В глобальном и региональном масштабе

О понимании проблемы информационного терроризма

Владимир АРЧАКОВ,
заместитель Государственного секретаря Совета Безопасности Республики Беларусь

В современном мире посредством информационных технологий повсеместно осуществляется манипулирование общественным сознанием с целью создания напряженности и хаоса. Дестабилизация отношений между социальными группами, общественными объединениями, партиями, движениями провоцирует конфликты, разжигает недоверие. Инспирирование политических, национальных, религиозных конфликтов и кризисов, дезинформация населения о работе органов власти подрывают устойчивость государств и наносят ущерб их жизненно важным интересам.

В политическом, международном, общественном дискурсе, публицистике и просто в обиходе возникают и достаточно широко используются термины, производные от слова «терроризм». Но термин «информационный терроризм» объективно не соответствует такому преступлению, как акт терроризма. Из-за малоизученности понятия «информационный терроризм» затруднено понимание истинных размеров и масштабов формируемых им угроз, поскольку они не поддаются подробному измерению по формальным признакам. Ни один из существующих механизмов сбора данных о правонарушениях не обеспечивает четкого отличия информационного терроризма от киберпреступлений *[1, с. 8–9]*. Необходимо теоретически разграничить понятия «терроризм», «информационный терроризм», «кибертерроризм» и некоторые другие для осмысленного восприятия в обществе, понимания опасности исследуемых явлений, компетентного возложения задач на правоохранительные органы, спецслужбы, другие ведомства и организации по выявлению, пресечению и предупреждению нанесения вреда личности, обществу и государству, в каких бы формах это ни происходило.

С другой стороны, по мнению М. Кенни, доцента кафедры международных отношений Питтсбургского университета (США), следует воздержаться от излишней драматизации ситуации, а возможно и понизить градус риторики вокруг информационного терроризма. Хотя некоторые страны уже испытали на себе информационные атаки со стороны террористических организаций либо политических оппонентов, ни одна из атак не достигла уровня тер-

ОБ АВТОРЕ

АРЧАКОВ Владимир Юрьевич.

Родился в 1967 году в г. Екатеринбурге (Россия). Окончил Свердловское высшее военно-политическое танко-артиллерийское училище (1988), Институт национальной безопасности Республики Беларусь (1996), Белорусский государственный экономический университет (2014). Проходил службу в Вооруженных Силах, органах государственной безопасности. С 2014 года – заместитель Государственного секретаря Совета Безопасности Республики Беларусь. Генерал-майор (2014).

Автор ряда научных работ.

Сфера научных интересов: национальная безопасность, государственное управление, социально-политическая аналитика, информационная безопасность.

рористического акта, не повлекла разрушительных социально-политических или индустриальных последствий. Но чтобы понять сущность информационного терроризма, необходимо четко уяснить, чем он на самом деле является *[2, с. 28–29]*.

Точки зрения на явление

В одном из докладов ФБР информационный терроризм весьма узко, на наш взгляд, определяется как «заранее спланированные, политически мотивированные атаки на информационные, компьютерные системы, программы и данные, которые выражаются в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов» *[3]*. Существенно расширено данное понятие доктором военных наук, профессором А.И. Исаковым, который считает, что «информационный терроризм осуществляется в области, охватывающей политические, философские, правовые, эстетические, религиозные и другие взгляды и идеи, то есть в духовной сфере, там, где ведется борьба идей. Информационный терроризм – это, прежде всего, форма негативного воздействия на личность, общество и государство всеми видами информации» *[4]*.

На протяжении 2013–2016 годов проблема информационного терроризма исследовалась на кафедре уголовного и уголовно-исполнительного права Саратовской государственной юридической академии. Согласно выводам кандидата юридических наук Д.А. Ковлагиной, под информационным терроризмом следует понимать использование интернета или иной информационной локальной сети, а также СМИ с целью негативного воздействия на органы власти и (или) население или достижения иных террористических целей (включая финансирование, обмен данными и др.) *[5, с. 183]*. В своей книге «Психология терроризма» политолог Д.В. Ольшанский пишет, что информационный терроризм – это пропагандистское воздействие на психику и сознание, оказываемое в целях формирования нужных мнений и суждений, направляющих поведение людей, и не оставляющее человеку возможностей для критической оценки получаемой информации *[6]*.

