УДК 343

ПОНЯТИЕ ИНФОРМАЦИОННОГО ТЕРРОРИЗМА

Абдулатипов А.М., Центр профессиональной подготовки МВД по РД, юридический колледж Дагестанского государственного университета, г. Махачкала, Российская Федерация, *shaavidin@mail.ru*

В статье автор обосновал актуальность изучения данного понятия. Анализируя научные исследования ряда современных учёных в этой сфере, автор приходит к выводу, что в настоящее время с учётом многогранности данного явления нет единого подхода к определению исследуемого понятия. В связи с этим, автор сделал попытку выявить характерные признаки данного понятия, раскрыть наиболее значимые элементы механизма его практических проявлений и на основе полученных данных дать определение. В определении учтено совершение террористических действий с помощью информационных средств и использование киберпространства террористическими группами для непосредственного совершения атак на информационные системы, информационно-телекоммуникационные сети или компоненты этих систем или сетей в террористических целях. Также данное понятие увязано с общим определением терроризма, предусмотренном в статье 205 УК РФ. На основе исследования автор сделал ряд выводов и предложений, имеющих теоретическое и практическое значение.

Ключевые слова: информационный терроризм, кибертерроризм, киберпространство, кибератаки, информационные средства.

DOI: 10.21779/2224-0241-2019-30-2-105-111

UDC 343

THE CONCEPT OF INFORMATION TERRORISM

Abdulatipov A.M., Vocational training center of the Ministry of Interior, Republic of Dagestan, law College of Dagestan State University, Makhachkala, Russian Federation, *shaavidin@mail.ru*

In the article, the author proved the relevance of the study of this concept. Analyzing the scientific research of a number of modern scientists in this field, the author concludes that at present, taking into account the diversity of this phenomenon, there is no single approach to the definition of the studied concept. In this regard, the author attempted to identify the characteristic features of this concept, to reveal the most significant elements of the mechanism of its practical manifestations and based on the data to define this concept. The definition takes into account the commission of terrorist acts by means of information and the use of cyberspace by terrorist groups to directly attack information systems, information and telecommunications networks or components of those systems or networks for terrorist purposes. This concept is also linked to the general definition of terrorism provided for in article 205 of the Criminal Code. Based on the study, the author made a number of conclusions and proposals of theoretical and practical importance.

Key words: information terrorism, cyberterrorism, cyberspace, cyberattacks, information tools.

DOI: 10.21779/2224-0241-2019-30-2-105-111

Терроризм, как любое негативное социальное явление испытывает постоянные изменения. В связи с возникшими на современном этапе потенциальными возможностями использования при совершении преступлений новейших информационных технологий, телекоммуникационных систем и средств, киберпространства, появился новый наиболее опасный вид терроризма, которого одни

называют кибертерроризмом либо электронным терроризмом, другие – информационным терроризмом.

Как известно, в настоящее время серьезная подготовка к совершению преступлений террористической направленности, как правило, требует активного использования информационных ресурсов, в том числе и в целях обеспечения широкой

средовой поддержки преступных акций. Для этого, например, ещё в конце прошлого и начале нынешнего столетия международными террористами, действовавшими в Чеченской Республике, было сформировано специальное подразделение. Созданное сепаратистским идеологом М. Удуговым так называемое «Информационное агентство «Кавказ-центр»», открыло одноименный сайт в сети Интернет. Это агентство занималось распространением дезинформации об успехах террористов и больших потерях федеральных сил с целью сформировать у мировой общественности и руководства иностранных государств негативное отношение к России. В этой преступной акции использовались более 100 финансируемых террористами сайтов на русском, английском, арабском, французском и других языках. Лидерами террористов были созданы информационные центры в Азербайджане, Грузии, Украине, Литве, Финляндии, Турции и Польше. Через эти структуры распространялись заведомо ложные сведения, призванные создать в общественном сознании Запада мифы о «зверствах русских солдат в отношении мирного населения», «гуманитарной катастрофе на Северном Кавказе».

