14. Петров С. А. Уголовно-правовая характеристика участников движения при нарушении правил, обеспечивающих безопасную работу транспорта // Российский следователь. 2016. № 7.

УДК 343.34
ББК 67.408.135

КИБЕРТЕРРОРИЗМ В РОССИИ И СТРАНАХ ЦЕНТРАЛЬНОЙ АЗИИ

А. С. Соколов, А. Ю. Поволотцкий
Алтайский государственный университет (Барнаул, Россия)

В статье рассмотрены понятие и признаки кибертерроризма. Проводится отграничение данного термина от других подобных понятий. Дается оценка случаев террористических атак на информационные ресурсы. Проанализированы основные способы совершения кибертерроризма. Показан вред, который может быть причинен актами кибертерроризма. Указаны отдельные причины, обусловливающие кибертерроризм.

Ключевые слова: терроризм, киберпреступность, кибертерроризм, информационный терроризм, компьютерный шпионаж, компьютерные вирусы, информационная безопасность, кибератака.

CYBER TERRORISM IN RUSSIA AND THE CENTRAL ASIAN COUNTRIES

A. S. Sokolov, A. Y. Povolotsky
Altai State University (Barnaul, Russia)

The article discusses the concept and signs of cyber terrorism. This term is distinguished from other concepts of concepts. An assessment of cases of terrorist attacks on information resources is given. The main ways of committing cyber terrorism are analyzed. The harm that can be caused by acts of cyber terrorism is shown. Some reasons for cyber terrorism are indicated.

Keywords: terrorism, cybercrime, cyber terrorism, information terrorism, computer espionage, computer viruses, information security, cyber attack.

Doi: https://doi.org/10.14258/ralj(2020)2.10

Исключительно быстрое развитие современных информационных и телекоммуникационных технологий достигает с каждым днем все новых и новых уровней, о чем свидетельствует их активное внедрение во все без исключения сферы жизнедеятельности человека. Информационные сети, глобальная сеть Интернет позволяют обмениваться информацией в считанные секунды. Внедрение компьютерных систем привело к автоматизации различных производственных и управленческих процессов. Современное общество уже не представляет себе существования и нормального функционирования без информационного обмена в информационно-телекоммуникационных системах.

Однако особенностью компьютерной сферы является то, что безошибочных программ в ней не бывает. Если в другой отрасли любой проект можно выполнить с большим запасом надежности, то в информационных технологиях и программах такая надежность весьма условна, а во многих случаях почти недостижима. Это, в свою очередь, привело к появлению нового вида правонарушений — компьютерной преступности.

Сам термин «компьютерная преступность» появился в зарубежной прессе еще полсотни лет назад, когда обнаружили первые нарушения с использованием электронно-вычислительных машин (ЭВМ). Сегодня это явление усиливается не только в локальном (национальном), но даже в планетарном масштабе. По мнению отечественных криминалистов, ЭВМ — многообещающее орудие для совершенных противозаконных действий. Экономический ущерб от таких преступлений уже сравнялся с преимуществами, полученными от воплощения достижений ЭВМ в жизнь. А социальные и моральные потери вообще не поддаются оценке.

Досадные факты говорят сами за себя. Например, в такой информационно развитой стране, как США, ежегодные материальные убытки от компьютерной преступности уже давно превышают десятки миллиардов долларов. Конечно, в РФ эта цифра гораздо меньшая. Но в РФ этот вид преступности имеет достаточно высокую латентность: правоохранителям известно лишь 10–15% подобных случаев, поскольку пострадавшие неохотно предоставляют информацию (это может повредить их репутации или вызвать повторные преступления).

Понятно, что угроза информационному ресурсу государства — угроза национальной безопасности. К сожалению, нормы и положения в этой сфере до сих пор четко не определены. Причина общеизвестна: развитие научно-технического прогресса создает благодатную почву для кражи денег с электронных систем взаиморасчетов, несанкционированного использования ЭВМ (для получения собственности или услуг), повреждения или уничтожения компьютерных сетей и программ, проникновение в чужие базы данных, незаконного копирования или фальсификации данных, шантажа, информблокады, шпионажа и т. д.

