УДК 343.34

Е. А. Капитонова

ОСОБЕННОСТИ КИБЕРТЕРРОРИЗМА КАК НОВОЙ РАЗНОВИДНОСТИ ТЕРРОРИСТИЧЕСКОГО АКТА

Аннотация.

Актуальность и цели. Кибератаки являются одной из наиболее опасных форм проявления современного терроризма. В то же время в российском праве, как и в юридической науке, отсутствует четкое понимание понятий, связанных с регулированием данной проблемы. Целями работы являются уточнение понятийного аппарата и формирование предложений по внесению изменений в законодательство.

Материалы и методы. Были использованы метод диалектики как общенаучный метод познания, позволяющий изучать явления и процессы окружающей действительности в их историческом развитии, а также частнонаучные методы (формально-юридический, сравнительно-правовой и метод системного анализа).

Результаты. Рассмотрено содержание предлагаемых различными авторами дефиниций кибертерроризма, проведено их сопоставление между собой и с западными аналогами. Автор привел и обосновал собственную точку зрения по данному вопросу. Определены недостатки правового регулирования уголовной ответственности за кибертерроризм в России. Предложено внести ряд изменений в Уголовный кодекс Российской Федерации с тем, чтобы обеспечить наказуемость всех возможных способов использования сети Интернет при совершении террористических актов.

Выводы. Сформулированные в исследовании теоретические положения направлены на выработку рекомендаций по совершенствованию российского законодательства и способны качественно повысить его уровень. Они также могут быть использованы в научной деятельности и учебном процессе учреждений высшего профессионального образования юридического профиля, при повышении квалификации практических работников и научно-педагогических кадров в области юриспруденции.

Ключевые слова: терроризм, террористический акт, кибертерроризм, преступления, сеть Интернет.

E. A. Kapitonova

FEATURES OF CYBERTERRORISM AS A NEW KIND OF TERRORIST ATTACKS

Abstract.

Background. Cyber attacks are one of the most dangerous forms of modern terrorism. At the same time in the Russian law, as well as in jurisprudence, there is no clear understanding of the concepts related to this problem. The objectives of the work is to clarify the conceptual apparatus and to generate proposals for amendments to the legislation.

Materials and methods. The author used the method of dialectics as a general scientific method of knowledge that allows to study the phenomena and processes of reality in their historical development, as well as private-scientific methods (formal-legal, comparative legal method and system analysis).

Results. The author considered the content of definitions of cyberterrorism offered by various authors, comparing them with each other and with Western simi-

lars. The researcher presented and proved her own point of view on this issue. Shortcomings of legal regulation of criminal responsibility for cyberterrorism in Russia were identified. It was suggested introduce a number of changes to the Criminal Code of the Russian Federation in order to ensure punishment for all possible ways to use the Internet for terrorist acts commitment.

Conclusions. Theoretical propositions formulated in the study are aimed at elaboration of recommendations on improving the Russian legislation and are able to raise the level thereof. They can also be used in the academic activity and in the educational process of higher professional education establishments of the law sphere, and in advanced studies for practicing staff and scientific-academic personnel in the sphere of jurisprudence.

Key words: terrorism, act of terrorism, cyber-terrorism, crime, Internet.

Модернизация общества и развитие информационных технологий привели к массовому использованию во всем мире Интернета. С появлением глобальной сети возникла одна из наиболее опасных разновидностей киберпреступности – кибертерроризм, который, по сравнению с традиционным терроризмом, при совершении террористических акций прибегает к новейшим достижениям науки и техники.

Впервые термин «кибертерроризм» употребил старший научный сотрудник Калифорнийского института безопасности и разведки Барри Коллин в 1980 г. В те годы предшественница Интернета – сеть ARPANET Управления перспективных разработок Минобороны США – объединяла всего несколько десятков компьютеров на территории одного государства. Тем не менее исследователь был уверен, что со временем возможности киберсетей будут взяты на вооружение террористами, хотя и полагал, что случится это никак не ранее первого десятилетия XXI в. Время опередило предсказания: первые попытки кибератак были зафиксированы правоохранительными органами уже в 1990-х гг. (например, в 1993 г. террористы в Литве угрожали взорвать Игналинскую АЭС посредством перехвата компьютерного контроля над ней при помощи вредоносной программы типа «троянский конь», а в июне 1998 г. международная группа хакеров Milw0rm получила доступ к Индийскому центру атомных исследований Bhabha Atomic Research Center (BARC) и создала фальшивую страницу сайта устрашающего характера). В 1997 г. специальный агент ФБР Марк Поллитт ввел в обиход новый юридический термин, предложив считать кибертерроризмом любую «умышленную, политически мотивированную атаку на информацию, компьютерные системы, программы и данные, которые приводят к насилию в отношении невоенных целей, групп населения или тайных агентов» [1].

