Научная статья
УДК 343.85:[343.34:004](470)

Андемиркан Борисович Абазов[1], Файрушин Тимур Аликович[2]
[1] Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, Нальчик, Россия, and-abazov@mail.ru
[2] Уфимский юридический институт МВД России, Уфа, Россия, fta200483@mail.ru

ТЕОРЕТИКО-ПРАВОВОЕ ОСМЫСЛЕНИЕ СОВРЕМЕННЫХ МЕХАНИЗМОВ БОРЬБЫ С ЦИФРОВЫМ ТЕРРОРИЗМОМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В представленной статье проведен анализ эффективности действующих механизмов контртеррористической деятельности в контексте распространения цифрового терроризма в Российской Федерации. Акцентируется внимание на необходимости теоретико-правового осмысления цифрового терроризма как относительно самостоятельной разновидности террористического функционирования. Отмечается наличие определенных сложностей выявления и расследования цифровых деяний террористической направленности. Автор приходит к выводу о необходимости повышения эффективности профилактико-предупредительной деятельности, в том числе ее переориентации на цифровую специфику современных террористических проявлений.

Ключевые слова: терроризм, террористическая идеология, цифровой терроризм, контртеррористическая деятельность, направления борьбы с терроризмом

Для цитирования: Абазов А. Б., Файрушин Т. А. Теоретико-правовое осмысление современных механизмов борьбы с цифровым терроризмом в Российской Федерации // Общество, право, государственность: ретроспектива и перспектива. 2024. № 4 (20). С. 43–50.

Original article

Andemirkan Borisovich Abazov[1], Fayrushin Timur Alikovich[2]
[1] North Caucasian Institute for Advanced Studies (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russia, and-abazov@mail.ru
[2] Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia, fta200483@mail.ru

THEORETICAL AND LEGAL UNDERSTANDING OF MODERN MECHANISMS OF FIGHTING DIGITAL TERRORISM IN THE RUSSIAN FEDERATION

Abstract. The presented article analyzes the effectiveness of the existing mechanisms of counter-terrorism activities in the context of the spread of digital terrorism in the Russian Federation. Attention is focused on the need for a theoretical and legal understanding of digital terrorism as a relatively independent type of terrorist functioning. The presence of certain difficulties in identifying and investigating digital acts of a terrorist nature is noted. The author comes to the conclusion about the need to increase the effectiveness of preventive and preventive activities, including its reorientation to the digital specifics of modern terrorist manifestations.

Keywords: terrorism, terrorist ideology, digital terrorism, counter-terrorism activities, areas of the fight against terrorism

For citation: Abazov A. B., Fayrushin T. A. Theoretical and legal understanding of modern mechanisms for combating digital terrorism in the Russian Federation // Society, law, statehood: retrospective and perspective. 2024. No. 4 (20). P. 43–50. (In Russ.)

Введение

Терроризм является глобальной проблемой современности, и российское государство в данном случае – не исключение в части столкновения с масштабным распространением данного противоправного явления. В современных условиях, когда российское общество переживает множество проблем, связанных с обострением геополитических конфликтов, а также динамичностью совершенствования внутригосударственной политики в различных сферах, серьезную угрозу национальной безопасности и стабильному развитию российского государства представляет распространение террористических проявлений.

По данным МВД России, в 2023 году было зарегистрировано 2382 преступления террористической направленности (+6,7 % к 2022 году). За первое полугодие 2024 года было зарегистрировано 1651 преступления террористического характера (+38,4 %). Представленные данные наглядно демонстрируют растущую угрозу распространения террористических проявлений в России, в связи с чем принципиальное значение приобретает оценка эффективности современных механизмов контртеррористической деятельности в целях их дальнейшего совершенствования.

