

Кибертерроризм как новая угроза

Пучков Денис Валентинович

Уральский государственный юридический университет, Екатеринбург, Россия
d.puchkov@loys.law, <https://orcid.org/0000-0002-5318-0338>

Аннотация. В статье рассмотрена одна из наиболее опасных сфер киберпреступности — кибертерроризм как новая угроза обществу. Определены уголовно-правовые проблемы отсутствия понятия «кибертерроризм» как в Отечественном, так и в Зарубежном законодательстве. Установлены основные направления развития кибертерроризма в кибернетическом пространстве и выявлены проблемы квалификации акта кибертерроризма как общепринятого террористического акта и его разграничения от незаконного посягательства на критическую информационную структуру Российской Федерации. Предлагаются внесение в действующее уголовное законодательство соответствующих изменений, а именно дополнение ст. 274.1 УК РФ особо-квалифицирующим признаком, а также обосновывается необходимость разъяснений положений ст. 205 УК РФ на уровне Верховного Суда Российской Федерации.

Ключевые слова: киберугрозы, кибератаки, кибертерроризм, уголовно-правовая охрана, кибербезопасность, информационная безопасность

Для цитирования: Пучков Д. В. Кибертерроризм как новая угроза // Виктимология. 2021. Т. 8, № 4. С. 382–390.

Scientific article

Cyberterrorism as a New Threat

Denis V. Puchkov

Ural State Law University, Ekaterinburg, Russia
d.puchkov@loys.law, <https://orcid.org/0000-0002-5318-0338>

Abstract. The article examines one of the most dangerous spheres of cybercrime — cyberterrorism as a new society threat. Both domestic and foreign legislation absence of criminal law definition for “cyberterrorism” is discussed. The author establishes the key dimensions of cyberterrorism development in cybernetic space and identifies the issues of qualifying regarding to an act of cyberterrorism as a generally accepted terrorist act and its differentiation from an illegal tampering with critical informatic structure of the Russian Federation. The author also suggests such amendments to the current Russian criminal law legislation as addition the article 247.1 of Criminal Code of the Russian Federation with especially aggravating circumstance and explains the necessity of making explanations of the article 205 of Criminal Code of the Russian Federation by the Supreme Court of the Russian Federation.

Keywords: cybertechnologies, cyberthreats, cyberattacks, cyberterrorism, regulation by criminal law, cybersecurity, cybercrime

For citation: Puchkov D. V Cyberterrorism as a New Threat. *Viktimologiya* [Victimology]. 2021, vol. 8, no. 4, pp. 382–390. (In Russ.)

Введение

Сегодня можно говорить о формировании электронной «нервной системы» развития, реализующейся в форме всепроникающей цифровой инфраструктуры, в рамках которой у подавляющего большинства организаций и населения имеется доступ в сеть «Интернет», а значительная доля людей при этом использует мобильные средства коммуникации. Масштабы их распространения, охват населения и значимость для человека позволила им занять значительное место даже в развивающихся странах. Следовательно, меры уголовно-правового противодействия становятся основным способом нивелирования преступных деяний в этой сфере.

Учитывая нахождение киберпреступности в кибернетическом пространстве, которое, как мы выяснили, не имеет каких-либо национальных границ, следует смело говорить о транснациональном характере данного вида преступности.

Транснациональная преступность классифицирована Организацией Объединенных наций и включает в себя 17 групп, в том числе компьютерные преступления.

Однако компьютерная информация проникает во все сферы жизнедеятельности человека, а, следовательно, способна влиять на все общественные отношения, в том числе достаточно чувствительные.

Наиболее опасной сферой киберпреступности является кибертерроризм.

Важно подчеркнуть, что в Конвенции Совета Европы о киберпреступности, которая вступила в силу 1 июля 2004 г.¹ некоторые преступные действия, широко обсуждаемые, но до сих пор спорные с точки зрения способов их криминализации, не отделяются в самостоятельные группы, при всей насущной необходимости гармонизации законодательства по всему миру. Одно из таких действий — «кибертерроризм» и использование

киберпространства для террористических целей (к примеру, вовлечение в осуществление преступления террористического характера либо другое содействие их реализации). При этом отсутствие общего определения понятия терроризма на международном уровне в наши дни затрудняет дискуссии о кибертерроризме как о явлении, криминализация которого чрезвычайно важна в качестве универсальной для международного сообщества в целом, что, в свою очередь, не мешает странам и международным организациям прилагать огромные усилия по борьбе с использованием Интернета террористическими организациями — к примеру, на уровне Европейского Союза существует проект Clean IT, основной целью которого является комплексная борьба с данным явлением.

