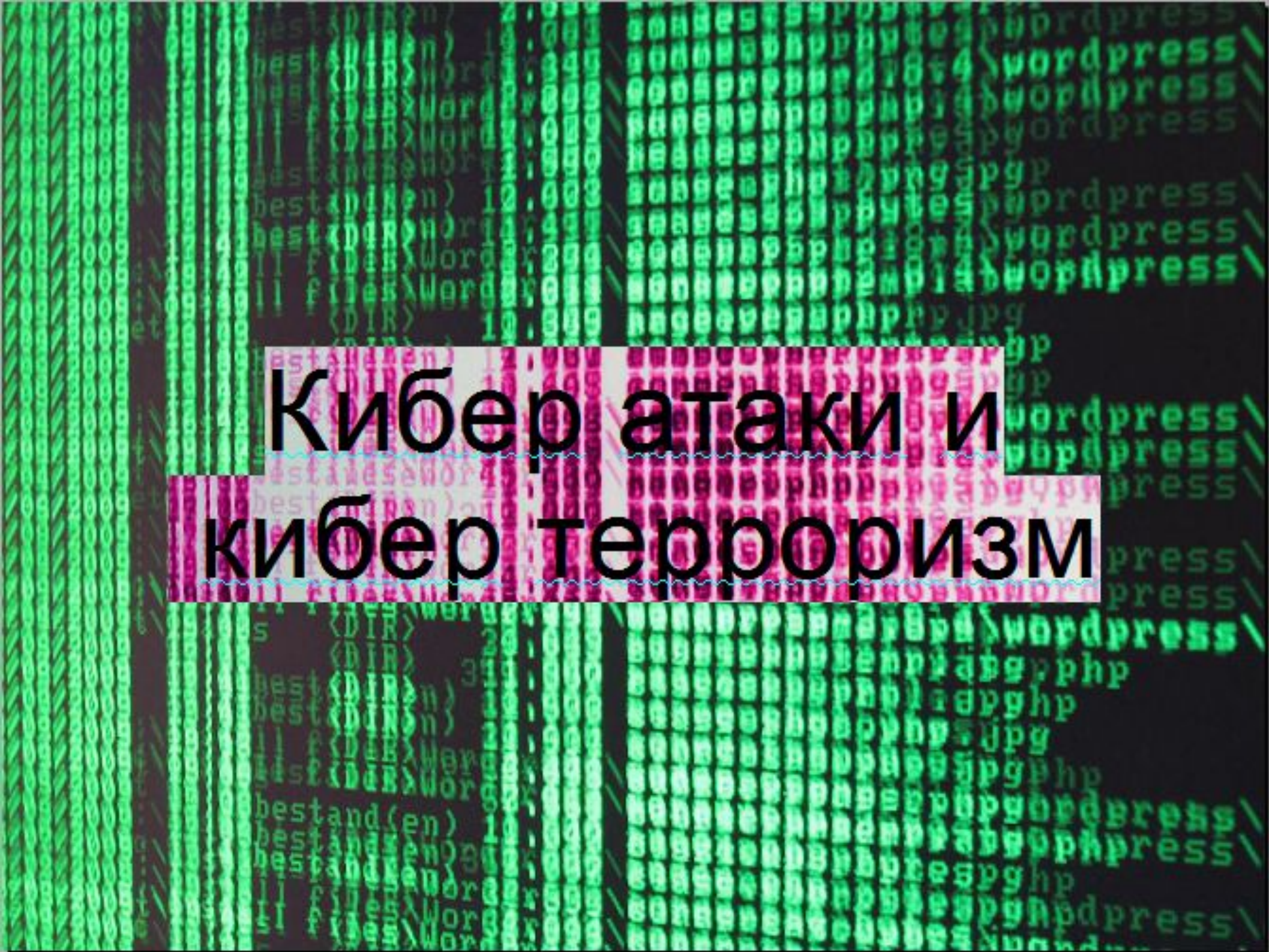
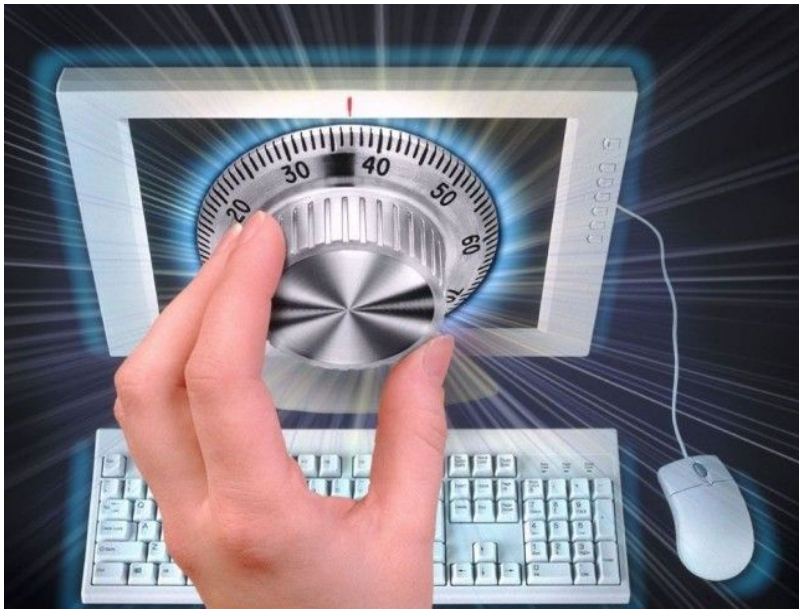

