ISSN 2500-4255

УДК 343.326
DOI 10.17150/2500-4255.2020.14(1).156-165

ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В РОССИИ И ЗА РУБЕЖОМ С ПОЗИЦИИ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКОГО ИЗМЕРЕНИЯ

Г.П. Кулешова[1], Е.А. Капитонова[2], Г.Б. Романовский[2]
[1] Средне-Волжский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), г. Саранск, Российская Федерация
[2] Пензенский государственный университет, г. Пенза, Российская Федерация

Информация о статье
Дата поступления
23 ноября 2018 г.
Дата принятия в печать
10 февраля 2020 г.
Дата онлайн-размещения
28 февраля 2020 г.

Ключевые слова
Кибертерроризм; противодействие кибертерроризму; уголовная ответственность; угроза; зарубежное законодательство

Финансирование
Подготовлено в рамках поддержанного РФФИ научного проекта № 17-03-00071-ОГН

Аннотация. В статье выделены юридические особенности противодействия кибертерроризму в российском и зарубежном праве в условиях развития современного информационного пространства. Показано, что такие принципы телекоммуникационных технологий, как открытость и общедоступность, используются террористическими организациями в их преступных целях. Анализ зарубежного законодательства говорит о том, что в большинстве стран мира отсутствует специальный состав преступления — кибертерроризм. В то же время указание на применение IT-технологий при распространении идей терроризма закрепляется как отягчающее обстоятельство. Авторы приходят к выводу, что в российской юридической науке нет единства по поводу дополнения Уголовного кодекса Российской Федерации специальным составом — кибертерроризм. В статье представлено мнение об отсутствии необходимости такой корректировки российского уголовного закона. Выделены различные признаки кибертерроризма, а также проведена его классификация на гибридный и кибертерроризм в чистом виде. В первом случае это использование Интернета для террористической деятельности: пропаганды, вербовки сторонников, их обучения, радикализации общества, сбора средств, получения данных, осуществления связи, планирования реальных террористических атак. Во втором случае это прямые атаки на киберинфраструктуру для достижения политических, религиозных и идеологических целей. Сформулирован вывод о преувеличении опасности кибертерроризма как угрозы всей инфраструктуре государства, поскольку стандартная киберпреступность наносит более значительный ущерб экономике любого государства. Но в силу отсутствия единого центра и по причине экстремистской идеологии данный вид преступности не может вселять такие социальные страхи, которые можно внушить обществу благодаря отсылкам к активности террористических организаций. Показано, что в США и странах Западной Европы кибертерроризм несет в себе в большей мере политическую нагрузку, обществу предлагается оценивать угрозу кибертерроризма через призму уровня защищенности каждого его члена. При этом проводится идеологическая обработка общества о необходимости наступательных действий в киберпространстве в отношении стран, от которых может исходить угроза. В данной связи авторы заключают, что повышенное внимание к проблеме кибертерроризма имеет ярко выраженную идейно-ценностную компоненту.

THE LEGAL BASIS OF COUNTERING CYBER-TERRORISM IN RUSSIA AND IN OTHER COUNTRIES FROM THE STANDPOINT OF ITS SOCIAL AND POLITICAL DIMENSION

Galina P. Kuleshova[1], Elena A. Kapitonova[2], Georgy B. Romanovsky[2]
[1] Middle Volga Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Saransk, the Russian Federation
[2] Penza State University, Penza, the Russian Federation

Article info
Received
2018 November 23
Accepted
2020 February 10

Abstract. The authors discuss the legal specifics of counteracting cyber-terrorism in Russian and in foreign law at the modern stage of the development of information space. They show that such principles of telecommunication technologies as transparency and accessibility are used by terrorist organizations for criminal purposes. The analysis of foreign legislation shows that legislations of most countries do not have a special crime of cyber-terrorism. At the same time, the use of IT in disseminat-

ISSN 2500-4255

Available online
2020 February 28

Keywords
Cyber-terrorism; counteracting cyber-terrorism; criminal liability; threat; foreign legislation

Acknowledgements
This research is financially supported by Russian Foundation for Basic Research within Project № 17-03-00071-ОГН

ing terrorist ideology is included in these legislations as an aggravating circumstance. The authors conclude that Russian legal scholars do not currently have a common opinion on adding a new special crime of cyber-terrorism to the Criminal Code of the Russian Federation. They argue that such amendment of Russian criminal law is not necessary. The authors also single out different features of cyber-terrorism and present its classification that includes a hybrid type and cyber-terrorism proper. In the former case, the Internet is used for terrorist activities: propaganda, recruitment of supporters, their training, radicalization of society, collecting funds and data, connections, planning of actual terrorist attacks. In the latter case, there are direct attacks against cyber-infrastructure with political, religious and ideological purposes. The authors conclude that the dangers of cyber-terrorism as a threat to the whole infrastructure of society are overstated because ordinary cyber-crimes inflict a much greater damage on the economy of any country. However, as these crimes are not coordinated from one center and because of the ideology of extremism, this type of crime cannot strike a social fear comparable with the fears that could be inspired by references to the activities of terrorist organizations. It is shown that in the USA and in Western Europe cyber-terrorism is greatly politically charged, and the society is encouraged to evaluate the threat of cyber-terrorism though the prism of the level of security of each member of this society. Besides, the society is indoctrinated to believe that it is necessary to carry out cyber-attacks against those countries that might pose a threat. In this connection, the authors conclude that a high level of attention to the problem of cyber-terrorism has a prominent ideological and value component.