Более умеренную, по мнению профессора А.И. Исакова, формулировку информационного терроризма дают российские правоведы В.П. Емельянов и В.А. Кульба, которые утверждают, что различного рода угрозы, действия по устрашению в адрес отдельных личностей и общества в целом являются преступлением с признаками терроризирования. В развитие своих взглядов они приводят отличительные признаки терроризирования, в числе которых – создание в обществе атмосферы страха и угроз. Авторы Словаря по уголовному праву считают, что терроризм вообще, и духовный в частности, представляет собой деятельность, выражающуюся в устрашении населения и органов власти с целью достижения преступных намерений.

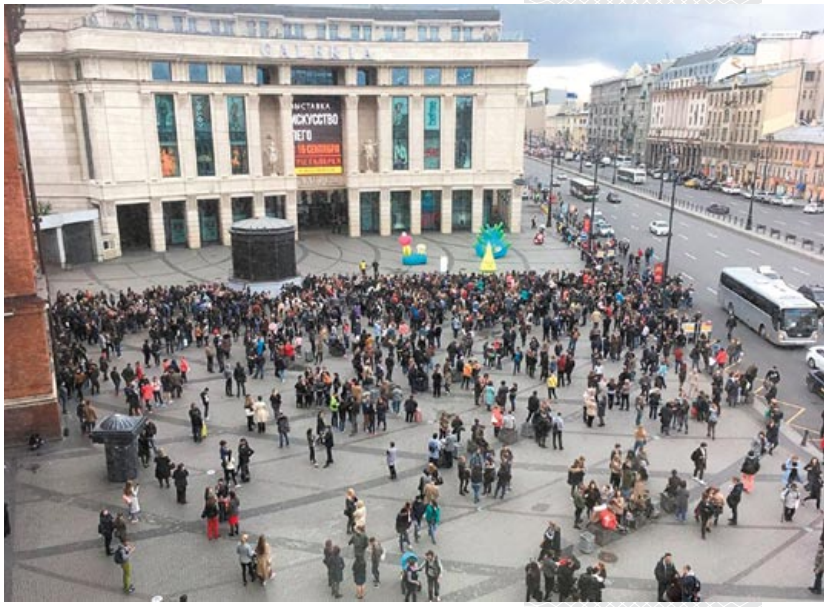
В общем и целом в приведенных трактовках возможно выделить несколько потенциальных целей информационного терроризма – это информационно-психологическое воздействие, радикализация отдельных лиц и групп, мобилизация массовой аудитории, дезориентация и дискредитация политического руководства, дестабилизация общественно-политической ситуации. В совокупности можно сделать вывод о правомерности понятия «информационный терроризм» как современного социально-политического явления, представляющего серьезную угрозу безопасности и жизненно важным интересам личности, общества и государства.

На основании вышеизложенного считали бы уместным дать следующее определение: информационный терроризм – это общественно опасная деятельность, мотивированная политическими, религиозными или иными идеологическими соображениями. Сущность ее выражается в информационном воздействии на органы власти и общественное мнение в целях устрашения, вынуждения к опреде-

ленным действиям, а также дестабилизации социально-политической обстановки, что влечет тяжкие последствия для различных сторон жизнедеятельности общества, государства и снижает способность социума к воспрепятствованию этому воздействию.

Необходимо отдельно и дополнительно сказать о том, что понятие «информационный терроризм» – более широкое, нежели «кибертерроризм», поскольку охватывает использование разнообразных методов и средств информационного воздействия не только на информационную инфраструктуру, но и на различные стороны человеческого общества: физическую, информационную, когнитивную, социальную. Хотя проявления информационного терроризма могут быть сопряжены и с выведением из строя сетей, ресурсов, объектов критической инфраструктуры. Даже сами по себе настойчивые, целенаправленные, буквально невыносимые с психологической точки зрения атаки на инфраструктуру могут рассматриваться как информационный терроризм.

