УДК 343.7

В.А. Мазуров

Кибертерроризм: понятие, проблемы противодействия

На основе анализа нормативных, научных и официальных источников дано определение кибертерроризма, кибертеракта, рассматриваются некоторые способы совершения преступлений террористической направленности, а также проблемы противодействия терроризму.

Ключевые слова: терроризм, компьютерные преступления.

Современный этап развития мирового сообщества характеризуется стремительным развитием научно-технического прогресса, в который включается и сфера высоких технологий. В Окинавской хартии глобального информационного общества отмечалось, что «...информационные телекоммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI в. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Информационно-коммуникационные технологии быстро становятся важным стимулом развития мирового сообщества» [1]. Вместе с тем, развитие научно-технического прогресса всегда сопровождается всплеском негативных общественных проявлений, в частности таких, как преступность.

Одновременно с развитием компьютерной техники появилась преступность, связанная с электронной обработкой информации, в том числе и преступность террористической направленности – «Террористический акт» (ст. 205 УК РФ), «Содействие террористической деятельности» (ст. 205-1), «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма» (ст. 205-2), «Заведомо ложное сообщение об акте терроризма» (ст. 207). По мнению специалистов, терроризм с использованием последних достижений в сфере высоких технологий не менее опасен, чем ядерный или бактериологический терроризм.

Арсенал компьютерных террористов – различные вирусы, логические бомбы – команды, встроенные заранее в программу и срабатывающие в нужный момент. Современные террористы используют Интернет в основном как средство пропаганды, передачи информации, а не как новое оружие. Однако можно предполагать, что компьютерный терроризм сегодня уже представляет реальную угрозу обществу. В настоящее время существует весьма мало систем, которые можно назвать надежно защищенными.

В связи с тем, что компьютерный терроризм уже представляет собой реальность, необходимо закрепить на государственном уровне обязанность государственных структур по разработке и внедрению технических, правовых и организационных мер, обеспечивающих защиту компьютерных сетей как одного из уязвимых элементов современного российского общества.

В российской юридической литературе проблемы компьютерного терроризма (кибертерроризма), его определение рассматриваются весьма слабо. Рядом авторов под кибертерроризмом понимается совокупность противоправных действий, связанных с покушением на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимущества при решении политических, экономических или социальных задач [2]. В.А. Голубев под кибертерроризмом понимает преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [3]. По мнению Ю.В. Гаврилова и Л.В. Смирнова, сущность кибертерроризма заключается в оказании противоправного воздействия на информационные системы, совершенного в целях создания опасности причинения вреда жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности [4]. Проблемы кибертерроризма рассматриваются в научных работах А.И. Примакина, В.Е. Кадулина, Ю.И. Жукова, В.И. Антюхова, Е.П. Кожушко, В. Замкового, М. Ильчикова и ряда других.

Террористический акт с использованием высоких технологий (кибертеракт). Рост и глобализация экономики, насыщенность её новыми телекоммуникационными технологиями, компьютеризация таких жизненно важных сфер деятельности общества как связь, энергетика, транспорт, системы хранения и транспортировки нефти и газа, финансовая и банковская системы, оборона и национальная безопасность, структуры обеспечения работы министерств и ведомств, переход на методы электронного управления технологическими процессами в производстве, по мнению российских и зарубежных экспертов, являются причиной все большего распространения террористических акций с помощью высоких технологий. На конференции по проблемам защиты от кибертеррора (США, Вашингтон, 2000 г.) отмечалось, что «...электронный терроризм – это не теория. Это реальность» [5]. Кибертерроризм является серьезной угрозой для страны, где есть банковская, транспортная и энергетическая системы, особенно для страны, в которой правительство, государственный и частный сектор экономики опираются на информационные сети и быстрый доступ к высоким технологиям. Отмечается стремительный рост пользователей сети Интернет. Так, в США их уже порядка 158 миллионов, в Европе – 95 миллионов, в Азии – 90 миллионов, в Африке – 3 миллиона. В России количество таких пользователей около 8 миллионов человек. Сегодня Интернет охватывает все страны мира, так как с применением новых технологий (использование мобильных спутниковых устройств связи) возможно подключение к сети Интернет с любой точки земного шара.

Преступление, совершенное в киберпространстве, – это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютера, компьютерных сетей и программ.

Под термином «кибертеракт» понимаются, как правило, действия по дезорганизации информационных систем, устрашающие население и создающие опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях [6].

