Друзья мои! Я очень рада
Войти в приветливый Ваш класс
И для меня уже награда
Вниманье ваших умных глаз.
Я знаю: каждый в классе гений.
Но без труда талант не впрок.
Скрестите шпаги ваших мнений-
Давайте же начнем урок!

Сетевые черви и защита от них

11 класс

Цели урока:

- получить представление о видах сетевых червей, способах их распространения и последствиях заражения ими компьютеров;
- познакомить со способами защиты от них.

План урока.

1. Актуализация знаний по теме «Защита от несанкционированного доступа к информации» (фронтальный опрос, доклад).
2. Объяснение нового материала «Сетевые черви и защита от них»(презентация).
3. Практическая работа.
4. Подведение итогов урока.
5. Запись домашнего задания.

1. Повторение

1. Какие способы защиты от несанкционированного доступа к информации вы знаете?
2. Как защищается информация в компьютере с использованием паролей?
3. Какие биометрические системы защиты информации вы знаете?
4. Что такое вредоносные программы?
5. Какую ответственность несут граждане России за создание, использование и распространение вредоносных программ?

1. Повторение

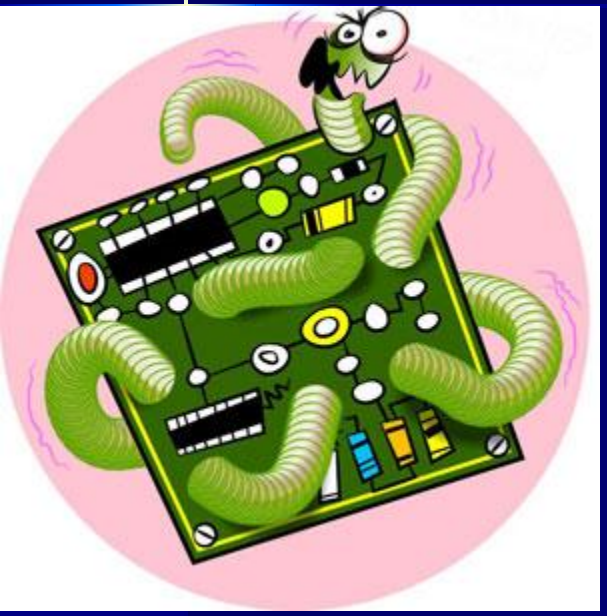
6. Какие способы проникновения вредоносных программ на компьютер вы знаете?
7. В чём назначение антивирусных программ?
8. Назовите наиболее популярные антивирусные программы?
9. Можно ли устанавливать на одном и том же компьютере две разные антивирусные программы?
10. В чём заключается принцип работы антивирусных программ?
11. Как антивирусная программа осуществляет поиск известных вирусных программ?
12. Как антивирусная программа осуществляет поиск новых вирусных программ?
13. Что такое антивирусный монитор и антивирусный сканер? Чем они отличаются?
14. В чём недостаток антивирусных программ?
15. Какие признаки заражения компьютера вы знаете?
16. Что необходимо сделать в первую очередь в случае заражения компьютера вирусом?

1. Повторение

17. Какие типы компьютерных вирусов существуют в зависимости от «среды обитания»?
18. Что вы о них знаете?
19. Какая антивирусная программа установлена на школьных компьютерах?
20. Кто является создателем этой антивирусной программы?
21. Доклад «Евгений Касперский».

2. Объяснение нового материала.

Сетевые черви - это вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей (Всемирную паутину, электронную почту и т. д.).



Активизация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

Основным признаком различия типов червей является способ их распространения, т.е. как он передает свою копию на удаленные компьютеры.

Многие сетевые черви **используют более одного способа** распространения своих копий по компьютерам локальных и глобальных сетей.

Типы компьютерных червей

WebWeb-черви
(через Web – серверы)

Скрипты

Почтовые черви
(через электронную почту)

Web-черви

Web-черви – это тип компьютерных червей, использующие для своего распространения Web-серверы.

Этапы заражения

1 этап:

червь проникает в компьютер-сервер и модифицирует (изменяет) Web-страницы сервера.