Описание исследования

К сегодняшнему дню на государственном уровне в России общепринятого понимания «кибертерроризм» не существует. В свою очередь, исследовательской службой Конгресса США сформулированы два основных подхода в понимании кибертерроризма:

— «основанный на эффекте. О кибертерроризме можно говорить, если компьютерные атаки порождают чувство страха, сопоставимое с традиционными актами терроризма, даже если атака проведена не террористами, а преступниками.

— основанный на намерениях. Кибертерроризм — незаконная, политически мотивированная компьютерная атака, проводимая в целях запугивания или принуждения правительства, или граждан для достижения дальнейших политических целей, или для нанесения большого ущерба или серьезного экономического урона» [2, р. 3].

Кибертерроризм трактуется посредством «умышленной, политически мотивированной атаки на информационные компьютерные системы, компьютерные программы и данные, проводимые субнациональными группами или секретными агентами в отношении невоенных целей, результатом которой являются

¹ Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) : заключена в Будапеште 23 ноября 2001 г. // СПС «Гарант». URL: <http://base.garant.ru/4089723/> (дата обращения: 15.04.2021).

насильственные действия»¹. При этом есть и другое мнение, что «к кибертерроризму возможно отнести любые действия террористов в сети, иначе таковым является любое использование Интернета в террористических целях»². Иную, более широкую трактовку воспроизводят М. Девост, Н. Поллард и Б. Хьютон, которыми кибертерроризм понимается как «сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые поддерживают или обеспечивают проведение террористических операций или актов» [4].

Кибертерроризм также был квалифицирован как атаки или серии атак террористов на ключевые объекты информационной инфраструктуры и попытки внушения чувства страха от их разрушительных последствий через политические, религиозные или идеологические рычаги [6, р. 14]. Эти определения имеют одну общую черту — действия должны быть актами, нацеленными на распространение общественных страхов и основываться на террористических намерениях и мотивах.

Существование значительной опасности кибертерроризма формируется, как правило, на основе невосприятости при осуществлении подобных террористических акций национальных границ, благодаря чему атаки могут совершаться из любой точки мира. Кибертерроризму как специфическому виду деятельности террористических групп свойственны определенные преимущества, среди которых Г. Вейманом выделены такие следующие:

— «методы кибертерроризма гораздо дешевле традиционных террористических инструментов;

— кибертерроризм дает большую анонимность, так что службам безопасности крайне сложно идентифицировать личность террориста в сети;

— глобальная сеть предоставляет огромный выбор целей для проведения эффективной кибератаки;

— акты кибертерроризма могут осуществляться дистанционно, тем самым сокращаются расходы на физическую и психологическую подготовку бойцов, а также снижается число потерь среди террористов;

— кибертерроризм обладает потенциалом более широкого прямого воздействия за счет возможности проведения атаки на огромное число пользователей в Сети, а также широкого освещения в СМИ, что является значимым фактором для террористов» [9, р. 6].

Практическая реализация кибертехнологий в деятельности террористических организаций способствовала существенному изменению как их деятельности, так и организации. Благодаря их применению произошел значительно быстрый переход к использованию сетевой структуры. Такая организация террористической деятельности способствовала повышению ее эффективности благодаря использованию глобальной сети для усиления кадрового и боевого потенциалов террористических организаций, а также «осуществлением пропаганды, проведением финансовых операций и операционного планирования, сбором информации, поддержанием связи и т. д.» [4], что, несомненно, также потребовало от государств необходимой степени уголовно-правового реагирования.

Террористическое киберпространство в данном случае включает в себя использование информационно-коммуникационных технологий, которые разработаны или предназначены для уничтожения или серьезного нарушения ключевых объектов инфраструктуры или важной информации. Развитие событий в компьютерных системах и сетях в настоящее время фактически размыли различия между киберпреступностью и кибертерроризмом.

