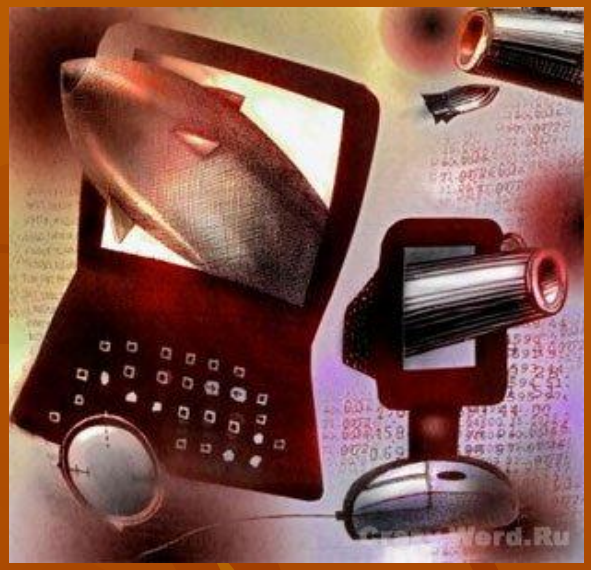
Киберпреступность и кибертерроризм

- **определение понятия «киберпреступность»;**
- **определение понятия «кибертерроризм»;**
- **способы, с помощью которых террористические группы используют Интернет в своих целях;**
- **основные виды киберпреступлений;**
- **арсенал кибертеррористов;**
- **история кибертерроризма;**
- **кибертерроризм XXI века;**
- **проблемы борьбы с киберпреступностью и кибертерроризмом**

Основные цели:

1. Дать определение понятиям «киберпреступность» и «кибертерроризм».
2. Дать общую характеристику киберпреступности и кибертерроризму.
3. Выделить основные разновидности киберпреступлений и кибертерроризма.
4. Описать историю кибертерроризма.
5. Определить проблемы борьбы с киберпреступностью и кибертерроризмом.

Развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых видов преступлений, в частности, к незаконному вмешательству в работу электронно-вычислительных машин, систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации, опасному социальному явлению, получившим распространенное название – «киберпреступность» и «кибертерроризм».



Кибертерроризм можно отнести к так называемым технологическим видам терроризма. 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.

Б. Колин ввел термин в научный оборот в сер. 1980-х гг.

Способы, с помощью которых террористические группы используют Интернет в своих целях:

1. Сбор денег для поддержки террористических движений.

2. Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени встречи людей, заинтересованных в поддержке террористов.

3. Вымогательство денег у финансовых институтов, с тем чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.

4. Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте.

5. Использование Интернета для информационно-психологического воздействия.

6. Перенесение баз подготовки террористических операций.

7. Вовлечение в террористическую деятельность ничего не подозревающих соучастников - например, хакеров, которым неизвестно, к какой конечной цели приведут их действия.

8. Использование возможностей электронной почты или электронных досок объявлений для отправки зашифрованных сообщений.

9. Размещение в Интернете сайтов террористической направленности, содержащих информацию о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также инструкции по их самостоятельному изготовлению. Только в русскоязычном Интернете десятки сайтов, на которых можно найти подобные сведения.

Конвенция Совета Европы выделяет 4 типа компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

- **незаконный доступ** — ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);
- **незаконный перехват** — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);
- **вмешательство в данные** — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
- **вмешательство в систему** — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Основные виды киберпреступлений, представленные в Конвенции Совета Европы:

- незаконный доступ в информационную среду;
- нелегальный перехват информационных ресурсов;
- вмешательство в информацию, содержащуюся на магнитных носителях;
- вмешательство в компьютерную систему;
- незаконное использование телекоммуникационного оборудования;
- мошенничество с применением компьютерных средств;
- преступления, имеющие отношения к деяниям, рассматриваемым в содержании Конвенции;
- преступления, относящиеся к «детской» порнографии;
- преступления, относящиеся к нарушениям авторских и смежных прав.

В зарубежном законодательстве понятие кибертеррорист часто трактуется как хакер.

Арсенал и тех, и других включает:

- **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, внедряемые в программу и срабатывающие при определенных условиях, например, по истечении определенного отрезка времени;
- **«троянские кони»**, позволяющие выполнять определенные действия без ведома хозяина (пользователя) зараженной системы);
- **средства подавления информационного обмена в сетях.**

История кибертерроризма

- **1970-е – начало 1980-х гг.** – зарождение кибертерроризма;
- **1983 г.** – в США была арестована первая группа хакеров под названием «банда 414»;
- **1993 г.** – в Лондоне в адрес целого ряда брокерских контор, банков и фирм поступили требования выплатить по 10-12 млн. ф. ст. отступных неким злоумышленникам;
- **1996 г.** – представители террористической организации «Тигры освобождения Тамил-Илама» провели сетевую атаку, направленную против дипломатических представительств Шри-Ланки;
- **сентябрь 1997 г.** – в результате действий неустановленного хакера была прервана передача медицинских данных между наземной станцией НАСА и космическим кораблем «Атлантис»;
- **январь 1999 г.** – появление в Интернете первого вируса под названием «Хеппи-99»;

