

***Поиск информации в сети
Интернет. Защита
информации от
несанкционированного доступа***

Типы адресации

- IP-адресация
- Удобна для компьютерной техники
- Может быть постоянным и временным
- DNS-адресация (доменная система имен)
- Удобна для пользователя

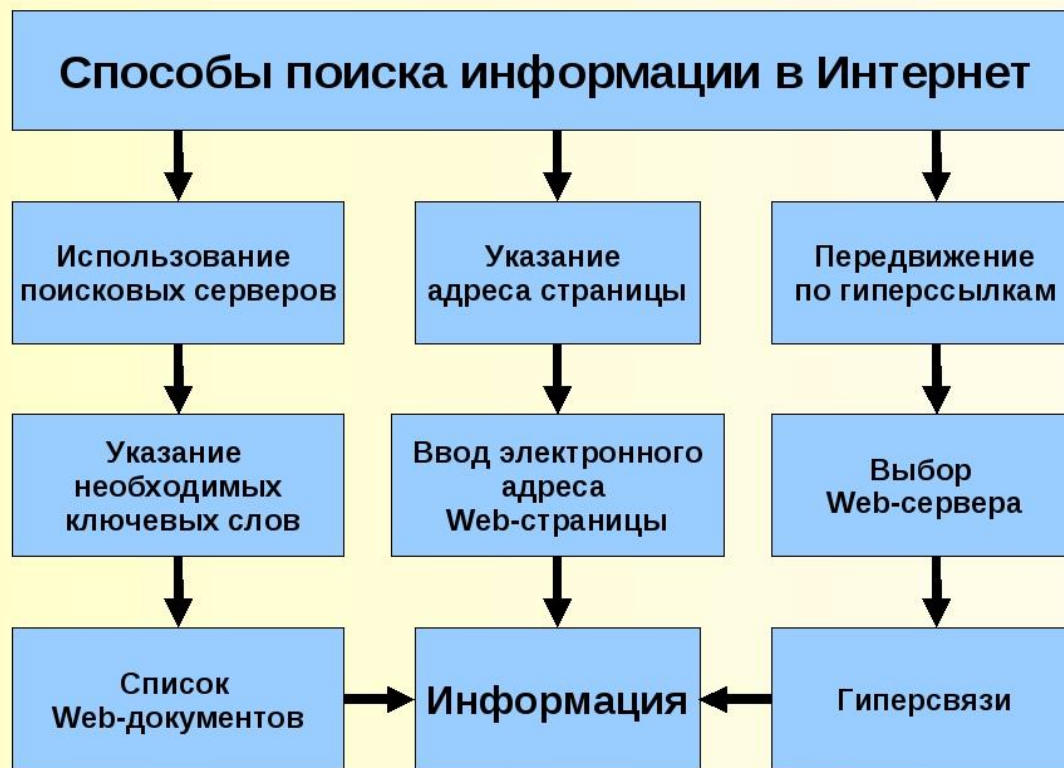
Домены верхнего уровня

- Административные
- com - коммерческие
- edu - образовательные
- net – компьютерные сети
- org - некоммерческие
- info - информационные
- Географические
- ru – Россия
- ua – Украина
- uk – Великобритания
- cd – Республика Конго
- tv – Тувалу

URL – унифицированный указатель ресурсов

- *Протокол://доменное имя/ путь доступа к файлу имя файла Web-страницы*

Способы поиска информации



Популярные поисковые системы

Яндекс

Найдётся всё

@mail.ru®

Google™
на русском

Rambler

YANHOO!®

gogo

Информационная безопасность

- процесс обеспечения конфиденциальности, целостности и доступности информации.