Развитие цифровых технологий в современном мире все больше обусловливает зависимость от них каждого человека в его повседневной жизни. Уже не являются какой-то экзотикой такие термины, как «цифровая экономика», «биткоины», «искусственный интеллект». Более того, обозначенные ими явления меняют параметры развития права, государства, общества. Биткоины, например, составляют реальную конкуренцию национальным валютам, а в научном мире уже нередки предложения о предоставлении хотя бы частичной правосубъектности цифровому интеллекту.

Террористическая угроза также меняет свою сущность. Первичная тактика террористов (конец XIX — начало XX в.) строилась на нанесении урона представителям государственной власти (в первую очередь убийство должностных лиц). В последующем к подобным акциям добавились акции устрашения, нацеленные на граждан, не связанных напрямую с официальными властями (захват заложников, угон самолета, взрывы в общественных местах). Интернет вносит свои коррективы и в данный вид преступной деятельности. Все больше промышленных объектов управляется с удаленных компьютеров, все больше информационных баз систематизируется благодаря облачным программам. Одновременно глобальная сеть позволяет получить легкий доступ к масштабной аудитории при полном отсутствии цензуры, благодаря чему распространение информации приобретает качественно иные формы.

Считается, что впервые о кибертерроризме как о явлении заговорил Барри Коллин (сотрудник Института безопасности и разведки, Калифорния, США) еще в 1980 г., когда только несколько компьютеров Министерства обороны США было объединено благодаря сети ARPANET [1]. Одними из первых, кто использовал Интернет в противоправных целях, считаются «Тамильские тигры», которые в 1998 г. в течение двух недель бомбили электронными письмами официальные учреждения Шри-Ланки, называя себя в них «черными интернет-тиграми». Примерно в это же время «Аум Синрикё» (данные были получены в ходе обысков в штаб-квартирах организации) разрабатывала возможность перехвата контроля над ядерными объектами. Апокалиптические сценарии неоднократно содержались в различных официальных отчетах. Впервые о «цифровом Пёрл-Харборе» было написано в 1995 г. Америка представлялась беззащитной жертвой даже самых незначительных компьютерных действий [2]. Такое нагнетание истерии происходило в течение десяти лет, вплоть до того, как Г. Вейманн в 2004 г. пошагово спроектировал его в ближайшем будущем [3; 4].

Россия также становилась объектом кибертеррористических атак. В сентябре 2017 г. (начало было дано 11 сентября) волна ложных сообщений о готовящихся терактах прокатилась по многим городам России. Противоправному воздействию подверглись информационные базы государственных учреждений. Общий ущерб

был оценен более чем в 300 млн р. Директор ФСБ России А. Бортников сообщил, что исполнителями были четыре гражданина России, находящиеся за рубежом[1]. При этом в СМИ озвучивались версии, согласно которым заказчиком таких планомерных действий могли выступать зарубежные спецслужбы, решившие апробировать новую методику гибридной войны. В октябре 2018 г. Великобритания открыто угрожала России осуществить кибератаку на электросети Москвы в случае актов агрессии против НАТО и их союзников[2]. Подобные действия российскими спецслужбами были оценены как государственный терроризм.

Необходимо указать, что в Российской Федерации отсутствует специальный уголовный состав, посвященный кибертерроризму. Нет ссылки на интернет-технологии в описании объективной стороны террористического акта (ст. 205 УК РФ). Это позволяет ряду ученых настаивать на включении дополнительного признака в некоторые составы преступлений террористического характера. Так, И.Г. Чекунов предлагает дополнить ст. 205 УК РФ частью 2, в которой следует установить ответственность за теракт с помощью несанкционированного проникновения в компьютерные системы [5, с. 43]. Данное предложение поддерживают Е.С. Саломатина [6] и Е.Н. Молодчая [7]. Однако значительное число авторов считают такое дополнение уголовного законодательства излишним. Так, Е.В. Старостина и Д.Б. Фролов указывают, что для привлечения к ответственности за кибертерроризм достаточно и тех формулировок, которые есть в ст. 205 УК РФ [8, с. 64]. Напомним, под террористическим актом понимается совершение не только взрывов и поджогов, но и иных действий, имеющих соответствующую направленность. Постановление Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» от 9 февраля 2012 г. № 1 также позволяет трактовать иные действия, как и осуществляемые в киберпространстве (п. 3)[3].

В.Н. Черкасов считает подобную детализацию нарушающей принципы уголовного закона, могущей привести к искусственному расширению понятийного аппарата и появлению таких новых составов, как кибермошенничество, киберклевета, кибершпионаж и др. Классификация может носить бесконечный характер [9, с. 10]. И.Р. Бегишев солидарен с данным мнением и указывает, что подобное дробление только запутает практических работников. Само же использование термина «кибертерроризм» возможно лишь в криминологических целях [10, с. 11].

Иными словами, современное российское уголовное законодательство не оперирует соответствующей терминологией, правовая база применительно даже к проработке возможного включения в УК РФ состава «кибертерроризм» не создана.

Анализ зарубежного уголовного законодательства также показывает нежелание вводить в него специальный состав, посвященный кибертерроризму, что не следует рассматривать как некий «заговор молчания». В отдельных странах есть лишь упоминание использования телекоммуникационных систем в террористических целях, что в большинстве случаев может рассматриваться как дополнительное отягчающее обстоятельство. Например, ст. 421-1 Уголовного кодекса Франции, предусматривая понятие акта терроризма, лишь дополняет, что оно будет распространяться и на преступные деяния в области информатики в случае выявления их целевой направленности. При этом сделана ссылка на книгу III Уголовного кодекса, устанавливающую уголовную ответственность за преступления в сфере компьютерной информации. После появления специальных электронных журналов и сайтов, пропагандирующих террористические действия, в УК Франции появилась ст. 421-2-5-2, которой введена уголовная ответственность за распространение в сети Интернет сообщений, изображений, иных информационных действий, включающих показ преднамеренных нападений на жизнь с демонстрацией приверженности к террористической идеологии.