Современные террористы активно используют возможности Интернета: легкий доступ в сеть, практически полное отсутствие цензуры, большой масштаб аудитории, анонимность и т.п. В наши дни они рассматривают глобальную сеть главным образом в качестве средства пропаганды и передачи информации. Так, например, одна из известнейших террористических организаций «Аль-Каида» в 2011 г. запустила онлайн-журнал для пропаганды своей деятельности на английском языке. Интернет-издание под названием Inspire («Вдохновляй») призывает и поощряет единомышленников сделать свой вклад в общее дело просвещения всех заинтересованных лиц, прислав статью, оставив комментарий или рекомендацию [2, с. 21].

Американский исследователь Дэн Вертон считает, что многие террористические организации создали в Интернете базы разведывательных данных, которые используются при подготовке атак [3, с. 72]. Расследование некоторых терактов подтвердило это суждение. К примеру, доказано, что террористическая группировка «Аум Синрике», осуществившая газовую атаку в токийском метро в 1995 г., предварительно создала компьютерную программу, которая была способна перехватывать сообщения полицейских радиостанций и отслеживать маршруты движения полицейских автомобилей.

Директор Джорджтаунского института обеспечения безопасности информации при Университете Джорджтауна и эксперт Центра исследований терроризма США Дороти Дэннинг считает, что деятельность террористов в сети Интернет можно разделить на три группы: активность, хакерство и кибертерроризм [4]. Под активностью она предлагает понимать простое использование компьютерных технологий (в целях пропаганды идей, привлечения денежных средств и новых последователей). В этом случае киберпространство выступает средством, содействующим объединению террористов, рекрутированию новых членов в террористические формирования. Широки и сетевые возможности сбора пожертвований – от простого перечисления средств указанными на сайте способами до функционирования полноценных интернет-магазинов (в частности, «Хезболла» через свой сайт продает книги, плакаты и футболки с собственной символикой).

Хакерство подразумевает противозаконные атаки на компьютерные сети, секретные базы данных и сайты для получения какой-либо информации или хищения денег. Кибертерроризм хотя и схож по способам его осуществления с хакерством, но все же представляет, по мнению Дэннинг, совсем другой вид компьютерных атак, который планируется с иными целями (нанесение крупного ущерба жизненно важным объектам инфраструктуры посредством использования информационных технологий).

Следует признать, что для нашей страны в настоящее время актуальны все три упомянутых вида деятельности. Наиболее распространена из них, по терминологии Дэннинг, простая активность террористов в Интернете. Еще по состоянию на 2009 г. МВД России ежегодно выявляло не менее 150 ресурсов, содержащих материалы террористической и экстремистской направленности, при этом большая часть подобных сайтов (около 70) обнаруживалась в российском сегменте сети [5, с. 63]. Специализированным подразделением МВД РФ в соответствии с законодательством постоянно закрываются сайты с негативным, противоречащим российскому законодательству контентом. Однако впоследствии не менее 15 % из них появляются вновь под другими именами на хостинговых ресурсах как российских, так и зарубежных провайдеров.

По мнению юристов и многих должностных лиц, кибертерроризм представляет собой серьезную угрозу человечеству, сравнимую едва ли не с оружием массового поражения. К примеру, МЧС России отмечает, что особенно уязвимыми для кибератак являются энергетические системы. В последние годы Россия активно внедряет в различные отрасли хозяйства автоматизированные и информационные технологии, что выводит вопрос борьбы с кибертерроризмом в разряд одной из важнейших государственных задач[1]. Предста-

[1] МЧС считает кибертерроризм одним из ключевых рисков. – URL: http://i-business.ru/blogs/16367 (дата обращения: 26.03.2015).

вители Федеральной службы безопасности России также заявляли об опасениях относительно возможных кибератак террористов на электронные сети государственных структур, которые управляют объектами «кризисной инфраструктуры» (атомные электростанции, ядерные реакторы, военные объекты, нефте- и газопроводы, ведущие предприятия оборонно-промышленного комплекса)[1].

Тем не менее в действующих российских правовых актах отсутствует определение кибертерроризма и способов его совершения. Это обстоятельство признается современными учеными в качестве одного из главных проблемных факторов выявления и противодействия кибератакам [6, с. 166].