Другим аспектом использования кибертехнологий террористическими группами явилось осуществление активной незаконной деятельности в сети «Интернет», направленной, прежде всего на обеспечение финансирования. Это во многом

¹ Singer P. The Cyber Terror Bogeyman. Brookings. November, 2012. URL: <http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer> (дата обращения: 16.04.2021).

² Цит. по : Kaplan, Eben. Terrorists and Internet // Council on Foreign Relations. 2009. 8 Jan. URL: <https://www.cfr.org/background/terrorists-and-internet> (дата обращения: 16.04.2021).

объясняется достаточно высоким уровнем прибыльности совершаемых обще криминальных преступлений (компьютерные кражи, кражи личных данных, махинации с банковскими картами и т. д.), которые часто превышает показатели доходности от торговли наркотиками [1, р. 2]. Поэтому можно сказать, что кибертеррористами используется весь известный криминальный потенциал кибертехнологий и злоупотреблений в Сети, в связи с чем, часто возникают сложности при квалификации совершаемых кибератак действительно к кибертерроризму из-за возникающих противоречий при определении мотивов или источников киберпреступлений.

Таким образом, можно заключить, что в киберпространстве понятие терроризма подразумевает киберпреступность как акт терроризма. Категорией киберпреступности и криминального злоупотребления возможностями информационно-коммуникационных технологий в киберпространстве являются террористические атаки. Для описания этого явления часто используется термин «кибертерроризм», но при его использовании важно понимать, что это не совсем новая категория преступлений. Кибертерроризм предназначен для запугивания или принуждения правительства, народа к определенным политическим или социальным действиям. Согласно этой логике, атака должна приводить к насилию в отношении лиц или имущества или, по меньшей мере, наносить серьезный ущерб.

Это позволяет говорить о значительных изменениях в идеологической доктрине и стратегических направлениях деятельности террористических группировок, принимающих во внимание весь потенциал использования кибернетических технологий. Ими в полном объеме стали использоваться все методы и формы реализации «информационной войны». В частности, исследователями выделены ряд ключевых видов информационных операций и направлений деятельности, реализуемых террористическими группировками повседневно:

— «Атаки на компьютерные сети. Проведение электронного (или кибер) джихада стало одной из важных целей сторонников

глобального джихада, которые активно используют потенциал Интернета в священной войне против Запада. В основном электронный джихад осуществляется посредством искажения информации или проведения DDoS-атак на сайты, контент которых противоречит ценностям ислама.

— Безопасность операций. Террористы вынуждены широко использовать методы защиты информации и конспирации, так как успех их операций зависит от сохранения секретности.

— Психологические операции. В основном психологические операции террористических групп направлены на продвижение насилия и запугивание гражданского населения посредством угроз смерти и разрушения (наибольший эффект достигается через видео и аудио материалы). Также террористы прибегают к психологическому воздействию в целях пропаганды, направленной на обращение детей в джихад и привлечение молодежи в свои ряды»¹.

Исходя из этого, следует констатировать развитие тенденций к росту технологической подготовленности террористических групп, деятельностной интеграции основных кибернетических технологий в собственную инфраструктуру, включая, в том числе и активное их использование для обеспечения собственной безопасности. Тем не менее, полученные Национальным антитеррористическим центром США сведения указали на то, что из 63 192 террористических актов, случившихся за период (1995–2005 гг.), ни один не был признан случаем кибертерроризма². На наш взгляд, все это связано с неоднозначностью понятий

¹ Основные виды информационных операций, к которым прибегают террористы даны по: Littleton M. Information Age Terrorism toward Cyberterror // Naval Postgraduate School. December 1995. URL: <https://calhoun.nps.edu/bitstream/handle/10945/7469/95Dec-Littleton.pdf?sequence=1&isAllowed=y> (дата обращения: 16.04.2021); Denning D. Information Operations and Terrorism. 2005 18 Aug. URL: https://www.researchgate.net/publication/255618829_Information_Operations_and_Terrorism_PREPRINT (дата обращения: 16.04.2021).