При этом они руководствовались принципом «чем чудовищнее ложь, тем быстрее в нее поверят» (к примеру, провокационное заявление Мовлади Удугова о причастности дагестанских граждан, погибших на атомоходе «Курск», к взрыву атомной подводной лодки) [1, с. 25].

Кибертерроризм представляет собой серьёзную угрозу для человечества, сравнимую с ядерным, бактериологическим и химическим оружием; причем степень этой угрозы в силу своей новизны не до конца ещё осознана и изучена. Опыт мирового сообщества в этой области со всей очевидностью свидетельствует о несомненной уязвимости любого государства, тем более что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара [2, с. 146].

При подведении итогов работы национального антитеррористического комитета (далее – НАК) за 2018 год Председатель НАК Бортников особо подчеркнул о защите информационного пространства от растущих террористических угроз. По его словам, Роскомнадзор, МВД, ФСБ и Генеральная прокуратура расширили внедрение автоматизированных систем мониторинга средств массовой коммуникации, что позволило выявить более 47 тыс. интернет-ресурсов, которые содержали материалы, связанные с деятельностью международных террористических организаций (МТО).

Это дало возможность пресечь деятельность по распространению противоправной информации более чем 64 тыс. интернет-ресурсов, из которых свыше 47 тыс. содержали материалы, связанные с деятельностью международных террористических организаций [3].

По его словам, руководители террористических группировок, используя в том числе цифровых технологий и информационно-телекоммуникационных систем, предпринимают попытки сформировать на территории России законспирированные ячейки, в основном, из молодежи, в том числе несовершеннолетних. В связи с этим дал поручение повысить готовность сил и средств оперативных штабов в субъектах РФ и морских районах к незамедлительному реагированию на террористические угрозы, снижение уязвимости различных объектов (в том числе мест массового скопления людей) от террористических посягательств.

Из-за актуальности данной проблемы для северокавказского региона с 4 по 5 октября 2018 года при поддержке НАК России в Республике Дагестан проведена V Международная научно-практическая конференция по противодействию экстремизму и терроризму в цифровом мире [4].

Конференция была посвящена религиозно-идеологическим и информационным аспектам противодействия радикальной пропаганде; изучению и внедрению в практику соответствующих органов власти международного и отечественного опыта противодействия кибертерроризму; совершенствованию системы мониторинга и аналитической работы в сфере обнаружения радикального контента в медиапространстве; выявлению информационных угроз и наиболее эффективных способов деконструирования и опровержения радикальной пропаганды, изменения негативного восприятия реальности приверженцами радикальных взглядов, а также проведению в отношении соответствующих категорий лиц в Российской Федерации, в странах СНГ и дальнего зарубежья наиболее успешных информационных кампаний.

Как известно, глобальную опасность информационного терроризма обуславливает отсутствие для него государственных границ и территориальных помех. Используя современные информационные технологии, террорист может угрожать информационным системам практически любого государства.

В связи с этим актуализировалась проблема определения понятия информационного терроризма.

В криминологической науке этот вид терроризма относят к киберпреступности (противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, взлом системы защиты, хищение или разрушение информации в террористических, корыстных или хулиганских целях, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ).

Нередко, формулируя определение современного информационного терроризма, многие

учёные и практики связывают его с такими киберугрозами, как взлом компьютеров, кибервойна и киберпреступность. Однако, несмотря на то, что все эти угрозы реализуются на виртуальном пространстве по конкретным мотивам и целям, они, как и другие террористические проявления, должны характеризоваться созданием реальной угрозы общественной безопасности, опасности для жизни или здоровья людей, нанесением ущерба жизненно важной инфраструктуре либо наступлением других тяжких последствий; направлены на запугивание населения, дестабилизацию общественно-политической или социально-экономической обстановки, саботаж, реализацию сепаратистских устремлений террористических формирований.

