Григорьев Н.Ю.
Родюков Э.Б.

СОВРЕМЕННЫЙ КИБЕРНЕТИЧЕСКИЙ ТЕРРОРИЗМ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

MODERN CYBERNETIC TERRORISM AND HIS SOCIAL CONSEQUENCES

Григорьев Николай Юрьевич, кандидат философских наук, доцент кафедры рекламы и связей с общественностью в медиаиндустрии, ФГБОУ ВПО «Московский государственный университет печати» имени Ивана Федорова, г. Москва, e-mail: nugrig@mail.ru
Родюков Эдуард Борисович, кандидат социологических наук, доцент кафедры социологии ФГВОУ ВПО «Военный университет» Министерства обороны Российской Федерации, г. Москва, член-корреспондент Академии военных наук, e-mail: groro@mail.ru
Eduard Rodyukov
Nikolay Grigoriev

Аннотация. Статья посвящена исследованию теоретических основ современного кибернетического терроризма. Учитывая, что информатизация сегодня охватывает все сферы общественной жизни, а значит, растет проблема информационной безопасности общества в целом и каждого человека в частности. Наряду с терроризмом в мировом масштабе в связи с процессами глобализации и интеграции в обществе грядет и изменение самих угроз, в частности угроза кибернетического терроризма.
Авторы анализируют различные научные подходы к пониманию сущности кибернетического терроризма и дают практические рекомендации, опираясь на опыт создания технологии антитеррористической информационной безопасности.
Abstract. The article is devoted to the study of the theoretical foundations of modern cyber terrorism. Given that policy now covers all spheres of public life and, therefore, increasing the problem of information security of society in General and each person in particular. Along with terrorism on a global scale in relation to processes of globalization and integration in the society is coming and a change in the threats, particularly the threat of cyber terrorism.
The authors analyze various scientific approaches to understanding the nature of cyber terrorism and provide practical recommendations based on the experience of creation of anti-terrorism technology information security.

Ключевые слова: кибернетический терроризма, киберпреступность, информационный криминал, кибератака, мобильная угроза,

компъютерный терроризм, международная информационная безопасность, антитеррористическая информационная безопасность.
Key words: cyber terrorism, cyber crime, information crime, cyber attack, the threat of mobile, computer terrorism, international information security, anti-terrorism information security.

Несмотря на все разговоры о мире и гуманизме, только за 50 лет после Второй мировой войны прошло 25–30 средних и более 400 малых войн. Они охватили не меньше стран, чем это было в последней мировой войне. В них погибло свыше 40 млн. и стали беженцами свыше 30 млн. человек. Сегодня специалисты выделяют следующие разновидности новых войн:

1. Локальные войны.
2. Военные конфликты.
3. Партизанская война.
4. Информационная война.
5. «Консциентальная» война (война сознаний).
6. Преэмптивная (опережающтй захват или силовое действие на опережение) война.
7. Террористическая война (терроризм) [3, с. 5–21].

Одной из современных разновидностей террористических войн является кибертерроризм. Термин «*кибертерроризм*» ввел в середине 1980-х гг. старший научный сотрудник американского Института безопасности и разведки Бэрри Коллин и обозначал он террористические действия в виртуальном пространстве.

Определить понятие «компьютерный терроризм» — достаточно трудная задача, поскольку нелегко установить четкую границу для отличия его от информационной войны и информационного криминала. Еще одна трудность состоит в том, что необходимо выделить специфику именно этой формы терроризма.

Е. Старостина предлагает следующее определение кибертерроризма: «это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей 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»[5].

Дороти Деннинг, профессор компьютерных наук Джорджтаунского университета и один из самых авторитетных экспертов в кибербезопасности говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенной с целью принудить органы вла-

сти к содействию в достижении политических или социальных целей»[8].

Одним из способов кибертерроризма является политически мотивированная атака на информацию. Она заключается в непосредственном управлении социумом с помощью превентивного устрашения. Это проявляется в угрозе насилия, поддержании состояния постоянного страха с целью достижения определенных политических или иных целей, принуждении к определенным действиям, привлечении внимания к личности кибертеррориста или террористической организации, которую он представляет. Так, например, за 2015 год число аккаунтов запрещенной в России террористической группировки «Исламское государство» (ИГ) выросло более, чем вдвое. А самый мощный всплеск произошел в 2014 г. — с 4378 до 11902 аккаунтов [6, с. 1,2].

