ИСТОРИЯ И ТЕОРИЯ ПОЛИТИКИ

DOI 10.35775/PSI.2026.130.1.013
УДК 32.321

И.Ю. ЗАЛЫСИН
доктор политических наук,
профессор РАНХиГС, Россия, г. Москва

С.Г. СТАРЦЕВА
кандидат политических наук,
РАНХиГС, Россия, г. Москва

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ: ОСНОВНЫЕ ТРАКТОВКИ

В работе рассматриваются трактовки сущности информационного терроризма. Изучение работ по проблеме информационного терроризма показывает, что среди исследователей отсутствует единство по поводу понимания его сущности. Одни авторы трактуют его как деструктивное воздействие на сознание и поведение людей. Другие относят к информационному терроризму любые действия, которые связаны с информационно-коммуникационными технологиями (ИКТ). Третьи отождествляют его с кибертерроризмом. Перспективным представляется подход, интерпретирующий информационный терроризм как вид терроризма, который состоит в создании в обществе атмосферы страха с помощью информационно-коммуникационных технологий для оказания влияния на адресную группу, не совпадающую с непосредственным объектом.

Ключевые слова: *терроризм, информационный терроризм, информация, информационно-коммуникационные технологии, информационная безопасность, информационное оружие, противодействие терроризму.*

Проблема информационного терроризма имеет большую теоретическую и практическую актуальность. Во-первых, терроризм, прежде всего в его квази-религиозной форме, превратился в глобальную угрозу для общества и государства [15]. Особую опасность представляет использование террористами информационных технологий для достижения своих целей. В доктрине информационной безопасности РФ подчеркивается: «Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников» [4]. Следует признать, что современные информационно-коммуникационные технологии (ИКТ) заметно повышают эффективность деятельности

террористов, позволяют им действовать анонимно, оперативно, масштабно, атаковать цели, которые ранее были им недоступны [19].

Во-вторых, несмотря на многочисленные публикации, посвященные различным аспектам информационного терроризма, в научной и публицистической литературе по данной проблеме наблюдается терминологическая нечеткость и понятийная неопределенность. Кроме того, ни на государственном, ни на международном уровне нет общепринятого и закрепленного в нормативных актах определения понятия «информационный терроризм» [20]. Это относится и к такому близкому к нему понятию, как «кибертерроризм». Как отмечает П.Н. Кобец, «в Российской Федерации дефиниция «кибертерроризм» в настоящее время не получила легального закрепления, несмотря на то, что относительно ее содержания многие годы не утихают споры между юристами, теоретиками, практиками, а также всеми остальными специалистами, исследующими вопросы борьбы с кибертерроризмом» [8. С. 99]. Такая ситуация создает затруднения в понимании сущности информационного терроризма, порождает законодательные пробелы в противодействии этому явлению, усложняющие борьбу с ним, «не позволяет вовремя выявлять и пресекать данный вид террористической деятельности» [13. С. 1020].

Можно выделить несколько трактовок сущности информационного терроризма. Ряд авторов рассматривает информационный терроризм как **деструктивное воздействие на сознание и поведение людей**. Так, по мнению В.А. Гафуровой, В.А. Камышовой, Д.В. Чернова, «информационный терроризм – это целенаправленное прямое воздействие на людей, их психику, сознание и поведение с целью внушения определенных идей, мнений и действия для достижения определенных действий» [2]. Близких позиций придерживаются А.А. Алоева, И.А. Алоев, А.З. Жуков, Н.Ю. Григорьев, Э.Б. Родюков, А.В. Таран и др. [1; 3; 14] По их мнению, с помощью ложной информации террористы формируют «противоречивое представление, негативное возмущение и ошибочное понимание» [14. С. 38], лишают людей возможности для критической оценки получаемых от них сведений и знаний [3. С. 175]. Н.Ю. Григорьев, Э.Б. Родюков полагают, что информационный терроризм опирается на распространение определенного типа слухов, направленных на дезориентацию массового сознания. Среди них названные авторы наиболее значимыми считают «слухи-пугало» и «агрессивные слухи» [2. С. 175-176].

Другой точки зрения придерживаются авторы, которые считают, что, в отличие от традиционного терроризма, **непосредственным объектом информационного являются ИКТ** (компьютерные системы, программы, персональные данные и т.д.) Террористы воздействуют на них с целью «искоренения моральных и нравственных ценностей», провоцирования межнациональных конфликтов, нарушения общественного порядка и т.д. [13. С. 1018].