Уголовное законодательство Италии имеет свою специфику. Так, помимо специальных составов за акты терроризма в УК Италии есть общая норма (ст. 280), позволяющая отнести к террористическому практически любое преступление, предусмотренное кодексом, если оно было совершено с данной целью. Внимание к кибертерроризму в Италии можно проследить

[1] Ущерб от телефонного терроризма в России составил 300 миллионов рублей. URL: https://ria.ru/defense_safety/20171005/1506292428.html.

[2] UK war-games cyber attack on Moscow // The Sunday Times. 2018. 7 Oct. URL: https://www.thetimes.co.uk/edition/news/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0.

[3] Российская газета. 2012. 17 февр.

на судьбе ст. 270-quinquies ее Уголовного кодекса, устанавливающей ответственность за обучение террористической деятельности. В 2005 г. эта статья была введена в УК Италии (благодаря Закону Джузеппе Писану, по фамилии инициатора — министра внутренних дел страны), но в 2015 г. получила важное дополнение — наказание увеличивается при обучении с использованием IT-технологий.

Понятие кибертерроризма содержится в уголовном законодательстве Пакистана. Оно было введено в 2007 г. указом президента страны (Prevention of Electronic Crimes Ordinance[4]). За использование компьютерных сетей в целях терроризма, повлекшее смерть человека, предусматривалась смертная казнь. В 2009 г. документ утратил силу, и только после масштабных обсуждений (с привлечением международных экспертов) в 2016 г. был принят Закон о предотвращении электронных преступлений (Prevention of Electronic Crimes Act[5]), в ст. 10 которого предусмотрена уголовная ответственность за кибертерроризм. Но и в этом случае происходит лишь отсылка к составам компьютерных преступлений с дополнением их террористической направленностью.

Таким образом, в некоторых зарубежных странах предпринята попытка применения мер уголовно-правового принуждения с целью противодействия кибертерроризму, однако представляется, что в существующей форме подобного рода регламентация говорит скорее о постановке проблемы, чем о возможном ее решении.

Большая доля скептицизма по отношению к самому явлению — кибертерроризму — присутствует в США и странах Западной Европы. Многие исследователи указывают, что на сегодняшний момент нет каких-либо достоверных данных о реальных возможностях террористических организаций внедриться в удаленные системы управления и нанести вред критически важным объектам инфраструктуры. В научной литературе приводятся ссылки на ежегодные доклады директоров национальной разведки США, в которых содержится оценка кибербезопасности страны. Например, в вводной части доклада Дэнниса Блэра за 2010 г. представлена общая оценка кибербезопасности, выделены перспективы развития киберпреступности. Лишь вскользь упоминается возможность преступников воздействовать с помощью удаленного доступа на критически важные объекты инфраструктуры. При этом формы противодействия кибертерроризму связаны с аморфным понятием «враг Америки» без его расшифровки. Далее, где дается базовая характеристика угроз со стороны основных террористических организаций, отсутствует упоминание о кибервозможностях преступников. Однако применительно к «Аль-Каиде» (организация запрещена в России) сделана небольшая ремарка о подготовке ею масштабной акции против США в целях нанесения наибольшего ущерба экономике страны [11]. Это позволило связать два тезиса воедино и ввести в медийный оборот новые страхи, связанные с кибертерроризмом, которые многими исследователями были встречены весьма скептически. Эксперт Совета по международным отношениям Роберт Кнайк приводит следующую статистику: из более чем 63 тыс. случаев терроризма в 2000–2010 гг. ни один не связан с кибертерроризмом. «Аль-Каида» никогда не имела возможностей для совершения кибератак на объекты США, которые могли бы привести даже к малозначительному ущербу. Единственный хакер (его ник — Irhabi 007), пойманный спецслужбами в Лондоне, который действовал по заданию террористов, имел весьма посредственные навыки [12]. Кстати, Р. Кнайк в своих экспертных оценках всегда сдержанно высказывается о кибертерроризме. Уже в 2015 г. этот эксперт поддерживал международные усилия по предотвращению компьютерных преступлений, приветствуя предложения по введению обязательной национальной ответственности государства, с чьей территории зафиксированы вредоносные кибератаки. Государство должно формировать национальную правовую базу таким образом, чтобы интернет-провайдеры были обязаны отслеживать вредоносные трафики и закрывать доступ к ним. Однако при этом он указывал, что данное предложение должно быть поддержано в первую очередь США. Для этого автор приводит информацию, согласно которой именно в Америке находится большинство серверов управления ботнетом — 21 % от общего числа в мире. На Россию и Китай (вместе взятые) приходится не более 5 %. Штаты явля-

[4] Prevention of Electronic Crimes Ordinance, 2007. URL: http://www.naseerahmad.com/information-technology/prevention-of-electronic-crimes-ordinance-pakistan-2007.html.

[5] Prevention of Electronic Crimes Act, 2016. URL: https://pcsw.punjab.gov.pk/Prevention%20of%20Electronic%20Crimes%20Act%2C%202016.

ются третьим по величине источником DDOS-атак. Это связано прежде всего с тем, что в США больше всего компьютеров и серверов с высокой пропускной способностью. Несмотря на это, ключевые американские провайдеры и хостинг-провайдеры, такие как GoDaddy и Rackspace, чьи мощные серверы часто используются для совершения вредоносных атак, саботируют любое вмешательство в свою внутреннюю политику конфиденциальности со стороны органов государственной власти [13].