Кибер атаки и
кибер тероризм

Кибератака

В широком смысле слова под кибератакой следует понимать любую попытку несанкционированного доступа к отдельному компьютеру или компьютерной сети.



Большинство кибератак проводится с целью получения доступа к управлению компьютером или к информации, хранящейся на нем. По подсчетам «Лаборатории Касперского» в настоящее время в Интернете присутствует около 4 млн. разных вирусов и до 70 тысяч вредоносных и потенциально опасных программ.

Серьезную опасность для государственных и бизнес-структур представляют DoS (отказ в обслуживании) и DDoS (распределенный DoS) сетевые атаки. Эти атаки направлены на то, чтобы сделать невозможным обслуживание системой своих легальных пользователей.

DoS-атаки могут причинять большие убытки тем компаниям, прибыльность которых напрямую зависит от численности клиентов. DoS-атакам подвергались такие сетевые ресурсы, как eBay, Yahoo, Mikrosoft, Amazon и многие другие.

Самым популярным приемом проведения таких атак является наводнение объекта атаки разными протоколами, обработка которых поглощает все вычислительные ресурсы системы.

DDoS-атаки используют те же приемы, но в атаке уже участвует не один компьютер, а множество. Первая такая атака была проведена в 1998г. и поразила своими возможностями. Даже каналы с очень высокой пропускной способностью не в состоянии выдержать одновременную атаку сотен компьютеров. При этом владельцы компьютеров, ведущих атаку, понятия не имеют об этих преступных действиях.

Архитектура DDoS-атаки обычно имеет 3 уровня. Управляет всем компьютер, находящийся на вершине пирамиды. С него производится несанкционированная, использующая несовершенство ПО, установка (например, с помощью компьютерного червя) программы, которую называют «мастер», на несколько компьютеров, работающих в Интернете.

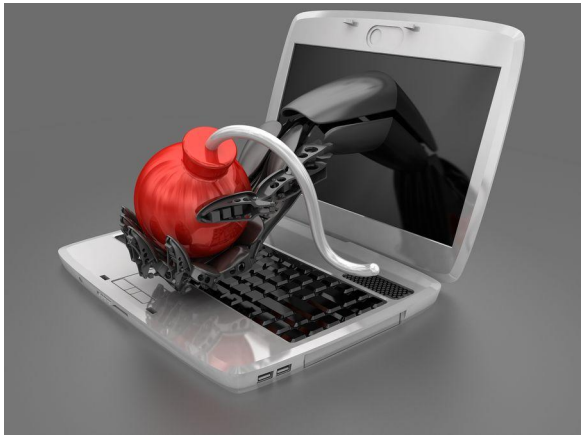
Компьютеры, зараженные этой программой, в свою очередь, с ее помощью заражают программой «демон» десятки или сотни компьютеров, с которых и будет вестись

Атака начинается по команде с компьютера первого уровня «мастерам». В этой команде содержится информация о времени и объекте DDoS-атаки. «Мастера» транслируют команду о проведении атаки «демонам», и те одновременно начинают атаковать выбранный объект.