- **1 мая 2000 г.** – из пригорода Манилы был запущен в Интернет компьютерный вирус «Я тебя люблю»;
- **август 1999 г.** – была развернута широкомасштабная кампания компьютерных атак Китая и Тайваня друг против друга. Кибертеррористы атаковали порталы государственных учреждений, финансовых компаний, газет, университетов;
- **11 сентября 2001 г.** – террористический акт против США;
- **2004 г.** – электронные ресурсы правительства Южной Кореи подверглись массированной атаке – вирусом оказались заражены десятки компьютеров, в частности министерства обороны Южной Кореи;
- в **2005–2006 гг.** было зафиксировано более 2 млн. компьютерных нападений на информационные ресурсы органов государственной власти, в том числе свыше 300 тыс. атак на интернет-представительство президента РФ;
- **6 февраля 2007 г.** – массированная атака на весь Рунет.

Кибертерроризм XXI века

Привлекательность использования киберпространства для современных террористов связана с тем, что для совершения кибертеракта не нужны большие финансовые затраты – необходим лишь персональный компьютер, подключенный к сети Интернет, а также специальные программы и вирусы.

Терроризм в глобальной компьютерной сети развивается динамично: Интернет-сайты появляются внезапно, часто меняют формат, а затем и свой адрес. Если в 1998 г. около половины из тридцати террористических групп, внесенных США в список «Иностранных террористических организаций», имели свои сайты, то сегодня почти все террористические группы присутствуют в Интернете.

Среди них – перуанские террористы из организаций «Сендеро Луминосо» и «Тупака Амару», боевики афганского движения «Талибан», грузинские националисты из группы «За свободную Грузию», «Тамильское движение сопротивления» и многие другие террористические структуры, функционирующие на различной организационной и идеологической основе.

«Аль Кайда», «Хезболла», «Хамас», «Организация Абу Нидаля», «Черные Тигры» (связанные с «Тиграми Освобождения Тамил Илама») не только используют киберпространство для пропаганды своих взглядов, но и в качестве оружия для нанесения ударов по объектам национальной инфрастуктуры, для атак на иностранные сайты и серверы.

Интернет-аудитория террористических сайтов используется для активизации потенциальных и реальных сторонников террористов; для влияния на международное общественное мнение, непосредственно не вовлеченное в конфликт; для деморализации «врага» – граждан, организаций и государств, против которых борются террористы.

К настоящему времени кибертерроризм стал суровой реальностью. Общее количество происходящих в мире кибератак очень трудно подсчитать, так как в силу разных причин не все они становятся достоянием гласности.

В этой связи некоторые эксперты предлагают перейти на новую систему Интернета, радикально отказавшись от его изначальной концепции полной открытости.

Основной смысл новой модели состоит в отказе от анонимности пользователей Сети, что позволит обеспечить ее большую защищенность от преступных посягательств. Компания Microsoft, к примеру, объявила о готовности выплачивать премию за выявление каждого кибертеррориста в размере 50 тыс. долл.

В. А. Голубев в качестве рекомендаций, направленных на противодействие опасным тенденциям и повышение эффективности борьбы с кибертерроризмом, предлагает следующее:

1. Организация эффективного сотрудничества с иностранными государствами, их правоохранительными органами и специальными службами, а также международными организациями, в задачу которых входит борьба с кибертерроризмом и транснациональной компьютерной преступностью.

2. Создание национального подразделения по борьбе с киберпреступностью и международного контактного пункта по оказанию помощи при реагировании на транснациональные компьютерные инциденты.

3. Расширение трансграничного сотрудничества (в первую очередь с Россией) в сфере правовой помощи в деле борьбы с компьютерной преступностью и кибертерроризмом.

4. Принятие всеобъемлющих законов об электронной безопасности в соответствии с действующими международными стандартами и Конвенцией Совета Европы о борьбе с киберпреступностью.

Уголовно-правовая борьба с киберпреступностью и кибертерроризмом – глобальная проблема в силу того, что киберпреступность носит трансграничный характер.

Поэтому для эффективной борьбы с киберпреступлениями необходимо не только принятие соответствующих уголовно-правовых норм на национальном уровне, но и выработка единых международных стандартов, таких как определение круга деяний, подлежащих криминализации, выработка единого понятийного аппарата и единой терминологии, пересмотр существующих уголовно-правовых норм с учетом стандартов, установленных международно-правовыми документами.

Заключение

Киберпреступность и кибертерроризм являются объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. С ростом использования информационных технологий в различных сферах деятельности человека растет и использование их в целях совершения преступлений.

Чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и других стран от всевозможных мастей кибертеррористов. О безопасности надо думать сегодня, завтра уже может быть поздно.