Важно отметить, что в настоящее время особое внимание уделяется отдельным разновидностям террористической деятельности, что представляется весьма справедливым. В данном контексте актуальным видится теоретико-правовое осмысление цифрового терроризма, поскольку эта разновидность активно формируется и распространяется в современных реалиях, связанных с повсеместными информатизацией и цифровизацией. Информационные и цифровые технологии становятся неотъемлемой частью жизни современного человека, и если раньше данные нововведения использовались лишь в отдельных профессиональных сферах, то сейчас эти технологии сопровождают решение многих бытовых и повседневных задач. Подобная ситуация, с одной стороны, является закономерным процессом развития цивилизации в условиях внедрения соответствующих технологий, с другой – существенно влияет на динамику совершенствования противоправной практики, и террористическая деятельность в этом случае не является исключением [1, с. 42]. Кроме того, специфика природы и распространения цифрового терроризма в российском обществе объективно обуславливает необходимость совершенствования существующих контртеррористических механизмов в целях повышения их эффективности в условиях развития указанной разновидности террористического функционирования.

Методы

Выбор методов обусловлен целями проводимого исследования. В ходе написания статьи использовались общенаучные (анализ, синтез) и специальные научные методы (сравнительно-правовой, формально-юридический, статистический и др.) для комплексного рассмотрения современных механизмов борьбы с терроризмом в Российской Федерации и конкретизации отдельных из них применительно к цифровой разновидности указанного преступного явления. Указанные методы с опорой на практику контртеррористической деятельности позволили оценить эффективность применяемых механизмов.

Результаты

Прежде чем перейти к анализу современных контртеррористических механизмов, видится целесообразным конкретизировать отдельные теоретические понятия по заявленной проблематике. В первую оче-

редь отметим, что понятие «цифровой терроризм» не регламентировано российским законодательством, что в целом отражает единую закономерность – правовую конкретизацию понятия «терроризм» на законодательном уровне и отсутствие регулирования специфических черт его разновидностей. В связи с вышеизложенным теоретико-правовое осмысление разновидностей терроризма активно проводится в научной и практической среде. Однако в контексте цифрового терроризма существует иная проблема – наличие множества смежных понятий и отсутствие единого подхода к содержательной характеристике данной разновидности. В рамках заявленной проблематики в качестве синонимов используется множество категорий, например, таких как кибертерроризм, компьютерный терроризм, информационный терроризм и т. д. Несмотря на их определенную схожесть, в том числе в части использования информационных и цифровых технологий, указанные понятия не являются тождественными. Кроме того, они неодинаковы по содержательным характеристикам с цифровым терроризмом.

Из вышеназванных терминов наиболее разработанным представляется «кибертерроризм», который активно используется в зарубежных правовых системах, а также в деятельности современных международных организаций. В настоящее время под кибертерроризмом принято понимать «идеологию насилия, которая воздействует на население путем устрашения, вмешивается в решения и действия органов государственной власти, применяет разнообразные формы насилия в киберпространстве» [2, с. 160]. Кибертерроризм отличается спецификой пространства, в котором совершаются террористические акты, а также объектами посягательства.

С вышеназванным понятием несколько схожа категория компьютерного терроризма, однако она имеет более узкое содержание в части ориентации на компьютерные технологии, программы и др., что далеко не всегда применяется в современном мире. Безусловно, компьютерная инфраструктура и обеспечение ее безопасности на территории конкретного государства имеет важное значение в настоящее время, однако постепенно информационные технологии уходят именно от привязки к компьютерам и используют потенциалы любых устройств, имеющих доступ в сеть Интернет.

В данном контексте актуализируется понятие «информационный терроризм», который в современной правовой науке определяется как «идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах информационного пространства, связанного с использованием информации, информационных технологий и (или) информационных ресурсов» [3, с. 109]. Следовательно, данная разновидность ориентирована непосредственно на информацию и различные ресурсы ее распространения, в рамках которых могут реализовываться террористические цели.

