**Кибертерроризм как новая форма терроризма**

**Введение**

Глобализация информационных процессов, также современной экономики, насыщенность ее новыми информационно-телекоммуникационными технологиями, информатизация таких жизненно важных сфер деятельности общества, как связь, энергетика, транспорт, системы хранения газа и нефти, финансовая и банковская системы, водоснабжение, оборона и национальная безопасность, открыла не только доселе новые, невиданные, впечатляющие возможности для прогрессивного развития человечества, но и вызвала одновременно ряд качественно новых глобальных угроз. С каждым годом использование информационных технологий охватывает все новые сферы жизнедеятельности. Информация как один из ключевых элементов этого процесса начинает играть все более важную роль в жизни человека, общества, государства на современном этапе развития.

Информационная безопасность является неотъемлемой составляющей концепции национальной безопасности, и чем глубже информатизация охватывает основные сферы жизнедеятельности человека, тем острее становится проблема информационной безопасности. Изменился мир, а вместе с ним и общество, а также характер преступлений. Так, наряду с терроризмом в мировом масштабе в связи с процессами глобализации и интеграции в обществе, переустройством мира грядет и изменение самих угроз, в частности угроза кибертерроризма не понаслышке знакома спецслужбам моих стран. И это угроза совсем не надуманна.

Специалисты по борьбе с терроризмом обеспокоены возможностью того, что террористические группировки могут прибегнуть к кибертерроризму во многих странах. Они предупреждают, что компьютеры могут быть использованы для нанесения серьезного удара по критически важным объектам инфраструктуры, что может привести к кровопролитию. Следовательно, терроризм и его проявления плавно перетекают в электронно-цифровую среду, поэтому и характер угроз террористов радикально меняется. Такие действия теперь приобретают новое название — «кибертерроризм», или «компьютерный терроризм».

**Глава 1. Понятие кибертерроризма**

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.

Само понятие **«кибертерроризм»** образовано слиянием двух слов: **«кибер»** («киберпространство») и **«терроризм»**. В русскоязычной литературе все чаще встречаются термины «виртуальное пространство», «виртуальный мир», что обозначает моделируемое с помощью компьютера информационное пространство, в котором существуют определенного рода объекты или символьное представление информации — место, в котором действуют компьютерные программы и перемещаются данные. Исходя из основного понятия терроризма и сочетания его с виртуальным пространством, можно вывести следующее определение. **Кибертерроризм** — это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта.

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.

Казалось бы, кибертерроризм угрожает в большей мере высокоразвитым в технологическом плане странам, например США. Но это только на первый взгляд. Мы уже могли наблюдать, как интенсивно развивается всемирная сеть Интернет, и какова динамика у компьютерной преступности. Ни в коем случае нельзя умолять его значения и для России.

В США проблема кибертерроризма стоит на одном из первых мест. Многие специалисты в Америке и Европе задают вопрос: как крупномасштабные и скоординированные атаки могли быть выполнены, если спецслужбы США контролируют все информационное пространство с помощью системы «Эшелон», в создании которой принимали участие спецслужбы США, Канады, Великобритании, Австралии и Новой Зеландии? На эту систему, предназначенную для тотального контроля электронных средств коммуникаций, были затрачены колоссальные средства. Но все безрезультатно.

Несмотря на «эшелонированность», террористы могут скоординировать свою деятельность и удачно провести акт терроризма. Этому может быть несколько объяснений:

· террористы использовали для взаимодействия неэлектронные средства телекоммуникаций;

· террористы маскировали свои сообщения с помощью криптографических или стенографических методов;

· алгоритм, заложенный в систему «Эшелон», неэффективен, или эта система предварительно была выведена из строя.

Террористы поддерживают свою деятельность другими преступлениями, совершенными через Интернет, например, получают доступ к базам кредитных карт или совершают различные формы прибыльного мошенничества. Информационные технологии также облегчают множество действий террористов и транснациональных преступных групп — от финансирования до создания необходимых документов. С помощью компьютерных технологий организованные преступные группы способны создать подложные документы, удостоверяющие личность, документы, свидетельствующие о ведении какой-либо деятельности, служащей прикрытием для их операций.

