (In Russ.).

Begishev I R. *Criminal law regulation of robotics*. Moscow: Prospekt Publ.; 2022. (In Russ.).

Begishev IR, Hisamova ZI. *Artificial intelligence and criminal law*. Moscow: Prospekt Publ.; 2024. (In Russ.).

Dokuev AA. *Criminal liability for the promotion of terrorist activities*. Moscow: Yurlitinform Publ.; 2016. (In Russ.).

Gracheva YuV, Malikov SV, Chuchaev AI. Preventing deviations in the digital world by criminal law means. *Law. Journal of the Higher School of Economics*. 2020;1:189-211. (In Russ.).

Kochoi SM. *Anti-terrorist criminal law*. Moscow: Prospekt Publ.; 2023. (In Russ.).

Kovlagina DA. *Information terrorism: the concept, criminal law and other counteraction measures*. Moscow: Yurlitinform Publ.; 2017. (In Russ.).

Krainsky VV, Mashko VV. Cyberterrorism: criminological characteristics and qualification. *The State and Law*. 2023;1:79-91. (In Russ.).

Lem S. *Sum of technologies*. Moscow: AST Publ.; 2021. (In Russ.).

Ovchinsky VS. *Criminology of the digital world*. Moscow: Norma: Infra-M Publ.; 2018. (In Russ.).

[19] Подобный подход отражен в Директиве Европейского парламента и Совета Европейского Союза 2017/541 от 15.03.2017 о противодействии терроризму, о замене Рамочного решения 2002/475/ПВД Совета ЕС и об изменении решения 2005/671/ПВД Совета ЕС (СПС «КонсультантПлюс»).

Russkevich EA. *Differentiation of responsibility for crimes committed using information and communication technologies and the problems of their qualification*. Dr. Sci. (Law) Diss. Moscow; 2020. (In Russ.).

Shwab K. *The Fourth Industrial Revolution*. Tr. from English. Moscow: «E» Publ. house; 2018. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Боков Дмитрий Константинович, кандидат юридических наук,
проректор Университета прокуратуры Российской Федерации
д. 15, 2-я Звенигородская ул., г. Москва 123022, Российская Федерация
dimbok@mail.ru

INFORMATION ABOUT THE AUTHOR

Dmitry K. Bokov, Cand. Sci. (Law), Vice-Rector of the University of the Prosecutor's Office of the Russian Federation, Moscow, Russian Federation
dimbok@mail.ru

Материал поступил в редакцию 1 февраля 2024 г.
Статья получена после рецензирования 26 мая 2024 г.
Принята к печати 15 июня 2024 г.

Received 01.02.2024.
Revised 26.05.2024.
Accepted 15.06.2024.