² Knake R. K. Cyberterrorism Hype v. Facts / Council on Foreign Relations. 2010 16 Feb. URL: <https://www.cfr.org/expert-brief/cyberterrorism-hype-v-fact> (дата обращения: 16.04.2021).

«кибертерроризма», о которых мы говорили выше, но и не только.

Действительно, ряд развитых стран, в том числе США ожидали кибератак террористических организаций, но исходя из доклада Федерального Бюро Расследований США этого не произошло, в силу осознания террористическими организациями того обстоятельства, что, используя кибернетические атаки, они не способны достигнуть основные цели и задачи террористического акта, выражающихся в устрашении населения и создании реальной опасности гибели человека, что является основополагающим для террора. Дополнительным фактором для отказа террористических организаций от кибератак стало отсутствие в рядах таких организаций профессиональных преступников-программистов. По мнению ФБР, большую угрозу, представляют программисты, оказывающие помощь террористическим организациям¹.

На наш взгляд, данные выводы Американских исследователей имеют под собой достаточно серьезные основания заложенные, в том числе и в российском уголовном законодательстве, а также в общественном сознании людей.

Например, при осуществлении террористического акта человек находится в страхе, прежде всего, за свою жизнь и жизнь своих близких, учитывая реальность гибели. Однако, в отношении кибернетических технологий, несмотря на имеющую уязвимость, человек не ощущает чувство страха смерти от находящегося у него в руках мобильного или компьютерного устройства, от используемой им кибернетической технологии. Данное происходит по причине ощущения себя в другом мире, не представляющем угрозы жизни человека.

Так, диспозиция статьи 205 УК РФ (террористический акт) не предусматривает в качестве средства или объекта преступления компьютерную технику, электронные или информационные телекоммуникационные

сети, так как понятие «терроризм» использовалось в международной практике для описания криминальных действий задолго до того, как были внедрены технологии электросвязи и компьютерных сетей.

Однако, в п. 3 вышеуказанного Пленума Высшая судебная инстанция, допускает в качестве способа совершения преступления, предусмотренного ч. 1 ст. 205 УК РФ, в части угрозы террористического акта использование радио, телевидения или иных средств массовой информации, а также информационно-телекоммуникационных сетей.

Таким образом, следует констатировать, что, по мнению Высшей инстанции электронные и информационно-телекоммуникационные сети не являются объектами террористических актов, но могут быть средством их совершения, учитывая возможность массового распространения информации с использованием данных средств, что на наш взгляд не является вполне корректным.

Не исключается, что достижение уровня страха человека возможно исключительно оказанием давления на его моральные и нравственные чувства, которые непосредственно связаны с его личностью. Однако, цель в данном случае состоит в том, чтобы посеять страх, вызвав панику и неопределенность в обществе с целью оказания влияния на правительство или граждан посредством насаждения той или иной политической, социальной или идеологической повестки дня².

Так, из доклада Разведывательного управления США «О Всемирной угрозе» 2019 г., следует, что правительство США ожидает и опасается угроз кибератак на критическую важную инфраструктуру в сфере здравоохранения, финансов, правительства и экстренных служб, с целью их разрушения [3].

Аналогичные опасения существуют и в Российской Федерации. В этой связи криминализация неправомерного воздействия

¹ Cronin C. The Growing Threat of Cyberterrorism Facing the U.S // American Security Project. 2019 25 June. URL: <https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/> (дата обращения: 16.04.2021).

² Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI: Terrorism, Technology, and Homeland Security. Testimony before the Senate Judiciary Subcommittee. 2004 24 Feb. URL: https://www.judiciary.senate.gov/imo/media/doc/lourdeau_testimony_02_24_04.pdf (дата обращения: 15.04.2021).

на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) является, на наш взгляд, верным шагом Российского государства, направленным на соблюдение национальной безопасности информационной критической инфраструктуры.

При этом в статье 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» даны основные понятия, подпадающие под действие данного Закона, среди которых: критическая информационная инфраструктура, ее объекты и субъекты.