Еще один подход к пониманию информационного терроризма можно условно назвать **расширительным**. Его сторонники относят к информационному терроризму **любые действия террористов, которые связаны с ИКТ**:

не только кибератаки на информационные системы политических противников, но и манипуляции массовым сознанием с помощью ИКТ. Так, некоторые авторы выделяют следующие виды информационного терроризма: информационно-психологический (манипулирование СМИ для дезинформации общества, запугивания и т.д.) и информационно-технический, осуществляемый с целью нанесения ущерба информационным государственным структурам с помощью вирусных программ, осуществления дистанционного управления объектами биологического и химического оружия и т.д. [2].

Такой подход нашел отражение в ряде официальных документов, например, Шанхайской организации сотрудничества, где информационный терроризм определяется как «противоправные действия посредством или в отношении информационных ресурсов», осуществляемые террористическими организациями и лицами, причастными к террористической деятельности [11].

Следует отметить, что за редким исключением авторы, изучающие информационный терроризм, в качестве его субъектов рассматривают только негосударственных акторов, «угрожающих безопасности и благополучию одной или нескольким нациям» [21]. Властные структуры абсолютным большинством из них не включаются в число агентов информационного терроризма.

Дискуссионный характер имеет и понятие «кибертерроризм», которое многие исследователи трактуют как синоним «информационного терроризма». Термин «кибертерроризм» был введен в 1980-х годах старшим научным сотрудником американского Института безопасности и разведки Б. Коллином для обозначения новой формы террористической деятельности в виртуальном пространстве [10]. До сих пор универсально принятое определение кибертерроризма отсутствует, а во многих работах вообще оно не дается и лишь раскрываются его рамки. По справедливой оценке ряда ученых, это «является проблемой и вызовом в противостоянии террористическим угрозам» [22. P. 1].

Ряд авторов, как уже отмечалось, отождествляют информационный и кибертерроризм. По мнению Ю.Н. Лагуткина, Ж.И. Мадалимбекова, Д.К. Омарова, «в XXI в. … появился новый вид терроризма – информационный терроризм или же кибертерроризм» [9. С. 850]. Другие называют кибертерроризм одной из форм информационного терроризма [12; 19]. Для А.В. Тарана кибертерроризм – «атака на информационную систему», выступающая как «инструмент и составляющая для информационного терроризма в целом» [14. С. 39].

Не все исследователи ставят знак равенства между этими двумя понятиями. Некоторые трактуют кибертерроризм как атаки на компьютерные системы, т.е. террор в киберпространстве, или компьютерный терроризм [17]. Под ним подразумевается использование террористами и террористическими организациями инструментов по незаконному вмешательству в работу информационных систем (незаконное получение информации, присвоение информации, вымогательство информации и т.д.) [5. С. 66].

Ряд авторов видит в кибертерроризме не только инструмент вредоносного воздействия на ИКТ, но и манипулирования массовым сознанием [7]. Такая

трактовка фактически ничем не отличается от расширительного подхода к пониманию информационного терроризма, о котором было сказано выше.

Так, по мнению С. Ифтихара, «кибертерроризм – это использование интернета, информационных средств и коммуникационных платформ для проведения террористических атак или пропаганды террористических идей» [16]. А.А. Стребкова выделяет два основных вида кибертерроризма: во-первых, «классический», который представляет собой атаки на компьютерные системы; во-вторых, «организационно-коммуникационный», предполагающий использование информационного пространства с целью взаимодействия между террористическими группами и их последователями, в частности, сбор информации для планирования терактов, сбор денежных средств для развития террористических организаций; вербовка и привлечение к террористической деятельности новых последователей; информационно-психологическое влияние на общество и т.д. [13. С. 1019]. Как мы видим, в понимании сущности такого близкого к информационному терроризму понятия, как кибертерроризм, также пока не хватает ясности.

Для выявления сущности информационного терроризма большое значение имеет определение его целей. В научной литературе к ним относят «дестабилизацию политического, общественного устройства общества, подрыв доверия к государственным институтам, изменение политического поведения масс, искажение информации, манипуляция общественным сознанием, пропаганда террористических идей, нарушение работы информационных систем и инфраструктуры и т.д. [1; 10; 16; 20].