Отечественной юридической наукой даже не выработано единой точки зрения относительно дефиниции понятия «кибертерроризм». Одни авторы под кибертерроризмом понимают совокупность противоправных действий, связанных с покушением на жизнь людей, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимущества при решении политических, экономических или социальных задач [7]. Другие оценивают его как преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, что создает опасность для жизни и здоровья людей, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [8]. Схожей точки зрения придерживается, кстати, директор Центра защиты национальной инфраструктуры ФБР США Рональд Дик, который в опубликованном еще в 2002 г. на сайте правительственной организации докладе назвал зависимость от компьютерных технологий «ахиллесовой пятой современного мира» и указал, что кибертерроризм – это новая форма терроризма, которая использует компьютеры и сети для разрушения государственной инфраструктуры и достижения своих целей[2].

Интересным представляется и суждение авторов, связывающих кибертерроризм с противоправным воздействием на информационные системы в целях создания опасности причинения вреда жизни, здоровью, имуществу неопределенного круга лиц путем формирования условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности (Ю. В. Гаврилов, Л. В. Смирнов) [9, с. 54]. Такая формулировка представляется наиболее обоснованной. Кибертерроризм способен разрушить информационную систему управления объектов инфраструктуры (транспорт, энергетика и т.п.) и вызвать наступление тяжких последствий, например крушение самолета, поезда, выброс отравляющих и загрязняющих веществ в окружающую среду, взрыв на атомных станциях, подобный аварии на Чернобыльской АЭС и др.

[1] ФСБ опасается возможных кибератак террористов на электронные сети госструктур // RG.RU – Российская газета. – URL: http://www.rg.ru/2009/04/15/fsb-sedov-anons.html (дата обращения: 26.03.2015).

[2] Cyber Terrorism and Critical Infrastructure Protection / FBI – The Federal Bureau of Investigation. – URL: http://www.fbi.gov/news/testimony/cyber-terrorism-and-critical-infrastructure-protection (дата обращения: 26.03.2015).

Отдельно следует оговорить случаи, когда устрашение населения достигается посредством публикации на подконтрольных террористам сайтах (или просто во всеобщем доступе, например на видеоканале YouTube) новостей, содержание которых способно вызвать панику и ощущение безнадежности у широких слоев населения. На подобных сайтах, к примеру, могут быть размещены фото- и видеоматериалы, носящие характер угрозы. Одними из первых применили с этой целью сеть боевики перуанской организации «Тупак Амару», когда в 1996 г. во время приема в японском посольстве они взяли в заложники несколько десятков человек. На созданных их последователями пропагандистских сайтах журналистам предлагалось получить комментарии по поводу происходящего у самих лидеров «Тупак Амару» буквально в режиме онлайн. Интернет-публикации с угрозами и предупреждениями о готовящихся терактах первой стала осуществлять организация «Аль-Каида». Со временем идея была подхвачена и другими радикальными группировками. Видеозаписи казней боевиками самопровозглашенного «Исламского государства» похищенных ими американских и британских журналистов в августе–декабре 2014 г. не только были опубликованы террористами, но и впоследствии широко разошлись по сети, в том числе за счет многочисленных новостных ресурсов, а также усилиями самих пользователей Интернета. Кадры, на которых журналисты сначала обращаются к правительству США, Великобритании и Японии с обвинениями в убийствах мирного населения при авиаударах по Сирии, а потом им отрезают голову, произвели сильнейшее впечатление на людей по всему миру. Такие действия однозначно зарекомендовали себя как один из успешнейших методов ведения психологической войны. А выдвигаемые при этом преступниками требования дают возможность утверждать, что подобные действия направлены на достижение именно террористических целей – оказать воздействие на принятие решений органами власти или международными организациями. Следовательно, и в таком случае мы имеем дело с самым настоящим терроризмом, а значит, понятие кибертерроризма необходимо расширить.

Внося собственный вклад в дефиницию рассматриваемого понятия, автор статьи считает возможным определить кибертерроризм как умышленное преступное посягательство на информационный ресурс либо использование этого ресурса, устрашающее население и создающее опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях.

При такой формулировке понятия способы совершения кибертеррористического акта должны быть разделены на две независимые друг от друга группы. К первой группе следует отнести преступные посягательства на объекты компьютерной инфраструктуры и информационные сети. Специалисты относят к таковым, например, выведение из строя информационных систем, которое приведет к бесконтрольному функционированию поражаемого объекта (что особенно опасно на предприятиях атомного и химического производства, а также в военной сфере для систем защиты и нападения) либо организацию разрушительных атак (уничтожение информационных ресурсов и линий коммуникаций либо физическое уничтожение структур, в которые

включаются информационные системы) [10, с. 43]. Во вторую группу способов совершения кибертеракта следует включить правомерное использование компьютерных технологий с целью размещения в сети информации, способной оказать на людей устрашающее воздействие и обладающей признаками совершенного террористического акта (как это было в случае с публикацией видео казни журналистов).