Ярким примером несоответствия общественной опасности кибертерроризма тому вниманию, которое уделяют противодействию данному явлению, служит подход И. Лачоу, который отмечает, что террористические организации не могут нанести существенный вред инфраструктуре государств с помощью телекоммуникационных технологий, они будут лишь использовать их для сопутствующей деятельности: вербовки адептов, пропаганды, распространения идей и устрашающей информации, сбора финансовых средств и др. [14].

Во многом общественное мнение о важности угрозы кибертерроризма в США формируется в докладах национальной разведки страны. В 2011 г. Джеймс Клэппер вообще не упоминает кибертерроризм в числе угроз, представляя общую канву развития преступлений в сфере компьютерной информации[6]. В 2012 г. директор национальной разведки США в качестве фактора риска указывает на глобальное распространение смартфонов и развитие облачных технологий систематизации информации. Но и в данном случае термин «кибертерроризм» не используется[7]. В качестве эффективной предупредительной меры указано тесное взаимодействие органов власти и частного сектора, работающего в сфере компьютерной информации. В докладе 2014 г. киберпространство поставлено на первое место среди глобальных угроз, а Россия обозначена как страна, представляющая проблему для киберполитики и сетевой безопасности США[8]. В докладе данный фактор четко назван угрозой интересам и ценностям Америки. Террористическим организациям в этой части уделено всего два предложения: «Проявили интерес к разработке наступательных кибервозможностей. Они продолжают использовать киберпространство для пропаганды и влияния, финансовой деятельности и вербовки сторонников». В докладе 2017 г. Россия обозначена уже как главная угроза кибербезопасности США. Основной акцент сделан на обвинение России во влиянии на выборы 2016 г. (подчеркивается, что подобные действия могли быть осуществлены только с согласия высших должностных лиц). Указано, что российские хакеры осуществили «разрушительные» кибератаки на критически важные объекты инфраструктуры США[9]. Ни в том, ни в другом случае какие-либо конкретные факты (тем более доказательства) не приводятся.

Подобные прогнозы делаются с целью формирования определенного общественного мнения для последующего обоснования дополнительных ограничений, налагаемых на интернет-общение, введения специальных форм регулирования коммуникативных технологий, расширения полномочий национальных спецслужб. Можно констатировать, что поскольку угроза возможных атак со стороны кибертеррористов не возымела нужный результат (профессор Военно-морской академии США Дж.Р. Лукас — младший назвал проблему кибертерроризма «значительно раздутой» [15]), западные разведывательные органы специально муссируют тему о кибервмешательстве России, Китая, Ирана в дела других стран. Р. Кнайк в 2017 г., представляя рекомендации администрации Д. Трампа, прямо советует рассматривать кибератаки как «вооруженное нападение, влекущее за собой военный ответ» [16]. Обозначенные выше примеры ярко иллюстрируют политический контекст определения кибертерроризма как угрозы обществу.

[6] Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence, 2010. URL: http://www.au.af.mil/au/awc/awcgate/dni/threat_assessment_10feb11.pdf.

[7] Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence, 2012. URL: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/hpscifinalunclasssfrfeb022012).pdf.

[8] Statement for the Record Worldwide Threat Assessment of the US Intelligence Community House Permanent Select Committee on Intelligence, 2014. URL: https://www.globalsecurity.org/intell/library/congress/2014_hr/140204-clapper.pdf.

[9] Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence, 2017. URL: https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf.

В российской и зарубежной юридической науке и общественно-политической мысли можно отметить некоторые разночтения в самом понимании кибертерроризма. Так, есть широкое понимание, включающее в себя любое использование компьютерной информации в террористических целях. То есть кибертерроризм охватывает как осуществление преднамеренных атак на объекты инфраструктуры в целях создания условий для техногенной катастрофы, так и использование Всемирной паутины в банальных преступных целях (кража информации, распространение вредоносных программ, хакерство) и для пропаганды и вербовки сторонников [17]. Имеется и узкая трактовка, предполагающая только такое воздействие на объекты инфраструктуры с помощью удаленного доступа, которое способно причинить определенный вред либо создать реальную угрозу [18, с. 64]. Присутствует и некоторая путаница. Например, в апреле 2017 г. группа депутатов Государственной Думы РФ предложила классифицировать как кибертерроризм создание групп смерти в социальных сетях. Чуть позже первым заместителем председателя Комитета Госдумы по государственному строительству и законодательству М. Емельяновым было высказано мнение о распространении данного понятия на вербовку сторонников идей терроризма через социальные сети. Данные инициативы не нашли законодательного подтверждения[10].

Представители зарубежной науки также признают отсутствие единства в понимании кибертерроризма. Так, Кембриджский центр исследований рисков представляет следующее определение рассматриваемого явления: это «акт политически мотивированного насилия, повлекший имущественный ущерб или вред жизни и здоровью граждан, вызванный удаленным цифровым вмешательством в технологические системы» [19]. Р. Литтлфилд считает, что кибертерроризм отличает от преступления в сфере компьютерной информации мотив [20].

В США чаще всего приводят слова эксперта ФБР М. Поллита, указывавшего на определенные страхи, которые аккумулирует в себе понятие кибертерроризма: «Страх случайной, насильственной виктимизации хорошо сочетается с недоверием и открытостью компьютерных технологий, которые усиливаются в страхе перед неизвестным. Легко не доверять тому, что невозможно контролировать». Эксперт дополняет, что в обществе присутствует заблуждение о возможности создания супермашины, которая будет контролировать все телекоммуникационные процессы, одновременно управляя всеми компьютерными системами страны. Благодаря этому появляется паническое настроение по поводу возможности единовременного контроля над сверхмашиной со стороны террористов. М. Поллит развеивает эти страхи, отмечая, однако, что информационное пространство, которое создается в том числе благодаря развитию телекоммуникационных технологий, нуждается в определенной защите. Следует добавить, что он выделяет собственно кибертерроризм, под которым понимает преднамеренную политически мотивированную атаку террористических организаций или их скрытых агентов на информационные потоки, компьютерные системы, данные или программы, которые приводят к насилию. Автор делает ремарку об узости данного определения [21].