Использование информационных технологий преступниками и террористами происходило одновременно с ростом их легального использования международным сообществом. Возможность быстрого внедрения новых технологий в террористические и преступные организации обусловливается и тем, что современные преступные организации существуют в виде сетей, в которых есть ячейки. В отличие от традиционной мафии с ее иерархическими корпорациями, медленно реагирующими на новшества, новые транснациональные преступные группы обладают колоссальной гибкостью. Они имеют квалифицированных технических специалистов в своих структурах или нанимают их извне

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, в том числе радикального толка, 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, компьютерного хулигана или компьютерного вора, который действует в корыстных или хулиганских целях. Но если действия членов этой организации приведут к тяжким последствиям, например, 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 в основном страны с неразвитой экономикой страны), а во-вторых — сложное пространство для выявления самого террориста

Наиболее активно методы информационного воздействия применяет террористическое движение **«Хезболла»**, руководство которой рассчитывает таким образом нанести Израилю больший ущерб, чем при проведении обычных боевых операций. В структуре «Хезболлы» выделена группа программистов, в задачи которой входит создание и обновление веб-страницы в Интернете для пропаганды проводимых организацией акций и доведения направленной информации до израильтян.

Большое внимание «Хезболла» придает таким традиционным методам, как воздействие на аудиторию через средства массовой информации. Для вещания на территории Южного Ливана и Северного Израиля задействованы принадлежащие организации радио- и телевизионный каналы. Помимо материалов агитационного характера по ним регулярно демонстрируются записи, сделанные при проведении боевых операций против израильских войск и армии Южного Ливана. По оценке специалистов «Хезболлы», трансляция подобных передач способствует снижению боевого духа военнослужащих противника, появлению у них упаднических настроений.

По мнению аналитиков, большинство транснациональных террористических организаций придерживаются рационального подхода, добиваясь прежде всего политических целей и используя тактику террора в надежде на общественное признание законности своей борьбы. К ним применимы превентивные меры информационно-психологического и пропагандистского воздействия. Так, известная экстремистская организация «Хамас» приостановила проведение актов терроризма, когда против подобных атак в период подготовки палестино - израильского соглашения в Осло выступила ранее активно поддерживающая её часть мусульманского населения. Но существуют организации, которые действуют по совершенно иной логике. К ним, в частности, относятся Аум Синрике и «Аль-каида». Руководители этих организаций, обладая так называемой манией величия и являясь (мягко говоря) безжалостными людьми, действуют исключительно со своими собственными убеждениями и верят, что проводимые ими акты терроризма либо радикально изменят ход истории, либо их позднее оправдает сама история. По мнению экспертов, на таких террористов не оказывают какого-либо воздействия пропагандистская и психологическая составляющие информационных мер противодействия. Здесь потребуется использовать весь арсенал имеющихся сил и средств, консолидировать государственные и общественные структуры для выявления и пресечения террористической деятельности

В 2006 году по решению Кунцевского суда была депортирована из России гражданка США М. МаКри, которая, по представленным материалам ФСБ России, разрабатывала конкретные планы по взрывам Голливуда и ряда государственных учреждений США, активно пыталась вступить в контакт посредством Интернета с лидерами известных мусульманских террористических организаций

Для организации подобных кибератак необходима значительно большая 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 лежит прежде всего 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.

Таким образом, угроза кибертерроризма в настоящее время является очень серьезной проблемой. Ее актуальность будет возрастать по мере развития и распространения информационно-телекоммуникационных технологий.

Примерами таких кибератак являются:

Армения — Азербайджан. В феврале 2000г. армянские хакерские группы Liazor (уполномоченные), предприняли компьютерную диверсию против 20 сайтов правительственных организаций и средств массовой информации Азербайджана в системе Интернет (действия осуществлялись с территории Армении, России, США). Армянские хакеры США создали и внедрили специальную компьютерную программу «Synergy Internet Systems» обеспечивающую негласный перехват и снятие информации с компьютеров. Одна из групп в составе трех человек была вскрыта и задержана 4 февраля 2000 г. полицией в Лос-Анджелесе.

Россия — Чечня. С 1999г. предпринимаются усилия по блокированию и подавлению работы зарубежных порталов чеченского сепаратистского движения. Только в течение одной недели в конце апреля — начале мая 2002 г. портал «Кавказ» подвергся 140 атакам (в том числе массированным DOS - атакам).