Этот термин впервые был предложен ещё в 80-х прошлого века старшим научным сотрудником Института безопасности и разведки (англ. Institute for Security and Intelligence) Барри Коллинсом, который использовал его в контексте тенденции к переходу терроризма из физического в виртуальный мир, возрастающего пересечения и сращения этих миров. Он определил его как использование компьютерных и телекоммуникационных технологий в террористических целях. В википедии компьютерный терроризм (кибертерроризм) также определяется как использование компьютерных и телекоммуникационных технологий (прежде всего, Интернета) в террористических целях [5].

Исследователи М.Дж. Девост, Б.Х. Хьютон, Н.А. Поллард определяют информационный терроризм как сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов [6].

Дороти Деннинг (Dorothy Denning), профессор компьютерных наук Джорджтаунского университета и один из самых авторитетных экспертов в области компьютерной преступности и кибербезопасности, в своей книге «Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику» говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенной с целью принудить органы власти к содействию в достижении политических или социальных целей» [7].

По мнению Е.А. Роговского, следуя этим определениям, можно выделить два вида кибертерроризма [8]:

- 1) непосредственное совершение террористических действий с помощью компьютеров и компьютерных сетей;
- 2) использование киберпространства террористическими группами в организационно-коммуникационных целях и с целью шантажа, но не для непосредственного совершения терактов.

Первый вид соответствует объединению понятий «киберпространство» и «терроризм» и

представляет собой умышленную атаку на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающую опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Например, перехват управления военным или инфраструктурным объектом в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти путем угрозы осуществления аварии (катастрофы) [9].

К первому виду кибертерроризма примыкают все осуществляемые с помощью Интернета, так называемые, «информационные» правонарушения против Конституции (антиконституционные призывы, угрозы конституционным правам и свободам человека и гражданина, распространение устрашающих слухов, угрозы информационному обеспечению государственной политики и др.).

Второй вид кибертерроризма – использование информационного пространства террористическими группами в организационно-коммуникационных целях (но не для непосредственного совершения терактов), проведение теоретического, военного, теологического обучения и пропаганды, а также рекрутирование новых членов и обеспечение связи между отдельными ячейками.

В настоящее время в научной литературе не существует общепризнанное определение понятия «информационный терроризм» («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 с использованием информационных средств, способствующих нагнетанию страха и напряженности в обществе с целью получения преимущества при решении политических, экономических или социальных задач. 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.

С юридической точки зрения, следует также разграничивать понятия информационного терроризма и использования информации в террористических целях. В средствах массовой информации часто допускают подмену данных понятий, рассматривая пропагандистскую деятельность в террористических целях как информационный терроризм.

Кроме того, не все учёные рассматривают понятия «информационный терроризм», «кибертерроризм (компьютерный терроризм)» как сино-

нимы, придавая им разный смысл.

Информационный терроризм они определяют как использование информационных средств в террористических целях, а также дезорганизация автоматизированных информационных систем, создающая опасность гибели людей, причинения имущественного ущерба или наступление иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях.

Основным признаком кибертерроризма (компьютерного терроризма) они видят атаки на компьютерные сети, аппаратно-программные комплексы государственных, оборонных учреждений, важных, особо важных и других объектов в целях дезорганизации их работы и саботажа, либо угрозы причинения физического ущерба с помощью компьютерных средств совершением подобных атак при невыполнении предъявленных террористами определённых требований (например, вывод информационно-телекоммуникационной сети какой-либо организации из строя, уничтожение персональных данных клиентов банков, выводом из строя «оцифрованных» заводов и энергетических объектов в террористических целях либо получения выкупа в целях финансирования терроризма).

Кроме того есть и таких учёные, которые считают, что это понятие придумали и раздувают в медиапространстве владельцы объектов производства средств информационной безопасности в рекламных целях.

По нашему мнению, такой подход к данной проблеме в корне не соответствует современным реалиям использования информационно-телекоммуникационных средств в практике не только террористических организаций, но и террористов-одиночек и исходящей от этого явления чрезмерной опасности.