2 этап:

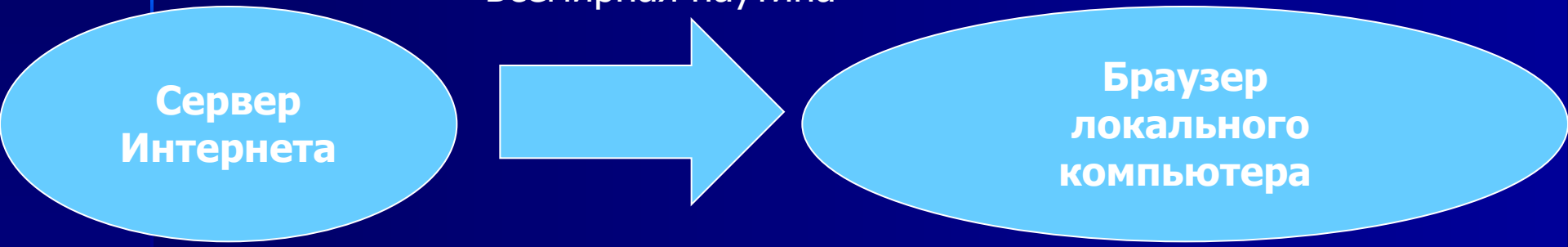
червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают в браузере зараженную Web-страницу), и таким образом проникает на другие компьютеры сети.

назад

Следующая страница

Скрипты – это программы на языках программирования JavaScript или VBScript, которые могут содержаться в файлах Web-страниц.

Заражение локального компьютера



Профилактическая защита от таких червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер. С этой целью наиболее эффективны **Web-антивирусные программы.**

Web-антивирусные программы

- межсетевой экран
- модуль проверки скриптов на языках JavaScript и на

Назад

Межсетевой экран

Следующая страница

Межсетевой экран (брандмауэр) — это программное или аппаратное обеспечение, которое проверяет входящую на компьютер информацию из локальной сети или Интернета, а затем отклоняет эту информацию или пропускает в компьютер в зависимости от параметров настройки брандмауэра.

Назначение: обеспечивает проверку всех Web-страниц, поступающих на компьютер пользователя. Каждая Web-страница перехватывается и анализируется межсетевым экраном на присутствие вредоносного кода.

Распознавание вредоносных программ

База данных

Эвристический алгоритм

назад

Результаты работы межсетевого экрана

Если Web-страница, к которой обращается пользователь, **содержит вредоносный код**, то доступ к ней блокируется. На экран выводится сообщение о том, что запрашиваемая страница заражена

Если Web-страница **не содержат вредоносного кода**, то она становится доступной для пользователя

Если на компьютере используются такие программы, как сетевые игры, которым требуется принимать информацию из Интернета или локальной сети, то межсетевой экран запрашивает пользователя о блокировании или разрешении подключения.

Если пользователь разрешает подключение, брандмауэр создает исключение, чтобы в будущем не тревожить пользователя запросами по поводу поступления информации для этой программы

Проверка скриптов в браузере.

Проверка всех скриптов, обрабатываемых в браузере, производится следующим образом - каждый запускаемый на Web-странице скрипт перехватывается модулем проверки скриптов и анализируется на присутствие вредоносного кода.

Результаты проверки скриптов

если скрипт содержит вредоносный код, модуль проверки скриптов блокирует его, уведомляя пользователя специальным всплывающим сообщением

если в скрипте не обнаружено вредоносного кода, то он выполняется

Почтовые черви

Способы распространения

червь либо отсылает свою копию в виде вложения в электронное письмо - в этом случае код червя активизируется при открытии (т.е. запуске) зараженного вложения.

червь отсылает ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (в этом случае червь активизируется при открытии ссылки на зараженный файл).