Другим способом кибертерроризма является информационная атака на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, совершаемая группировками или отдельными лицами. Такая атака позволяет проникать в атакуемую систему, перехватывать управление или подавлять средства сетевого информационного обмена, осуществлять иные деструктивные воздействия, в том числе в сети Интернет.

Но в чем проявляется кибертерроризм или какова его тактика воздействия в глобальной сети Интернет? Если говорить о видах воздействия или о различных приемах кибертерроризма, то к ним можно отнести:

— нанесение ущерба отдельным физическим элементам информационного пространства (разрушение сетей электропитания, наведение помехи др.);

— кражу или уничтожение информационного, программного и технического ресурсов, имеющих общественную значимость, путем преодоления систем защиты, внедрения вирусов и т. п.;

— воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления;

— раскрытие и угрозу опубликования или само опубликование закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодах шифрования, принципах работы систем шифрования, успешном опыте ведения информационного терроризма и др.;

— захват каналов средств массовой информации с целью распространить дезинформацию, слухи, продемонстрировать мощь террористической организации и объявить свои требования;

— уничтожение или активное подавление линий связи, неправильную адресацию, искусственную перегрузку узлов коммутации;

— проведение информационно-психологических операций;

— ложную угрозу акта кибертерроризма, влекущую за собой серьезные экономические последствия;

— воздействие на операторов, разработчиков информационных и телекоммуникационных сетей и систем путем насилия или угрозы насилия, шантаж, подкуп, использование нейролингвистического программирования, гипноза, средств создания иллюзий, мультимедийных средств для ввода информации в подсознание или ухудшения здоровья человека и др. [2, с. 37].

Рост информационных технологий дает террористам возможность получить существенную прибыль при относительно низком риске. Они могут финансировать свою деятельность, не обращаясь к силовым нападениям или грабежам банков, которые увеличили бы риск обнаружения. Террористы весьма активно используют информационные ресурсы для решения организационных и финансовых вопросов, обеспечения связи, планирования актов терроризма и осуществления контроля над их проведением.

Сеть Интернет может быть использована транснациональными террористическими организациями для тщательного изучения своих новых кандидатов, ведения пропаганды, минуя контроль со стороны государственных органов, вывода из строя правительственных компьютерных сетей и пр. В настоящее время практически все более или менее крупные исламистские организации имеют свои сайты в Интернете. В сети существует масса сайтов, на которых детально излагаются рецепты и схемы изготовления оружия и взрывчатых веществ из подручных материалов, способы их использования и т. д. Многочисленные чаты и форумы, существующие в Интернете, идеально приспособлены для передачи зашифрованных посланий, а современные технологии позволяют легко распространять в сети карты и фотографии.

Для кибертерроризма характерно и то, что все известные сегодня хакерские группы и отдельные лица не стремятся афишировать свои данные и выступают исключительно под псевдонимом. При этом следует отличать хакера-террориста от простого хакера, который действует в корыстных или хулиганских целях. Но если действия таких субъектов приведут к тяжким последствиям, на-

пример, к гибели людей, то подобного рода хулиганство нельзя расценивать иначе как терроризм.

Главное в тактике кибертерроризма состоит в том, чтобы это киберпреступление имело опасные последствия, стало широко известно населению, получило большой общественный резонанс и создавало атмосферу угрозы повторения акта без указания конкретного объекта. Так, руководители ряда радикальных мусульманских организаций Ближнего Востока придают все большее значение использованию в своей деятельности именно современных информационных технологий, рассматривая их в качестве эффективного оружия в борьбе с режимами Израиля, Саудовской Аравии и поддерживающими их западными странами. Это, во-первых, достаточно недорогое средство совершения акта терроризма (поэтому к кибертерроризму прибегают и страны с неразвитой экономикой), а во-вторых — сложное пространство для выявления самого террориста.

Для организации кибератак необходима значительная квалификация их исполнителей, так как в ряде случаев кибертеррористические действия могут оказаться более предпочтительными, чем акты обычного терроризма. Проведение кибератак обеспечивает высокую степень анонимности и требует большего времени реагирования. Выработка методов антитеррористической борьбы изначально находится в области противодействия обычному терроризму. Осуществление атаки через информационные системы вообще может оказаться нераспознанным как акт терроризма, а будет воспринято, например, как случайный сбой системы.