Кибертеракт – это серьезная угроза человечеству, сравнимая с ядерным, бактериологическим и химическим оружием. Степень этой угрозы в силу своей новизны не в должной мере осознана и изучена. Кибертеракт не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. Обнаружить и нейтрализовать виртуального террориста весьма проблематично из-за слишком малого количества оставляемых им следов и их виртуальной специфики.

Террористический акт с использованием высоких технологий – это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информационные системы, создающая реальную опасность для жизни людей или наступления иных тяжких последствий.

Кибертеррористы не только совершают террористические акты с помощью электронных сетей, но и имеют возможность получать доступ к конфиденциальной информации, государственной тайне. На многих сайтах государственных органов власти выложены сведения различной степени важности. Например, схемы подземных коммуникаций, строящиеся стратегические объекты, расположение объектов жизнеобеспечения. В дополнение к этому преступники могут получить доступ к личным данным многих пользователей сети, начиная с адреса и номера телефона и заканчивая подробной информацией о личности [7].

Директор Центра защиты национальной инфраструктуры ФБР США Рональд Дик в докладе, опубликованном на сайте Федерального бюро расследований, отмечает, что «...в мире сформировалась новая форма терроризма – «кибертерроризм», который использует компьютер и сети связи для разрушения частей национальной инфраструктуры и достижения своих целей. Мы каждый день сталкиваемся с компьютерными атаками на правительственные организации. Ахиллесова пята современного мира – растущая зависимость от компьютерных систем и информационных технологий» [8].

В отличие от обычного террориста, который для достижения своих целей использует взрывчатку или стрелковое оружие, кибертеррорист использует современные информационные технологии, компьютерные системы и сети, специальное программное обеспечение, предназначенное для несанкционированного проникновения в компьютерные системы и организации удаленной атаки на информационные ресурсы жертвы. В первую

очередь – это компьютерные программные закладки и вирусы, в том числе и сетевые, осуществляющие съём, модификацию или уничтожение информации, так называемые «логические бомбы», «троянские» программы и иные виды информационного оружия [9].

В киберпространстве могут быть использованы различные приемы для совершения террористического акта:

– нанесение ущерба отдельным элементам киберпространства, разрушение сетей электропитания, наведение помех, использование специальных программ, стимулирующих разрушение аппаратных средств;

– хищение или уничтожение информационного, программного и технического ресурсов киберпространства, имеющих стратегическую значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок;

– воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления; раскрытие и угроза опубликования закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодов шифрования, принципах работы систем шифрования;

– захват каналов телекоммуникационного вещания с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;

– уничтожение и активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммуникации, воздействие на операторов, разработчиков информационных и телекоммуникационных систем с целью совершения ими перечисленных выше действий [10].

Информационный террористический акт отличается от форм воздействия на киберпространство, прежде всего своими целями, которые остаются свойственными политическому террористическому акту. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия. В то же время тактика и приемы информационного террора существенно отличаются от тактики информационной войны и приемов информационного криминала. Главное в тактике информационного террора состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен населению и получил большой общественный резонанс.

Кибертеракт ориентируется на использование различных форм и методов вывода из строя информационной инфраструктуры государства или на использовании информационной инфраструктуры для создания обстановки, приводящей к катастрофическим последствиям для общества и государства. Существует прямая зависимость между степенью развития информационной инфраструктуры, компьютеризацией страны и количеством актов кибертеррора. В настоящее время проблема кибертеррактов актуальна для стран, лидирующих в области использования систем спутниковой связи и глобальных сетей.

Основным способом террористического акта в сфере высоких технологий является 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.

Информационные атаки высокого уровня подразделяют на две большие категории:

– выведение из строя информационных систем. Хакерские атаки этого типа являются наиболее распространенными, они направлены на временное выведение из строя отдельных систем управления и контроля или искажение программной информации. Результат таких действий – бесконтрольное функционирование поражаемого объекта, что особо опасно на направлениях атомного, химического производства, а также в военной сфере – электронные системы защиты и нападения;

– разрушительные атаки. Информационные террористические операции против объектов информационных систем могут привести к уничтожению информационных ресурсов и линий коммуникаций либо к физическому уничтожению структур, в которые включаются информационные системы. Если системы задействованы в критических инфраструктурах, то при наихудшем развитии событий сетевые информационные атаки могут привести к столь же масштабным последствиям, что и традиционные террористические акты, осуществленные с помощью взрыва.