Югославия — США (НАТО). Весной 1999г. в период боевых действий зафиксированы скоординированные действия югославских хакеров, направленные на блокирование компьютерных сетей управления группировки ОВС НАТО в Италии, а также политически мотивированные вторжения в сетевые порталы штаб-квартиры НАТО, Минобороны США, ряда других структур. Отслеживались также действия третьих сторон в контексте конфликта вокруг Косово (греческие хакерские группы студентов университетов г. Афины, Салоники, Кания согласованными действиями проникли в систему компьютерного центра ВС США на военном объекте в штате Аризона).

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

Искажение информации или блокирование работы информационных систем в финансовой сфере может иметь следствием экономический кризис, а выход из строя, скажем, электронно-вычислительных систем управления войсками и оружием — непредсказуемые необратимые последствия. Так, цели, на которые направлены атаки кибертеррористов, соответствуют национальной информационной инфраструктуре. Это:

· оборудование, включая компьютеры, периферийное, коммуникационное, теле, видео и аудиооборудование;

· программное обеспечение;

· сетевые стандарты и коды передачи данных;

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

· люди, задействованные в информационной сфере.

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 кибертерррристов могут стать как гражданские, так и военные объекты

Возможность захвата систем управления военными спутниками, наведения и запуска ракет, а также комплексами противовоздушной обороны уже давно существует. Примером может служить вывод из строя комплексов противовоздушной обороны Ирака во время операции «Буря в пустыне». Закладки, заложенные в комплексах противовоздушной обороны, стоявших на вооружении Ирака и купленных в основном в Европе, блокировали нормальную работу систем, и американские воздушные силы смогли практически беспрепятственно проникнуть в воздушное пространство этой ближневосточной страны

**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.

Еще одна цель кибертеррористических атак — разрушение объектов информационных систем. Это может привести к уничтожению информационных ресурсов и линий коммуникаций либо к физическому уничтожению структур, в которые включаются информационные системы. Если же системы задействованы в критических инфраструктурах, то при наихудшем развитии событий сетевые информационные атаки могут привести к столь же масштабным последствиям с жертвами, что и традиционные акты терроризма.

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.

Борьба с киберпреступностью, в частности с кибертерроризмом, имеет больше шансов на успех, если подходить к ней с различных сторон. Правовые средства - это лишь одна сторона. Однако важнее предупредить, чем реагировать, лучше предотвратить преступление прежде, чем оно случится, посредством превентивных мер.

Если обратиться к общей теории отечественной криминологии, то она выделяет два вида предупреждения преступности: общее (общесоциальное) и специальное. Первое реализует антикриминогенный потенциал общества в целом, всех его институтов. Второе имеет целенаправленный на недопущение преступлений характер. Общее (общесоциальное) предупреждение охватывает крупные, имеющие долговременный характер виды социальной практики в самом широком смысле этого слова. Особое внимание следует обратить на духовную сферу жизни общества, так как нравственность всегда противостоит преступности, а безнравственность интенсивно продуцирует ее.

Меры специального предупреждения преступности разнообразны и классифицируются по разным основаниям. Так, специально-криминологические меры различаются:

· по содержанию — экономические, политические, культурно-воспитательные и др.;

· по масштабам действия — общегосударственные, региональные и др.;

· по правовой характеристике — специально-криминологические: базирующиеся на нормах права, но ими не регламентированные, например правовое просвещение, воспитание, и детально урегулированные юридическими нормами, например административный надзор милиции за лицами, освобожденными из мест лишения свободы.

К превентивным мерам можно отнести повышение уровня образования в области понимания безопасности в киберпространстве, а также привлечение общественного внимания к проблеме информационного терроризма. Если люди будут знать, что представляет собой кибертерроризм и что он преследует, откуда исходит, а также как предотвращать попытки подобных кибератак, то, несомненно, процент киберпреступлений должен снизиться. Во всеобщем противостоянии террористической опасности трудно переоценить роль международного права. Именно на его основе международному сообществу удалось возвыситься над политико-идеологическими, национально-этническими, религиозными и иными противоречиями и предрассудками, сформировать систему глобального противодействия различным террористическим вызовам, в том числе через глобальную сеть Интернет.

Однако наличие огромной информационной системы, находящейся в частных руках, когда контроль над этой системой должен осуществляться государством, обусловливает очень серьезные препятствия регулированию и контролю. Существующая в США концепция публично-частных партнерств — идея, признанная не во всем мире. Она с трудом работает в Соединенных Штатах и часто действует как альтернатива: вместо правоохранительных органов Интернет контролируется провайдерами. И все же имеется законодательное «противоядие».