Чаще всего жертвами преступных кибератак становятся частные лица, не обладающие достаточными знаниями в области информационной безопасности. В 2010г. жертвами злоумышленников стали сотни миллионов пользователей Интернета. Даже крупные корпорации, содержащие штат квалифицированных специалистов по компьютерной безопасности, не всегда могут успешно противостоять таким атакам.

Вот только некоторые из успешных кибератак, проведенных недавно:

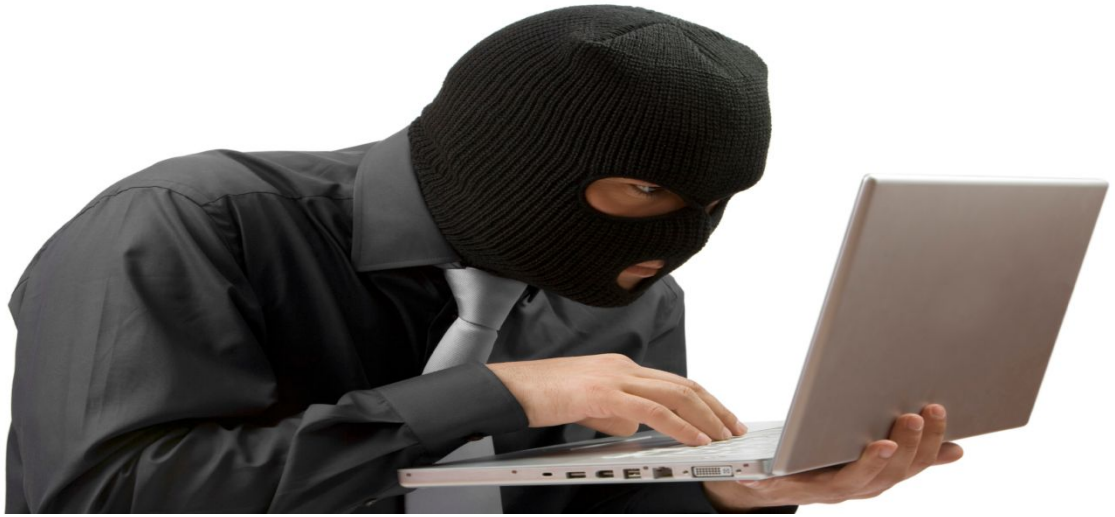
1. В результате кибератаки с принадлежащего корпорации Sony сервиса Playstation Network были похищены личные данные 77 млн. пользователей. Похищенная информация включала и номера кредитных карт пользователей. Предварительно ущерб от этой атаки оценивают в 1,25 млрд. долларов.
2. Кибератака почтового сервиса Google Gmail увенчалась взломом сотен учетных записей пользователей, среди которых были высокопоставленные чиновники США, правительственные чиновники некоторых азиатских стран и китайские оппозиционеры.
3. С помощью компьютерного червя Stuxnet была парализована иранская АЭС в Бушере, что привело к приостановке их ядерной программы.



Кибератаки Пентагона стали уже привычным явлением. Масштабы преступной деятельности в Интернете постоянно растут и принимают все более опасные формы. Поэтому вопросы противодействия преступным посягательствам во Всемирной сети становятся все более актуальными.

Кибертерроризм

Кибертерроризм - использование интернет-нападений в террористической деятельности, включая акты преднамеренного, крупномасштабного разрушения компьютерных сетей, особенно персональных компьютеров, приложенных к Интернету, посредством инструментов, таких как компьютерные



Кибертерроризм может быть также определен как намеренное использование компьютера, сетей и общественного Интернета, чтобы вызвать разрушение и вред для личных целей. Цели могут быть политическими или идеологическими, так как это может быть замечено как форма терроризма.