Способы несанкционированного доступа к информации

Социальная инженерия

Dos или DDos - атаки

Вирусные атаки

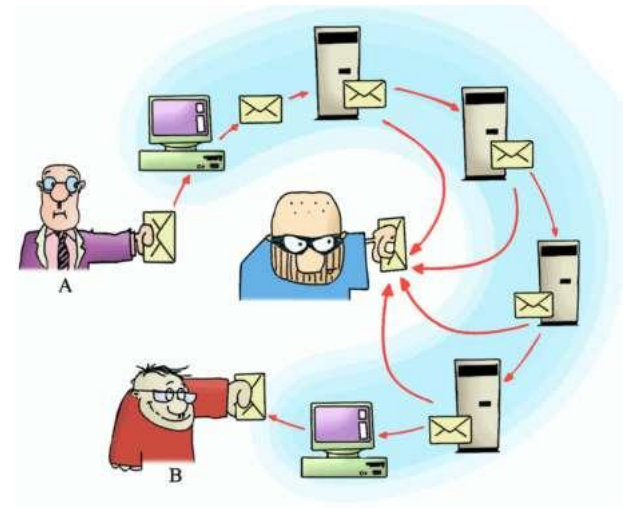
Социальная инженерия

метод
несанкционированного
доступа к
информационным
ресурсам, основанный на
особенностях психологии
человека



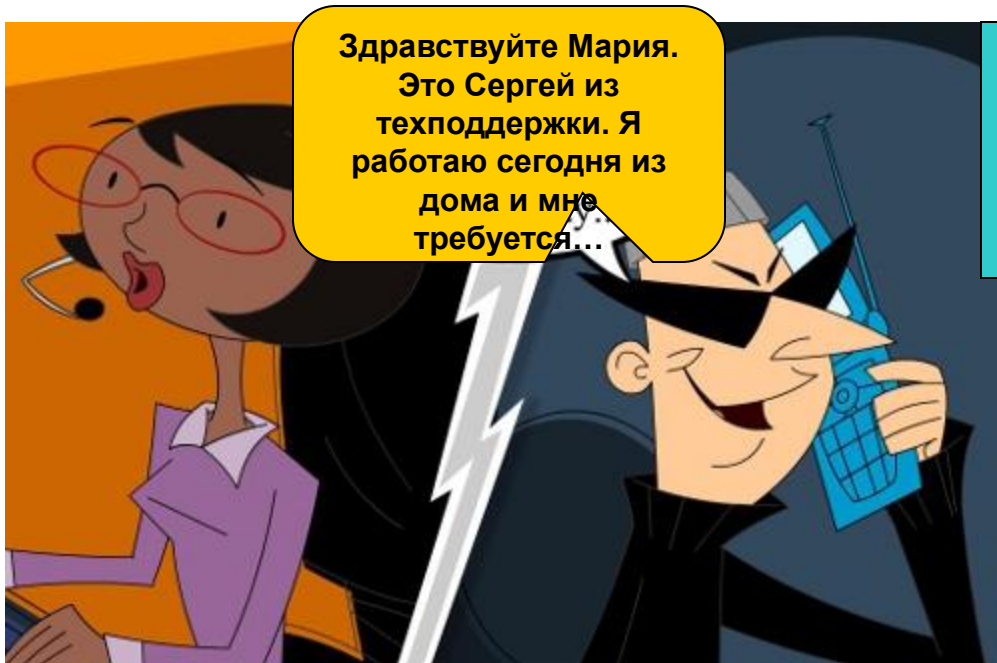
Методы социальной инженерии

- Претекстинг
- Фишинг
- Кви про кво
- Троянская программа
- Сбор сведений из открытых источников
- «Дорожное яблоко»
- Обратная социальная инженерия



Претекстинг

- набор действий, проведенный по определенному, заранее готовому сценарию (претексту)



Здравствуйте Мария.
Это Сергей из
техподдержки. Я
работаю сегодня из
дома и мне
требуется...

Злоумышленнику необходимо
получение конфиденциальной
информации. При этом требуется
предварительное исследование, для
обеспечения доверия.