Кроме того, глобальное распространение информационно-коммуникативных технологий в обществе привело к появлению и развитию принципиально нового вида терроризма — информационного терроризма или кибертерроризма. Большое значение в этом контексте приобретает научно-методическое обеспечение деятельности правоохранительных органов РФ и странах Центральной Азии по определения теоретических, а также тактических аспектов противодействия информационному терроризму (кибертерроризму).

Отдельные теоретические аспекты информационного терроризма (кибертерроризма) как фактора угрозы национальной безопасности России и стран Центральной Азии, исследовались в трудах В. А. Мазурова [1], В. С. Овчинского [2], Е. В. Старостиной [3, 4], О. А. Степанова [5], Т. Л. Тропиной [6, 7], Ф. А. Услинского [8]; диссертационных исследованиях Е. Н. Молодчей [9, 10], С. В. Зарубина [11]; сборниках статей и тезисов по указанной проблематике [12–14].

Главной целью данной работы является непосредственный анализ явления кибертерроризма, исследование характеристики этого противоправного деяния в киберпространстве, а также вопрос о минимизации негативных последствий преступной деятельности по использованию информационных технологий на территории России и стран Центральной Азии.

Кибертерроризм начал зарождаться в 1970-х гг. Так, в 1983 г. был арестован первый «виртуальный преступник» — группа хакеров под названием «Банда 414» (г. Милуоки, шт. Висконсин, США), которая сломала 60 компьютеров (некоторые из них принадлежали Лос-Аламосской национальной лаборатории в шт. Нью-Мексико). С начала 1990-х гг. проявления кибертерроризма фиксируют почти ежегодно.

Сам термин «кибертерроризм» образовывается слиянием двух понятий: «кибер» («киберпространство») и «терроризм». В публикациях ученых и практиков часто встречаются термины «виртуальное пространство» и «виртуальный мир». Принимая за основу понятия терроризма и сочетание его с виртуальным пространством, можно предложить такое определение: кибертерроризм — это комплексная модель, которая выражается в намеренной, политически мотивированной атаке на информацию, которая обрабатывается компьютером и компьютерными системами, что в результате создает определенную опасность для жизни или здоровья людей, наступление иных тяжких последствий, если такое действие совершается в целях нарушения общественной безопасности, устрашения населения, провоцирование военного конфликта.

Киберпреступность можно определить как противоправные действия, которые совершаются в так называемом «виртуальном пространстве». Такое пространство определяют как моделируемое с помощью компьютера информационное пространство, где находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом

другом виде. При этом такие сведения находятся в процессе определенного движения локальными и глобальными компьютерными сетями, хранятся в памяти физического или виртуального устройства, другого носителя, который специально предназначен для такого хранения, обработки и передачи информации.

В значительной степени отечественные ученые оперируют понятием кибертерроризма, часто понимая под ним и «кибервойны», и «кибератаки» и т. п., что неправильно как с методологической точки зрения, так и относительно отражения современных реалий этой сферы безопасности.

Даже в западной научной литературе термин «кибертерроризм» и описание возможных последствий актов кибертерроризма имеет преимущественно идеологически пропагандистскую и абстрактно-теоретическую особенность, обусловливается провозглашенной во времена президентства Дж. Буша младшего «глобальной войной с терроризмом». До последнего времени большинство реальных угроз критически важной инфраструктуре информационно развитых государств (США, Великобритания, Германия) поступали не от отдельных террористических групп, которые просто изменили непосредственную тактику ведения своей борьбы, а от специально подготовленных информационно и материально обеспеченных специализированных групп, функционирующих в интересах тех или иных государств, что фактически было действиями их «военной машины».

В фундаментальном труде «Кибервойна и кибертерроризм» дается следующее определение кибертерроризма: «Кибертерроризм — это политически мотивированные атаки, совершаемые субнациональными группами или тайными агентами или отдельными индивидами против информационных и компьютерных систем, компьютерных программ или данных, результатом которых является насилие против нонкомбатантов» [15, с. 13]. Это определение содержит две ключевые компоненты, помогающие отделить кибертерроризм от всех других форм киберпреступлений: наличие доказанной «политической мотивации» и желание осуществить «насилие против нонкомбатантов».