По большому счету, информационный терроризм, как и кибертерроризм, – это психоэмоциональные категории, не подпадающие под признаки составов террористических преступлений, а поэтому по сути терроризмом не являются. В понятиях «информационный терроризм», «кибертерроризм» скорее подчеркивается эффект воздействия на массовое сознание людей в особо неприемлемом, устрашающем, вероломном, безнравственном, трудноразрешимом ключе. К подобной категории можно отнести и так называемый телефонный терроризм, то есть ложные сообщения о неких террористических угрозах. Причем в ряде случаев подобным явлениям в их более отчетливом, квалифицируемом виде могут соответствовать совершенно конкретные уголовные и административные правонарушения. Например, компьютерным терроризмом могут быть преступления против информационной безопасности, информационным терроризмом – нарушения законодательства



▲ Эвакуация людей из торгового центра в Санкт-Петербурге из-за ложного сообщения о минировании. 2017 год

о СМИ, телефонным терроризмом – заведомо ложные сообщения об опасности. Некоторая сложность в понимании этих явлений состоит именно в их зачастую пограничном с преступлениями характере, трудности квалификации и применения обычных правовых методов пресечения и профилактики. При отсутствии ясной правовой квалификации не могут включаться и существующие международные механизмы. Противодействовать информационному терроризму, без труда осуществляемому из-за пределов множества национальных границ, особенно затруднительно.

Не следует также путать с информационным терроризмом использование информационных технологий в целях подготовки и осуществления реальной террористической деятельности, например вербовку боевиков для участия в террористических организациях, использование сетевой информации для изготовления средств террора, координацию с помощью ИКТ определенных действий конкретных террористов при совершении терактов, демонстрирование в СМИ и глобальной сети захваченных заложников и т. д. В данном случае речь идет о совершении террористических преступлений, квалифицированных нормами уголовного законодательства, и

«виртуальные» факторы при всей их неоднозначности и сравнительной новизне уходят на второй план.

Преследуемые цели определяют и сближают понятия

Несмотря на отнесение информационного терроризма к сфере информационных воздействий, нельзя пренебрегать и тем, что в это понятие очевидно и преднамеренно закладывается определенная связь с фактической террористической деятельностью. Надо понимать, что это не просто деструктивное, негативное, антиобщественное информационное воздействие. Речь об информационном терроризме может идти тогда, когда организующие его субъекты (источники) преследуют те же цели, что и при реальной террористической деятельности, а именно: оказание воздействия на принятие решений органами власти, воспрепятствование политической или иной общественной деятельности, устрашение населения, дестабилизация общественного порядка. Именно такой смысл заложен и в определении информационного терроризма в международных актах Беларуси и России, СНГ, ШОС по вопросам обеспечения международной информационной безопасности: «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях» *[7; 8; 9]*.

Например, к информационному терроризму возможно отнести распространение ложной информации о предполагаемых или якобы совершенных терактах, устрашающее навязывание информации о действительно совершенных где-либо и когда-либо актах терроризма или иной активной деятельности террористов и террористических организаций, пропаганду идей террористического характера, нагнетание информации о происходящих или надвигающихся бедах, бедствиях, социальных катаклизмах, неспособности государства и общества противостоять иным угрозам, в том числе непосредственно в информационной сфере, и т. п. Все это осуществляется в противовес неким социальным отношениям, иной общественной идеологии, спокойствию и стабильности, нередко в увязке с общими претензиями к какому-либо государству, социальной группе, системе взглядов и обычаев, отдельным лицам, ответственным за реализацию политической воли или принятие решений. Другими словами, это попытка принудить объекты информационного воздействия из-за боязни возможных террористических акций или иных угроз к невыгодным им мерам (что-либо предпринять, скорректировать, принять во внимание, от чего-либо отказаться и т. д.). Хотя мотив может быть и проще – например, реализовать неудовлетворенные амбиции, отомстить, а то и просто «поиздеваться» над массами людей из хулиганских или иных антиобщественных побуждений.