ФИШИНГ

- разновидность социальной инженерии, целью которой является получение доступа к конфиденциальным данным пользователей — логинам и паролям



Пример фишингового письма от платёжной системы Яндекс. Деньги, где внешне подлинная веб-ссылка ведёт на фишинговый сайт

Обратите
внимание –
название сайта
дано
неправильно

Яндекс

деньги 

Уважаемый пользователь,

Согласно пункту 4.4.3.6. Соглашения об использовании Системы "Яндекс Деньги", Ваш аккаунт должен пройти реактивацию счета в системе.

Для выполнения реактивации проследуйте по ссылке:

<https://money.yandex.ru/login.php?passport=QWELB&idkey=324389205282404&ncmd=627958>

Либо свяжитесь с одним из наших операторов:

ООО "ПС Яндекс.Деньги". 101049, г. Москва, ул. Вавилова, дом 40
тел.: +7 (495) 739-03-80

ООО "ПС Яндекс.Деньги", Петербургский филиал. 191190, г. Санкт-Петербург, ул. Радищева, д. 38,
тел.: +7 (812) 334-30-46

Письмо сгенерировано автоматически, пожалуйста, не отвечайте на него.

С уважением, ООО "ПС Яндекс.Деньги"



Дизайн =
Студия Артемия Лебедева

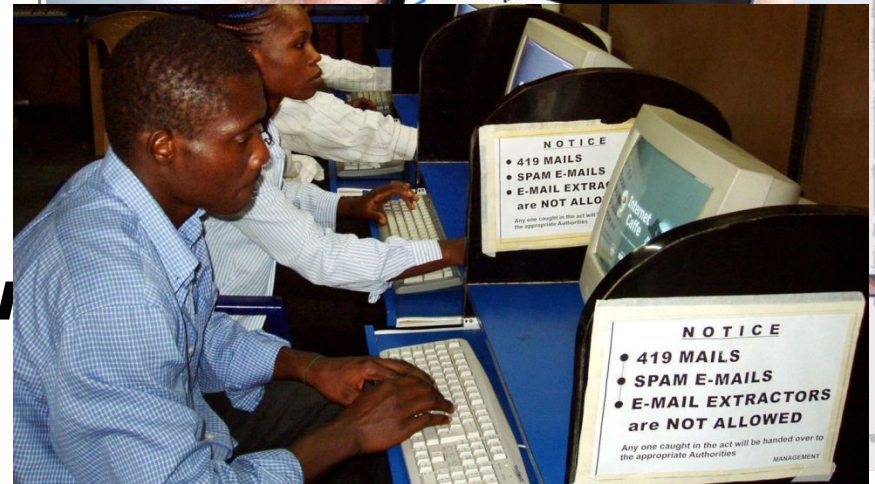
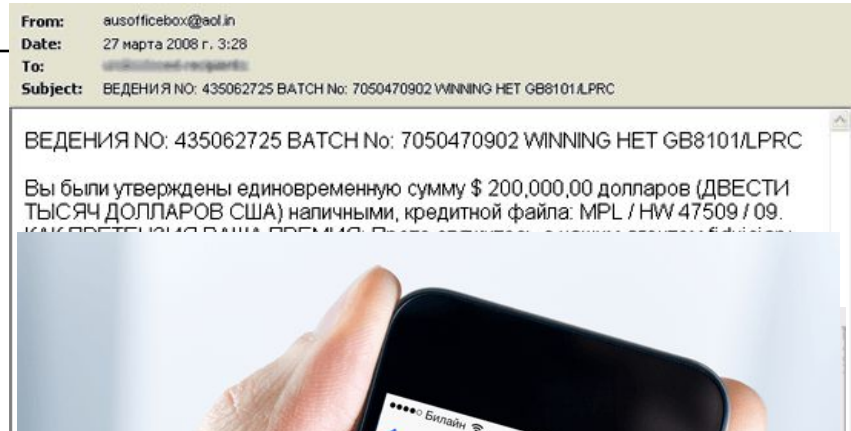
Copyright 2002 - 2006
"Яндекс", "PayCash"
[Мобильная версия](#)