Исходя из анализа представленных субъектов и объектов критической инфраструктуры, на которые могут, произведены преступные посягательства, предусмотренные ст. 274.1 УК РФ следует констатировать, что все объекты являются объектами жизнеобеспечения (здравоохранение, транспорт, связь, энергетика и др.) в смысле, данном ему Пленумом Верховного Суда Российской Федерации в своем постановлении № 1 от 09.02.2012 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности», а именно «под иными действиями понимаются: устройство аварий на объектах жизнеобеспечения; разрушение транспортных коммуникаций; заражение источников питьевого водоснабжения и продуктов питания; распространение болезнетворных микробов, способных вызвать эпидемию или эпизоотию; радиоактивное, химическое, биологическое (бактериологическое) и иное заражение местности и иные действия.

Так, посягательства на объекты жизнеобеспечения криминализированы ст. 205 УК РФ (преступление против общественной безопасности), 215.2 УК РФ (преступление против общественной безопасности), 281 УК РФ (преступление к которым законодатель отнес объекты энергетика, электросвязи и жилищно-коммунального хозяйства, дороги, мосты, здания больниц, то есть идентичные перечню ст. 274.1. УК РФ (преступления в сфере компьютерной информации).

Однако, по нашему мнению, учитывая глобальную цифровизацию объектов жизнеобеспечения данные преступления могут затрагивать общественные отношения не только в сфере компьютерной информации, но и посягать на общественную безопасность.

К примеру, с помощью кибератаки можно отключить систему энергетика объекта здравоохранения, что повлечет, например, в условиях пандемии коронавирусной инфекции COVID-19 отключение аппаратов Искусственной вентиляции легких и, как следствие, приведет к гибели людей или, учитывая подключение всех объектов дорожной инфраструктуры к единой компьютерной системе, возможно отключение всех светофоров дорожной сети, что приведет к аварийности и тяжким последствиям.

Так, в июне 2019 года Агентство Питания и Медикаментов США (U.S. Food and Drug Administration — FDA) выявило проблемы кибербезопасности с некоторыми инсулиновыми помпами Medtronic MiniMed, используемыми для контроля диабета. Уязвимость может позволить кому-то управлять насосом через другие устройства, которые подключаются к насосу через беспроводное соединение. Они могут поразить владельца слишком большим или слишком малым количеством инсулина, изнуряющего или убивающего пациента. При этом сами устройства были выпущены еще в 2008 году и лишь после обнаружения таких уязвимостей 11 моделей были отозваны¹.

Исходя из доклада «Киберпреступность: угрозы в период пандемии COVID-19», подготовленного международной исследовательской организацией Global Initiative Against Transnational Organized Crime (GIATOC) от 2 апреля 2020 года [2] следует, что: «12–13 марта 2020 г. университетская больница Брно, вторая по величине в Чешской республике, была атакована с помощью

¹ Turner T. Medical Device Cyber Attacks: TV Plot or Dangerous Reality? // Drugwatch. 2019 11 July. URL: <https://www.drugwatch.com/news/2019/07/11/medical-device-cyber-attacks-tv-plot-or-dangerous-reality/> (дата обращения: 16.04.2021).

вредоносной программы Ransomware¹. Медицинское учреждение было вынуждено прервать все операции и перевести всех пациентов в другую больницу². Университетская больница Брно является местом тестирования и лечения COVID-19, о чем было известно из средств массовой информации³. Киберпреступники, с целью получения выкупа, готовы были поставить под угрозу безопасность зараженных пациентов⁴. При этом GIATOC, основываясь на исследовании Британской Национальной службы здравоохранения (NHS) отмечает, что больницы и поликлиники до сих пор являются предпочтительными целями для кражи данных кража, с целью вымогательства, под угрозой распространения конфиденциальной информации пациентов. Бесспорно, данные действия аморальны, и при этом недешевы, учитывая выкуп, но, по мнению организации, вряд ли приведут к смертельному исходу.

Данные примеры, показывают, что направленность кибертерроризма, фактически идентична, но направлена на угрозу жизни

человека опосредованным способом, учитывая дистанционность использования технологий, что при этом не делает такие акты менее опасными.