На международном уровне действуют более 12 универсальных антитеррористических договоров в борьбе с различными проявлениями терроризма на суше, на воде, в воздухе и в глобальном информационном пространстве — сети Интернет.

Современная система международного сотрудничества в борьбе с терроризмом сложилась в основном за последние четыре десятилетия. На глобальном уровне она функционирует под эгидой ООН и ее специальных учреждений, прежде всего ИМО, ИКАО и МАГАТЭ. Так, различные аспекты МИБ затрагиваются в документах «восьмерки» — таких, как Заключительный документ Совещания стран «группы семи» и России на уровне министров, состоявшегося в Париже 30 июля 1996 г.

В Заключительном документе зафиксирован комплекс конкретных мер, выработанных на уровне «восьмерки» и направленных на развитие сотрудничества между государствами в данной области. Это прежде всего внутренние меры по предотвращению терроризма: укрепление сотрудничества между внутригосударственными участниками борьбы с терроризмом во всех его проявлениях, в частности в области недопущения перемещений террористов, а также сдерживания, преследования и применения санкций против террористов.

Особого внимания заслуживает призыв в адрес государств рассмотреть вопрос об опасности, связанной с использованием террористами сетей и систем передачи информации в целях совершения преступных действий, и необходимости изыскания средств, соответствующих национальному законодательству, для предотвращения таких действий. Немаловажна и группа мер, направленная на укрепление международного сотрудничества. В этой связи содержится призыв ко всем государствам по содействию, изучению и разработке международной конвенции о нападениях с применением взрывчатых веществ и других актах терроризма, создающих коллективную опасность для людей.

**Терроризм** — явление многоплановое: тут политические, правовые, психологические, философские, исторические, технологические и иные аспекты. Не случайно международному сообществу так и не удалось выработать общеприемлемое юридическое определение терроризма, хотя сущностное наполнение этого феномена для всех понятно. Присутствуют и противозаконное насилие, как правило, с применением оружия, и стремление запугать широкие слои населения, и невинные жертвы, а применительно к актам терроризма, выходящим за рамки государственных границ, в трансграничные компьютерные сети, информационные системы — международный элемент.

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.

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

В 1999 г. по инициативе России Совет Безопасности ООН впервые занялся комплексным рассмотрением темы терроризма без привязки к конкретной ситуации, которая создавала бы угрозу миру и безопасности. К этому его побудил глобальный масштаб террористической опасности, в том числе способной создать угрозу миру и безопасности всех государств. Совет Безопасности ООН в принятой в 1999г. Резолюции 1269 призывает все государства в полном объеме осуществлять международные антитеррористические конвенции и присоединиться к тем из них, участниками которых они не являются. Предлагается также как можно Скорее принять еще не принятые конвенции, в частности по проблемам кибертерроризма.

В последнее время на передний план выдвигаются вопросы противодействия терроризму в сфере компьютерного пространства. В качестве основы для общих подходов к постановке задач на предотвращение, своевременное пресечение или устранение последствий кибертеррористов можно исходить из двух основных направлений:

1) действия, преследующие разрушение сетевой инфраструктуры и несанкционированный доступ к конфиденциальной информации высокой степени секретности, и

2) действия, преследующие возможность намеренного искажения информации в средствах массовой информации, размещаемых в Интернете.

Методология предотвращения и оперативного реагирования на действия первого направления сводится к традиционным способам поддержания информационной безопасности в сетях и обеспечивается мерами на всех уровнях ее реализации.

Методология предотвращения действий, отнесенных ко второму направлению, менее традиционна. Она опирается в основном на законодательный и административный уровень информационной безопасности.

Эти методологии имеют общий характер, который необходимо развивать более тщательно каждым государством и координировать свои действия между собой по выработанной единой системе.

На практике немаловажную роль играют действия по предотвращению и оперативному пресечению террористических действий с использованием сетевых технологий — антитеррористической информационной безопасности (АИБ). Речь идет о проблемах информационной безопасности в узком понимании, а именно только применительно к сетевой инфраструктуре (сетевая транспортная Среда, технологии, информационно-вычислительные ресурсы и т. п.). 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 привилегий, 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: </i> 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.