Одни учёные и практики склонны считать его самостоятельной формой терроризма, такой же, как и политический, идеологический, религиозный, национальный, этнический и т. д. Другие рассматривают его как способ совершения указанных форм терроризма. Исследование показывает, что и те, и другие доводы имеют под собой теоретические и практические основания, так как в практике такой вид терроризма в чистом виде встречается редко.

Такие же сложности возникают и при разграничении кибертерроризма от таких схожих понятий, как: преступления в сфере компьютерной информации, информационная война, информационное оружие и информационного криминала и т. д.

Именно разные подходы в науке и на практике создают проблему определения кибертерроризма как самостоятельной его формы и свидетельствуют о взаимосвязи всех его аспектов, и отсут-

ствии однозначного ответа об определяющем значении какого-либо из них для формирования общепринятой дефиниции. Эта неопределенность говорит о сложности этого явления и необходимости привлечения к его исследованию учёных разных направлений в мировом масштабе.

В связи с отсутствием общепринятого определения данного понятия некоторые учёные зачастую, «кибертерроризмом» называют проявления киберпреступности, кибервойны или «обычно-го» терроризма.

Абсолютное большинство учёных под кибертерроризмом признают только действия индивидов, независимых групп или организаций. А любая форма кибератаки, предпринимаемая правительственными и иными государственными организациями, считают проявлением кибервойны.

Евгений Касперский, основатель Лаборатории Касперского, в настоящее время считает, что термин «кибертерроризм» является более точным, чем термин «кибервойна». Он утверждает, что «с сегодняшними атаками, вы понятия не имеете о том, кто это сделал или, когда он снова нанесет удар. Это не кибервойна, а кибертерроризм». Он также приравнивает масштабные кибероружия, такие как вирусы Flame и NetTraveler, которые обнаружила его компания, приравнивая их к биологическому оружию, утверждая, что во взаимосвязанном мире, у них есть потенциал, чтобы быть столь же разрушительным [10].

Такое смешение понятий было характерно на ранней стадии исследования данной проблемы. В дальнейшем многие учёные-криминологи стали более корректно относиться к определению основных отличительных признаков кибертерроризма, позволяющих относить его к одной из форм терроризма.

Так, Е.Старостина отмечает, что «кибертерроризм» отличается от других форм воздействия на киберпространство, прежде всего, своими целями, которые остаются свойственными политическому терроризму вообще. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия. В то же время тактика и приемы его применения существенно отличаются от тактики информационной войны и приемов информационного криминала. Кибертеррорист весьма отличается от хакера, компьютерного хулигана или компьютерного вора, которые действуют в корыстных или хулиганских целях. Главное в тактике информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен населению и получил большой общественный резонанс. Как правило, требования сопровождаются угрозой повторения акта без указания конкретного объекта [11].

Она предлагает следующее определение кибертерроризма: это – «комплексная акция, выра-

жающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающая опасность для жизни или здоровья людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта» [11]. При этом исследователь квалифицирует кибертерроризм как разновидность киберпреступности.

По мнению Р. Р. Газизова, отличительной чертой информационного терроризма является его дешевизна и сложность обнаружения. Система «Интернет», связавшая компьютерные сети по всей планете, изменила правила, касающиеся современного оружия. Анонимность, обеспечиваемая Интернетом, позволяет террористу стать невидимым и, как следствие, практически неуязвимым и ничем (в первую очередь жизнью) не рискующим при проведении преступной акции. Положение усугубляется тем, что преступления в информационной сфере, в число которых входит и кибертерроризм, влекут за собой наказание существенно меньшее, чем за осуществление "традиционных" террористических актов [12].

Стремление многих учёных и практиков отнести его к отдельной форме терроризма, скорее всего, обусловлено огромными возможностями информационных технологий и информационного пространства на современном этапе развития общества.

В научной литературе встречается двоякий подход к определению понятия «кибертерроризм»: узкий и широкий [13].