Все вышеназванные понятия тесно взаимосвязаны между собой, поскольку ориентированы на информационные технологии и интернет-пространство, однако от них предлагается отличать такую разновидность, как цифровой терроризм, который также весьма многоаспектно характеризуется в настоящее время. Так, отдельные авторы определяют цифровой терроризм как «кибератаку, использующую или эксплуатирующую компьютерные или коммуникационные сети, чтобы вызвать достаточное разрушение, вызвать страх или запугать общество в соответствии с поставленной идеологической целью» [4, с. 9]. По нашему мнению, данное определение не отражает цифровой специфики анализируемого явления. Цифровой терроризм во многом ориентирован на современные цифровые технологии, которые активно развиваются в современном мире и предоставляют гораздо большие масштабы преступной практики нежели компьютерные технологии.

Специфика цифрового терроризма связана не только с его ориентацией на циф-

ровые технологии и информационное пространство, но и с тем, что высока степень анонимности совершаемых деяний, а также неограничен круг объектов. В данном случае речь идет об объектах материального мира – компьютерная техника, личные гаджеты и др., однако объект посягательства может выступать мировоззрение населения в целом, т. е. распространение террористических идей и взглядов и их укоренение в сознании людей [5, с. 27]. Цифровой терроризм, безусловно, имеет трансграничный характер противоправного формирования и развития, а также ему присуща высокая скорость и существенный масштаб распространения в современном мире.

Цифровой терроризм за счёт специфики природы его развития является наиболее сложной разновидностью анализируемой преступной деятельности, поскольку технологическая составляющая и динамика её совершенствования позволяет преступным сообществам постоянно использовать новые схемы противоправного воздействия. Кроме того, в следственной практике регистрируют подобные деяния крайне редко, что свидетельствует не об их отсутствии, а о высокой степени латентности.

В современных геополитических условиях цифровой терроризм рассматривается также в контексте государственной и международной безопасности. Так, например, цифровой терроризм определяют как «разновидность информационного оружия в гибридно-информационной войне, представляющую собой информационно-психологическое воздействие на человека методами социальной инженерии с целью формирования у него террористического мировоззрения для дальнейшего использования его в совершении террористических актов» [6, с. 209]. Данное определение особенно актуально в контексте обострения геополитического конфликта на постсоветском пространстве и проведения активной антироссийской пропаганды со стороны многих зарубежных государств, что носит в том числе и ярко выраженную террористическую направленность в целях дестабилизации российского общества и государства. В указанном контексте рождаются выводы о наличии феномена «ментального терроризма», который формируется на фоне цифровизации общества [7, с. 51].

Говоря о противодействии цифровому терроризму, отметим, что в данном контексте контртеррористическая деятельность традиционно ориентирована на два основных направления:

выявление и расследование преступных деяний, а также назначение соразмерных и справедливых наказаний для виновных лиц;

профилактико-предупредительное воздействие в целях минимизации негативного воздействия террористической идеологии на российское население.

Оба вышеназванных направления имеют важнейшее практическое значение, однако в рамках каждого из них в настоящее время имеются существенные проблемы.

Анализируя современное состояние практики выявления и расследования преступных деяний террористической направленности следует отметить, что данное функционирование является высоко эффективным. В настоящее время многие факты террористических проявлений успешно выявляются еще на этапе подготовки, что позволяет существенно минимизировать масштабы их негативных последствий. Однако в случае с цифровым терроризмом проблемы его выявления и расследования по-прежнему связаны с технической оснащенностью и доступом различных специализированных программ для компетентных подразделений. Учитывая трансграничный характер цифровых террористических деяний, а также отсутствие возможности получения доступа к различным информационным ресурсам, находящимся в юрисдикциях других государств [8, с. 200], сложности расследования подобных преступлений будут сохраняться, однако в данном контексте значительно повышается роль профилактико-предупредительного воздействия, за счет которого можно эффективно нивелировать потенциальное преступное влияние. В рамках данного направления контртеррористи-

ческой деятельности также актуально рассматривать необходимость формирования оперативной реакции со стороны населения на факты цифрового терроризма, что имеет существенное информационное значение для компетентных органов.