2007 "ПС Яндекс.Деньги"
[О проекте](#)
[Статистика](#)
[Реклама](#)
[Обратная связь](#)

Встречающиеся фишинговые схемы

Использованием брендов известных компаний

- Подложные лотереи
- Ложное программное обеспечение
- Телефонный фишинг
- «Нигерийские письма»

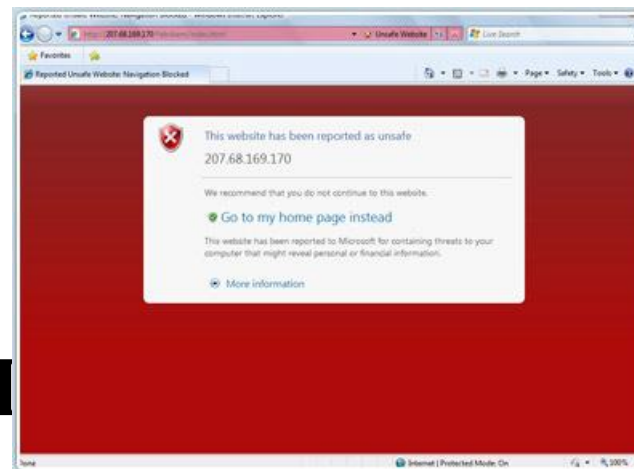


Методы защиты разработанные корпорацией Microsoft

○ Windows Internet Explorer



○ Использование фильтра Smart Screen



○ Windows Live H

○ Microsoft Office Outlook

Методы защиты с точки зрения пользователя

**Относитесь с подозрением к сообщениям,
в которых вас просят указать ваши
личные данные**

- Не заполнять полученные по электронной почте анкеты, предполагающие ввод личных данных
- Не переходите по ссылкам в электронных письмах в формате HTML

Технологические методы защиты

- **Убедитесь, что ваша антивирусная программа способна блокировать переход на фишинговые сайты или фишинг-фильтром**
- Регулярно проверяйте состояние своих банковских счетов и просматривайте банковские выписки
- **Следите за тем, чтобы у вас всегда была установлена последняя версия обновлений безопасности**