При узком определении понятия «кибертерроризм» используется такой же подход, как и в случае с общим понятием «терроризм», то есть к актам кибертерроризма можно отнести лишь такие атаки на компьютерные системы (особенно через Интернет), которые угрожают имуществу или жизни и здоровью людей либо способны повлечь серьёзные нарушения функционирования инфраструктурных объектов и осуществляются негосударственными агентами. Прочие атаки необходимо расценивать как проявления киберпреступности или кибервойны.

Определение в широком смысле заключается в использовании информационных технологий террористическими группами и террористами-одиночками для достижения своих целей; может включать использование информационных технологий для организации и приведения в исполнение атак против телекоммуникационных сетей, информационных систем и коммуникационной инфраструктуры либо обмен информацией, а также угрозы с использованием средств электросвязи. Примерами могут служить взлом информационных систем, внесение вирусов в уязвимые сети, дефейс веб-сайтов, DoS-атаки, террористические угрозы, доставленные электронными средствами связи.

В научной литературе встречаются следующие способы совершения кибертерроризма:

- использование различных средств воздействия на информационное пространство в целях нанесения ущерба отдельным его физическим элементам: например, влияния на их работоспособность вплоть до вывода из строя отдельных компонентов и полного вывода из строя и остановки систем жизнеобеспечения; разрушения транспортной логистики, сетей электропитания, создания помех либо уничтожения или активного подавления линий связи; разрушения аппаратно-программных средств; неправильной адресации и перегрузки узлов коммуникации и т.д. О последствиях таких кибератак можно судить на примере кибератаки США в марте-апреле 2019 года на энергетические объекты Венесуэлы, в результате которой на всей территории этого государства наступил энергетический коллапс, так называемый, «блэкаут»;

- проведение информационно-психологических операций, распространение пропагандистских материалов о террористических структурах, их целях и задачах, намеченных устрашающих действиях, протестных акциях;

- размещение в социальных сетях обращений к массовой аудитории с сообщениями о признании своей ответственности за совершенные террористические акты и т.д.;

- похищение и угроза публикации данных, являющихся государственной тайной либо иной закрытой информацией;

- использование возможностей видеоконференцсвязи либо захват электронных СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;

- добыча информации для планирования организации и совершения преступлений террористической направленности;

- сбор денег для финансирования террористических организаций путем применения психического либо угрозы физического насилия, обмана, вымогательства, шантажа и т. д.;

- оказание информационно-психологического воздействия на лицо либо группу лиц с целью распространения дезинформации и тревожных слухов, создания панических настроений среди населения;

- размещение в социальных сетях или рассылка открытых и зашифрованных инструкций о способах и методах совершения террористической деятельности, о компонентах и способах изготовления взрывчатых веществ и взрывных устройств, ядов, отравляющих веществ, информации о явке для обсуждения обстоятельств планируемой акции, флеш-моба и т.д.

- привлечение к пособничеству в террористической деятельности специалистов, оказывающих платные информационные услуги, «вёмную» без понимания ими сущности своих действий (биз-

несменов, хакеров, программистов и других специалистов в сфере информационных технологий);

- использование технологических возможностей информационно-телекоммуникационных систем для расширения потенциала малых террористических групп, действующих по децентрализованному принципу (так называемых террористических ячеек), из которых в дальнейшем можно сформировать террористическую сеть;

- применение специальных технических средств и программ (компьютерных программных закладок, вирусов, используемых для съема, модификации или уничтожения информации, «логических бомб», троянских программ и т. д.) для несанкционированного доступа в компьютерные системы и совершение удаленных атак на информационные ресурсы выбранного объекта, например, получение неправомерного доступа к государственным и военным секретам, банковской информации и персональным данным;

- распространение ложных угроз нанесения кибератак, которые могут повлечь дестабилизацию общественно-политической или социально-экономической обстановки.