Частный случай управления доступом — квотирование ресурсов. Как правило, отказ в обслуживании происходит из-за исчерпания какого-то ресурса системы. Однако благодаря квотированию можно ограничить объем ресурсов, доступный каждому из субъектов, и создать резерв для суперпользователя, чтобы он имел возможность вмешиваться и исправлять ситуацию.

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 задачами 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.

Угроза кибертерроризма в настоящее время является очень сложной и актуальной проблемой не только зарубежом, но и в России. К сожалению, она будет усиливаться по мере развития и распространения информационных технологий

И все же существует надежда. Предприняты следующие меры. Для повышения эффективности борьбы с компьютерными преступлениями и обеспечения информационной безопасности государства, бизнеса, общества ГУСТМ МВД России намерено укреплять взаимодействие и сотрудничество между правоохранительными органами, общественными и коммерческими структурами. В частности, начальник этого Управления специальных технических мероприятий МВД России генерал-лейтенант Б. Мирошников заявил: «Российское общество нуждается сегодня в широком освещении как проблем информационной безопасности во всем их разнообразии, так и путей их преодоления. Демонстрация достижений отечественной индустрии безусловно будет способствовать претворению в жизнь Доктрины информационной безопасности России».

Для того чтобы привлечь кибертеррориста к ответственности, этот вид преступления следует отразить в законе. Для этого необходимы системный подход и наличие непротиворечивых подходов и концепций к существующей проблеме. Только в этом случае можно будет эффективно бороться со злоумышленником.

**Заключение**

Страны с высокой производительностью в сфере информационных технологий и с низкой способностью противостоять преступлениям, совершенным с помощью компьютеров и телекоммуникационных технологий, становятся приютом для транснациональной преступности и терроризма. Понятие зоны безопасности приобретает иное значение, когда вместо обычного оружия используются информационные технологии, позволяющие организовать заговор, финансировать и, возможно, даже исполнять серьезные преступления.

Действительно, 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.

# А.И.Бойко, С.И.Ушаков

# Компьютерная форма терроризма и ее легализация

**//Актуальные проблемы борьбы с терроризмом в Южном регионе России.-Ростов-на-Дону,2000.-С.55-57**

То, что сегодня принято называть прогрессом, развивается настолько стремительно, что некоторые его последствия осознаются обществом слишком поздно, когда для исправления ситуации требуются уже значительные усилия. Существует даже мнение, что при переходе некоторой критической точки прогресс начинает работать на уничтожение человечества. Такая ситуации сложилась, например, с экологией. Подобная картина наблюдается и в области информационных технологий.

Снабженный все более и более совершенными орудиями труда, человек неизбежно попадает в прямую зависимость от них. И наиболее ярко эта зависимость проявляется в сфере накопления, обработки и обмена информацией. В знающих руках то, что призвали быть средством, облегчающим управление потоками информации, может стать орудием преступления хулиганского или продиктованного алчностью.

Образующаяся информационная инфраструктура государств становится стратегическим ресурсом, который требует постоянного внимания. Подобно тому, как заболевание нервной системы вызывает изменения в физическом и психическом состояния человека, любые деструктивные действия в информационной сферы имеют самые серьезные последствия для управляемых систем и общества в целом. Между тем современные исследователи единодушно отмечают, что открытые сети сегодня - это средств информационного противоборства в руках политиков, бизнесменов, религиозных организаций, террористических групп и преступно группировок.

Компьютерные манипуляции являются, ввиду своей потенциальной высокой разрушительной мощи, привлекательной средством политической или экономической борьбы организованная групп с корпорациями или государством. Материально-техническое оснащение таких электронных диверсантов стоит гораздо меньше "интеллектуального" багажа знаний, обращенных в острие удара в системы баз данных, и направленных на разрушение или шпионаж.

Представим, к примеру, что Интернет вдруг перестал функционировать. Одна хакерская группа заявила Конгрессу США, что этого можно добиться меньше чем за час. Или - во всех крупных городах отключилось электричество. Нанятые правительством США хакеры добились этого в 1997 году за четыре дня. Или - вдруг перестала работать система неотложной помощи "911". Один шведский хакер довольно быстро парализовал систему "911" во всем штате Флорида всего два года назад. Такие атаки менее трагичны чем похищение ядерной ракеты, однако именно они могут оказаться самым эффективным оружием. "Психологическое воздействие информационного оружия нельзя недооценивать, — полагает Фрэнк Киллюффо, директор отдела информационного оружия центра стратегических и международных исследований при правительстве СЩА. - Используя эту силу, террористы могут добиться таких результатов, которых им никогда не получить путем вооруженной атаки. Мы самая технологически развитая страна в мире, и это значит, что нам есть что терять. США не готовы, к примеру, потерять свою силу. А как долго страна сможет продержаться, лишившись всех своих баз данных? А что будет, если вдруг все системы электронной коммерции будут выведены из строя?"