Опережающее воздействие эффективно в большей степени в ситуациях, когда профилатико-предупредительная работа направлена на борьбу с распространением идеологии терроризма, поскольку внутренние установки индивидов, изменяемые в контексте противоправных взглядов, становятся не только основой преступного поведения террористической направленности, но и предполагает в целом одобрение и принятие идей насильственных способов решения различных конфликтов, что в целом способствует развитию преступности на территории российского государства. В то время как терроризм в настоящее время активно используется в целях дестабилизации конкретных территорий, наращивания степени социальной напряженности и обеспечения конкретных политических решений, люди, которые непосредственно вовлекаются в данное противоправное функционирование преследуют свои собственные цели, которые организаторы вышеназванной деятельности умело маскируют под общественные интересы [9, с. 71]. Путём беспрецедентной информационной антироссийской кампании, развернутой при участии западного разведсообщества, предпринимаются попытки создания очагов социальной напряжённости, формирования конфликтных ситуаций в российском обществе. Увеличилась вербовочная активность иностранных спецслужб по вовлечению российских граждан, в первую очередь молодёжи, в террористическую деятельность [10, с. 440].

Утопичным представляется организация такого общественного взаимодействия, при котором в социуме и у индивидов не возникает никаких существенных проблем, поскольку подобное состояние совершенно неестественно. Кроме того, несмотря на эффективную борьбу со стороны государства с выявлением и пресечением деятельности террористических организаций, следует предположить, что данные преступные сообщества будут сохранять свое функционирование в различных формах. В связи с этим особое практическое значение приобретает развитие правосознания и мировосприятия российского населения в целях формирования устойчивой неприязни к идеям и взглядам террористической направленности [11, с. 119].

В рамках представленного исследования видится необходимым подчеркнуть, что с момента начала специальной военной операции в Донбассе наблюдаются существенные изменения в формах и способах распространения террористической идеологии. В настоящее время данная деятельность организовывается уже не только непосредственно преступными сообществами, но и поддерживается отдельными государствами и их спецслужбами, что значительно расширяет ресурсный потенциал противоправного воздействия. На практике встречаются попытки массовой вербовки представителей российского населения, склонения их к совершению террористических актов, диверсий, саботажа и т. п. [12, с. 97].

Несмотря на то, что специальная военная операция носит конкретные цели обеспечения государственной безопасности России и защиты прав и законных интересов российских граждан и выступает результатом множественных нарушений ранее заключенных международных соглашений, в российском обществе за счет социальной напряженности создается благодатная почва для формирования и развития террористических взглядов. В условиях возникновения социально-экономических сложностей индивидам свойственно обосновывать свои проблемы через призму неэффективности государственной деятельности, что в совокупности с успешной и масштабной антироссийской пропагандой позволяет вовлекать в террористическую деятельность достаточно большое количество людей [13, с. 210]. Особую актуальность в данном контексте приобретает именно ресурсное содействие террористическим группам, что

может осуществляться в том числе на основе поддержания их идей и взглядов.

Говоря о ресурсном поддержании террористов, акцентируем внимание на вопросах борьбы с их финансированием. В настоящее время широко распространены ситуации, когда в интернет-пространстве отдельные индивиды, а также целые организации осуществляют сбор денежных средств на различные нужды, под которыми на самом деле скрывается террористическое функционирование [14, с. 321]. Другие люди сами того не осознавая направляют средства на развитие террористических формирований. В данном контексте значительно повышается актуальность развития не только правосознания населения, но и уровня цифровой грамотности, что напрямую связано с умением работать с различными информационными ресурсами и распознавать подозрительные. Несмотря на то, что в настоящее время в России постепенно формируются определенные стандарты применения цифровых технологий, в том числе хозяйствующими субъектами и органами власти, частные лица, как правило, не обладают даже минимальными компетенциями в данной сфере [15, с. 48].