В то же время не следует слишком широко трактовать возможность устрашения населения и государственной власти посредством применения сети. Квалифицируя кибертерроризм, необходимо помнить о другом его признаке – создании реальной опасности гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий. Забывая об этом, некоторые юристы доходят в собственных рассуждениях до весьма парадоксальных выводов: в частности, приводят в качестве примера кибертеррористической деятельности скандал, связанный с сайтом WikiLeaks (публикация в открытом доступе материалов об Ираке, Афганистане, а также дипломатической переписки госдепартамента США) [11, с. 62]. Информационные источники свидетельствуют, что по состоянию на март 2015 г. основателю WikiLeaks Джулиану Ассанжу не предъявлено обвинений в преступлениях террористического характера. Официальное обвинение связано с изнасилованием, и хотя многие источники свидетельствуют о возможном желании американских властей инкриминировать данному гражданину разглашение гостайны, даже такая квалификация очень далека от общепринятой трактовки терроризма.

В связи с тем, что в понятии кибертерроризма нами были выделены две самостоятельные группы деяний, противодействие этому явлению также следует условно разделить на два направления. В отношении терактов, совершаемых посредством компьютерных технологий, наиболее действенными методами борьбы являются организационно-правовые меры, направленные на пресечение любых попыток несанкционированного доступа к информационным ресурсам (в том числе программно-аппаратные методы и средства защиты информации). Что касается использования Интернета с целью информационного сопровождения террористической деятельности, то здесь следует обратить особое внимание на блокировку экстремистских сайтов и ресурсов.

Организационные меры по борьбе с кибертерроризмом принимаются как на международном, так и на национальном уровнях. Впервые вопрос о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности был вынесен на рассмотрение ООН в декабре 1998 г., когда по инициативе Российской Федерации Генеральной Ассамблеей (ГА) была принята первая резолюция, затрагивающая эту проблему. С тех пор Генеральный секретарь ежегодно представляет ГА ООН доклады, в которых государства – члены Организации Объединенных Наций выражают свое мнение по этому вопросу и подчеркивают необходимость коллективных действий, направленных на практическое сотрудничество в целях обмена передовым опытом и информацией. Кроме того, было создано две группы правительственных экспертов. Первая из них проводила заседания в 2004 и 2005 гг., но с учетом сравнительной новизны вопросов, связанных с защитой киберпространства, так и не смогла достичь консенсуса в отношении заключительных выводов. Новая группа начала работу в 2009 г. и к 2010 г. сумела не

только завершить обсуждения, но и согласовать доклад, посвященный существующим и потенциальным угрозам киберпространства и изучению возможных коллективных мер по их устранению. В дальнейшем было принято решение продолжить эту работу, чтобы развить данное направление международного сотрудничества и, возможно, перевести его из разряда обсуждений в число регулируемых сфер жизнедеятельности[1].

Также на международном уровне действует Конвенция о компьютерных преступлениях, подписанная государствами – членами Совета Европы в Будапеште 23 ноября 2001 г.[2] Этот документ устанавливает порядок взаимодействия стран в борьбе с преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем, а также всеми видами правонарушений, связанных с использованием компьютерных средств, с содержанием данных и с нарушением авторских и смежных прав. Многие меры, предусмотренные Конвенцией и направленные на недопущение несанкционированного вмешательства в работу компьютерных систем, могут выступить своеобразным заслоном на пути к совершению террористических преступлений. Россия, однако, отказалась подписывать данную Конвенцию, поскольку уполномоченных должностных лиц не устроило содержание пункта «b» ст. 32, которым предусматривается санкционированный доступ одного государства-участника к компьютерным данным, хранящимся на территории другого государства, без предварительного получения согласия последнего. В приведенной формулировке российская сторона усмотрела возможность нанесения ущерба суверенитету и национальной безопасности государств-участников.