Специалисты отмечают, что вслед за прогрессом технологии идет и изменение структуры преступлений. Для того чтобы просто выяснить личность человека, взломавшего информационный узел, необходимы специфические знания (не говоря уже о сборе доказательств, ведь обычно улик не остается).

Актуальность проблем компьютерного терроризма для России двойственна: с одной стороны, страна не настолько богата, чтобы переоборудовать современными средствами управления свои химпредприятия, атомные электростанции, что сделает их неуязвимыми для нападений интеллектуальных диверсантов. С другой стороны, государственные спецслужбы ведут активную разведывательную и контрразведывательную работу в сфере электронных коммуникаций и компьютерных сетей.

В уголовно-правовом законодательстве рост компьютерных технологий еще не имеет достойного отражения. Уже сегодня очевидно, что  с помощью компьютера можно совершить целый ряд преступлений - составы, предусмотренные ст. 215-217, 243, 263, 276 и пр.

Создающие опасность для общества действия в целях устрашения населения или оказания воздействия на принятие решений органами власти (существо терроризма) также расположены к компьютерному способу. Можно предложить в связи с этим корректировки диспозиций названных статей в том смысле, чтобы они включали указание на особый (более опасный) способ совершения преступлений. Более всего расположены к этому преступления, помещенные законодателем в гл. 24 УК РФ, поскольку компьютерные технологии представляют собой сверхдоступный способ общения людей.

**Проблемы борьбы с кибертерроризмом в современных условиях**

Жизнедеятельность  каждого человека сегодня в большей или меньшей степени зависит от телекоммуникационных технологий,  используемых практически во всех сферах общественной жизни. Мир вступил в новую эпоху — эпоху информационного общества.

Число пользователей сети Интернет постоянно растет. В США их  158 миллионов, в Европе - 95, в Азии - 90, в Латинской Америке - 14, а в Африке - 3. В России, по разным оценкам, количество пользователей Интернет составляет около 8 миллионов. Подключение к сети Интернет возможно с любой точки земного шара. Если же говорить о развернутой инфраструктуре, то в таком контексте Интернет охватывает сегодня более 150 стран мира [1].

Стремительное развитие  информатизации привело и к появлению  новых видов преступлений, таких как компьютерная преступность и компьютерный терроризм.

Как новое и недостаточно изученное преступное явление, кибертерроризм заслуживает отдельного внимания и требует особого подхода к решению этой,  опасной для человечества, проблемы. Особую озабоченность у правоохранительных органов вызывают террористические акты, связанные с использованием глобальной сети Интернет, из открытых источников которой, можно получить технологию изготовления биологического, химического и даже ядерного оружия террористов. Взламывая сайты, кибертеррористы получают доступ к информации разного рода, в том числе секретной.

На наш взгляд, кибертерроризм - это несанкционированное вмешательство в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, удаление или модификация компьютерных данных, вызывающая дезорганизацию работы критически важных элементов инфрастуктуры государства и создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий [2].

Таким образом, под «кибертерроризмом» или «компьютерным терроризмом»  следует понимать  преднамеренную, мотивированную атаку на информацию, обрабатываемую компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей или наступление других тяжких последствий, если такие действия были содеянные с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта.

 Растущую популярность кибертерроризма можно объяснить   еще и тем, что  осуществить кибертерракт намного дешевле, чем  приобретать  для тех же целей оружие.

Террористические акты в киберпространстве могут совершаться не только отдельными лицами или террористическими группами, но и одним государством против другого. В этом кибертерроризм ничем не отличается от любого другого вида терроризма. Экстремистские группировки, сепаратистские силы, проповедники идей, противоречащих общечеловеческим ценностям, интенсивно используют современные технологии для пропаганды своей идеологии и ведения информационных войн.

Информационное оружие может стать идеальным средством для электронных террористов,  что делает вопрос информационной безопасности важным аспектом как национальной, так и международной безопасности.