На наш взгляд, в качестве примеров информационного терроризма можно привести известные действия лондонского безработного Г. МакКиннона, который удалял более чем со 100 оборонных и космических компьютеров в разных частях США важные системные файлы, приводя компьютеры в неработоспособное состояние на программном уровне, стирал всевозможные лежавшие на жестких дисках военные документы и устанавливал на отдельные машины хакерский инструмент (2001–2002 годы) *[10]*, повсеместный страх повторного насилия сразу после трагедии в Беслане (2004) *[11]*, ложные сообщения об аварии на Балаковской АЭС и вспышке легочной чумы в Саратовской области России (2004, 2009) *[12, с. 106]*, взрывах в американском Белом доме и ранении президента Б. Обамы (2013) *[13]*, планируемых терактах против северокорейского лидера Ким Чен Ына во время киносеансов (2014) *[14]*, угрозах в адрес семьи президента США на ленте «Твиттера» американского еженедельника «Ньюсуик» *[15]*, взлом сайта министерства обороны Чили от имени «Исламского государства» *[16]*, вывод из строя электронных систем французского телеканала TV5 Monde с размещением

угроз в адрес президента Франции Ф. Олланда и французских военнослужащих, участвовавших в операциях против радикальных исламистов в Африке и на Ближнем Востоке (2015) *[17]*, и др.

Ключевым элементом является то, что в условиях современного развития информационно-коммуникационных технологий добиться основной цели террористов – массового информационного шока – возможно и без взрывов, поджогов, затоплений, иных действий, создающих опасность гибели людей, причинения им телесных повреждений. В свою очередь, это в меньшей степени рискованно и для самих террористов. Необходимо повториться: как только начинают звучать прямые угрозы подготовки и совершения актов терроризма в отношении конкретных объектов (субъектов), а также распространяется информация о подготавливаемых или совершаемых действиях террористического характера, это следует воспринимать не в качестве информационного терроризма, а расценивать как криминализированные деяния и предпринимать соответствующие меры реагирования.

И наконец, особая важность понимания явления информационного терроризма состоит в том, что оно, как правило, сопутствует реальной террористической деятельности. По мнению некоторых авторов, информационный терроризм даже причинно первичен и «родительски порождает вторичный физический терроризм» *[18]*. Во всяком случае, можно утверждать: если государство, общество, социальные группы подвергаются воздействиям, которые возможно расценивать как информационный терроризм, необходимо всерьез готовиться к возникновению подлинной террористической угрозы.

Происхождение опасных воздействий

Источником информационного терроризма прежде всего являются террористические организации, которые не только осуществляют реальную террористическую деятельность (или подготовку к ней), но и всячески обеспечивают ее информационное сопровождение. Или наоборот, нагнетают обстановку для дестабилизации массового сознания, а затем «добивают» его настоящим актом терроризма. Наглядным примером могут служить «Исламское государство», «Аль-Каида», одно присутствие которых в информационном пространстве уже дестабилизирует международную обстановку и формирует в ней атмосферу ужаса и непредсказуемости.

Это также экстремистские организации и группирования, деятельности которых присущи бескомпромиссность, агрессивность, претензии на абсолютную правоту, установки на незаконное применение силы. Настойчивая, тенденциозная подача идеологизированной информации, противоречащей общепринятым морально-нравственным нормам, содержащей пропаганду насилия, жестокости, антиобщественного поведения, безусловно, нагнетает обстановку и способствует росту социальной напряженности, тем более что экстремизм и терроризм – схожие по природе явления, существующие если не вместе, то рядом в жизни общества.

К источникам информационного терроризма следует отнести также радикальные религиозные, псевдорелигиозные, сектантские организации. Именно в их среде зарождаются идеи экстремизма и терроризма, а всевозможное массовое информационное воздействие на людей составляет важнейший элемент их деятельности, обеспечивающий пополнение, распространение и обновление приверженцев и мотивацию сообществ. Нередко такие организации и объединения запрещены национальным законодательством, что обусловливает их противостояние власти и общепринятой общественной идеологии, необходимость демонстрирования своей силы и непреклонного следования «идее».

Нужно упомянуть и отдельных лиц, по каким-либо причинам желающих «взбудоражить» обстановку. Их мотивы, как правило, это намерение «отомстить»,

хулиганские побуждения или попросту желание «острых ощущений».