Типы кибертеррористических способностей.

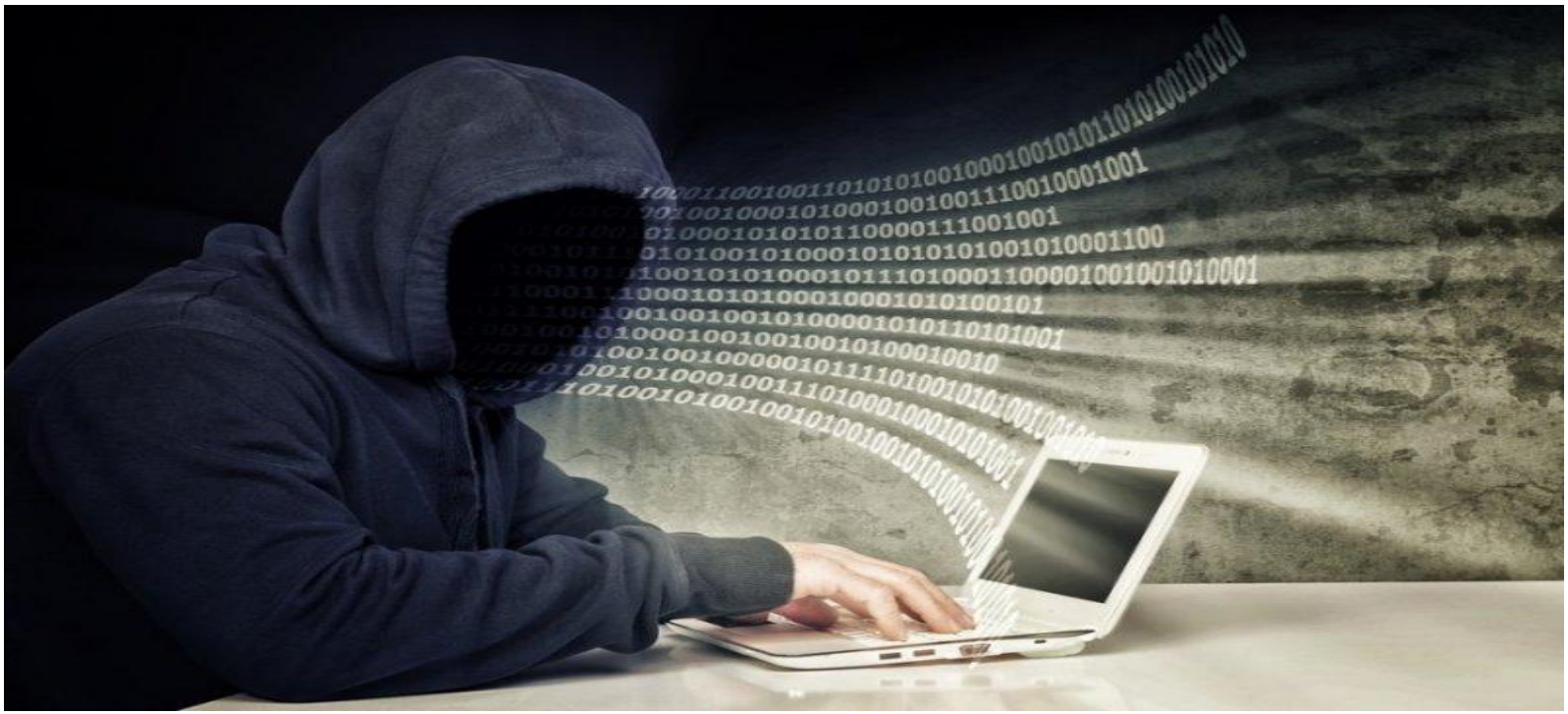
1. Просто неструктурированный: способность провести основных работников против отдельных инструментов использования систем, созданных кем-то еще. Организация обладает небольшим целевым анализом, командным пунктом или изучением способности.

2. Продвинуто структурированный: способность провести более сложные нападения на многократные системы или сети и возможно, изменить или создать основные инструменты взламывания. Организация обладает элементарным целевым анализом, командным пунктом и изучением способности.

