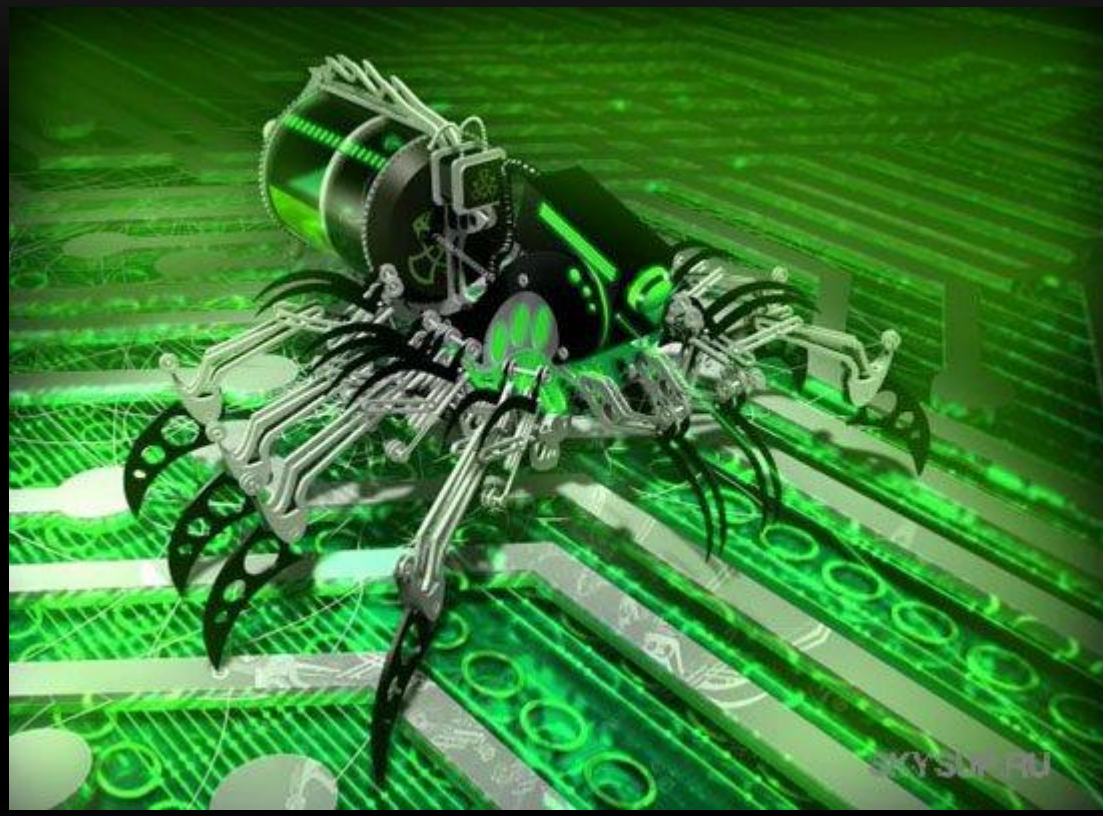
ВОПРОСЫ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ И СЕТЕЙ

ВИРУС

Вирус — разновидность компьютерных программ, отличительной особенностью которых является способность к саморепликации. Также вирусы способны выполнять прочие произвольные действия без ведома пользователя, в том числе наносящие вред ему и/или компьютеру. Используется для создания ботнетов (Об этом далее).



ФИШИНГ

Мошенники могут присылать вам ссылки на различные известные ресурсы, однако…

Оригинальный домен сайта

Фальшивый домен сайта

Вы можете ввести свои данные на фальшивом сайте, разработанным специально для этих целей. Такие сайты создать очень легко, т.к. браузеры свободно показывают исходный код всех сайтов.