Практическая реализация вредного влияния

Рассматривая средства информационного терроризма, следует руководствоваться тем, что это, прежде всего, информационно-психологическое воздействие. Поэтому главное средство информационного терроризма – СМИ. Именно они, включая и интернет, предназначены для информационной «обработки» широких масс людей. Безусловно, подавляющая часть информации не имеет никакого отношения к информационному терроризму и иному деструктивному влиянию на социум. Однако ее другая часть, являющаяся предметом данного исследования, представляет собой все ту же информацию, но сконструированную из определенного контента и подаваемую необходимым образом. Причем речь идет не о неких сверхсложных, экстраординарных технологиях воздействия на «мозги», а вполне обычных для СМИ психологических эффектах, манипулятивных приемах, навязчивости, ярких и динамичных формах преподнесения информации.

Фактически неограниченные возможности для информационного терроризма, как и для других массовых информационных воздействий, обусловлены развитием интернета как средства массовой информации и коммуникации. По оценкам аналитиков компании «Майкрософт», к 2020 году интернетом постоянно будут пользоваться 4 млрд человек – вдвое больше, чем сегодня. К нему будет подключено 50 млрд различных устройств, а объем интернет-трафика возрастет в 50 раз *[19, с. 24]*. Рассматривая роль массовых коммуникаций и их влияние на политические процессы, политологи отмечают, что власть знаний и информации становится решающей в управлении обществом, оттесняя на второй план влияние денег и государственное принуждение. Пример тому – «цветные» революции в Восточной Европе и на постсоветском пространстве, «арабская весна», другие известные социальные катаклизмы, спровоцированные, а зачастую и спродуцированные потрясениями в информационном пространстве.

Другие «традиционные» СМИ затруднительно использовать в целях информационного терроризма. Как правило, телевидение, радио, органы печати имеют национальную принадлежность, законность их деятельности в значительной степени контролируется государственными инструментами. Однако возможности этих СМИ полностью перекрываются интернетом и могут оказываться попросту неинтересными для «информационных террористов».

Отдельно можно отметить и другое средство реализации массового информационного воздействия, в том числе информационного терроризма, которое существует рядом со СМИ, а иногда весьма существенно их дополняет – это так называемые и уже упоминавшиеся слухи. Одни из них запускаются в массовое сознание в периоды социального напряжения. Такие «слухи-пугала» наиболее часто основаны на якобы резком ухудшении перспектив, например, скачках цен (Россия, 1990–1991; Чили, 1971–1973; Никарагуа, Афганистан, 1980). Подобные им слухи – о «грядущем контрнаступлении реакции», близком военном перевороте, «неотвратимом отмщении пособникам режимов», а также акциях террора (как в США после терактов 2001 года).

Другой тип слухов – агрессивные, которые не просто вызывают негативные настроения, а конкретно направлены на стимулирование агрессивного эмоционального состояния и поведенческого «ответа», жесткого действия. Слухи такого рода возникают в ситуациях острых противоречий, связанных с социальными межгрупповыми, межэтническими и межнациональными конфликтами. Короткие, рубленые фразы сообщают о конкретных «фактах», взывающих к отмщению, формируют аффективную общность «мы» (нормальные люди) в противовес общности «они» (зверствующие нелюди). Например, «негры вырезают белое население» (Заир, 1960), «беспорядки в Панаме вызваны кубинскими

агентами» (США, 1964), «новая власть грабит страну, отправляя зерно на Кубу и в Россию» (Никарагуа, 1980), а также слухи о «зверствах» российских войск в Чечне, Украине, Сирии и аналогичные – о «зверствах национальных боевиков» в отношении федеральных войск *[6]*.

Еще одним средством информационного терроризма можно назвать индивидуальные средства коммуникации – телефонную связь, почтовые отправления, сообщения в иных формах. Казалось бы, это весьма ограниченное средство, при помощи которого трудно всколыхнуть, напугать большие массы людей. Вместе с тем упоминавшийся телефонный терроризм может быть осуществлен в непредсказуемом масштабе. В сентябре – октябре 2017 года в десятках российских городов, включая Москву, с различных объектов эвакуировалось, по всевозможным оценкам, более одного миллиона человек после анонимных телефонных сообщений о минировании. В связи с произошедшим были возбуждены уголовные дела по статье 207 УК РФ (заведомо ложное сообщение об акте терроризма), и это, на наш взгляд, является именно проявлением информационного терроризма, в отличие, например, от телефонного звонка ребенка о минировании школы или сообщения лица в неадекватном состоянии о якобы готовящемся теракте.