Интересным выглядит определение кибертерроризма, представленное зарубежными экспертами в 2017 г. для Туниса с целью его применения в деятельности государственных органов власти и спецслужб страны. В нем выделены следующие признаки:

– осуществляется через киберпространство отдельными лицами, группами или организациями, находящимися под непосредственным влиянием со стороны террористических движений и (или) их лидеров;

– мотивировано желанием осуществить политические или идеологические изменения;

– обусловливает насилие, благодаря которому физические и психологические последствия могут выходить далеко за пределы непосредственной жертвы или цели воздействия [22].

При этом кибертерроризм классифицируется на гибридный и кибертерроризм в чистом виде. В первом случае это использование Интернета для террористической деятельности: пропаганды, вербовки сторонников, их обучения, радикализации общества, сбора средств, получения данных, осуществления связи, планирования реальных террористических атак, во втором — прямые атаки на киберинфраструктуру для достижения политических, религиозных и идеологических целей.

Кибертерроризм в чистом виде разделяется на разрушительный и подрывной. Разрушительный кибертерроризм — это порча функ-

[10] URL: https://news.rambler.ru/politics/36582739-v-gosdume-vystupili-za-klassifikatsiyu-verbovki-v-terroristy-cherez-sotsseti-kak-kiberterrorizm.

ций информационной системы для нанесения ущерба или уничтожения виртуальных и физических активов. Наиболее популярным способом является использование компьютерных вирусов, «червей», троянских программ, а также вымогательство. Подрывной кибертерроризм подразумевает взлом компьютерных сетей, обеспечивающих критическую инфраструктуру (медицинская помощь, транспорт, финансовые системы и т.д.), нарушающий нормальный образ жизни общества, государства, граждан.

Обращает на себя внимание тот факт, что в настоящее время наибольшее распространение приобретает гибридный кибертерроризм, связанный с пропагандой террористических идей, обучением сторонников, их вербовкой и подготовкой для совершения одиночных атак. Интернет, благодаря своей открытости, влияет и на структуру террористических организаций, все больше превращающихся в сетевое сообщество, не имеющее централизованного управления. В странах Западной Европы введен в оборот термин «одинокий волк», которым характеризуют современного террориста, не имеющего прямого контакта с самой организацией, манипулирующей его сознанием с использованием новых информационных технологиий [23]. Именно гибридный кибертерроризм представляет в настоящее время наибольшую опасность.

Началом использования Интернета для проведения масштабных акций считается арест Абдуллы Оджалана, лидера Курдской рабочей партии. Он был арестован 16 февраля 1999 г., и в этот же день, спустя всего несколько часов после ареста, массовые акции протеста прокатились по всему миру. 17 февраля были захвачены греческие посольства и иные дипломатические представительства по всему миру (Оджалан был арестован на территории греческого посольства в Кении), в том числе и в Москве [24]. В настоящее время террористические организации озабочены шифрованием передаваемых сообщений для координации собственных действий. Франческо Полино, заместитель прокурора Итальянской Республики, прямо называет в своем докладе российский Telegram мессенджером, который используют террористы по рекомендации своих кураторов. Использование данного мессенджера происходило во время массовых беспорядков в Иране, в некоторых областях Китая, при координации деятельности преступных групп в Афганистане. Это привело к тому, что в Иране мессенджер был официально запрещен 30 апреля 2018 г.[11] Напомним, в нашей стране уже более года мы являемся свидетелями конфликта, в котором участвуют Telegram и Роскомнадзор, а также российские спецслужбы.

Гибридный кибертерроризм, связанный с пропагандой террористических идей, оказывает самое прямое влияние на массовое сознание граждан. По силе психологического воздействия эффект от него зачастую значительно превышает последствия непосредственной террористической атаки [25]. В условиях нестабильности социально-политической обстановки во всем мире террористические организации осознали, что благодаря точечным воздействиям, не требующим значимых финансовых затрат и глубокого знания компьютерных систем, можно достигать весьма далеко идущих результатов. Эффект будет усиливаться при внедрении сторонников террористических организаций в критически важную инфраструктуру, что обусловливает введение специальных процедур допуска для работников, имеющих доступ к компьютерным системам [26]. Все это позволяет указывать на появление либо кибер-халифата [27], либо электронного джихада [28], как это представлено в зарубежных криминологических исследованиях.

Проведенные за рубежом исследования и активизация темы кибертерроризма в массовом сознании граждан привели к созданию государственных структур, призванных оказывать противодействие данному явлению в общенациональном масштабе, а также помощь любому пользователю электронных технологий. Так, в Великобритании создан Национальный центр кибербезопасности[12]. Сформирован аналогичный центр и в структуре НАТО[13], но его задачи носят уже военный характер. По-видимому, по такому же пути следует идти и Российской Федерации, тем более что «Лаборатория Касперского» выполняет некоторые функции, характерные для зарубежных центров. Но здесь следует активнее внедрять механизмы государственно-частного партнерства и на базе лидеров рынка в области обеспечения информационной безопасности создать государственный центр, нацеленный на работу в общенациональном масштабе.

[11] URL: https://www.newsru.com/world/30apr2018/teleiran.html.