Для  информационных актов характерны следующие инструменты  их совершения:

-          различные виды атак, позволяющие проникнуть в атакуемую сеть или перехватить управление сетью;

-          компьютерные вирусы, в том числе — сетевые (черви), модифицирующие и уничтожающие информацию или блокирующие работу вычислительных систем;

-          логические бомбы  - наборы команд, которые внедряются в программу и срабатывают при определенных условиях  (например, по истечении определенного отрезка времени);

-          "троянские кони", позволяющие выполнять определенные действия без ведома хозяина зараженной системы;

-   средства подавления информационного обмена в сетях [2].

            Сложность в предупреждении кибертерроризма заключается в ряде  характеризующих его аспектов:

-          латентность (скрытность);

-          трансконтинентальность (трансграничность);

-          информация, информационные ресурсы, информационная техника могут выступать целью преступных посягательств, средой, в которой совершаются правонарушения и орудием преступления;

-          легкость уничтожения и изменения компьютерной информации (следов преступления).

Согласно статистике, за первое полугодие 2002 года, случаи компьютерных взломов и распространения компьютерных вирусов резко возросли. Из отчета Института Разработки Программного Обеспечения Карнеги Мелон (the Carnegie Mellon Software Engineering Institute) видно, что количество компьютерных инцидентов, выросло от шести случаев в 1988 до 52 658 в 2001 году [3].

Компьютерный терроризм  все более стремительно  и «эффективно» приобретает окраску международного, глобального зла и в соответствии с рядом международных документов  кибертерроризм относится к числу международных преступлений.

Не на последнем месте в настоящее время стоит и политическая мотивация нанесения кибератак по различным инфраструктурам развитых государств. Основными мишенями   электронных террористов стали  США,  Великобритания, Германия, Австралия, Бразилия, Дания. Увеличилось противостояние цифрового мира против США в ответ на политику, проводимую по отношению к Ираку и поддержке Израиля. Подтверждением этого может  служить недавняя атака Юникс Секьюрити Гадз на ряд корпоративных и правительственных систем в знак протеста против планируемой Американо-Британской военной акции против Ирака.

Число кибератак против Американских Правительственных органов в сентябре вдвое превышало число атак в августе. Тому пример – появление нового червя VBS/Nedal (Laden наоборот). Для своего распространения червь использует текст, связанный с печальными событиями 11 сентября 2001 г. в Нью-Йорке. VBS/Nedal - разрушительный вредоносный код, уничтожающий содержимое исполняемых файлов. Он распространяется по электронной почте, рассылая себя каждому адресату, найденному в Адресной Книге Microsoft Outlook на зараженном компьютере. Тема инфицированного письма: "Osama Bin Laden Comes Back!" (Осама Бен Ладен возвращается). В теле письма находится текст,  призывающий стереть с лица земли Израиль и США.

В борьбе с  кибертерроризмом  нельзя недооценивать противника, полагаясь на отсутствие у него достаточного опыта, знаний, квалифицированных и подготовленных кадров. Имеют  место  заявления исламских фундаменталистов о том, что Аль-Каеда и другие мусульманские экстремистские группы во всем мире в качестве оружия  против Запада  для осуществления своих террористических акций планируют  использовать Интернет. Экстремисты открыто заявляют, что все виды высоких технологий   активно изучаются правоверными, дабы воспользоваться самыми современными достижениями в целях электронного джихада.   При этом акцент ставится  на  разрушительное  воздействие на национальные инфраструктуры.  Как заявил один из лидеров преступных группировок Ближнего Востока: "…Очень скоро мир станет свидетелем атак на фондовые биржи Нью-Йорка, Лондона и Токио".

Смелость таких высказываний и публичное   заявление об использовании кибертехнологий с агрессивными целями, прямо свидетельствует о глобализации проблемы кибертерроризма и всех его проявлений. Экстремисты уже не скрывают возможность использования "всех видов технологий" в целях защиты мусульманской земли. Группы джихада разбросаны по всему миру, и в своей деятельности  активно используют Интернет. Неоднократными становятся заявления, о том, что  Аль-Кайеда  имеет высококвалифицированных специалистов по компьютерным технологиям. Ряд мусульманских хакерских группировок угрожает кибератаками  правительственным сайтам США и Израиля. Не удивительно, если завтра мы услышим о мировом экономическом кризисе вследствие атак на основные компьютерные системы крупнейших компаний.