Краткий итог

Исследовав источники и средства информационного терроризма, следует еще раз подтвердить, что это явление представляет собой разновидность деструктивного информационно-психологического воздействия на массовое сознание, которое, в свою очередь, уже в определенной степени изучено и даже находит отражение в отдельных международных актах *[20]*. Именно этим необходимо руководствоваться, чтобы четко понимать компетенции государственных структур в выработке мер противодействия информационному терроризму, а не полагаться исключительно на антитеррористические службы.

▲ **VIII Международная встреча высоких представителей, курирующих вопросы безопасности. Тверская область, Россия. Май 2017 года**

Необходимо отметить, что всевозможные целенаправленные информационные воздействия на массовое сознание вызывают серьезную тревогу как в глобальном, так и в региональном масштабе. В последнее время этой теме, в частности, была посвящена VIII Международная встреча высоких представителей, курирующих вопросы безопасности, состоявшаяся в Тверской области России в мае 2017 года и собравшая представителей 95 стран мира. Такие же проблемы рассматривались и на сессии Совета коллективной безопасности ОДКБ в Минске в ноябре 2017 года, где главы Армении, Беларуси, Казахстана, Кыргызстана, России и Таджикистана подписали межгосударственное соглашение о сотрудничестве в области обеспечения информационной безопасности. Хотя надо признать, что до всеобщего понимания необходимости устанавливать единые и справедливые правила поведения в информационном пространстве еще далеко.

Очевидна необходимость дальнейшей нормативной разработки проблематики информационной безопасности личности, общества и государства, а также выделения информационной безопасности в качестве самостоятельного предмета теории и социальной практики. Процессы и технологии воздействия информационной среды на духовную сферу обладают качественной спецификой, которая

определяет необходимость рассмотрения этой темы в концептуальном, методологическом и методическом плане. На основе концептуальных подходов следует постоянно совершенствовать и законодательную базу в сфере информационной безопасности.

Требуется дальнейшая координация деятельности законодательных, правоохранительных и других государственных органов, чтобы на основе прочного правового фундамента и параметров развития информационного общества обеспечивать соблюдение интересов и безопасность личности, общества и государства в информационной сфере. Надо сказать, что именно на решение этих задач нацелена созданная в 2017 году Межведомственная комиссия по безопасности в информационной сфере при Совете Безопасности Республики Беларусь *[21]*.

Большое значение имеет интеллектуальное развитие общества, поскольку всевозможные манипуляции с общественным сознанием во многом затруднены в высокообразованной аудитории с устойчивой системой обоснованных взглядов, а также знающей существо данной проблемы и обладающей опытом целенаправленной социально-психологической защиты.