[12] URL: https://www.ncsc.gov.uk.

[13] URL: https://www.nato.int/cps/en/natohq/topics_78170.htm.

Борьба с киберпреступностью (а значит, и с кибертерроризмом) будет иметь значимый эффект только при объединении усилий всего международного сообщества. Криминализация таких действий в одной стране может быть легко обойдена отсутствием ответственности в другой [29]. Предлагается ввести универсальную юрисдикцию, при которой государство, подвергнувшееся атаке, может требовать ее расследования, наказания виновных и возмещения ущерба от государства, с территории которого было осуществлено нападение [30]. В 2016 г. в Грозном по инициативе России (под патронажем Совета безопасности РФ) была проведена конференция, посвященная проблемам кибербезопасности, на которой присутствовали делегаты из 75 стран. Основная опасность была обозначена как «война в условиях мира»[14].

Таким образом, правовые основы противодействия кибертерроризму через призму общественно-политического измерения основываются на следующих общих моментах:

1. В настоящее время кибертерроризм является значительно преувеличенной угрозой. Стандартная киберпреступность наносит более существенный ущерб экономике любого государства. Но в силу отсутствия единого центра и по причине экстремистской идеологии она не может вселять такие социальные страхи, которые можно внушить обществу благодаря отсылкам к активности террористических организаций. Таким образом, в США и странах Западной Европы тема кибертерроризма несет в себе в большей мере политическую нагрузку. При малоубедительности представления опасности от киберпреступлений со стороны террористических организаций в США муссируется тема о киберугрозах со стороны России, Китая и Ирана и проводится идеологическая обработка общества о необходимости наступательных действий в киберпространстве в отношении указанных стран.

2. Во всем мире существуют определенные разночтения в понимании кибертерроризма. Эксперты признают, что зачастую невозможно провести грань между данным явлением и проявлением обычной преступности в сфере компьютерной информации. Традиционно есть широкое (любое использование компьютерных сетей в террористических целях) и узкое (действия, направленные на нанесение конкретного вреда инфраструктуре, жизни и здоровью граждан) понимание кибертерроризма.

3. В Российской Федерации отсутствует специальный состав уголовного преступления — кибертерроризм, что вписывается в общую зарубежную логику уголовно-правовой политики. В большинстве стран мира также отсутствует такой специальный состав преступления. В то же время заслуживает поддержки дополнение Уголовного кодекса РФ примечанием, согласно которому совершение преступления террористической направленности с использованием телекоммуникационных технологий является отягчающим обстоятельством и влечет за собой повышенные меры ответственности.

[14] Делегаты из 75 стран оказались в Грозном без смотрящего. URL: https://www.kommersant.ru/doc/2997208.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Collin B. The Future of CyberTerrorism / B. Collin // XI Annual International Symposium on Criminal Justice Issues. — Chicago : Univ. of Illinois, 1996. — P. 285–289.

2. Lewis J. Cyber Terror: Missing in Action / J. Lewis // Knowledge, Technology & Policy. — 2003. — Vol. 16, iss. 2. — P. 34–41.

3. Weimann G. Cyberterrorism: How Real Is the Threat? / G. Weimann. — URL: https://www.usip.org/sites/default/files/sr119.pdf.

4. Weimann G. Cyberterrorism: The Sum of All Fears? / G. Weimann // Studies in Conflict & Terrorism. — 2005. — № 28. — P. 129–149.

5. Чекунов И.Г. Киберпреступность: понятие и классификация / И.Г. Чекунов // Российский следователь. — 2012. — № 2. — С. 37–44.

6. Саломатина Е.С. Перспективы развития законодательства в сфере борьбы с кибертерроризмом / Е.С. Саломатина // Закон и право. — 2009. — № 1. — С. 47–48.

7. Молодчая Е.Н. Политика противодействия кибертерроризму в современной России: политологический аспект : дис. … канд. полит. наук : 23.00.02 / Е.Н. Молодчая. — Москва, 2011. — 188 с.

8. Старостина Е.В. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом / Е.В. Старостина, Д.Б. Фролов // Законодательство и экономика. — 2005. — № 5. — С. 62–66.

9. Черкасов В.Н. Информационная безопасность. Правовые проблемы и пути их решения / В.Н. Черкасов // Информационная безопасность регионов. — 2007. — № 1. — С. 6–14.

10. Бегишев И.Р. Проблемы противодействия посягательствам на информационные системы критически важных и потенциально опасных объектов / И.Р. Бегишев // Информационная безопасность регионов. — 2010. — № 1. — С. 9–13.

11. Blair D. Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence / D. Blair. — USA : National Intelligence, 2010. — URL: https://www.dni.gov/files/documents/Newsroom/Testimonies/20100203_testimony.pdf.

12. Knake R.K. Cyberterrorism Hype v. Fact / R.K. Knake // Council on Foreign Relations. — 2010. — 12 Febr. — URL: https://www.cfr.org/expert-brief/cyberterrorism-hype-v-fact.

13. Knake R.K. Cleaning Up U.S. Cyberspace / R.K. Knake // Council on Foreign Relations. — 2015. — Dec. — URL: https://cfrd8-files.cfr.org/sites/default/files/pdf/2015/12/Cleaning_Up_CyberBrief.pdf.

14. Lachow I. Terrorist Use of the Internet: The Real Story / I. Lachow, R. Courtney // Research Gate. — 2007. — № 45. — P. 100–103.

15. Singer P.W. The Cyber Terror Bogeyman / P.W. Singer // Brookings. — 2010. — 1 Nov. — URL: https://www.brookings.edu/articles/the-cyber-terror-bogeyman.

