4. Кибертерроризм как часть терроризма в информационной среде

Число совершаемых преступлений в глобальном информационном пространстве стремительно растет год от года. Однако, несмотря на то, что на данный момент лидирующие позиции среди киберпреступлений занимают преступления экономической направленности, все большие обороты набирают преступления террористического характера, совершенные посредством использования «высоких технологий». Этому способствуют преимущества глобальной сети, обладающей многими возможностями, в том числе: простота доступа, широкая аудитория, независимость от географического расположения, высокая скорость обмена информацией, анонимность и что, немаловажно – трудности в обнаружении и осуществлении контроля правоохранительными органами. Сейчас для общения с единомышленниками, преступникам не нужно собираться на конспиративных квартирах или организовывать «тайные кружки», для этого необходимо всего лишь иметь персональный компьютер или мобильный телефон, имеющий выход в Интернет. Вследствие чего виртуализированные террористические решения могут беспрепятственно и бесконтрольно проникать в каждый дом. К тому же число пользователей «всемирной сети» стремительно увеличивается год от года и на сегодня уже насчитывает примерно 3,4 миллиардов пользователей, причем в России данная цифра составляет 85 миллионов человек в возрасте более 12 лет или 69 % населения. Глобальная сеть сегодня охватывает практически все сферы общества, что формирует у современного человека так называемую компьютерную зависимость, в связи с чем, кибертерроризм можно назвать самой опасной угрозой для государства и общества в целом, требующей проведения тщательного анализа и исследования самой сущности терроризма и методов борьбы с ним.

Проблемой кибертерроризма сегодня озабочено все мировое сообщество, поскольку имеющиеся сведения в этой области указывают о несомненной уязвимости любого государства, учитывая, что кибертеррорист имеет возможность угрожать информационным системам, которые могут быть расположены практически в любой точке земной поверхности. При этом найти и обезвредить виртуального террориста весьма непросто по причине небольшого количества оставляемых преступником следов, чего нельзя сказать о реальном мире, в котором следов совершенного преступления остается намного больше.

Для осуществления своих преступных намерений кибертеррористы привлекают высококлассных хакеров, которые взламывая сайты, обеспечивают им доступ к разного рода информации, включая секретную. Преступники получают доступ к личным данным многих пользователей сети, которые в последующем используют для их вербовки, похищают конфиденциальные данные о кредитных картах, что дает им возможность воровать деньги.

Термин «кибертерроризм» вошел в нашу жизнь в середине 1980-х годов, его автором стал Бэрри Коллин, работавший старшим научным сотрудником

в американском Институте безопасности и Разведки. Термин обозначал террористические действия в виртуальном пространстве и применялся только для прогнозов на будущее. Сам автор нового термина не мог и предположить, что о реальном кибертерроризме заговорят уже через десятилетие.

Среди всех разновидностей киберпреступлений, спектр которых стремительной увеличивается год от года, выделяют 2 основных вида кибертерроризма:

- первый вид, это кибертерроризм в так называемом «чистом виде», когда террористические действия совершаются с помощью компьютеров и компьютерных сетей,
- второй вид – это использование глобального информационного пространства в организационно-коммуникационных целях террористических групп.

Для первого вида кибертерроризма характерны следующие инструменты совершения:

- различные виды атак, которые позволяют несанкционированно проникнуть в атакуемую сеть или перехватить управление сетью;
- распространение компьютерных вирусов, которые модифицируют и уничтожают информацию или блокируют работу вычислительных систем;
- введение в программу логических бомб, срабатывающих при определенных условиях;
- использование так называемых «троянских коней», позволяющих выполнять вредоносные действия без ведома владелица зараженной системы;
- средства нарушения и подавления информационного обмена в сетях.

По сведениям аналитиков, наибольший интерес для террористов представляют следующие сферы: военная и ядерная, энергетическая, финансовая, сфера транспортных перевозок, в том числе воздушный транспорт. Так, в 2007 году Израильская армия опробовала форму ведения кибервойны. Военным хакерам из Израиля удалось тайно внедрить «троянский вирус» в код программного обеспечения сети сирийской противовоздушной обороны, благодаря чему израильтяне получили возможность управлять системой противовоздушной обороны противника. Поэтому, когда израильские самолеты наносили удары по атомной энергетической установке в Сирии, на экранах сирийских радаров было все спокойно.

Вирус «Flame» сегодня является наиболее мощным средством компьютерного шпионажа и относится к категории сложного кибероружия. С его помощью могут быть элементарно взломаны военные и пассажирские лайнеры, оборудованные чипом со встроенной функцией контроля полета, посредством доступа к микрочипу через Интернет. Взломщик получает доступ к системе управления движением самолета и имеет возможность вывести машину из строя.