Для кибертерроризма характерны специфические формы насилия. Если традиционными методами терроризма являются убийства, взрывы, поджоги, захват заложников и др., то при кибертерроризме используются достижения новейших технологий, современной техники, включая компьютерную технику, киберпространство, радиотелевизионную и другую аппаратуру, информационно-телекоммуникационную систему. Он не имеет географических границ, четкой линии фронта, не ограничено никакими нормами, отличается скрытностью и несистематическим характером при подготовке террористических акций. Во всех случаях для совершения кибертеррористического акта используются информационные методы и ресурсы.

Анализируя научные исследования ряда современных учёных, можно сделать вывод о том, что в настоящее время с учётом многогранности данного явления нет единого подхода к определению

исследуемого понятия, хотя очевидно, что его неотъемлемыми чертами являются угроза жизни и безопасности людей, политическая мотивировка применяемых насильственных действий.

С учётом характерных признаков данного понятия и наиболее значимых элементов механизма его практических проявлений и на основе полученных данных нами предпринята попытка определения данного понятия, не претендуя на его универсальность.

При этом мы придерживаемся позиции определения данного понятия в узком смысле.

Таким образом, информационный терроризм (кибертерроризм) – это преднамеренные атаки на информационные системы, информационно-телекоммуникационные сети или компоненты этих систем или сетей, на компьютерные сети, аппаратно-программные комплексы государственных, оборонных учреждений, важных, особо важных и других объектов, в том числе физических лиц, в целях дезорганизации их работы и саботажа, совершение с использованием информационных средств действий, устрашающих население, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях, если эти деяния создают опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий.

В данном определении учтены оба вида совершения кибертерроризма: во-первых, непосредственное совершение террористических действий с помощью информационных средств и, во-вторых, использование киберпространства террористическими группами для непосредственного совершения атак на информационные системы, информационно-телекоммуникационные сети или компоненты этих систем или сетей в террористических целях. Также данное понятие увязано с общим определением терроризма, предусмотренном в статье 205 УК РФ.

Литература

1. Абдулатипов А. М., Сайгитов У. А. Терроризм в Дагестане. Криминологическое исследование: учебное пособие. Махачкала: Издательско-полиграфический центр ДГУ, 2002.
2. Голубев В. Электронный терроризм – новое лицо терроризма. // Всемирный антикриминальный антитеррористический форум: Мировое сообщество против глобализации преступности и терроризма: 2-я междунар. конф. М.: Изд-во «Экономика», 2004.
3. «Обстановка сложная, но контролируемая»: в НАК подвели итоги борьбы с терроризмом в 2018 году. URL: <https://russian.rt.com/russia/article/581846-nak-protivodeistvie-terrorizm-itogi-2018> (дата обращения: 24.01.2019).
4. Итоги V международной конференции по противодействию терроризму. URL: <http://www.mrkizilyurt.ru/press/news/itogi-v-mezhdunarodnoiy-konferentzii-po-protivodeistviyu-terrorizmu/> (дата обращения: 19.02.2019).
5. Википедия. URL: https://ru.m.wikipedia.org/wiki/Компьютерный_терроризм. (дата обращения: 24.01.2019).

6. *Томас Т.Л.* Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма: материалы междунар. конф. М., 2002.
7. Википедия. URL: https://ru.m.wikipedia.org/wiki/Компьютерный_терроризм. (дата обращения: 24.01.2019).
8. *Роговский Е.А.* Россия в борьбе с международным терроризмом грани повышения позитивного образа страны // Россия и Америка в XXI веке: электронный научный журнал. 2007. №3. URL: <http://www.rusus.ru/?act=read&id=66>. (дата обращения: 24.01.2019).
9. *Голубев В.А.* Кибертерроризм как новая форма терроризма? URL: <http://www.crime-research.org> (дата обращения: 24.01.2019).
10. Кибертерроризм — определения, классификация, опасность. URL: <http://elcomrevue.ru/opredelenie-kiberterrorizma/> (дата обращения: 24.01.2019).
11. *Старостина Е.* Терроризм и кибертерроризм – новая угроза международной безопасности // Центр исследования компьютерной преступности: Интернет-издание. URL: <http://www.crime-research.ru/articles/starostina> (дата обращения: 24.01.2019).
12. *Газизов Р.Р.* Информационный терроризм // Проблемы противодействия преступности в современных условиях: материалы междунар. науч.-практ. конф. 16-17 окт. 2003 г. Ч. I. Уфа: РИО БашГУ, 2003. 280с.
13. Кибертерроризм — определения, классификация, опасность. URL: <http://elcomrevue.ru/opredelenie-kiberterrorizma/> (дата обращения: 24.01.2019).