В контексте борьбы с терроризмом достаточно часто упоминается правовое просвещение и правовое воспитание, которые, безусловно, актуальны, но в отношении цифрового терроризма должны иметь технологическую отсылку. В данном случае принципиальное значение приобретает информирование населения о современных средствах и способах совершения террористических деяний в цифровых форматах, схемах вовлечения населения в подобную противоправную деятельность. Особенно актуальна данная информация для представителей молодежи, поскольку, с одной стороны, они в большей степени используют различные цифровые технологии, с другой – данная категория населения наиболее интереса представителям преступных сообществ в части возможности управления их сознанием и поведением.

Заключение

Таким образом, в настоящее время существует острая необходимость теоретико-правового осмысления цифрового терроризма как относительно самостоятельной разновидности террористического функционирования. Специфика данного явления порождает не только особенности его формирования и развития, но и отдельные традиционные средства и методы контртеррористической деятельности будут далеко не всегда эффективны по отношению к цифровому терроризму.

На основе проведенного исследования следует сделать вывод о том, что сейчас наиболее эффективным направлением контртеррористической деятельности представляется выявление и расследование преступлений, однако в случае с цифровым терроризмом функционирование компетентных органов также сталкивается с рядом сложностей, в том числе технического и юрисдикционного характера. В связи с этим значительно повышается актуальность профилактико-предупредительного воздействия, которое должно быть ориентировано не только на идеологическую составляющую терроризма, но и на специфику цифровых его проявлений.

СПИСОК ИСТОЧНИКОВ

1. Боков Д. К. Цифровая инфраструктура терроризма: стратегия уголовно-правового противодействия // Lex Russica (Русский закон). 2024. Т. 77. № 7 (212). С. 39–48.

2. Тамбиев С. А., Кочесокова З. Х. Международный опыт противодействия кибертерроризму // Право и управление. 2023. № 2. С. 160–164.

3. Саунина Е. В, Бажина И. Д. Международный опыт правового регулирования противодействия информационному терроризму // Вестник Нижегородского университета имени Н. И. Лобачевского. 2022. № 1. С. 108–115.

4. Абазов К. М. Проблема использования современных информационно-коммуникационных технологий международными террористическими организациями // Вопросы безопасности. 2018. № 3. С. 1–9.

5. Даллакян К. А. Трансформация терроризма в информационно-цифровом обществе // Вестник Уфимского юридического института МВД России. 2023. № 4 (102). С. 25–30.

6. Стародубцева М. А. Цифровой терроризм: проблема юридического обоснования политологического термина // Государство и право в эпоху глобальных перемен : материалы международной научно-практической конференции / под редакцией Д. Л. Проказина. Барнаул : Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Барнаульский юридический институт Министерства внутренних дел Российской Федерации», 2022. С. 208–209.

7. Савушкина М. А. Ментальный терроризм как метод ведения гибридной войны в цифровом обществе // Вестник Челябинского государственного университета. 2024. № 7 (489). С. 48–54.

8. Кочесокова З. Х. Сравнительный анализ российского и международного законодательного регулирования кибертеррористических преступлений // Пробелы в российском законодательстве. 2023. Т. 16. № 4. С. 198–202.

9. Силенков В. И. К вопросу об онтологическом контексте осмысления терроризма // Профессиональное юридическое образование и наука. 2023. № 2 (10). С. 70–72.

10. Тарчоков Б. А. Развитие экстремистских и террористических преступлений, совершаемых при помощи цифровых технологий // Евразийский юридический журнал. 2023. № 7 (182). С. 439–440.

11. Кряжев В. С. К вопросу о необходимости комплексного подхода к исследованию терроризма и экстремизма для целей обеспечения национальной безопасности // Сибирские уголовно-процессуальные и криминалистические чтения. 2023. № 3 (41). С. 118–125.

12. Розенко С. В. Цифровые технологии как средство развития террористической идеологии в Российской Федерации: проблемы противодействия и наказуемости // OeconomiaetJus. 2023. № 3. С. 94–99.

13. Коркмазов А. В. Современные тенденции цифрового экстремизма и терроризма // Пробелы в российском законодательстве. 2023. Т. 16. № 4. С. 208–212.