Схожая работа ведется на уровне СНГ. В 2001 г. в Минске было подписано Соглашение о сотрудничестве в борьбе с преступлениями в области компьютерной информации[3]. Стороны оговорили понятия «преступления в сфере компьютерной информации», «вредоносные программы» и «неправомерный доступ», определили перечень уголовно наказуемых деяний и формы сотрудничества в области их предупреждения и пресечения. Однако понятие кибертерроризма, как и любые связи такого рода преступлений с террористическими, Соглашением не установлено. Этот нормативный акт направлен, скорее, на борьбу с хакерством, составляющим в терминологии Дороти Дэннинг один из возможных способов совершения кибертерроризма, но не исчерпывающий это явление. В завершение отметим, что Российская Федерация ратифицировала Соглашение о сотрудничестве в борьбе с престу-

[1] Доклад группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности / Организация Объединенных Наций. – Нью-Йорк, 2012. – URL: http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33_Russian.pdf (дата обращения: 26.03.2015).

[2] Конвенция Совета Европы о компьютерных преступлениях (23 ноября 2001 г., Будапешт) / Council of Europe – Treaty Office. – URL: http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm (дата обращения: 26.03.2015).

[3] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в области компьютерной информации (Минск, 1 июня 2001 г.) // Исполнительный комитет СНГ. – URL: http://www.cis.minsk.by/page.php?id=866 (дата обращения: 26.03.2015).

плениями в области компьютерной информации только в 2008 г. с оговоркой, что возможен отказ в исполнении запроса компетентного органа другой стороны об оказании содействия в случае, если такое исполнение может нанести ущерб суверенитету или безопасности РФ.

Что касается непосредственно России, то в нашей стране в настоящее время действует Федеральный закон «Об информации, информационных технологиях и о защите информации» [12]. В нем установлены принципы правового регулирования отношений в этой сфере, одним из которых является «обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации» (п. 5 ст. 3). В ст. 16 Закона приводится и понятие «защита информации», под которой понимается принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Непосредственные меры по защите информации предусмотрены рядом нормативно-правовых актов, включающих в себя, помимо вышеупомянутого закона, также указы Президента РФ [13], постановления Правительства РФ [14], несколько государственных стандартов, организационно-распорядительные документы ФСБ России (по вопросам, связанным с защитой сведений, составляющих государственную тайну) и Федеральной службы по техническому и экспортному контролю (ФСТЭК) [15]. (ФСТЭК России выступает уполномоченным органом по вопросам защиты информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере.)

Проблема уголовной ответственности за совершение террористического акта с использованием компьютерных технологий и сети Интернет не находит отражения в действующем российском законодательстве. Наказуемыми считаются лишь деяния, совершенные с использованием СМИ, в форме публичных призывов к осуществлению террористической деятельности или публичного оправдания терроризма (ч. 2 ст. 205.2 УК РФ). При этом используется обобщенный термин «средства массовой информации», к числу которых в соответствии с Законом РФ «О средствах массовой информации» [16] относится и сетевое издание, т.е. сайт в Интернете, зарегистрированный в качестве СМИ в соответствии с законом. Однако создание сайта, содержащего информацию террористического характера, незаконно, поэтому регистрироваться указанный информационный ресурс в качестве средства массовой информации априори не может, а следовательно, и рассматриваться в качестве СМИ он не должен. Получается, что отсутствие упоминания Интернета в ст. 205.2 Уголовного кодекса РФ влечет неоднозначные подходы в юридической практике при квалификации данного преступного посягательства.

Очень важным в сложившейся ситуации представляется предложение И. Г. Чекунова дополнить ч. 2 ст. 205 отдельным пунктом, устанавливающим

ответственность за террористический акт с несанкционированным доступом в компьютерные системы или информационно-коммуникационные сети, осуществляющие автоматизированное управление опасными технологическими производствами и предприятиями жизнеобеспечения с целью нарушения их функционирования и создания аварийной ситуации и угрозы техногенной катастрофы [17, с. 43]. Аналогичное суждение высказывает Е. С. Саломатина, предлагающая усилить уголовную ответственность за совершение теракта с использованием «компьютеров, информационных систем и телекоммуникационных сетей, связанных с критическими элементами инфраструктуры» [18, с. 47–48]. Понятию «критически важные объекты инфраструктуры» при этом придается смысл, аналогичный предусмотренному п. 5 Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов: объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени [19].

В юридической литературе встречаются, однако, и противоположные мнения. Некоторые исследователи полагают, что для квалификации кибертерроризма достаточно и имеющихся формулировок ст. 205 УК РФ. Так, Е. В. Старостина и Д. Б. Фролов указывают, что признаки, установленные применительно к данному преступлению, полностью охватывают признаки кибертерроризма (к каковым они относят политическую окраску, совершение деяний с целью создания напряженной атмосферы в обществе, публичность, а также направленность не на конкретных лиц, а на неопределенный круг граждан) [20, с. 64]. Указанное деяние хотя и не носит характера взрыва или поджога, но вполне подпадает под категорию «иных действий».

