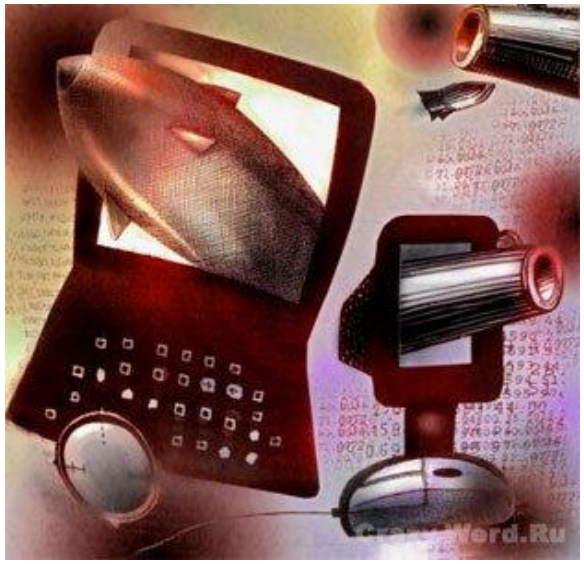
КИБЕРПРЕСТУПНОСТЬ И КИБЕРТЕРРОРИЗМ

Разработали:
Обухов Д. И.
Сухарев С. А.
Группа 111

СОДЕРЖАНИЕ

- **определение понятия «киберпреступность»;**
- **определение понятия «кибертерроризм»;**
- **способы, с помощью которых террористические группы используют Интернет в своих целях;**
- **основные виды киберпреступлений;**
- **арсенал кибертеррористов;**

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.

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.

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.

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

Рекомендации по борьбе:

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.

СПАСИБО ЗА ВНИМАНИЕ!