Спецслужбы западных стран оценивают реальную угрозу кибертерроризма  и разрабатывают превентивные меры. Прорабатываются несколько возможных сценариев развития событий,  в частности, возможной атаки на компьютерные системы фондовых бирж.

Последствия компьютерных вторжений, вероятнее всего,  будут  двух типов: вторжение в данные и вторжение в системы управления и контроля.

***Вторжение в данные*** – это нападения на сайты, сетевые компьютеры, системы платежей и связанные с этим базы данных.

***Вторжение в системы управления и контроля*** будет направлено на отключение или разрушение государственной или корпоративной инфраструктуры.

Последствиями  вторжения в данные будут банкротство коммерческих структур, воровство, уничтожение важной деловой информации, потеря интеллектуальной собственности, снижение репутации и/или снижения цены акции. Вторжение в системы управления и контроля представляет большую опасность - сбой работы коммуникаций, транспорта, передачи данных, финансовых систем оплаты и др.

Европейский Совет еще в 90-е годы  указывал на “всемирные масштабы терроризма”. Заявление, принятое в ноябре 1995 года в Ла-Гомере, предусматривало  тесное сотрудничество органов полиции и юстиции посредством обмена информацией о террористических группировках.

События 11 сентября 2001 года показали, что терроризм - это лишь один из вызовов в сфере безопасности, на которые должна ответить многоуровневая система Европы.

Дошедшая из-за Атлантики волна шока застала европейские государства в значительной мере врасплох. Атаки на Нью-Йорк и Вашингтон вывели международный терроризм не только количественно, но и качественно на новый уровень: их подготовка и реализация требовали использования  новых информационных технологий в своих преступных целях.

Подтверждением может служить и совсем свежая новость: датская антиглобалистская организация Global Roots планирует провести в Интернет акцию протеста против очередного саммита Европейского Союза, который пройдет в Копенгагене 12-13 декабря. Участники  Global Roots собираются организовать распределенную DoS-атаку на официальный сайт саммита и вывести его строя. В акции примут участие около 10000 человек, которые не смогут приехать в Данию и лично участвовать в демонстрациях протеста [4].

По мнению авторов, для киберпреступников наиболее характерны два способа  совершения кибератак: способ непосредственного доступа к компьютерной информации и способ удаленного доступа к компьютерной информации.

Непосредственный доступ к электронно-вычислительным машинам, системам или компьютерным сетям представляет собой действия преступника по уничтожению, блокированию, модификации, копированию компьютерной информации, а также нарушению работы компьютерного оборудования или компьютерной сети путем отдачи со­ответст­вующих команд с компьютера, в памяти которого находится информация либо  который планируется вывести из строя.

Анализ проведенного нами исследования показал, что удаленный способ доступа к электронно-вычислительной машине, системе или сети представляет собой опосредованную связь с определенным, находящимся на расстоянии,  компьютером (сетевым сервером) и имеющейся на нем информацией. Такая связь может быть осуществлена через локальные или глобальные компьютерные сети, иные средства связи. К сетевым системам, наряду с обычными (непосредственный доступ), осуществляемыми в пределах одной компьютерной системы, применяется специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве - так называемые  сетевые (или удаленные) атаки (remote или network attacks). Этот вид атак наиболее опасен, как потенциальное оружие кибертеррористов. Под такой атакой обычно понимают информационное разрушающее воздействие на распределенную вычислительную систему, программно осуществляемую по каналам связи. Результаты такого воздействия, например, на систему управления критической инфрастуктуры или ядерным реактором, по своим последствиям могут иметь характер катастрофы глобального значения.

            Таким образом, проблему борьбы с кибертерроризмом сегодня уже надо ставить на один уровень с терроризмом и организованной преступностью. При этом необходимо осуществлять комплексный подход к решению этой проблемы на международном уровне.

В плане  эффективности сотрудничества правоохранительных органов разных государств, направленного на противодействие компьютерному терроризму, необходимо радикально пересмотреть существующую сложную процедуру принятия решений по борьбе с этим видом преступлений, возникшую, в частности, из-за согласования документов, подлежащих ратификации. Такую процедуру на первом этапе можно было бы  упростить, отказавшись от соглашений, используя рамочное постановление. На втором этапе на вопросы внутренней безопасности, имеющие трансграничную значимость, целесообразно распространить процедуру принятия решений в Совете  Европы большинством голосов.