16. Knake R.K. A Cyberattack on the U.S. Power Grid: Contingency Planning Memorandum No. 31 / R.K. Knake // Council on Foreign Relations. — 2017. — Apr. — URL: https://cfrd8-files.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf.

17. Васенин В.А. Информационная безопасность и компьютерный терроризм / В.А. Васенин // Научные и методологические проблемы информационной безопасности : сб. науч. тр. / под ред. В.П. Шерстюка. — Москва, 2004. — С. 67–84.

18. Современный терроризм: сущность, типология, проблемы противодействия / под ред. Ю.В. Гаврилова, Л.В. Смирнова. — Москва : Юрид. ин-т МВД РФ, 2003. — 66 с.

19. Cyber Terrorism: Assessment of the Threat to Insurance / T. Evan, E. Leverett, S.J. Ruffle, A.W. Coburn [et al.]. — Univ. of Cambridge, 2017. — 42 p.

20. Littlefield R. Cyber Terrorism: Understanding and Preventing Acts of Terror within our Cyber Space / R. Littlefield. — URL: https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb.

21. Pollitt M.M. Cyberterrorism — Fact or Fancy? / M.M. Pollitt // Computer Fraud & Security. — 1998. — Iss. 2. — P. 8–10.

22. Zerzri M. The Threat of Cyber Terrorism and Recommendations for Countermeasures / M. Zerzri // Center for Applied Policy Research. — 2017. — № 4. — URL: https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf.

23. Polino F. Il Contrasto alle nuove Forme di Terrorismo internazionale / F. Polino // Associazione Magisratura Indipendente. — 2017. — 6 marzo. — URL: http://www.magistraturaindipendente.it/il-contrasto-alle-nuove-forme-di-terrorismo-internazionale.htm.

24. Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy / D.E. Denning // IWS. — 1999. — 10 Dec. — URL: http://www.iwar.org.uk/cyberterror/resources/denning.htm.

25. Gross M.L. The Psychological Effects of Cyber Terrorism / M.L. Gross, D. Canetti, D.R. Vashdi // Bulletin of the Atomic Scientists. — 2016. — Vol. 72, iss. 5. — P. 284–291.

26. Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment / Z.M. King, D.S. Henshel, L. Flora, M.G. Cains [et al.] // Frontiers in Psychology. — 2018. — № 5. — P. 9–39.

27. Alkhouri L. Hacking for ISIS: The Emergent Cyber Threat Landscape / L. Alkhouri, A. Kassirer, A. Nixon // Flashpoint. — 2016. — Apr. — URL: https://fortunascorner.com/wpcontent/uploads/2016/05/Flashpoint_HackingForISIS _April2016-1.pdf.

28. Heickerö R. Cyber Terrorism: Electronic Jihad / R. Heickerö // Journal Strategic Analysis. — 2014. — Vol. 38, iss. 4. — P. 554–565.

29. Якимова Е.М. Международное сотрудничество в борьбе с киберпреступностью / Е.М. Якимова, С.В. Нарутто. — DOI: 10.17150/1996-7756.2016.10(2).369-378 // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10, № 2. — С. 369–378.

30. Tehrani P.M. Cyber Terrorism Challenges: The Need for a Global Response to a Multi-jurisdictional Crime / P.M. Tehrani, N.A. Manap, H. Taji // Computer Law & Security Review. — 2013. — Vol. 29, iss. 3. — P. 207–215.

REFERENCES

1. Collin B. The Future of Cyber-Terrorism. *XI Annual International Symposium on Criminal Justice Issues*. Chicago, University of Illinois, 1996, pp. 285–289.

2. Lewis J. Cyber Terror: Missing in Action. *Knowledge, Technology & Policy*, 2003, vol. 16, iss. 2, pp. 34–41.

3. Weimann G. *Cyberterrorism: How Real Is the Threat?* URL: https://www.usip.org/sites/default/files/sr119.pdf.

4. Weimann G. Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*, 2005, no. 28, pp. 129–149.

5. Chekunov I.G. Cybercrimes: Definition and Classification. *Rossiiskii sledovatel' = Russian Investigator,* 2012, no. 2, pp. 37–44. (In Russian).

6. Salomatina E.S. Prospects for the Development of Legislation in the Field of Combating Cyber-terrorism. *Zakon i pravo = Law and Right,* 2009, no. 1, pp. 47–48. (In Russian).

7. Molodchaya E.N. *Politika protivodeistviya kiberterrorizmu v sovremennoi Rossii: politologicheskii aspect*. *Kand. Diss.* [The Policy of Counteracting Cyberterrorism in Modern Russia. Political Science Aspect. Cand. Diss.]. Moscow, 2011. 188 p.

8. Starostina E.V. Ways of improving the legislative system of counteracting cyber-terrorism in Russian and in other countries. *Zakonodatel'stvo i ekonomika = Legislation and Economy,* 2005, no. 5, pp. 62–66. (In Russian).

9. Cherkasov V.N. Information Security. Legal Problems and their Solutions. *Informatsionnaya bezopasnost' regionov = Information Security of Regions,* 2007, no. 1, pp. 6–14. (In Russian).

10. Begishev I.R. Problems of Counter Action to the Criminal Encroachments on the Information Systems of Critical and Potentially Dangerous Objects. *Informatsionnaya bezopasnost' regionov = Information Security of Regions,* 2010, no. 1, pp. 9–13. (In Russian).

11. Blair D. *Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence*. USA, National Intelligence, 2010. Available at: https://www.dni.gov/files/documents/Newsroom/Testimonies/20100203_testimony.pdf.

12. Knake R.K. Cyberterrorism Hype v. Fact. *Council on Foreign Relations*, 2010, February 12. Available at: https://www.cfr.org/expert-brief/cyberterrorism-hype-v-fact.