Нет общего мнения по поводу определения объекта актов терроризма. Причем мнение колеблется от межгосударственной направленности, когда объектом становятся не только отдельные международные организации, но и целые государства, народы, до узкогрупповой, даже личностной, когда объектом становится конкретное лицо (политический или государственный деятель) либо случайное лицо. Действия кибертеррористов могут быть направлены как на гражданские, так и на военные объекты.

По мнению американских экспертов, наиболее уязвимыми точками инфраструктуры являются энергетика, телекоммуникации, авиационные диспетчерские, финансовые электронные и правительственные информационные системы, а также автоматизированные системы управления войсками и оружием. Так, в атомной энергетике изменение информации или блокирование информационных центров может повлечь за собой ядерную катастрофу или прекращение подачи электроэнергии в города и на военные объекты.

Так, цели, на которые направлены атаки кибертеррористов, соответствуют национальной информационной инфраструктуре. Это:

1) оборудование, включая компьютеры, периферийное, коммуникационное, теле, видео и аудиооборудование;

2) программное обеспечение;

3) сетевые стандарты и коды передачи данных;

4) информация как таковая, которая может быть представлена в виде баз данных, аудио-, видеозаписей, архивов и др.;

5) люди, задействованные в информационной сфере [5, с. 12].

Следует выделить первые три цели, так как они взаимосвязаны и едва ли могут рассматриваться отдельно. Физические компоненты инфраструктуры представляют собой комплекс аппаратных средств (оборудования) и программного обеспечения, работающий по согласованным и унифицированным стандартам. Таким образом, эти объекты можно рассматривать как своего рода служебную структуру, обеспечивающую работоспособность всей информационной структуры. Мишенями кибертеррристов могут стать как гражданские, так и военные объекты.

Целью кибертеррористов может стать как выведение из строя информационных систем, так и разрушение объектов информационных систем

Выведение из строя информационных систем характеризуется прежде всего тем, что именно такие атаки наиболее распространены. Они направлены на выведение из строя отдельных интернет-служб или переадресацию информации. Такие кампании осуществляются чаще всего так называемыми временными кибертеррористами — частными лицами, не связанными напрямую с террористическими группами, однако разделяющими их идеи.

Информация, играющая решающую роль в функционировании как государственной власти, так и общественных институтов, становится самым слабым звеном национальной инфраструктуры государства на современном этапе развития, поэтому проблема международного терроризма приобретает в условиях информационного противостояния новое звучание. Это связано прежде всего с двумя аспектами:

1) с использованием террористами информационной инфраструктуры для развития сетевых способов собственной организации

2) с прямым террористическим воздействием на объекты информационных инфраструктур [1].

В сфере международных отношений терроризм представляет острую угрозу прежде всего для международной безопасно-

сти, поскольку подвергает опасности стабильность и мирный характер во взаимоотношениях между отдельными государствами, а также группами государств, провоцирует напряженность в отношениях между ними, нередко способствует разжиганию опасных международных конфликтов, препятствует их разрешению. Терроризм на международной арене выступает и как инструмент вмешательства во внутренние дела государств, дезорганизует международные связи, грубо нарушает права человека, международный правопорядок. Вот почему следует проблему терроризма рассматривать на международном уровне как прямую угрозу международной безопасности, а угрозу кибертерроризма — как вторую составляющую такого рода угроз.

Восемь ведущих государств мира, включая Россию, приняли Окинавскую хартию глобального информационного общества от 22 июля 2000 г., по которой в целях развития глобального информационного общества предлагается предпринять «согласованные действия по созданию безопасного и свободного от преступности киберпространства».

Вхождение человечества в XXI в. омрачено ростом террористической опасности в самых различных ее проявлениях. Методы террористов становятся все более разнообразными и изощренными. Увеличение числа и роста экстремистских группировок сопровождается их возрастающей технической оснащенностью.

Чтобы активно и плодотворно противостоять международному кибертерроризму, следует базироваться на следующих важнейших основополагающих признаках:

— следовать нормам и принципам международного права;

— всеобщее осуждение и признание противоправности терроризма во всех его проявлениях (кибертерроризм);

— международное сотрудничество и обмен информацией между государствами;

— неотвратимость ответственности кибертеррористов, совершивших преступление;

— действенность антикибертеррористических мер [5].

Все основные принципы должны быть признаны международным сообществом и каждым государством в отдельности, чтобы эффективно противостоять кибертерроризму.