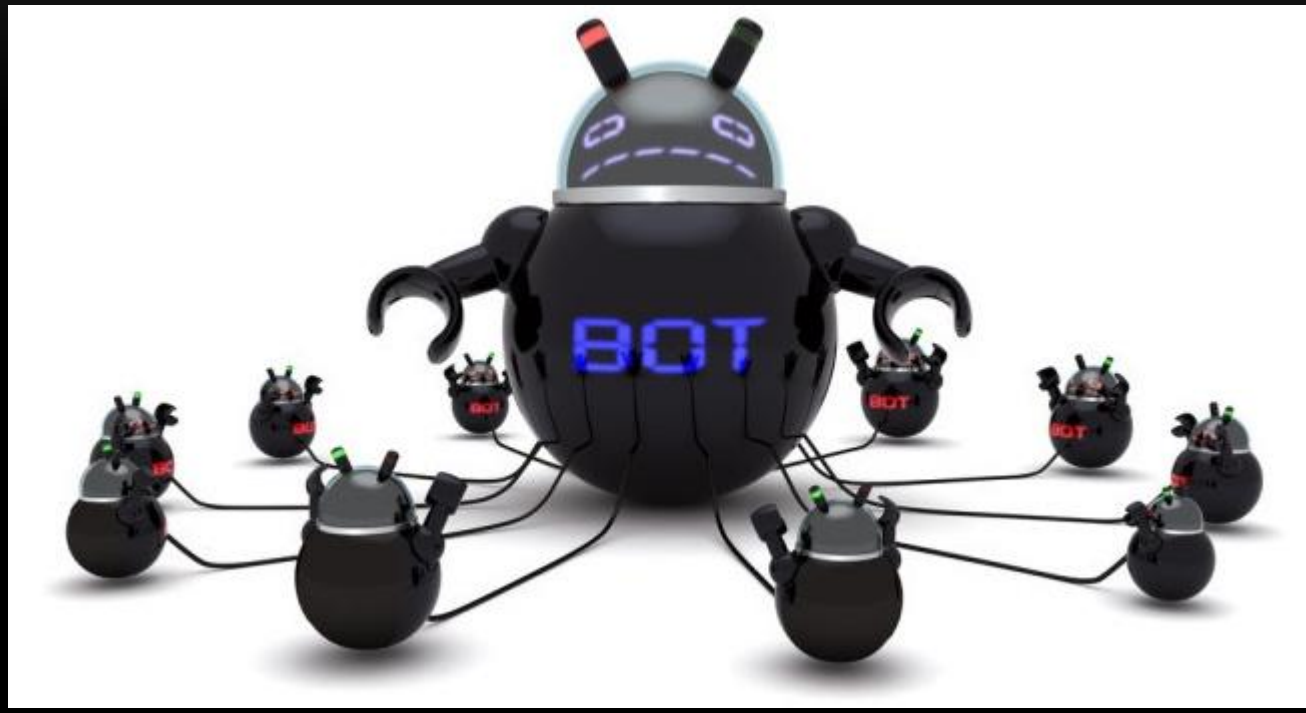
ТРОЯНСКИЕ ЧЕРВИ

Троянские черви (‘Трояны’) - тип программ, используемых для проникновения на компьютер пользователя и использования информации на нём в своих целях. Распространяется программами с расширением .exe (т.к. присутствует возможность ‘склеить’ exe-шник с вредоносной программой).

БОТНЕТЫ

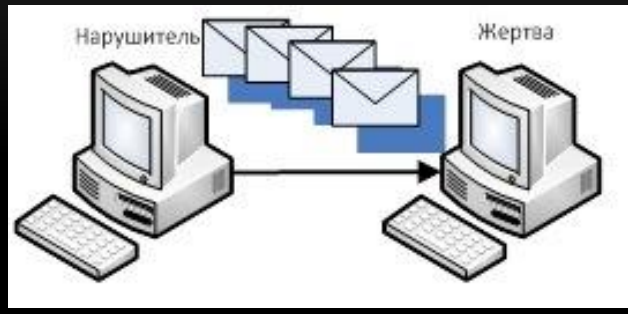
Ботнет – сеть из зараженных устройств, расположенных по всему миру.

Компьютеры, объединённые в ботнет используются для совместной DDoS атаки (Об этом далее).



DoS И DDoS АТАКИ

DoS-атака (отказ в обслуживании) – это атака, приводящая к парализации работы сервера или персонального компьютера вследствие огромного количества запросов, с высокой скоростью поступающих на атакуемый ресурс.



DDoS-атака (распределенный отказ в обслуживании) – это разновидность DoS-атаки, которая организуется при помощи очень большого числа компьютеров, благодаря чему атаке могут быть подвержены сервера даже с очень большой пропускной способностью Интернет-каналов.

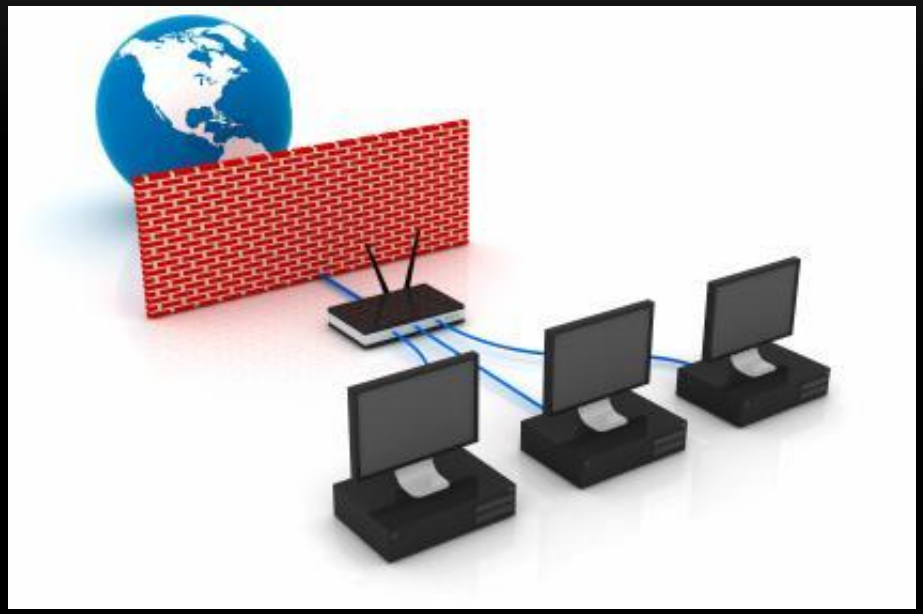
СПОСОБЫ ЗАЩИТЫ В СЕТИ ИНТЕРНЕТ

ИСПОЛЬЗОВАНИЕ АНТИВИРУСА

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

ИСПОЛЬЗОВАНИЕ ФАЕРВОЛА

Фаервол (firewall, сетевой экран) предназначен для защиты компьютерных сетей или отдельных узлов от несанкционированного доступа. Одна из его основных задач — не пропускать (фильтровать) сетевые пакеты, не подходящие под заданные критерии.



ПРЕЗЕНТАЦИЮ ПОДГОТОВИЛ

Майнич Никита