«Словарь терроризма» описывает кибертерроризм как «преступление, к которому в будущем будет прибегать криминалитет, используя компьютеры». При этом отмечается, что «кибертеррористы имеют политическую мотивацию для их преступлений» [16, с. 61]. М. Каветли предлагает следующее определение кибертерроризма: «Под кибертерроризмом понимается незаконное нападение со стороны негосударственных субъектов в отношении компьютеров, сетей и информации, содержащейся в них, которое осуществляются с целью запугивания правительства (или населения) или с целью достижения определенного поведения субъекта, который запугивается. Кибератака может пониматься как кибертерроризм только в том случае, если это приводит к физическому насилию против лиц или собственности или возникновению значительного страха в связи с возможностью осуществления таких последствий [17, с. 1].

Также к наиболее удачным следует отнести определение, предложенное американским исследователем К. Уилсоном: «…это использование компьютеров как оружия политически мотивированными международными или национальными группами или тайными агентами, которые наносят или угрожают нанести ущерб или посеять панику с целью повлиять на население или правительство для изменения политики» [18].

Кибертерроризм — это вид террористической деятельности, который заключается в намеренной комплексной атаке на компьютерную информацию, включая захват, выведение из строя и разрушение объектов, создает угрозу возникновения чрезвычайной ситуации в телекоммуникационных сетях, причинения значительного имущественного ущерба либо наступления иных подобных опасных последствий. Такое совершают с целью нарушить общественную безопасность, запугать население, спровоцировать военный конфликт, усугубить международные отношения, оказать влияние на органы власти или привлечь внимание общественности к определенным политическим, религиозным или другим организациям. Характерным отличием кибертерроризма от киберпреступности является его открытость, когда требования террориста широко оповещаются.

Общеизвестно, что экономика и обороноспособность государств сегодня в значительной степени зависит от нормального функционирования глобальных компьютерных сетей. А нарушение их работоспособности приводит к довольно серьезным последствиям. Но современные государственные и международные правовые институты, организационные структуры плохо подготовлены к адекватному противодействию новым угрозам.

И это глобальная проблема, сегодня ни одно государство не может преодолеть ее последствия самостоятельно. Особенно развитые страны, где зависимость от новых информационных технологий наибольшая. Соответственно, увеличение такой зависимости автоматически приводит к увеличению убытков, угрозы национальной безопасности. А это обусловливает необходимость вкладывать еще большие средства для создания действенных систем защиты, которые к тому же требуют постоянного обновления.

По данным «Лаборатории Касперского», для предотвращения опасных киберугроз в мире есть специально созданное кибероружие (программные и аппаратные средства). Современные информационные системы, форумы, порталы и др. заставили человечество отказаться от тайны частной жизни и подсознательно сделало его публично доступным, что также приводит и к взлому мобильных гаджетов (большинство людей ежедневно пользуется различными средствами коммуникации: мобильными телефонами, смартфонами, ноутбуками и т. д., которые являются объектами посягательства со стороны киберпреступников и кибертеррористов).

Учитывая вышеизложенное, к кибертерроризму на территории России и в странах Центральной Азии можно отнести: незаконные вмешательства в работу компьютерных систем и сетей, кражу, присвоение, вымогательство компьютерной информации, организацию удаленной атаки на информационные ресурсы, закладку и разработку компьютерных вирусов, которые осуществляют снятие, модификацию или уничтожения такой информации. Для информационных актов характерны такие средства преступной деятельности, как компьютерные вирусы, логические бомбы, «троянские кони» и прочее [1, с. 43].

При этом особый интерес для кибертеррористов представляют государственные информационные системы, объектами их деятельности становятся важные элементы государственной инфраструктуры (системы управления и функционирования атомных объектов, электростанций, железных дорог, аэропортов и т. п.).

Кибертерроризм является видовым, а информационный терроризм — это родовое понятие одного негативного явления — терроризма.

Кибертерроризм может рассматриваться как угроза кибернетической безопасности. Специальными субъектами обеспечения кибернетической безопасности являются государственные органы, кроме общих функций, уполномоченные на осуществление борьбы с киберпреступностью и кибертерроризмом, а также на обеспечение кибернетической защиты объектов национальной критической инфраструктуры.

Кибертерроризм направлен на проникновение в информационно-телекоммуникационную систему, перехват управления, подавления средств сетевого информационного обмена и осуществления других деструктивных действий. Опасность такого вида информационного терроризма состоит в том, что он не имеет национальных границ и в проблематичности выявления террориста в информационном пространстве, ведь хакеры осуществляют террористическую деятельность через подставные компьютеры, что затрудняет его идентификацию и определение местонахождения.