13. Knake R.K. Cleaning Up U.S. Cyberspace. *Council on Foreign Relations*, 2015, December. Available at: https://cfrd8-files.cfr.org/sites/default/files/pdf/2015/12/Cleaning_Up_ CyberBrief.pdf.

14. Lachow I., Courtney R. Terrorist Use of the Internet: The Real Story. *Research Gate*, 2007, no. 45, pp. 100–103.

15. Singer P.W. The Cyber Terror Bogeyman. *Brookings*, 2010, November 1. Available at: https://www.brookings.edu/articles/the-cyber-terror-bogeyman.

16. Knake R.K. A Cyberattack on the U.S. Power Grid: Contingency Planning Memorandum No. 31. *Council on Foreign Relations*, 2017, April. Available at: https://cfrd8-files.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf.

17. Vasenin V.A. Information Security and Computer Terrorism. In Sherstyuk V.P. (ed.). *Nauchnye i metodologicheskie problemy informatsionnoi bezopasnosti* [Scientific and Methodological Problems of Information Security]. Moscow, 2004, pp. 67–84. (In Russian).

18. Gavrilov Yu.V., Smirnov L.V. (eds.). *Sovremennyi terrorizm: sushchnost', tipologiya, problemy protivodeistviya* [Modern Terrorism: Essence, Typology, Problem of Counteraction]. Moscow Law Institute of Russian Ministry of the Interior Publ., 2003. 66 p.

19. Evan T., Leverett E., Ruffle S.J., Coburn A.W., Bourdeau J., Gunaratna R., Ralph D. *Cyber Terrorism: Assessment of the Threat to Insurance*. University of Cambridge, 2017. 42 p.

20. Littlefield R. *Cyber Terrorism: Understanding and Preventing Acts of Terror within our Cyber Space*. Available at: https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb.

21. Pollitt M.M. Cyberterrorism — Fact or Fancy? *Computer Fraud & Security*, 1998, iss. 2, pp. 8–10.

22. Zerzri M. The Threat of Cyber Terrorism and Recommendations for Countermeasures. *Center for Applied Policy Research*, 2017, no. 4. Available at: https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf.

23. Polino F. Il Contrasto alle nuove Forme di Terrorismo internazionale. *Associazione Magisratura Indipendente*, 2017, 6 marzo. Available at: http://www.magistraturaindipendente.it/il-contrasto-alle-nuove-forme-di-terrorismo-internazionale.htm. (In Italian).

24. Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *IWS*, 1999, December 10. Available at: http://www.iwar.org.uk/cyberterror/resources/denning.htm.

25. Gross M.L., Canetti D., Vashdi D.R. The Psychological Effects of Cyber Terrorism. *Bulletin of the Atomic Scientists*, 2016, vol. 72, iss. 5, pp. 284–291.

26. King Z.M., Henshel D.S., Flora L., Cains M.G., Hoffman B., Sample C. Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. *Frontiers in Psychology*, 2018, no. 5, pp. 9–39.

27. Alkhouri L., Kassirer A., Nixon A. Hacking for ISIS: The Emergent Cyber Threat Landscape. *Flashpoint*, 2016, April. Available at: https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf.

28. Heickerö R. Cyber Terrorism: Electronic Jihad. *Journal Strategic Analysis,* 2014, vol. 38, iss. 4, pp. 554–565.

29. Yakimova E.M., Narutto S.V. International cooperation in cybercrime counteraction. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2016, vol. 10, no. 2, pp. 369–378. DOI: 10.17150/1996-7756.2016.10(2).369-378. (In Russian).

30. Tehrani P.M., Manap N.A., Taji H. Cyber Terrorism Challenges: The Need for a Global Response to a Multi-jurisdictional Crime. *Computer Law & Security Review*, 2013, vol. 29, iss. 3, pp. 207–215.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Кулешова Галина Петровна — профессор кафедры уголовного права и криминологии Средне-Волжского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), доктор социологических наук, г. Саранск, Российская Федерация; e-mail: kuleshova62@yandex.ru.

Капитонова Елена Анатольевна — доцент кафедры уголовного права Пензенского государственного университета, кандидат юридических наук, г. Пенза, Российская Федерация; e-mail: e-kapitonova@yandex.ru.

Романовский Георгий Борисович — заведующий кафедрой уголовного права Пензенского государственного университета, доктор юридических наук, профессор, г. Пенза, Российская Федерация; e-mail: up406@mail.ru.

INFORMATION ABOUT THE AUTHORS

Kuleshova, Galina P. — Professor, Chair of Criminal Law and Criminology, Middle Volga Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Doctor of Sociology, Saransk, the Russian Federation, e-mail: kuleshova62@yandex.ru.

Kapitonova, Elena A. — Ass. Professor, Chair of Criminal Law, Penza State University, Ph.D. in Law, Penza, the Russian Federation; e-mail: e-kapitonova@yandex.ru.

Romanovsky, Georgy B. — Head, Chair of Criminal Law, Penza State University, Doctor of Law, Professor, Penza, the Russian Federation; e-mail: up406@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Кулешова Г.П. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения / Г.П. Кулешова, Е.А. Капитонова, Г.Б. Романовский. — DOI: 10.17150/2500-4255.2020.14(1).156-165 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 1. — С. 156–165.

FOR CITATION

Kuleshova G.P., Kapitonova E.A., Romanovsky G.B. The legal basis of countering cyber-terrorism in Russia and in other countries from the standpoint of its social and political dimension. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 1, pp. 156–165. DOI: 10.17150/2500-4255.2020.14(1).156-165. (In Russian).