К основным целям терроризма в киберпространстве следует отнести попытки воспрепятствования или разрушение процесса функционирования компьютерных систем или сетей информационной инфраструктуры государства или органов управления. Подобные преступные действия в отношении критически важных объектов информационной инфраструктуры представляют собой значительную угрозу, которая может иметь самые серьезные последствия для всего общества. Потенциальными целями могут быть государственные структуры, телекоммуникационные сети, навигационные системы для судоходства и воздушного движения, системы управления водными ресурсами, энергетические и финансовые системы, имеющие жизненно важное значение для социума. Эти факты предполагают адекватную правовую оценку их как уголовных преступлений, поскольку атаки кибертеррористов могут обладать значительным потенциалом для полного или частичного разрушения значительной части национальной информационной инфраструктуры [8, p. 49].

Заключение

При этом, создание угрозы наступления таких тяжких последствий от данных преступных посягательств на критическую информационную инфраструктуру носят также общественно-опасный характер и подлежат, на наш взгляд криминализации в качестве особо-квалифицирующего признака ст. 274.1 УК РФ.

В свою очередь, диспозиция ст. 205 УК РФ подлежит также разъяснению Пленумом ВС РФ, в части расширения перечня иных действий и посягательств, определяемых как террористический акт, с целью четкого разграничения со ст. 274.1 УК РФ.

Такого рода криминализация диспозиции ч. 1 ст. 205 УК РФ, предусматривающая санкцию от 10 до 15 лет лишения свободы будет крайне полезной для национальной безопасности, критической информационной инфраструктуры и человека в частности.

¹ Ransomware является типом вредоносного программного обеспечения, которое препятствует доступу пользователей к их системным или личным файлам и требует выплаты выкупа, чтобы восстановить доступ. (См.: Ransomware // Malwarebytes. URL: <https://www.malwarebytes.com/ransomware/> (дата обращения: 16.04.2021)).

² Sophie Porter. Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak // Healthcare IT News. 2020 19 Mar. URL: <https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak> (дата обращения: 16.04.2021) ; Czech Republic's second-biggest hospital is hit by cyberattack // Prague Morning. 2020 13 Mar. URL: <https://www.praguemorning.cz/czech-republics-second-biggest-hospital-is-hit-by-cyberattack/> (дата обращения: 16.04.2021) ; Millman R. Coronavirus test results delayed by cyber-attack on Czech hospital // SC Media. 2020 16 Mar. URL: <https://www.scmagazineuk.com/coronavirustest-results-delayed-cyber-attack-czech-hospital/article/1677194> (дата обращения: 16.04.2021).

³ Catalin, Cimpanu. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak // ZDNet. 2020 13 Mar. URL: <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/> (дата обращения: 16.04.2021).

⁴ Suzanne, Barlyn. Global cyber attack could spur \$53 billion in losses: Lloyd's of London // Reuters. 2017 17 Jul. URL: <https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB> (дата обращения: 16.04.2021).

Данный вывод подтверждается и зарубежным опытом. Так, в Законе о терроризме США (Terrorism Act) от 2000 г правоохранительным органам было предоставлено право расценивать в качестве террористических действий те или иные действия, которые «вмешиваются или серьезно

нарушают работу какой-либо электронной системы» [10, с. 32].

Следует сделать вывод, что террористические организации продолжают наращивать свои ресурсы в этой области, а кибератаки будут продолжены, в том числе с корыстными целями.

СПИСОК ИСТОЧНИКОВ

1. Theohary C. A., Rollins J. *Terrorist Use of the Internet: Information Operations in Cyberspace*. CRS Report for Congress. March 8, 2011. URL: <https://fas.org/sgp/crs/terror/R41674.pdf>
2. Mahadevan P. *Cybercrime. Threats during the COVID—2019 pandemic*. Global Initiative Against Transnational Organized Crime. April, 2020. URL: <https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf>
3. Coats D. R. *Worldwide Threat Assessment of the US Intelligence Community*. Senate Select Committee on Intelligence. January 29, 2019. URL: <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>
4. Devost M. G., Houghton B. K., Pollard N. A. *Information Terrorism: Can You Trust Your Toaster?* The Terrorism Research Center. September, 1998. URL: <http://www.devost.net/papers/suntzu.pdf>
5. Gordon S., Ford R., *Cyberterrorism?* // *Computers & Security*. 2002. Vol. 21, Iss. 7. P. 636–647, [https://doi.org/10.1016/S0167-4048\(02\)01116-1](https://doi.org/10.1016/S0167-4048(02)01116-1)
6. Dunn M., Mauer V. (eds.) *International Critical Information Infrastructure Protection Handbook*. Zurich : Center for Security Studies at ETH. vol. II, 2006. 235 p. URL: <https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf>
7. Millman R. *Coronavirus test results delayed by cyber-attack on Czech hospital* // SC Media. March, 16 2020. URL: <https://www.scmagazineuk.com/coronavirustest-results-delayed-cyber-attack-czech-hospital/article/1677194>
8. Schjolberg S., Ghernaoui-Helie S. *A Global Treaty on Cybersecurity and Cybercrime*. Second edition. Oslo.: AiTOslo, 2011. 97 p. URL: <https://docplayer.net/8426890-A-global-treaty-on-cybersecurity-and-cybercrime.html>
9. Weimann G. *Cyberterrorism. How Real Is the Threat?* // United States Institute of Peace. Special Report. 12 p. URL: <http://www.usip.org/sites/default/files/sr119.pdf>
10. Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, Нидерландах, Польше) // Вестник Томского государственного педагогического университета. 2006. № 11 (62). С. 30–35.