В качестве примера террористической киберугрозы ядерной структуре государства, можно привести многократные кибератаки на ядерные системы

Ирана. В компьютерной системе Иранского центра по обогащению урана в 2010 году был обнаружен вирус под названием «Stuxnet», годом позже атомная структура Ирана подверглась атаке вирусом, получившим название «Stars», а еще через год, в 2012 году наиболее опасным вирусом «Flame», причинившими значительный ущерб ядерной безопасности Ирана.

Часто обвинения государств в совершении кибератак выдвигаются абсолютно безосновательно. В причастности российских хакеров к кибератакам, повлиявшим на результаты выборов президента США в ноябре 2016 года, в ходе которых президентом был избран Дональд Трамп, заявили члены демократического меньшинства в Конгрессе США, призвав к созданию независимой комиссии для расследования «вмешательства России в выборы в США». При этом обвинения были выдвинуты при отсутствии всяческих доказательств со стороны американской разведки. Данный факт начальник пресс-службы Госдепартамента США Джон Кирби объяснил стремлением защитить источники информации и методы работы американских спецслужб.

Второй вид кибертерроризма, заключающийся в использовании глобального информационного пространства в организационно-коммуникационных целях террористических групп тоже представляет собой серьезную социально опасную угрозу для человечества, которую нельзя недооценивать. К данному виду кибертерроризма относятся:

- сбор информации, используемой для планирования терактов; сбор денежных средств для поддержки террористических движений;
- проведение террористическими группами агитации и пропаганды о своих целях и задачах, планируемых действиях, формах протеста;
- проведение информационно–психологического воздействия на массовую аудиторию с целью шантажа, создания паники, распространения ложной информации и тревожных слухов;
- проведение организационной деятельности, включая размещение в открытом доступе инструкций по самостоятельному изготовлению взрывных устройств, сообщений о времени встреч заинтересованных людей и тому подобное;
- анонимная вербовка и привлечение к террористической деятельности соучастников, оказывающих различные информационные услуги, включая бизнесменов и хакеров;
- расширение потенциала малых террористических групп, имеющих возможность осуществлять свои операции децентрализованно, применяя коммуникационные технологии для планирования и координации своих действий.

Помимо интернет-сайтов, созданных террористическими организациями, для организации взаимодействия террористы активно используют в своих преступных целях социальные сети, авторские блоги, интернет-форумы, известные видеопорталы, где в свободном доступе размещают видеозаписи, пропагандирующие экстремистские идеи «джихада». История «Сирийской весны» во многом была большой технологической ошибкой правительства Башара Асада. После разблокировки социальных

сетей правительством государства в 2011 году в социальных медиа оппозицией стали активно размещаться видеообращения террористической направленности, так основатель «Свободной армии Сирии» в YouTube-обращении заявил: «Этот режим можно убрать лишь силой и кровопролитием. В любом случае наши потери не будут больше, чем сейчас, когда правительство пытает и убивает наших людей, выбрасывая их тела на свалки». Вскоре блокировать социальные интернет сервисы в Сирии стало некому, на смену законному правительству пришли новые «звёзды ютюба» – исламские боевики.

Широкое распространение среди экстремистски настроенной молодежи получил флэшмоб, который представляет собой заранее спланированную массовую акцию, в которой большая группа людей, сбор которой организуется посредством сети Интернет, появляется в общественном месте и выполняет заранее оговоренные действия. Можно казать, что за последние десять лет террористические организации прочно обосновались во всех сегментах Интернета и используют его в качестве основного инструмента по распространению своих идей.

Следует отметить, что активная борьба с кибертерроризмом ведется всем мировым сообществом, однако, несмотря на это, с каждым годом число комментариев, содержащих призывы к насилию и совершению террористических действий в социальных сетях возрастает.

По заявлению руководителя антитеррористического центра СНГ Андрея Новикова на 15-м совещании руководителей спецслужб органов безопасности и правоохранительных органов иностранных государств-партнеров ФСБ РФ, состоявшемся в июле 2016 года, за последние 10 лет в антитеррористическую повестку дня все чаще включаются проблемы использования террористами новых информационно-коммуникационных технологий, а опасность их проявлений и масштабы распространения год от года возрастают. Было отмечено, что сегодня важно сформировать и опробовать технологии своевременного выявления и нейтрализации попыток совершения террористами кибердиверсий.