Информационный терроризм

Презентацию подготовил студент факультета УВД группы Д-22
Кобрисов А.

Информация – новый вид терроризма.

- Информация, широко освещаемая в СМИ, воспринимается социумом как реальность. Ресурс Youtube - видеоролики - захватил уже 95% Интернета, способствуя деградации пользователей, опуская их на уровень до возникновения письменности. Просто смотреть, не напрягаясь, даже чтобы прочесть - самый лёгкий способ получения информации. В этом – одна из причин могущества телевидения. Яркий, красивый видеоряд способен внедрить в мозг ленивого обывателя любую ложь. Леность – фундаментальный порок людей, который используется для порабощения сознания.
- Цель информационных войн - запугать массы мнимой угрозой: «исламским терроризмом», «иракским химоружием», «страшными сербами» или «страшными москалями» для украинцев. Обработанное таким образом массовое сознание не только не видит реальную угрозу со стороны информационного агрессора, оно делает народы слепым оружием в его руках. Перепуганные лживым образом «кровавого диктатора» (Каддаффи, Хусейна, Милошевича…) иракские, ливийские, югославские, украинские и прочие «повстанцы» выходят на майданы, своими руками разрушая собственную страну, действуя во благо США.

Информационный терроризм – что это?

- Информационный терроризм – прямое воздействие на психику и сознание людей в целях формирования нужных мнений и суждений, определенным образом направляющих поведение л

Виды информационного терроризма:

- информационно-психологический терроризм
- информационно-технический терроризм

Информационно-психологический терроризм

– контроль над СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористических организаций; воздействие на операторов, разработчиков, представителей информационных и телекоммуникационных систем путем насилия или угрозы насилия, подкупа, использование методов гипноза, средств создании иллюзий, мультимедийных средств для ввода информации в подсознание и т. д.;

Информационно-технический терроризм

– нанесение ущерба отдельным физическим элементам информационной среды государства; создание помех, использование специальных программ, стимулирующих разрушение систем управления, или, наоборот, внешнее террористическое управление техническими объектами (в т. ч. самолетами), биологические и химические средства разрушения элементной базы; уничтожение или активное подавление линий связи, неправильное адресование, искусственная перегр утации и т. д.

Кибертерроризм

— нападение на компьютерные сети. Первые примеры компьютерного терроризма появились в конце 1990 х гг., что связано как с развитием сетей, так и с увеличившейся ролью компьютеров во всех сферах ж

Кибертеррористический акт

- политически мотивированный акт, проведенный с помощью компьютерных и коммуникационных средств, применение которых непосредственно создает или потенциально может создать опасность для жизни и здоровья людей, повлекло или может повлечь значительный ущерб материальным объектам, наступление общественно опасных последствий или целью которого является привлечение максимально возможного внимания к политическим

ям

Способы совершения кибертеракта:

- получение несанкционированного доступа к государственным и военным секретам, банковской и личной информации;
- нанесение ущерба отдельным физическим элементам информационного пространства, например, разрушение сетей электропитания, создание помех, использование специальных программ для разрушения аппаратных средств;
- кража или уничтожение информации, программ и технических ресурсов путем преодоления систем защиты, внедрения вирусов, программных закладок;
- воздействие на программное обеспечение и информацию;
- раскрытие и угроза публикации закрытой информации;
- захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;
- уничтожение или активное подавление линий связи, неправильная адресация, перегрузка узлов коммуникации;
- проведение информационно-психологических операций и т.д.

5 самых известных хакеров в истории

1. Роберт Тэппэн Моррис

Даже если вы почти ничего не знаете о компьютерных вирусах, всё равно наверняка слышали о так называемых «червях». Первым, кто запустил такой вирус в сеть, был Роберт Тэппэн Моррис.

Аспирант Корнельского университета Моррис создал своего «червя» и 2-го ноября 1988-го года выпустил его в сеть, чем парализовал работу шести тысяч компьютеров в США. Впоследствии он утверждал, что просто хотел посмотреть, насколько разросся интернет, и то, что получилось — последствия вышедшего из-под контроля эксперимента. Однако «червь» оказался кое-чем куда большим, чем просто тест: он читал /etc/passwd, пытаясь подобрать пароли к учётным записям. В конце концов Моррис был оштрафован и приговорён к трём годам условно.