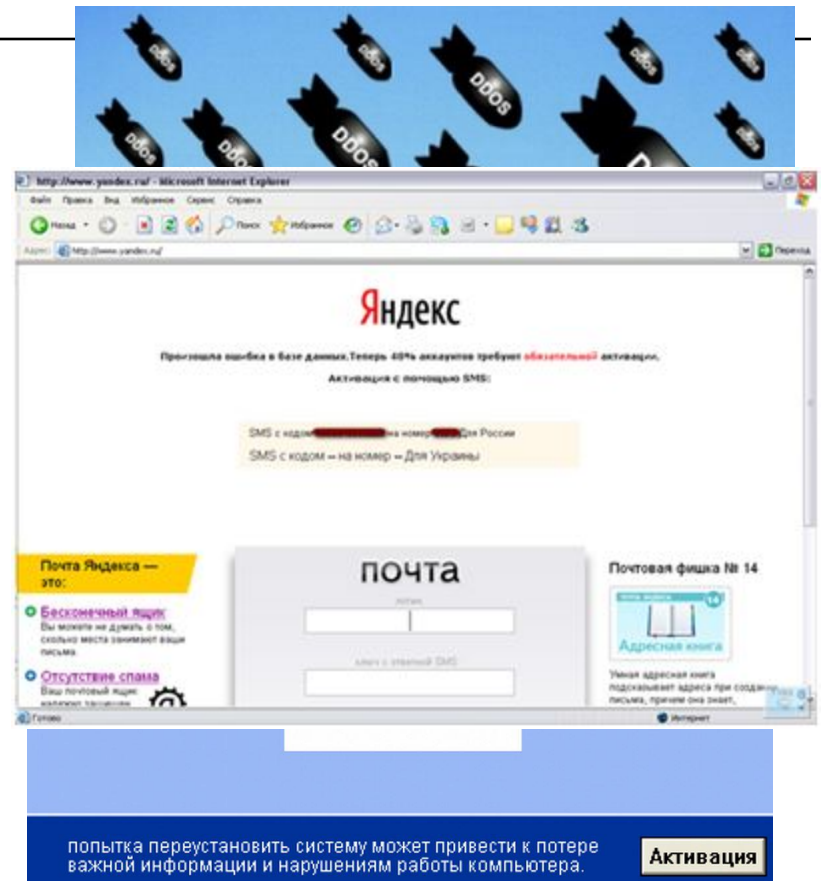
Троянская программа

вредоносная программа, используемая злоумышленником для сбора, разрушения или модификации информации, нарушения работоспособности компьютера или использования ресурсов пользователя в своих целях



Цели троянских программ

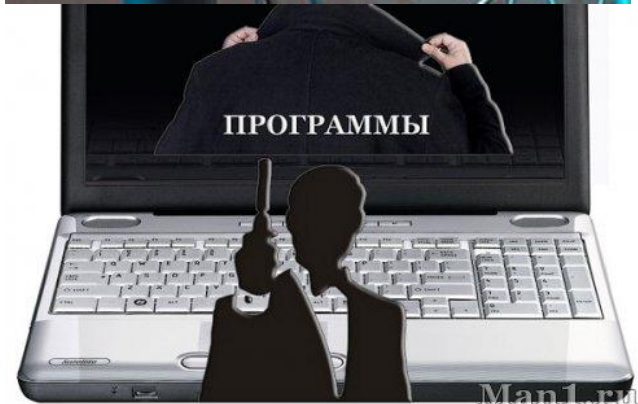
- **закачивание и скачивание файлов**
- копирование ложных ссылок, ведущих на поддельные вебсайты
- **создание помех работе пользователя, баннеры**
- похищение персональных данных
- **распространение вредоносных программ для проведения DDOS-**



Цели троянских программ

уничтожение данных
(стирание или
переписывание данных на
диске, труднозамечаемые
повреждения файлов)

- **использование адресов электронной почты для рассылки спама**
- шпионство за пользователем
- дезактивация или создание помех работе антивирусных программ и файервола
- удаленное

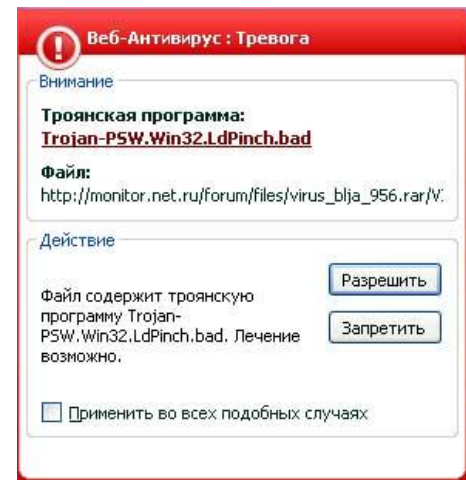
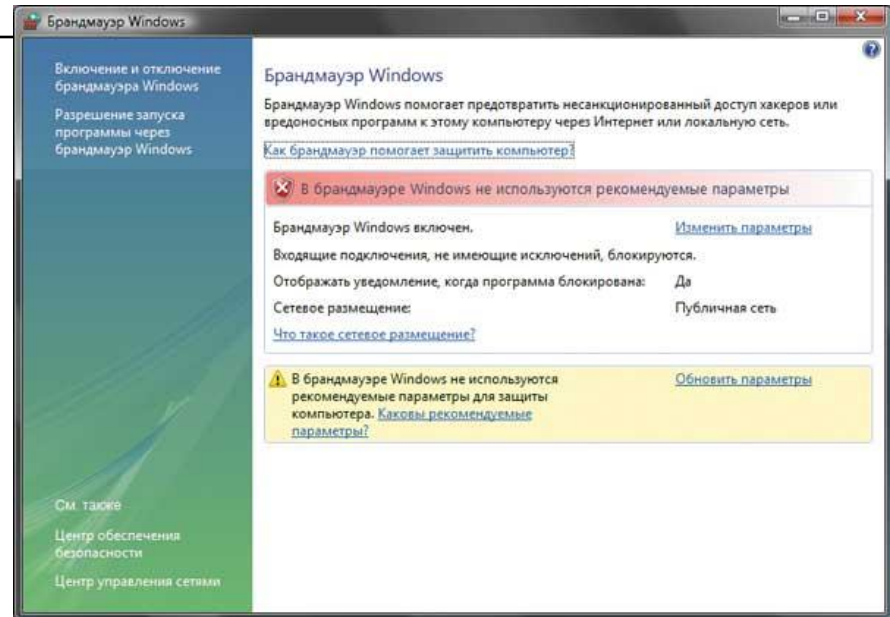