В. Н. Черкасов также возражает против введения в уголовный закон самостоятельного понятия кибертерроризма, считая, что без него вполне можно обойтись, поскольку значение этого понятия находит выражение в других текстуальных формах («неправомерный доступ», «перехват информации», «нарушение работы информационно-телекоммуникационной системы») [21, с. 10]. Ученый также отмечает, что если только вступить на путь расширения понятийного аппарата российского Уголовного кодекса, то уже в ближайшее время придется вводить в него новые статьи, криминализирующие «кибермошенничество, киберклевету, кибершпионаж, киберподделку, киберхалатность, киберсаботаж и так далее до бесконечности, точнее, до исчерпания УК РФ».

Немного иначе, но тоже негативно, относится к выделению кибертерроризма в отдельный состав И. Р. Бегишев. По его мнению, внедрение в уголовное право нового понятия способно «запутать практических работников правоохранительных органов при квалификации данных деяний», поскольку в основном преступные деяния, совершенные кибертеррористами, подпадают под действие гл. 28 УК РФ «Преступления в сфере компьютерной информации» [22, с. 11]. Исследователь предлагает отказаться от использования понятия кибертерроризма в уголовном законе и применять его только в криминологических целях.

Со своей стороны придерживаемся мнения, что, поскольку возможные последствия кибертерроризма по степени тяжести могут быть соразмерны последствиям реального террористического акта, введение уголовной ответственности за совершение теракта с использованием информационных сетей, включая Интернет, в качестве квалифицированного состава в ст. 205 УК РФ действительно необходимо. В случае же, если для совершения теракта использовались взлом системы либо вредоносные программы («вирусы»), деяние в любом случае необходимо квалифицировать по совокупности преступлений, с применением одного из составов, закрепленных в гл. 28 УК РФ.

Статьи 272–274 Уголовного кодекса, посвященные вопросам ответственности за преступления в сфере компьютерной информации, в настоящее время не содержат каких-либо упоминаний о террористической деятельности. Так, несмотря на то, что кибертерроризм может проявляться в виде кибератак посредством использования вредоносных программ, ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» этого положения не учитывает. Для устранения данного пробела в праве представляется необходимым либо добавить в ст. 205 УК РФ квалифицированный состав (о чем говорилось ранее), либо внести в ч. 3 ст. 273 УК РФ в качестве особо квалифицирующего признака ответственность за создание и использование вредоносных компьютерных программ в террористических целях.

Кроме того, кибертеррористы при совершении террористических актов при помощи электронных сетей порой могут иметь возможность получения доступа к конфиденциальной информации либо государственной тайне. Сведения различной степени важности, которые содержатся в базах данных органов государственной власти с ограничением доступа к ним (схемы подземных коммуникаций, информация о строящихся стратегических объектах, личные данные граждан), потенциально могут попасть в руки к террористам. Тем не менее ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» подобную возможность не учитывает, поскольку не предусматривает особую ответственность за данное преступное деяние, совершенное в террористических целях. Пробелы в праве предлагается восполнить аналогично: посредством внесения изменений либо в статью о теракте, либо в положения гл. 28 УК РФ [23, с. 146].

Вопрос о криминализации неправомерного доступа к государственным информационным системам и содержащимся в них информационным ресурсам (в том числе размещенным в сети Интернет или функционирующим в составе критически важных объектов) обсуждается в Правительстве России с осени 2009 г. Министерство юстиции РФ опубликовало на своем сайте проект федерального закона, вводящего ответственность за соответствующее правонарушение. В соответствии с законопроектом Уголовный кодекс РФ предлагалось дополнить ст. 272.1 «Неправомерный доступ к государственным информационным системам и (или) содержащимся в них государственным информационным ресурсам», санкция которой предусматривала бы в качестве наказания лишение свободы на срок до трех лет. В качестве квалифицирующего признака данного преступления особое внимание обращалось на необходимость наступления в результате совершения деяния определенных последствий: уничтожение, блокирование, модификацию либо копи-

рование информации, нарушение функционирования государственной информационной системы. Однако окончательного решения (по состоянию на март 2015 г.) по данному вопросу принято так и не было.

В целях усиления борьбы с кибертеррористической деятельностью в юридической литературе также предлагается привлекать к ответственности всех соучастников распространения в Интернете информационных материалов террористического характера (организаторов, исполнителей и пособников, в том числе по вопросам финансирования), придать безусловный характер их экстрадиции и стараться ликвидировать все террористические сайты [24, с. 16].