2. Кевин Митник

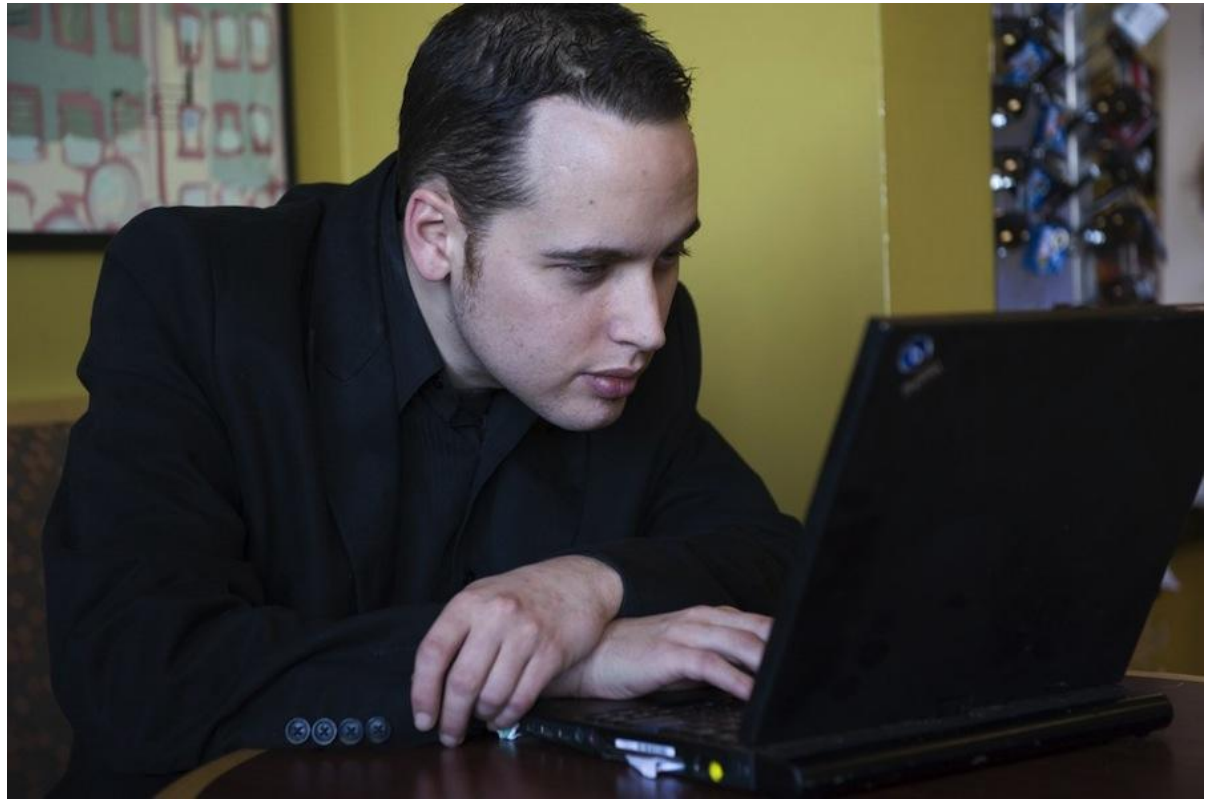
Митник взломал автобусную систему Лос-Анджелеса с помощью подделки проездного документа. Позже, в возрасте 12-ти лет, он стал телефонным мошенником — сначала забавлялся, перенаправляя сигнал домашнего телефона на таксофон и слушая, как владельцев домашних телефонов перед разговором просят опустить десять центов. Потом просто стал звонить бесплатно куда хотел. А через несколько лет Митника уже разыскивали по всей стране за взлом сети Digital Equipment Corporation и кражу их программ. Это, возможно, был его первый заметный взлом, но позднее парень влез и в сети телефонных гигантов Nokia и Motorola.

ФБР поймало его в 1995-м году после взлома ведущего американского специалиста по компьютерной безопасности Цутому Симомуры. Митник был приговорён к пяти годам лишения свободы

3. Эдриан Ламо

В 2002-м и 2003-м годах Ламо взломал системы нескольких крупных компаний просто ради удовольствия, а после проинформировал компании об ошибках в их системах безопасности. Среди объектов, атакованных хакером, были Microsoft, Yahoo и New York Times, где он добавил свою контактную информацию в базу данных экспертов.