References

1. Theohary C. A., Rollins J. *Terrorist Use of the Internet: Information Operations in Cyberspace*. CRS Report for Congress. March 8, 2011. URL: <https://fas.org/sgp/crs/terror/R41674.pdf>
2. Mahadevan P. *Cybercrime. Threats during the COVID—2019 pandemic*. Global Initiative Against Transnational Organized Crime. April, 2020. URL: <https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf>
3. Coats D. R. *Worldwide Threat Assessment of the US Intelligence Community*. Senate Select Committee on Intelligence. January 29, 2019. URL: <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>
4. Devost M. G., Houghton B. K., Pollard N. A. *Information Terrorism: Can You Trust Your Toaster?* The Terrorism Research Center. September, 1998. URL: <http://www.devost.net/papers/suntzu.pdf>

5. Gordon S., Ford R., Cyberterrorism? *Computers & Security*. 2002;21(7):636-647, [https://doi.org/10.1016/S0167-4048\(02\)01116-1](https://doi.org/10.1016/S0167-4048(02)01116-1)
6. Dunn M., Mauer V. (eds.) *International Critical Information Infrastructure Protection Handbook*. Zurich : Center for Security Studies at ETH. vol. II, 2006. URL: <https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf>
7. Millman R. *Coronavirus test results delayed by cyber-attack on Czech hospital*. SC Media. March, 16 2020. URL: <https://www.scmagazineuk.com/coronavirustest-results-delayed-cyber-attack-czech-hospital/article/1677194>
8. Schjolberg S., Ghernaouti-Helie S. *A Global Treaty on Cybersecurity and Cybercrime. Second edition*. Oslo: AiTOslo, 2011. URL: <https://docplayer.net/8426890-A-global-treaty-on-cybersecurity-and-cybercrime.html>
9. Weimann G. *Cyberterrorism. How Real Is the Threat?* United States Institute of Peace. Special Report. 2004 Dec. URL: <http://www.usip.org/sites/default/files/sr119.pdf>
10. Gromov E. V. Development of criminal legislation on crimes in the sphere of computer information in foreign countries (USA, Great Britain, Netherlands, Poland). *Vestnik Tomskogo gosudarstvennogo pedagogicheskogo universiteta* [Bulletin of Tomsk State Pedagogical University]. 2006;(11):30-35.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Пучков Денис Валентинович, кандидат юридических наук, старший преподаватель кафедры уголовного права Уральского государственного юридического университета. 620137, г. Екатеринбург, ул. Комсомольская, д. 21.
d.puchkov@loys.law
<https://orcid.org/0000-0002-5318-0338>

INFORMATION ABOUT AUTHOR

Denis V. Puchkov, Candidate of Law Sciences, Senior Lecturer, Criminal Law Department, Ural State Law University.
21 Komsomolskaya st., Ekaterinburg 620137, Russia.
d.puchkov@loys.law
<https://orcid.org/0000-0002-5318-0338>

Дата поступления статьи / Received: 21.08.2021.

Дата рецензирования статьи / Revised: 20.10.2021.

Дата принятия статьи к опубликованию / Accepted: 15.12.2021.