Подводя итог рассмотрению кибертерроризма, следует отметить, что совершение высокотехнологичных террористических акций в XXI в. способно вызвать глобальный информационный кризис и поставить под угрозу существование отдельных регионов мира. Ситуация осложняется тем, что уголовно-правовое противодействие кибертерроризму в России пока не в должной степени отвечает серьезности такой угрозы.

В этой связи совершенствование уголовно-правовой политики в области противодействия совершению кибератак террористами должно стать одним из приоритетных ее направлений.

Список литературы

1. **Krasavin, S.** What is Cyber-terrorism? / S. Krasavin // Computer Crime Research Center (CCRC). – URL: http://www.crime-research.org/library/Cyber-terrorism.htm (дата обращения: 26.03.2015).
2. **Касьяненко, М. А.** Правовые проблемы при использовании Интернета в транснациональном терроризме / М. А. Касьяненко // Информационное право. – 2012. – № 1. − С. 21–25.
3. **Verton, D.** Black Ice: The Invisible Threat of Cyber-Terrorism / D. Verton. – N. Y. : McGraw-Hill Osborne Media, 2003. – 273 p.
4. **Denning, D. E.** Is Cyber Terror next? / D. E. Denning // SSRC – Social Science Research Council. – URL: http://essays.ssrc.org/sept11/essays/denning.htm (дата обращения: 26.03.2015).
5. **Соловьев, И. Н.** Правовое обеспечение борьбы с преступлениями в сфере информационных технологий / И. Н. Соловьев // Административное и муниципальное право. – 2009. – № 3. – С. 63–65.
6. **Молодчая, Е. Н.** Политика противодействия кибертерроризму в современной России: политологический аспект : дис. … канд. полит. наук / Молодчая Е. Н. – М., 2011. – 188 с.
7. **Васенин, В. А.** Информационная безопасность и компьютерный терроризм / В. А. Васенин / Центр исследования компьютерной преступности. – URL: http:// www.crime-research.ru/articles/vasenin (дата обращения: 26.03.2015).
8. **Голубев, В. А.** Кибертерроризм – угроза национальной безопасности / В. А. Голубев // Центр исследования проблем компьютерной преступности. – URL: http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism (дата обращения: 26.03.2015).
9. Современный терроризм: сущность, типология, проблемы противодействия / под ред. Ю. В. Гаврилова, Л. В. Смирнова. – М. : ЮИ МВД РФ, 2003. – 66 с.
10. **Мазуров, В. А.** Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров // Доклады ТУСУРа. – 2010. – № 1. – С. 41–45.
11. **Матвиенко, Ю. А.** Предупредить – значит вооружить (Кибертерроризм вчера, сегодня и завтра) / Ю. А. Матвиенко // Информационные войны. – 2011. – № 2. – С. 60–70.

12. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 21 июля 2014 г.) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.
13. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена : Указ Президента РФ от 17 марта 2008 г. № 351 (ред. от 25 июля 2014 г.) // Собрание законодательства РФ. – 2008. – № 12. – Ст. 1110.
14. Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям : Постановление Правительства РФ от 18 мая 2009 г. № 424 // Собрание законодательства РФ. – 2009. – № 21. – Ст. 2573.
15. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11 февраля 2013 г. № 17 // Российская газета. – 2013. – № 136.
16. О средствах массовой информации : Закон РФ от 27 декабря 1991 г. № 2124-1 (в ред. от 2 июля 2013 г., с изм. от 24 ноября 2014 г.) // Российская газета. – 1992. – № 32.
17. **Чекунов, И. Г.** Киберпреступность: понятие и классификация / И. Г. Чекунов // Российский следователь. – 2012. – № 2. – С. 37–44.
18. **Саломатина, Е. С.** Перспективы развития законодательства в сфере борьбы с кибертерроризмом / Е. С. Саломатина // Закон и право. – 2009. – № 1. – С. 47–48.
19. Об одобрении Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов : Распоряжение Правительства РФ от 27 августа 2005 г. № 1314-р // Собрание законодательства РФ. – 2005. – № 35. – Ст. 3660.
20. **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.
21. **Черкасов, В. Н.** Информационная безопасность. Правовые проблемы и пути их решения / В. Н. Черкасов // Информационная безопасность регионов. – 2007. – № 1. – С. 6–14.
22. **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.
23. **Капитонова, Е. А.** Современный терроризм : моногр. / Е. А. Капитонова, Г. Б. Романовский. – М. : Юрлитинформ, 2015. – 216 с.
24. **Паненков, А. А.** Предложения по оптимизации борьбы с использованием сети Интернет в террористических целях / А. А. Паненков // Правовые вопросы связи. – 2011. – № 2. – С. 15–21.