Известный как «бездомный хакер», Ламо чаще всего работал, подключаясь к сети в интернет-кафе и публичных библиотеках. Многие считают, что им двигала жажда славы. Вторжение Ламо в сеть NY Times в 2003-м привлекло к нему внимание противников киберпреступности, он был пойман и приговорён к шести месяцам домашнего ареста и двум годам испытательного срока.



4. Гэри Маккиннон (aka Solo)

Лондонский хакер Гэри Маккиннон шотландского происхождения действовал не столько для удовольствия, сколько преследовал политические цели.

В 2002-м году Маккиннон влез в компьютеры министерства обороны США, армии, флота, ВВС и НАСА. Впоследствии он заявил, что искал доказательства сокрытия информации об НЛО, утаивания информации об альтернативных источниках энергии и о других технологиях, потенциально полезных для общества.

Это не шутка. Маккинон рассказал, что имеет основания полагать, что правительство США скрывает инопланетные технологии, которые могли бы решить глобальный энергетический кризис. Впрочем, хакер-самоучка признаёт, что мог «случайно» удалить целую кучу других файлов и, возможно, повредить некоторые жесткие диски, когда пытался замести следы. Однако он до сих пор настаивает, что ничего особенного не произошло.

Правительство США в свою очередь заявляет, что атака Маккиннона обошлась в $800 000, а также ставит под сомнение, что хакер действительно искал информацию об НЛО.

5. Рафаэль Грей (aka Curador)

Рафаэль Грей называл себя праведником и настаивал, что он всего лишь пытался помочь сайтам электронной коммерции, когда взломал их базы данных для кражи номеров кредитных карт и личной информации 26 000 американских, британских и канадских клиентов в 2000-м году.

Затем 18-летний уэльский подросток заявил, что просто пытался привлечь внимание к уязвимостям в системах безопасности. Правда, не до конца понятно, зачем он в таком случае разместил похищенные номера карт в открытом доступе в интернете, но это уже другой вопрос.

В 2001-м году Грей был приговорен к трём годам принудительного психиатрического лечения.

Вывод:

- Традиционный терроризм не угрожал обществу как таковому, не затрагивал основ его жизнедеятельности. Современный высокотехнологичный терроризм способен продуцировать системный кризис в любом государстве с высокоразвитой информационной инфраструктурой. В настоящее время во многих странах мира уже созданы на государственном уровне или находятся на стадии реализации программы, предоставляющие большие полномочия национальным спецслужбам по контролю за информационными системами.

СПИСОК ЛИТЕРАТУРЫ:

1. Информационная война. Информационное противоборство: теория и практика : монография / В. М. Щекотихин, А. В. Королёв, В. В. Королёва и др. ; под общ. ред. В. М. Щекотихина. – М. : Академия ФСО России, ЦАТУ, 2010. – 999 с.

2. Супиченко, С. Интернет экстремизм и терроризм/ С. Супиченко. – Информационно-аналитический журнал ЦАТУ: Ассиметричные угрозы и конфликты низкой интенсивности. – № 5. – 2008. – С.57–62.

3. Чукуэн, С. Международный терроризм в информационную эпоху/ С. Чукуэн. – Информационно-аналитический журнал ЦАТУ: Ассиметричные угрозы и конфликты низкой интенсивности. – № 8. – 2009. – С.55–59.

4. http://www.crime-research.org/library/terror3.htm “Кибертерроризм” – миф или реальность? В.А.Голубев

5. http://www.rusus.ru/?act=read&id=66 Россия в борьбе с международным терроризмом. Грани повышения позитивного образа страны. Роговский Е.А.

6. http://www.agentura.ru/press/about/jointprojects/novgaz/nakhackers/ НАК ищет контакт с хакерами-патриотами. Андрей Солдатов.

7. http://www.crime.vl.ru/index.php?p=1114&more=1 Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику.

8. http://www.crime.vl.ru/index.php?p=1025&more=1 Компьютерная атака и кибертерроризм: уязвимость и политические вопросы для Конгресса.