References

1. *Abdulatipov A. M., Saigitov U. A.* Terrorism v Dagestane. Kriminologicheskoe issledovanie: uchebnoe posobie. Makhachkala: Izdatel'sko-poligraficheskii tsentr DGU, 2002.
2. *Golubev V.* Elektronnyi terrorizm – novoe litso terrorizma. // Vsemirnyi antikriminal'-nyi antiterroristicheskii forum: Mirovye soobshchestvo protiv globalizatsii prestupnosti i terrorizma: 2-ya mezhdunar. konf. M.: Izd-vo «Ekonomika», 2004.
3. «Obstanovka slozhnaya, no kontroliruemaya»: v NAK podveli itogi bor'by s terrorizmom v 2018 godu. URL: <https://russian.rt.com/russia/article/581846-nak-protivodeistvie-terrorizm-itogi-2018> (дата обращения: 24.01.2019).
4. Itogi V mezhdunarodnoi konferentsii po protivodeistviyu terrorizmu. URL: <http://www.mrkizilyurt.ru/press/news/itogi-v-mezhdunarodnoy-konferentsii-po-protivodeistviyu-terrorizmu/> (дата обращения: 19.02.2019).
5. Википедия. URL: https://ru.m.wikipedia.org/wiki/Комп'ютерний_тероризм. (дата обращения: 24.01.2019).
6. *Tomas T.L.* Sderzhivanie asimetrichnykh terroristicheskikh ugroz, stoyashchikh pered obshchestvom v informatsionnuyu epokhu // Mirovye soobshchestvo protiv globalizatsii prestupnosti i terrorizma: materialy mezhdunar. konf. M., 2002.
7. Википедия. URL: https://ru.m.wikipedia.org/wiki/Комп'ютерний_тероризм. (дата обращения: 24.01.2019).
8. *Rogovskii E.A.* Rossiya v bor'be s mezhdunarodnym terrorizmom grani povysheniya pozitivnogo obraza strany // Rossiya i Amerika v XXI veke: elektronnyi nauchnyi zhurnal. 2007. №3. URL: <http://www.rusus.ru/?act=read&id=66>. (дата обращения: 24.01.2019).
9. *Golubev V.A.* Kiberterrorizm kak novaya forma terrorizma? URL: <http://www.crime-research.org> (дата обращения: 24.01.2019).
10. Kiberterrorizm — opredeleniya, klassifikatsiya, opasnost'. URL: <http://elcomrevue.ru/opredelenie-kiberterrorizma/> (дата обращения: 24.01.2019).
11. *Starostina E.* Terrorizm i kiberterrorizm – novaya ugroza mezhdunarodnoi bezopasnosti // Tsentr issledovaniya komp'yuternoi prestupnosti: Internet-izdanie. URL: <http://www.crime-research.ru/articles/starostina> (дата обращения: 24.01.2019).
12. *Gazizov R.R.* Informatsionnyi terrorizm // Problemy protivodeistviya prestupnosti v so-vremennykh usloviyakh: materialy mezhdunar. nauch.-prakt. konf. 16-17 okt. 2003 g. Ch. I. Ufa: RIO Bash-GU, 2003. 280s.
13. Kiberterrorizm — opredeleniya, klassifikatsiya, opasnost'. URL: <http://elcomrevue.ru/opredelenie-kiberterrorizma/> (дата обращения: 24.01.2019).

*Поступила в редакцию 29 апреля 2019 г.
Received 29 April, 2019*