Терроризм носит международный характер и, в соответствии с рядом международных документов, относится к числу международных преступлений. В свою очередь, кибертерроризм и информационный терроризм — это новые формы проявления терроризма. Рассмотрим сначала кибертерроризм.

Эта форма вызывает особую озабоченность у экспертов в связи с высокой уязвимостью компьютерных систем управления критической инфраструктурой (транспорт, атомные электростанции, водоснабжение и энергетика), подключённых к сети Интернет. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии.

В свою очередь, эксперты рассматривают кибертерроризм как преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создаёт 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. [1]

Основная суть кибертерроризма заключается в осуществлении противоправного воздействия на информационные системы, совершенного в целях создания опасности причинения вреда жизни, здоровью или имуществу неопределённого круга лиц путём создания условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности[2].

Термин «киберпространство» означает место, в котором действуют компьютерные программы и перемещаются данные. Цель кибертеррористов — вычислительные системы, управляющие различными процессами, и циркулирующая в них информация. Условно кибертерроризм можно разделить на два вида:

1) совершение с помощью компьютеров и компьютерных сетей террористических действий;

2) использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов.

Первый вид кибертерроризма представляет собой умышленные атаки на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающие опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Подобные действия совершаются в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти.[3]

Компьютерные хакеры сканируют Интернет в поисках компьютерных систем, имеющих ошибки в конфигурации (это совокупность настроек программы, задаваемая пользователем) или недостаток необходимого программного обеспечения для защиты. Единожды заражённый вредоносной программой компьютер может попасть под удалённый контроль хакера, который через Интернет имеет возможность наблюдать за содержимым компьютера или использовать его для атаки на другие компьютеры. Лёгкой мишенью являются носители, имеющие ошибки в программном обеспечении, конфигурации, недостатки антивирусной программы, иногда даже антивирусные программы содержат вредоносный вирус.

Приёмы кибер-атак: вирусы, сетевые черви, которые уничтожают информацию или блокируют работу вычислительных систем, так называемые логические бомбы — команды, встроенные заранее в программу и срабатывающие в нужный момент, «троянские кони», которые выполняют определённые запрограммированные действия, средства подавления информационного обмена в сетях и организации DdoSатак (отказ в обслуживании). [4]

Информационный терроризм — воздействие на сознание и психику масс с целью формирования необходимых террористам суждений и мнений, которые в дальнейшем определённым образом направляют поведение людей. Виды информационного терроризма:

1) информационно-психологический терроризм — контроль над СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористических организаций; воздействие на операторов, разработчиков, представителей информационных и телекоммуникационных систем путем насилия или угрозы насилия, подкупа, введения наркотических и психотропных средств, использование методов нейролингвистического программирования, гипноза, средств создании иллюзий, мультимедийных средств для ввода информации в подсознание и т. д.;

2) информационно-технический терроризм — нанесение ущерба отдельным физическим элементам информационной среды государства; создание помех, использование специальных программ, стимулирующих разрушение систем управления, или, наоборот, внешнее террористическое управление техническими объектами (в т. ч. самолётами), биологические и химические средства разрушения элементной базы и т. д.; уничтожение или активное подавление линий связи, неправильное адресование, искусственная перегрузка узлов коммутации и т. д.[5]

Очевидно, что кибератаки, исходя из целей и методов информационного воздействия, могут быть отнесены к одному из видов информационного терроризма. Деструктивные воздействия же при этом всегда будет осуществляться с применением киберпространства. Из вышеизложенного видно, что термин «информационный терроризм» является более общим, чем «кибертерроризм»; охватывает вопросы использования разнообразных методов и средств информационного воздействия на различные стороны человеческого общества (физическую, информационную, когнитивную, социальную).

Вербовка используется для мобилизации симпатизирующих лиц к более активной поддержке террористов и их действий. Глобальный охват сети предоставляет террористам беспрецедентный уровень прямого контроля над содержанием своих посланий. Это значительно повышает их возможности для формирования восприятия у различной целевой аудитории и манипулирования не только своим образом, но и образом своих врагов. Террористами используются большие возможности интерактивных коммуникаций для содействия своим группам в соцсетях и даже прямого контакта с их подписчиками. Таким образом, для террористов — это довольно лёгкий способ донести свою мысль в сознание масс, пропагандировать свою идеологию большему количеству людей. В конечном счёте, путём использования форумов можно втянуть в дискуссию публику — не важно, если это сторонники этой группы или противники, что может помочь террористам обозначить свою позицию и тактику и потенциально увеличить уровень поддержки и общей привлекательности. Таким образом, террористы предают публичности свою деятельность. Информационный «вброс» в массы, дезинформация, сведения о лидерах, манифестах, публикация видео с угрозами и массовыми казнями — есть не что иное, как средство психологического воздействия на сознание, виртуальная война. В настоящее время насчитывается более 5 тыс. веб-сайтов, созданных и поддерживаемых организациями, которые международное сообщество признало террористическими. Некоторые из них создаются сразу на множестве популярных языков, создавая массированный источник пропаганды.[6]

Ведущие мировые державы признают, что угроза кибертерроризма и информационного терроризма является актуальной проблемой современности глобального характера, причём она будет неуклонно нарастать по мере развития и распространения информационных технологий. Поэтому эффективное международное сотрудничество в области предупреждения и ликвидации последствий кибер- и информационных атак имеет огромное значение. Однако на данный момент нет эффективных международных нормативно правовых актов, предупреждающих подобные атаки.

Список литературы

1. Голубев В. А. Кибертерроризм. Угроза национальной безопасности [Электронный ресурс].
2. Будник Г. И. Кибертерроризм как угроза основам конституционного строя Российской Федерации: понятие, сущность и проблемы противодействия // Молодой ученый. — 2016, № 8.
3. Голубев В. А. Кибертерроризм — миф или реальность? [Электронный ресурс].
4. Компьютерная атака и кибертерроризм: уязвимость и политические вопросы для Конгресса данных [Электронный ресурс]. — URL: http://www.crime.vl.ru/index.php?p=1025&more=1
5. Королев А. Киберпространство и информационный терроризм // Центр анализа террористических угроз [Электронный ресурс]. — URL: http://www.catu.su/analytics/1250-kiberprostranstvo-i-informacionnyj-terrorizm
6. Проблема терроризма в сети Интернет [Электронный ресурс]. — URL: http://www.sibsiu.ru/antiterror/?p=111