ЛИТЕРАТУРА

1. Кибератаки: современная террористическая угроза / пер. с англ. С. Берец // Борьба с преступностью за рубежом. – 2016. – № 9. – С. 6–13.
2. Кенни, М. Кибертерроризм в пережившем вирус Stuxnet мире / М. Кенни; пер. с англ. С. Берец // Борьба с преступностью за рубежом. – 2017. – № 3. – С. 28–42.
3. Газизов, Р.Р. Информационный терроризм [Электронный ресурс] / Р.Р. Газизов // Проблемы противодействия преступности в современных условиях: материалы междунар. науч.-практ. конф., Уфа, 16–17 октября 2003 г. Часть I. / Уфа: РИО БашГУ, 2003. – Режим доступа: http://kalinovsky-k.narod.ru/b/ufa20034/30.htm. – Дата доступа: 02.10.2017.
4. Исаков, А.И. Информационный терроризм [Электронный ресурс] / А.И. Исаков // Научно-аналитический журнал «Обозреватель-Observer». – Режим доступа: http://observer.materik.ru/observer/N5-6_02/5-6_10.htm. – Дата доступа: 10.11.2017.
5. Ковлагина, Д.А. Информационный терроризм / Д.А. Ковлагина // Вестник Саратовской государственной юридической академии. – 2013. – № 6 (95). – С. 181–184.
6. Ольшанский, Д.В. Психология терроризма [Электронный ресурс] / Д.В. Ольшанский. – СПб.: Питер, 2002. – 288 с. – Режим доступа: http://scienceport.ru/filess/psi_terror.pdf. – Дата доступа: 15.11.2017.
7. Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Национальный правовой интернет-портал Республики Беларусь, 13.01.2015, 3/3080. – Режим доступа: http://www.pravo.by/upload/docs/op/A01300055_1421096400.pdf. – Дата доступа: 16.01.2018.
8. Соглашение Совета глав правительств Содружества Независимых Государств «Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности» [Электронный ресурс] // Право Беларуси. – Минск, 2015. – Режим доступа: http://mail.lawbelarus.com/011560. – Дата доступа: 16.01.2018.
9. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/902289626. – Дата доступа: 16.01.2018.
10. Самый масштабный взлом Пентагона или сетевые кошки-мышки [Электронный ресурс]. – Режим доступа: https://lenta.ru/articles/2005/06/09/hacker/. – Дата доступа: 18.11.2017.
11. Горев А.И. Информационный терроризм: современное состояние / А.И. Горев // Информатизация и информационная безопасность правоохранительных органов: Труды XIV Междунар. науч. конференции, 24–25 мая 2005 г. – М.: Изд-во Акад. управления МВД России, 2005. – С. 170–174.
12. Россошанский, А.В. Риски и угрозы информационного терроризма в России [Электронный ресурс] / А.В. Россошанский // Человек. Сообщество. Управление. – 2011. – № 3. – Режим доступа: https://cyberleninka.ru/article/n/riski-i-ugrozy-informatsionnogo-terrorizma-v-rossii. – Дата доступа: 18.11.2017.
13. Крупные атаки хакеров в 2001–2016 годах: хронология [Электронный ресурс]. – Режим доступа: http://tass.ru/info/1408961. – Дата доступа: 18.11.2017.
14. В Госдепартаменте США не комментируют исчезновение интернета в КНДР [Электронный ресурс]. – Режим доступа: http://korrespondent.net/world/3459511-v-hosdepartamente-ssha-ne-kommentyruuit-yscheznovenye-ynterneta-v-kndr. – Дата доступа: 19.11.2017.
15. СМИ: хакеры взломали сайт журнала Newsweek и разместили на нем угрозы в адрес семьи Обамы [Электронный ресурс]. – Режим доступа: http://tass.ru/obschestvo/1758606. – Дата доступа: 19.11.2017.
16. MKRU: Хакеры ИГ взломали сайт минобороны Чили [Электронный ресурс]. – Режим доступа: http://www.mk.ru/incident/2015/02/24/khakery-ig-vzlomali-sayt-minoborony-chili.html. – Дата доступа: 20.11.2017.
17. Крупные атаки хакеров в 2001–2016 годах: хронология [Электронный ресурс]. – Режим доступа: http://tass.ru/info/1408961. – Дата доступа: 20.11.2017.
18. Кулибаба, А.Н. Информационный терроризм [Электронный ресурс] / А.Н. Кулибаба. – Режим доступа: http://law.edu.ru/doc/ document.asp?docID=1252544. – Дата доступа: 25.11.2017.
19. Велев, С. Путь противодействия кибертерроризму – устойчивость к внешним воздействиям / С. Велев // Борьба с преступностью за рубежом. – 2016. – № 11. – С. 24–28.
20. Рекомендации по сближению и гармонизации законодательства государств – членов ОДКБ в сфере информационно-коммуникационной безопасности / [Электронный ресурс]: постановление Парламентской Ассамблеи ОДКБ, 27 ноября 2014 г., № 7–6. – Режим доступа: http://os.x-pdf.ru/20bezopasnost/207604-1-parlamentskaya-assambleya-organizacii-dogovora-kollektivnoy-bez-o.php. – Дата доступа: 25.11.2017.
21. О Межведомственной комиссии по безопасности в информационной сфере [Электронный ресурс]: Указ Президента Республики Беларусь, 16 ноября 2017 г., № 413 // Национальный правовой Интернет-портал Республики Беларусь, 18.11.2017, 1/17351. – Режим доступа: http://www.pravo.by/upload/docs/op/P31700413_1510952400.pdf. – Дата доступа: 25.11.2017.