3. Скоординированный по комплексу: способность к скоординированному нападению, способному к порождению массового разрушения против интегрированной, разнородной обороноспособности (включая криптографию). Способность создать современные инструменты взламывания. Очень способный целевой анализ, командный пункт и организация, изучающая способность.

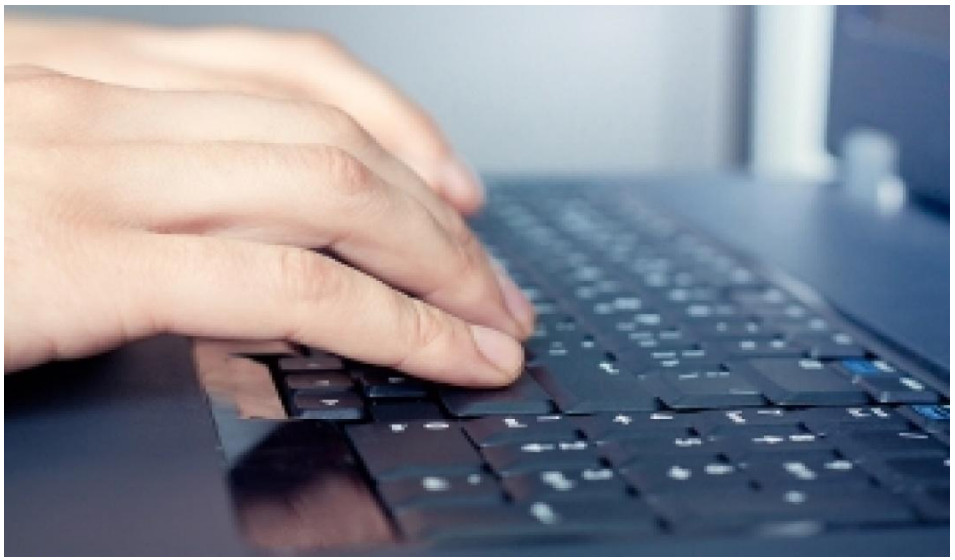
Примеры

Операция может быть сделана любым где угодно в мире, поскольку это могут быть выполненные тысячи миль далеко от цели. Нападение может нанести серьезный ущерб критической инфраструктуре, которая может привести к жертвам. Нападение на инфраструктуру может быть энергосистемами, денежными системами, дамбами, СМИ и личной информацией.



1.

В 1998 испанские протестующие бомбардировали Институт Глобальной связи (IGC) с тысячами поддельных электронных писем. Электронная почта была связана и недоставленная пользователям ISP, и линии поддержки были связаны с людьми, которые не могли получить их почту. Протестующие также spammed IGC штат и учетные записи, забитые их веб-страница с поддельными заказами кредитной карты, и угрожаемый использовать ту же самую тактику против организаций, используя услуги IGC. Они потребовали, чтобы IGC прекратили принимать веб-сайт для Журнала Euskal Herria, нью-йоркской публикации, поддерживающей баскскую независимость. Протестующие сказали, что IGC поддержал терроризм, потому что секция на веб-страницах содержала материалы по террористической группе ЭТА, которая взяла на себя ответственность за убийства испанских политических и сотрудников службы безопасности и нападения на военные установки. IGC наконец смягчился и потянул место из-за «почтовых бомбежек».



2.

В 1998 этнические тамильские партизаны попытались разрушить шри-ланкийские посольства, послав большие объемы электронной почты. Посольства получили 800 электронных писем в день за двухнедельный период. Сообщения читали, «Мы - Интернет Черные Тигры, и мы делаем это, чтобы разрушить Ваши коммуникации». Власти разведки характеризовали его как первое известное нападение террористами против компьютерных систем страны.

3.

В 1999 хакеры напали на компьютеры НАТО. Компьютеры затопили их электронной почтой и поразили их отказом в обслуживании (DoS). Хакеры выступали против бомбежек НАТО китайского посольства в Белграде. Компании, общественные организации и академические учреждения были засыпаны высоко политизированными электронными письмами, содержащими вирусы из других европейских стран.

Спасибо
за
внимание!