На практике немаловажную роль играют действия по предотвращению и оперативному пресечению террористических действий с использованием сетевых технологий — антитеррористической информационной безопасности (АИБ) [2]. Речь идет о проблемах информационной безопасности в узком понимании, а именно

только применительно к сетевой инфраструктуре. Отсюда общее определение АИБ и постановка задач на действия по предотвращению, оперативному реагированию на террористические действия в сетевой среде с использованием информационных технологий могут быть сформулированы следующим образом:

АИБ — это совокупность механизмов, инструментальных средств, методов, мер и мероприятий, позволяющих предотвратить, обнаружить, а в случае обнаружения — оперативно реагировать на действия, направленные на:

— разрушение инфраструктуры сети посредством вывода из строя системы управления ею;

— несанкционированный доступ к информации, охраняемой законом и носящей конфиденциальный характер или высокий уровень секретности;

— намеренное искажение информации, предоставляемой в сетях общего пользования.

Конечно, понятие АИБ не претендует и не может претендовать на общность, абсолютную полноту охвата и законченность изложения возможных целей. Они определяются состоянием развития компьютерных, коммуникационных и информационных технологий, которые развиваются весьма динамично. Однако АИБ должна быть в поле зрения международного сотрудничества государств для успешной работы в данном направлении. Сегодня же приходится констатировать тот факт, что вопросы международного правового регулирования не только в области предотвращения использования Интернета в террористических целях, но и более общие, влияющие на АИБ проблемы традиционной противоправной деятельности пока не только не решены, но и не разрабатываются. Налицо отставание международно-правовых аспектов развития Интернета от ее инфраструктурно-технических и научно-технических.

Если подходить к вопросу о мерах по предотвращению кибертерроризма сугубо комплексно, то следует выделить следующие моменты. Государствам следует сделать акцент на политике безопасности не только на общегосударственном уровне, но и на административном, более низком, однако не менее важном.

Необходимо защищаться на операционном уровне при реализации общей политики безопасности в интернет-сетях. Операционные регуляторы ориентированы прежде всего на людей и должны обеспечить сокращение ущерба от совершенных атак путем своевременной реакции, оперативного и качественного восстановления. Каждый сотрудник должен иметь минимум при-

вилегий, необходимых для выполнения обязанностей. Таким образом, если злоумышленник и проникнет в организацию, он не сможет принести ощутимого ущерба.

Немаловажен и программно-технический уровень. Для противостояния атакам со стороны террористов в Интернете необходимо предусмотреть следующие меры:

— *пароли:* ни один компьютер корпоративной сети не должен быть защищен паролем, который легко разгадать, в том числе с помощью словаря. Надежность паролей следует регулярно проверять;

— *сеть:* меняйте конфигурацию сети сразу при обнаружении брешей. Безопасность сети также должна проводиться регулярно;

— *«заплаты»:* ответственный за систему безопасности должен подписаться на списки рассылки по вопросам безопасности и своевременно информировать сотрудников о новых «дырах» в системе защиты;

— *контроль:* следует регулярно проверять надежность всех систем и анализировать файлы журнала регистрации [4].

Не следует забывать о возможном физическом воздействии. Ведь компьютерная система может быть выведена из строя физическим воздействием на нее. Классическими примерами таких воздействий могут быть пожар и взрыв бомбы. В последнее время появились устройства, специально предназначенные для уничтожения компьютерных систем. Посредством резкого всплеска напряжения в сетях питания, коммуникаций или сигнализации с амплитудой, длительностью и энергией всплеска они способны привести к сбоям в работе оборудования или к его полной деградации.

Если не исходить от частного к общему, то невозможно построить крепкую и надежную международно-информационную систему безопасности от посягательств со стороны компьютерных террористов. Проникая во все сферы жизнедеятельности государств, информационная экспансия расширяет возможности развития международного сотрудничества, формирует глобальное информационное пространство, в котором информация приобретает свойства ценнейшего элемента национального достояния, его стратегического ресурса.

Международное сотрудничество позволяет получить доступ к новейшим информационным технологиям, участвовать в мировом разделении труда в области информационных услуг, средств информатизации и информационных продуктов. Но становится очевидным и тот факт, что наряду с положительными моментами такого процесса создается реальная угроза использования достижений в информационной сфере в целях, не совместимых с за-

дачами поддержания мировой стабильности и безопасности, соблюдением принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. Как раз к числу таких угроз относится терроризм с использованием современных сетевых технологий.

