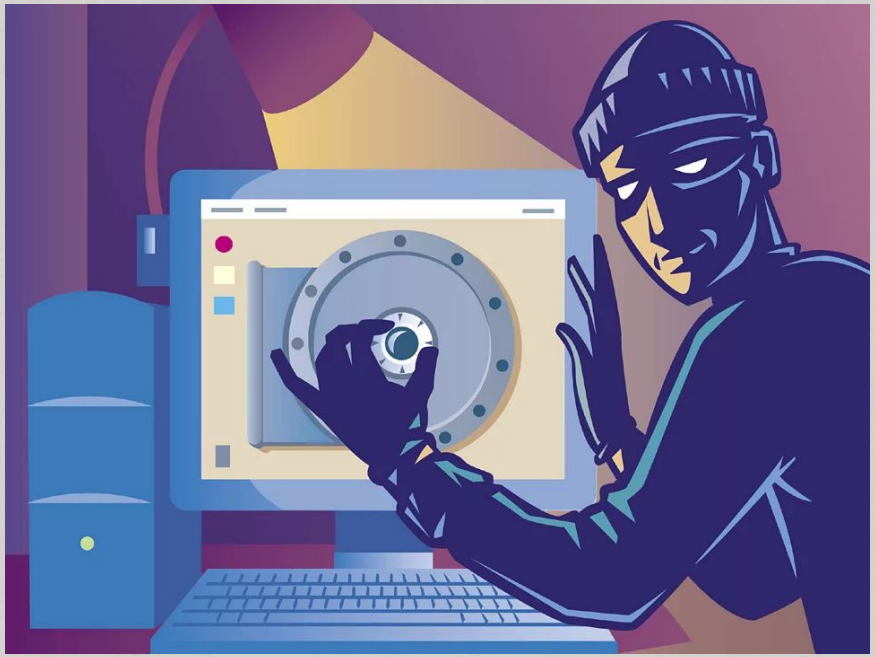
Информационная преступность в сети Интернет

Преступление – это общественно опасное деяние, запрещённое уголовным кодексом.

По характеру:

- ✔*Корыстные*
- ✔*Экономические*
- ✔*Насильственные*
- ✔*Терроризм*

Киберпреступность - это преступность в так называемом «виртуальном пространстве».



Терроризм – глобальная проблема человечества

Террор – слово латинского происхождения, что означает «страх», «ужас».

Терроризм – это использование насилия и угрозы для достижения публичных политических целей.

Термин «кибертерроризм» ввел Б. Колин **в научный оборот в середине 80-х годов**

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.

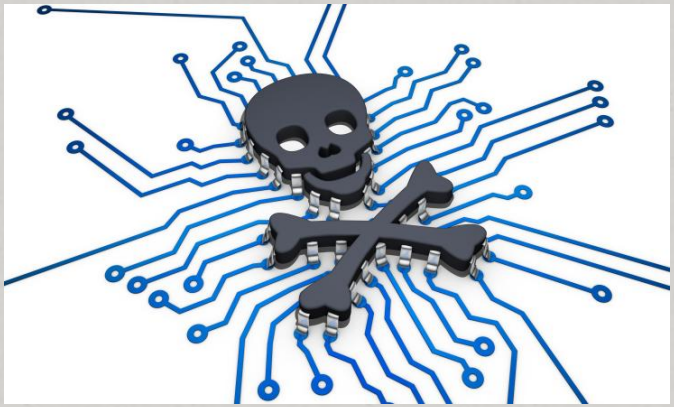
7. Вовлечение в террористическую деятельность ничего не подозревающих соучастников - например, хакеров, которым неизвестно, к какой конечной цели приведут их действия.

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

- незаконный доступ
- незаконный перехват
- вмешательство в данные
- вмешательство в систему



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

Исследователи М. Дж. Девост, Б. Х. Хьютон, Н. А. Поллард определяют информационный терроризм (а кибертерроризм является его разновидностью) как:

- соединение преступного использования информационных систем с помощью мошенничества или злоупотреблений с физическим насилием, свойственным терроризму; и
- сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов.

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.

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.

Терроризм — политика, основанная на систематическом применении террора Несмотря на юридическую силу термина «терроризм», его определение вплоть до настоящего времени остается неоднозначным. *Проблема в том, как ограничить определение терроризма, чтобы под него не подпадали деяния легитимных борцов за свободу.*

Заключение

Следует уделить внимание также термину «сетевая война», этот вид войны как «новый способ ведения конфликтов на социальном уровне, без традиционного использования военной силы, когда протагонисты используют сетевые формы организации и связанные с ней доктрины, стратегии и технологии, которые соответствуют эпохе информационного общества».

Сетевую войну можно также определить как противоборство в информационной сфере, ведущееся с применением информационного оружия, информационных технологий и наиболее острых средств информационно-психологического воздействия. Кибертерроризм - одна из форм сетевой войны. От других форм ее отличает наличие цели - террористы совершают свои действия в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти.

Спасибо за внимание!