References

1. Krasavin S. *Computer Crime Research Center (CCRC)*. Available at: http://www.crime-research.org/library/Cyber-terrorism.htm (accessed 26 March 2015).
2. Kas'yanenko M. A. *Informatsionnoe pravo* [Information law]. 2012, no. 1, pp. 21–25.
3. Verton D. *Black Ice: The Invisible Threat of Cyber-Terrorism*. New York: McGraw-Hill Osborne Media, 2003, 273 p.
4. Denning D. E. *SSRC – Social Science Research Council*. Available at: http://essays.ssrc.org/sept11/essays/denning.htm (accessed 26 March 2015).
5. Solov'ev I. N. *Administrativnoe i munitsipal'noe pravo* [Administrative and municipal law]. 2009, no. 3, pp. 63–65.

6. Molodchaya E. N. *Politika protivodeystviya kiberterrorizmu v sovremennoy Rossii: politologicheskiy aspekt: dis. kand. polit. nauk* [Policy of cyberterrorism counteraction in modern Russia: political aspect: dissertation to apply for the degree of the candidate of political sciences]. Moscow, 2011, 188 p.
7. Vasenin V. A. *Tsentr issledovaniya komp'yuternoy prestupnosti* [Computer crime research center]. Available at: http://www.crime-research.ru/articles/vasenin (accessed 26 March 2015).
8. Golubev V. A. *Tsentr issledovaniya problem komp'yuternoy prestupnosti* [Computer crime research center]. Available at: http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism (accessed 26 March 2015).
9. *Sovremennyy terrorizm: sushchnost', tipologiya, problemy protivodeystviya* [Modern terrorism: essence, typology, problem of counteraction]. Eds. Yu. V. Gavrilov, L. V. Smirnov. Moscow: YuI MVD RF, 2003, 66 p.
10. Mazurov V. A. *Doklady TUSURa* [Reports of TUSUR]. 2010, no. 1, pp. 41–45.
11. Matvienko Yu. A. *Informatsionnye voyny* [Information wars]. 2011, no. 2, pp. 60–70.
12. *Sobranie zakonodatel'stva RF* [Collection of RF legislation]. 2006, no. 31 (part 1), art. 3448.
13. *Sobranie zakonodatel'stva RF* [Collection of RF legislation]. 2008, no. 12, art. 1110.
14. *Sobranie zakonodatel'stva RF* [Collection of RF legislation]. 2009, no. 21, art. 2573.
15. *Rossiyskaya gazeta* [Russian newspaper]. 2013, no. 136.
16. *Rossiyskaya gazeta* [Russian newspaper]. 1992, no. 32.
17. Chekunov I. G. *Rossiyskiy sledovatel'* [Russian investigator]. 2012, no. 2, pp. 37–44.
18. Salomatina E. S. *Zakon i pravo* [Law and rights]. 2009, no. 1, pp. 47–48.
19. *Sobranie zakonodatel'stva RF* [Collection of RF legislation]. 2005, no. 35, art. 3660.
20. Starostina E. V., Frolov D. B. *Zakonodatel'stvo i ekonomika* [Legislation and economics]. 2005, no. 5, pp. 62–66.
21. Cherkasov V. N. *Informatsionnaya bezopasnost' regionov* [Regional information security]. 2007, no. 1, pp. 6–14.
22. Begishev I. R. *Informatsionnaya bezopasnost' regionov* [Regional information security]. 2010, no. 1, pp. 9–13.
23. Kapitonova E. A., Romanovskiy G. B. *Sovremennyy terrorizm: monogr.* [Modern terrorism: monograph]. Moscow: Yurlitinform, 2015, 216 p.
24. Panenkov A. A. *Pravovye voprosy svyazi* [Legal issues of communication]. 2011, no. 2, pp. 15–21.

Капитонова Елена Анатольевна
доцент, кафедра уголовного права,
Пензенский государственный
университет
(Россия, г. Пенза, ул. Красная, 40)

E-mail: e–kapitonova@yandex.ru

Kapitonova Elena Anatol'evna
Associate professor, sub-department
of criminal law, Penza State University
(40 Krasnaya street, Penza, Russia)

УДК 343.34
Капитонова, Е. А.

Особенности кибертерроризма как новой разновидности террористического акта / Е. А. Капитонова // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2015. – № 2 (34). – С. 29–41.