В некоторых работах в качестве атрибутивного признака информационного терроризма указывается его цель – **устрашение общества и властных структур.** В частности, Э. Талышинский отмечает: «... В научной, аналитической и экспертной литературе под информационным терроризмом понимаются целенаправленные действия, осуществляемые с использованием информации и информационно-коммуникационных технологий в целях посеять страх, вызвать хаос и неопределенность в обществе, подорвать доверие к государственным и общественным институтам, дестабилизировать политическую и экономическую обстановку в государстве или регионе. К таким действиям относятся распространение дезинформации, фейковых новостей, пропагандистские кампании, кибератаки на информационные ресурсы, а также манипулирование общественным сознанием через социальные сети и другие цифровые каналы» [20].

Нам представляется перспективным такой подход к пониманию сущности информационного терроризма. Если исходить из того, что информационный терроризм является разновидностью родового понятия «терроризм», то его определение, на наш взгляд, должно включать атрибутивные признаки последнего. К ним чаще всего относят:

– направленность, прежде всего, против мирного населения;

– наличие двух объектов (непосредственного и отдаленного);

– использование страха для достижения своих целей (слово «террор» в переводе с латинского означает «страх», «ужас»);

– отсутствие каких-либо нравственных ограничений при выборе средств деятельности, включая различные формы принуждения и др.

С учетом вышесказанного можно определить информационный терроризм следующим образом: **это вид терроризма, который состоит в создании с помощью информационно-коммуникационных технологий атмосферы страха, непосредственно направленной на гражданское население, которое выступает как инструмент воздействия на адресную группу (правительство, лидеры оппозиции и др.) для достижения определенных целей.**

«Обычный» терроризм связан с использованием насилия [6], его информационная разновидность тоже предполагает, хотя и часто скрытое, **навязывание** определенных настроений, эмоций, чувств, оказывающих деструктивное влияние на личность. Распространяя с помощью ИКТ ложную информацию, слухи, фейки о готовящихся или совершенных терактах, осуществляя психологические операции по деморализации различных групп общества, террористы стремятся их запугать, посеять панику, неуверенность, заставить власти совершать грубые ошибки, которыми террористические группировки надеются воспользоваться.

Что касается соотношения понятий информационный и кибертерроризм, то они, на наш взгляд, очень близки с точки зрения целей и средств. Кибертеррористы также стремятся запугать, деморализовать целевые группы и таким образом добиться нужных результатов. На это указывают зарубежные и российские исследователи. Так, профессор Джорджтаунского университета Д. Дэннинг определяет кибертерроризм как «противозаконные атаки или угрозы атак на компьютеры, сети и хранимую в них информацию для устрашения или принуждения правительства или граждан к какому-либо действию в политических или общественных целях» [17]. П.Н. Кобец тоже считает, кибератаки в отношении информационных систем и пропаганда террористической идеологии и деятельности в информационно-телекоммуникационных сетях осуществляются «для запугивания общественности, органов государственной власти и международных организаций» [7. С. 92]. Аналогичную позицию занимают У. Тафойа [19], Д.В. Пучков [10. С. 384].

Однако, по нашему мнению, в кибертерроризме ИКТ выступают не только в роли инструмента, но и **главного объекта** террористических атак, а информационный терроризм в основном использует электронные технологии как **средство**.