Кибертерроризм — это вид террористической деятельности, который заключается в намеренной комплексной атаке на компьютерную информацию, включая захват, выведение из строя и разрушение объектов, создает угрозу возникновения чрезвычайной ситуации в телекоммуникационных сетях, причинения значительного имущественного ущерба, либо наступления иных общественно опасных последствий. Такие атаки совершают с целью нарушения общественной безопасности, устрашения населения, провокаций военного конфликта, осложнения международных отношений, оказания влияния на органы власти или привлечение внимания общественности к определенным политическим, религиозным или другим организациям. Характерным отличием кибертерроризма от киберпреступности является его открытость, когда требования террориста широко оповещаются.

На сегодня кибертерроризм в России и странах Центральной Азии является одним из самых опасных видов преступности. Кибератаки могут нанести значительный ущерб на локальном, государственном и даже международном уровне. Ведь внешние кибератаки могут преследовать и более серьезные цели, чем пассивный сбор данных, а объектами кибертерроризма могут быть денежная и секретная информация, аппаратура контроля над космическими приборами, ядерными электростанциями, военными комплексами и тому подобное.

Библиографический список

1. Мазуров В. А. Кибертерроризм: понятие, проблемы противодействия // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1–1 (21).

2. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В. С. Овчинский. М., 2017.

3. Старостина Е. Подход к выработке единого понятия «кибертерроризм» (научное обоснование, сравнительная характеристика) // Право и жизнь. Независимый правовой журнал. 2006. № 101.

4. Старостина Е. В., Фролов Д. Б. Защита от компьютерных преступлений и кибертерроризма: вопросы и ответы. М., 2005.

5. Степанов О. А. Актуальные проблемы противодействия кибертерроризму : монография. М., 2014.

6. Тропина Т. Л. Киберпреступность и кибертерроризм // Организованная преступность, терроризм и коррупция. Криминологический ежеквартальный альманах. М., 2003. Вып. 2.

7. Тропина Т. Л. Киберпреступность и кибертерроризм: договоримся о понятиях // Проблемы преступности: традиционные и нетрадиционные подходы : сборник статей. М., 2003.

8. Услинский Ф. А. Кибертерроризм в России: его свойства и особенности // Право и кибербезопасность. 2014. № 1 (4).

9. Молодчая Е. Н. Политика противодействия кибертерроризму в современной России: политологический аспект : автореф. дис. … канд. политич. наук: 23.00.02. М., 2011.

10. Молодчая Е. Н. Политика противодействия кибертерроризму в современной России: политологический аспект : дисс. … канд. политич. наук: 23.00.02. М., 2011.

11. Зарубин С. В. Разработка алгоритмов и моделей противодействия кибертерроризму : автореф. дис. … канд. тех. наук: 05.13.18, 05.13.19. Воронеж, 2009.

12. Блокчейн технологии в противодействии рискам кибертерроризма : монография / Е. А. Антонян, И. И. Аминов, М. В. Рукинов и др. ; под общей ред. Е. А. Антонян. М., 2019.

13. Критически важные объекты и кибертерроризм : монография : в 2 ч. / О. О. Андреев и др. ; под ред. В. А. Васенина. М., 2008.

14. Правовое регулирование борьбы с киберпреступностью, кибертерроризмом и трафиком людей: опыт Европейского Союза / отв. ред. В. Г. Киютин, А. П. Новиков. Бишкек; М., 2010.

15. Cyber Warfare and Cyber Terrorism (edited by Lech J. Janczewski and Andrew M. Colarik). Hershey, PA: Information Science Reference, 2008.

16. Thackrah J. R. Dictionary of Terrorism. NY.: Taylor & Francis, 2004.

17. Myriam Dunn Cavelty. Cyberwar: concept, status quo, and limitations [Electronic resource] / Center for Security Studies (CSS), ETH Zurich. Access mode: www.sta.ethz.ch

18. Clay W. Computer Attack and Cyberterrorism (Vulnerabilities and Policy Issues for Congress) [Electronic resource] / Federation of American Scientists. URL: http://www.fas.org/sgp/crs/terror/index.htm