14. Ахъядов Э. С.-М., Дадашов М. М., Маказиева З. Д. Преступления террористической направленности в эпоху цифровизации // Аграрное и земельное право. 2024. № 5 (233). С. 319–321.

15. Рожкова А. Ю. Профилактика «цифрового терроризма»: правовой аспект // Профессиональное юридическое образование и наука. 2024. № 3 (15). С. 47–52.

REFERENCES

1. Bokov D.K. Digital infrastructure of terrorism: strategy of criminal-legal counteraction // Lex Russica (Russian law). 2024. Vol. 77. No. 7 (212). P. 39–48. (In Russ.)

2. Tambiev S. A., Kochesokova Z. Kh. International experience of counteracting cyberterrorism // Law and Management. 2023. No. 2. P. 160–164. (In Russ.)

3. Saunina E. V, Bazhina I. D. International experience of legal regulation of counteracting information terrorism // Bulletin of the Lobachevsky University of Nizhny Novgorod. 2022. No. 1. P. 108–115. (In Russ.)

4. Abazov K. M. The problem of using modern information and communication technologies by international terrorist organizations // Security Issues. 2018. No. 3. P. 1–9. (In Russ.)

5. Dallakyan K. A. Transformation of terrorism in the information and digital society // Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2023. No. 4 (102). P. 25–30. (In Russ.)

6. Starodubtseva M. A. Digital terrorism: the problem of legal justification of a political science term // State and law in the era of global changes: materials of the international scientific and practical conference / edited by D. L. Prokazin. Barnaul: Federal State Budgetary Educational Institution of Higher Professional Education «Barnaul Law Institute of the Ministry of Internal Affairs of the Russian Federation», 2022. P. 208–209. (In Russ.)

7. Savushkina M. A. Mental terrorism as a method of waging a hybrid war in a digital society // Bulletin of the Chelyabinsk State University. 2024. No. 7 (489). P. 48–54. (In Russ.)

8. Kochesokova Z. Kh. Comparative analysis of Russian and international legislative regulation of cyberterrorist crimes // Gaps in Russian legislation. 2023. Vol. 16. No. 4. P. 198–202. (In Russ.)

9. Silenkov V. I. On the issue of the ontological context of understanding terrorism // Professional legal education and science. 2023. No. 2 (10). P. 70–72. (In Russ.)

10. Tarchokov B. A. Development of extremist and terrorist crimes committed with the help of digital technologies // Eurasian Law Journal. 2023. No. 7 (182). P. 439–440. (In Russ.)

11. Kryazhev V. S. On the Need for an Integrated Approach to the Study of Terrorism and Extremism for the Purposes of Ensuring National Security // Siberian Criminal Procedure and Forensic Readings. 2023. No. 3 (41). P. 118–125. (In Russ.)

12. Rozenko S. V. Digital Technologies as a Means of Developing Terrorist Ideology in the Russian Federation: Problems of Counteraction and Punishability // OeconomiaetJus. 2023. No. 3. P. 94–99. (In Russ.)

13. Korkmazov A. V. Modern Trends of Digital Extremism and Terrorism // Gaps in Russian Legislation. 2023. Vol. 16. No. 4. P. 208–212. (In Russ.)

14. Akhyadov E. S.-M., Dadashov M. M., Makazieva Z. D. Terrorist-related crimes in the era of digitalization // Agrarian and land law. 2024. No. 5 (233). P. 319–321. (In Russ.)

15. Rozhkova A. Yu. Prevention of «digital terrorism»: legal aspect // Professional legal education and science. 2024. No. 3 (15). P. 47–52. (In Russ.)

Информация об авторах:
Абазов А. Б. – кандидат юридических наук;
Файрушин Т. А. – без ученой степени.

Information about the authors:
Abazov A. B. – Candidate of Law;
Fayrushin T. A. – no academic degree.

Статья поступила в редакцию 05.10.2024; одобрена после рецензирования 18.11.2024; принята к публикации 28.11.2024.

The article was submitted 05.10.2024; approved after reviewing 18.11.2024; accepted for publication 28.11.2024.