Таким образом, анализ работ по проблеме информационного терроризма показывает, что в научной литературе отсутствует единство по поводу понимания его сущности. Понятийная неопределенность мешает глубокому изучению данного явления, снижает эффективность противодействия ему. Борьба с информационным терроризмом требует использования системы мер (силовых, просветительских, информационно-пропагандистских и др.), неотъемлемой частью которых должно быть всестороннее исследование учеными-обществоведами этой глобальной угрозы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алоева А.А., Алоев И.А., Жуков А.З.** Информационный терроризм – угроза национальной безопасности в условиях цифровизации // Пробелы в российском законодательстве. 2020. Т. 13. № 6.
2. **Гафурова В.А., Камышова В.А., Чернов Д.В.** Информационный терроризм как новая форма терроризма // Научный Лидер. 2023. № 48 (146) // https://scilead.ru/article/5419-informatsionnij-terrorizm-kak-novaya-forma-te.
3. **Григорьев Н.Ю., Родюков Э.Б.** Информационный терроризм // Вестник университета. 2015. № 5.
4. Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // https://mid.ru/ru/foreign_policy/official_documents/1539546/.
5. **Жуков А.З.** Пути совершенствования методов по противодействию кибертерроризму в Российской Федерации // Пробелы в российском законодательстве. 2020. Т. XIII. № 4.
6. **Залысин И.Ю.** Политическое насилие (теоретико-методологический анализ). Автореф. дис... д-ра полит. наук. М., 1995.
7. **Кобец П. Н.** Особенности феномена кибертерроризма в условиях XXI столетия и меры по противодействию этому явлению // Научный портал МВД России. 2022. № 1 (57).
8. **Кобец П. Н.** Отечественные и зарубежные подходы по разработке понятийного аппарата в сфере борьбы с кибертерроризмом и предложения по совершенствованию данного нормотворческого процесса // Правопорядок: история, теория, практика. 2022. № 1 (32).
9. **Лагуткина Ю.Н., Мадалимбеков Ж.И., Омарова Д.К.** Противодействие стран Российской Федерации и Республики Казахстан информационному терроризму // Постсоветские исследования. 2022. № 8 (5).
10. **Пучков Д.В.** Кибертерроризм как новая угроза // Виктимология. 2021. Т. 8. № 4.
11. **Симонова Э.Ю.** Сравнительный анализ основных подходов к определению кибертерроризма в современной мировой политической науке // Общество: политика, экономика, право. 2018. № 6 // https://cyberleninka.ru/article/n/sravnitelnyy-analiz-osnovnyh-podhodov-k-opredeleniyu-kiberterrorizma-v-sovremennoy-mirovoy-politicheskoy-nauke
12. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности // https://docs.cntd.ru/document/902289626.
13. **Стребкова А.А.** Информационный терроризм // Вопросы российской юстиции. 2020. № 9.
14. **Таран А.В.** Классификация информационных угроз современному обществу // Вестник РУДН. Серия Политология. 2009. № 2.

15. **Чепров К.Е.** Исламский терроризм на постсоветском пространстве: основные этапы эволюции // Евразийский Союз: вопросы международных отношений. 2025. Т. 14. № 5 (70).
16. **Iftikhar S.** Cyberterrorism as a global threat: a review on repercussions and countermeasures // PeerJ Computer Science. 2024. Jan 15. № 10 // https://doi.org/10.7717/peerj-cs.1772/.
17. **Denning D.E.** Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. 2000. May 23 // http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf.
18. **Purdy E.** Cyberterrorism // https://www.ebsco.com/research-starters/political-science/cyberterrorism.
19. **Tafoya W.L.** Cyber Terror. FBI Law Enforcement Bulletin (ноябрь 2011) // https://web.archive.org/web/20120420162544/http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror.
20. **Talyshinsky E.** Information Weapons: Concept, Methods, Dynamics // Universum: общественные науки: электрон. научн. журн. 2025. № 7 (122) // https://7universum.com/ru/social/archive/item/20519.
21. **Talyshinsky E.** Information Terrorism: Concept, Forms and Modern Threats // Universum: общественные науки: электрон. научн. журн. 2025. № 8 (123) // https://7universum.com/ru/social/archive/item/20677.
22. **Webb K.** Informational Terrorism in the New Security Environment // Journal of Informational Warfare. 2007. Vol. 6. № 2.
23. **Yunos Z., Sulaman S.** Understanding Cyber Terrorism from Motivational Perspectives // Journal of Information Warfare. Vol. 16. № 4 (Fall 2017).

I.YU. ZALYSIN
Doctor of political sciences, professor
of Russian Academy of National Economy
and Public Administration (RANEPA),
Moscow, Russia

S.G. STARTSEVA
Candidate of Political Sciences,
Russian Academy of National Economy
and Public Administration (RANEPA),
Moscow, Russia

INFORMATION TERRORISM: MAIN INTERPRETATIONS

The paper examines interpretations of the essence of information terrorism. A review of literature on information terrorism reveals a lack of consensus among researchers regarding its essence. Some authors interpret it as a destructive impact on people's consciousness and behavior. Others classify any actions related to information and communications technologies (ICT) as information terrorism. Still others equate it with cyberterrorism. A promising approach interprets information terrorism as a type of terrorism that involves creating an atmosphere of fear in society using information and communications technologies to influence a target group that is not the immediate target.

Key words: *terrorism, information terrorism, information, information and communications technologies, information security, information weapons, counterterrorism.*