Отличие троянских программ от компьютерных вирусов

Принципиальное различие троянских программ и вирусов состоит в том, что вирус представляет собой самостоятельно размножающуюся программу, тогда как троянец не имеет возможности самостоятельного распространения. Однако в настоящее время довольно часто встречаются гибриды — вирусы (в основном e-mail и сетевые черви), вместе с которыми распространяются троянские программы.

Методы защиты

Защита компьютера с помощью антивирусной программы. В паре с антивирусом могут работать брандмауэры или файерволы.



Методы защиты

- Работа в системе с ограниченными правами
- Загрузка файлов только из проверенных источников
- Не допускать к компьютеру посторонних
- Использовать малораспространенные программы для работы в сети



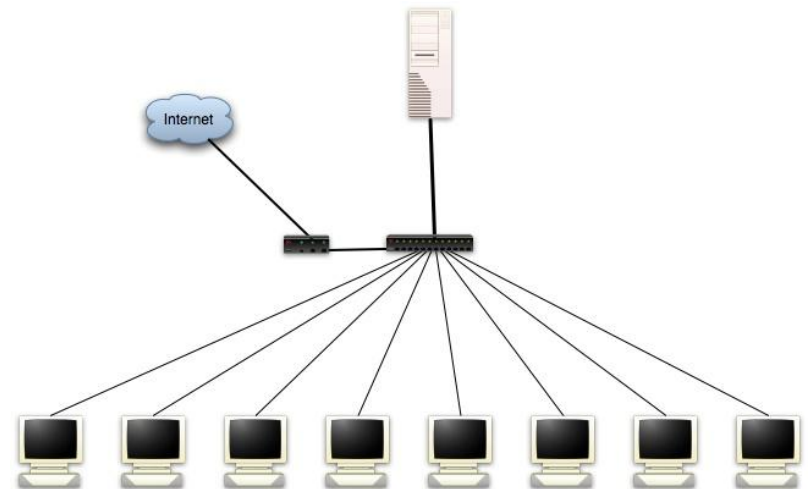
DOS – атака (отказ в обслуживании)

хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён.



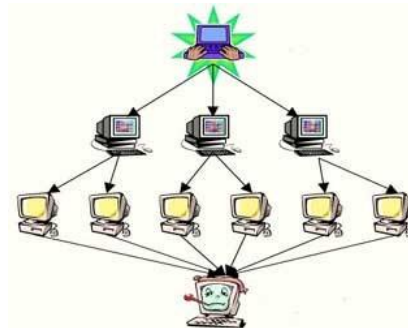
Способы защиты

- облачная технология
- использование нескольких удаленных серверов
- обратная DDOS-атака



DDOS – атака (распределенный отказ в обслуживании)

Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDOS-атаке**. Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищенной крупной компании или правительственной организации.





Спасибо за внимание!!