Очевидна потребность в международно-правовом регулировании процессов международного взаимодействия всех субъектов, участвующих в поддержании и развитии сетевой инфраструктуры и информационных ресурсов. Необходима отвечающая интересам мировой безопасности согласованная международная платформа по проблеме информационной безопасности, учитывающая вопросы антикибертеррористической направленности.

Генеральная Ассамблея ООН в Резолюциях 5 3/70 от 4 декабря 1998 г. и 54/49 от 1 декабря 1999 г. подняла вопрос о целесообразности разработки международных принципов, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствующих борьбе с информационным терроризмом и преступностью. Чтобы выработать конкретные положения программы действий, необходимо направить все силы на предотвращение следующих угроз в сфере информационной безопасности:

— действия международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющие угрозу информационным ресурсам и критически важным инфраструктурам государств;

— использование информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;

— манипулирование информационными потоками, дезинформация и сокрытие информации с целью исказить психологическую и духовную среду общества, эрозия традиционных культурных, нравственных, этнических и эстетических ценностей [8].

Но, некоторые государства, претендующие на мировое господство, пытаются сегодня противопоставить окружающему миру свою военную мощь и экономическую силу. Так в начале октября 2014 г. в США была обнародована новая оперативная концепция сухопутных войск США — «Победа в сложном мире. 2020–2040». Впервые в концепции официально признаны сферы войны [3, с. 22–54]:

1. Традиционные боестолкновения с использованием летального оружия.

2. Внутриполитические гражданские конфликты.
3. Противоборства в сфере дипломатии.
4. Информационные воины.
5. Финансово-экономические войны.
6. Жесткое технологическое противоборство.
7. Поведенческие войны (целенаправленное воздействие на поведение больших групп населения и элитных структур стран — потенциальных источников вероятных угроз).

При этом в концепции выделяют пять полей противоборства: суша, море, воздух, космос и киберпространство. Поэтому, Россия и другие страны должны осознавать, что киберпространство — это серьезно, и это оказывает существенное, если не главное, влияние на политическую, государственную и национальную независимость. И здесь возможны и кибертерроризм и информационная война.

Угроза кибертерроризма в настоящее время является очень сложной и актуальной проблемой не только за рубежом, но и в России. К сожалению, она будет усиливаться по мере развития и распространения информационных технологий. Но определенные шаги уже начали предприниматься. В Совете Федерации РФ предложили увеличить в школах часы курса «Основ безопасности жизнедеятельности» (ОБЖ) для разъяснения ученикам признаков террористических угроз. Для взрослых антитеррористическое воспитание пойдет через возрождение нравственных ценностей [7, с. 3].

Но, международный терроризм, перешедший в сферу информационно-коммуникационного поля, не знает границ. Он не имеет ни национальной, ни религиозной принадлежности. Террористы и кибертеррористы — это бросившие вызов культуре, цивилизации, обществу преступники, компромисс с которыми невозможен и которые должны предстать перед судом.

Долг мирового сообщества государств — защитить общество, защитить мир. Вопрос обеспечения информационной безопасности как одной из важных составляющих национальной безопасности государства особенно остро возникает в контексте появления транснациональной трансграничной компьютерной преступности и кибертерроризма.

Библиографический список

1. Васенин, В.А. Критически важные объекты и кибертерроризм. М.: МЦНМО, 2008. — 607 с.

2. Гаврилин, Ю. В., Смирнов, Л.В. Современный терроризм: сущность, типология, проблемы противодействия. М.: ЮИ МВД России, Книжный мир, 2003. — 64 с. — ISBN 5-804-0144-7.
3. Гибридные войны XXI века: материалы межвузовского круглого стола. — М: ВУ, 2015. — 310 с.
4. Соколов, А. В., Степанюк, О.М. Защита от компьютерного терроризма. Справочное пособие. СПб.: БХВ-Петербург, 2002. — 496 с. — ISBN 5-941570-76-3.
5. Старостина, Е. В., Фролов, Д.Б. Защита от компьютерных преступлений и кибертерроризма. Вопросы и ответы. М.: «Эксмо», 2005. — 192 с. — ISBN: 5-699-10862-9.
6. Трифонова, Е. Интернет-террористам ищут адекватный ответ // Независимая газета. — 23.09.2015. — С. 1,2.
7. Трифонова, Е. По экстремизму ударят искусством // Независимая газета. — 18.03.2016. — С. 3.
8. Устинов, В.В. Международный опыт борьбы с терроризмом: стандарты и практика. — М.: «Юрлитинформ», 2002. — 560 с. — ISBN 5-93295-056-0.