До недавнего времени информационная инфраструктура России не представлялась сколько-нибудь уязвимой в отношении рассматриваемых террористических актов. Причи-

ной этого в первую очередь можно считать низкий уровень её развития, а также наличие значительной доли неавтоматизированных операций при осуществлении процесса управления. Вместе с тем в последние годы многие государственные и коммерческие структуры приступили к активному техническому переоснащению своих предприятий, организаций. Информационная составляющая таких организаций реализуется практически исключительно на технических и программных средствах иностранного производства, что в определенной степени повышает угрозу успешных атак со стороны кибертеррористов.

Научно-технические достижения и инновации, ускорившие глобализацию, а также рост производительности и благосостояния в мире могут быть использованы отдельными лицами или группировками как средство террора. Компьютерный террористический акт способен стать действенным орудием массовой дезорганизации. Уже сегодня кибертеррорист может нанести больший вред, используя в преступном арсенале вычислительную машину, нежели взрывное устройство [3]. Информационные технологии рассматриваются как средство, помогающее террористам объединяться в группировки, действовать скрытно и совершать нападения на элементы национальных инфраструктур. Все более доступными для террористов становятся средства, позволяющие разрушить компьютерные системы и другие электронные устройства.

Особую угрозу мировым информационным системам представляет соединение технологического и научного потенциала развитых стран и особенно России. Ситуация осложнена тем, что нормативная база, на основе которой ведется контроль за экспортом высоких технологий из развитых стран, не в должной мере отвечает серьезности угрозы. Совершать кибертеракты сегодня способна любая из существующих в настоящее время террористических организаций – Ирландская организация ИРА, «Аль-Кайда», баскская организация ЭТА, религиозные движения типа алжирских или египетских фундаменталистов, чеченские незаконные вооруженные формирования и т.п. [7].

Таким образом, высокотехнологичные террористические акции новой эпохи способны сегодня продуцировать системный кризис всего мирового сообщества и поставить под угрозу существование отдельных регионов мира, что не было характерно для традиционных террористических актов.

Литература

1. Окинавская хартия глобального информационного общества. Принята 22 июля 2000 г. // Дипломатический вестник. – 2000. – № 8 [Электронный ресурс]. – Режим доступа: http://www.mcrt.ru/index.php?nodeid=1218, свободный (дата обращения: 24.05.2010).

2. Васенин В.А. Информационная безопасность и компьютерный терроризм [Электронный ресурс]. – Режим доступа: www. crime-research.ru, свободный (дата обращения: 24.05.2010).

3. Голубев В.А. Кибертерроризм – узроза национальной безопасности [Электронный ресурс]. – Режим доступа: www.crive-research.ru, свободный (дата обращения: 24.05.2010).

4. Гаврилов Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю.В. Гаврилов, Л.В. Смирнов. – М.: ЮИ МВД РФ, 2003. – 66 с.

5. Сайтарлы Т. Опыт США в расследовании компьютерных преступлений [Электронный ресурс]. – Режим доступа: www.crime-research.org/news/2000/09, свободный (дата обращения: 24.05.2010).

6. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. – № 10. – С. 24–25.

7. Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2001: угрозы и нейтрализация [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/articles/vagif, свободный (дата обращения: 24.05.2010).

8. Гриняев С. США развертывают систему информационной безопасности. В России же дальше разговоров дело пока не идет: независимое военное обозрение № 45 (405) [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/ security /part3 /rus-edu.shtml, свободный (дата обращения: 24.05.2010).

9. Безруков Н.Н. Компьютерные вирусы. – М.: Наука, 1991. – 159 с.

10. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. – М.: Право и закон, 1998. – С. 29–37.

Мазуров Валерий Анатольевич
Канд. юр. наук,Доцент каф. уголовного права и криминологии,
Алтайский государственный университет,г. Барнаул
Тел.: (385-2) 36-73-77, т.р. (385-2) 26-20-91, 8-903-995-79-51
Эл. адрес: sas@asu.ru

V.A. Mazurov
Cyberterrorism: concept, counteraction problems

The author of the article defines cyberterrorism and cyberact of terrorism. The definitions are based upon the analysis of standard, scientific and official sources. The author considers some ways of committing crimes of terrorism and also a problem of counteraction of terrorism.
Keywords: terrorism,computer crimes.