Вывод: В обоих случаях эффект одинаков — активизируется код червя

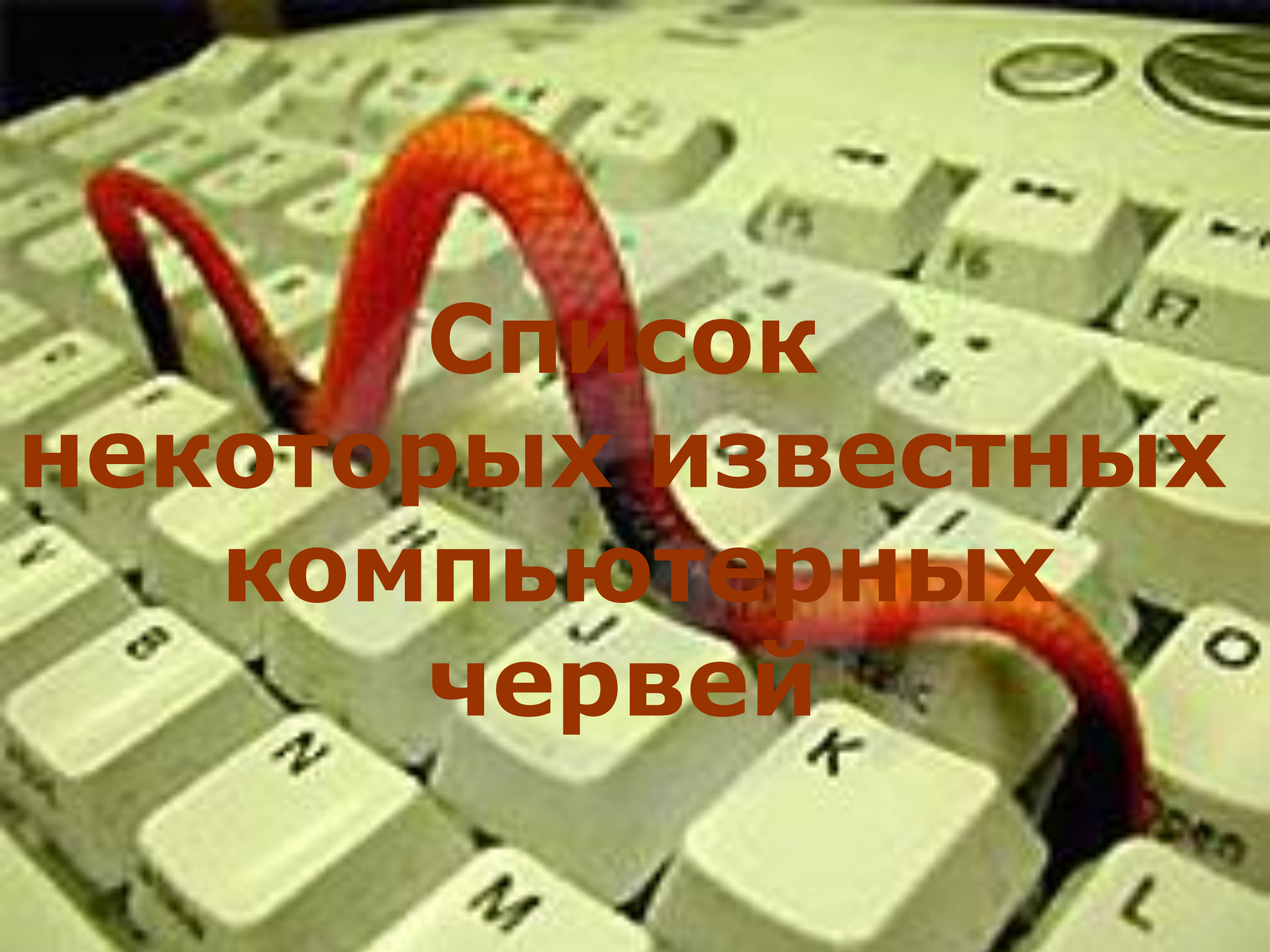
Лавинообразная цепная реакция распространения почтового червя заключается в том, что червь после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя.

Профилактическая защита

не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.

рекомендуется своевременно устанавливать обновления системы безопасности операционной системы и приложений

Познакомимся со списком некоторых известных компьютерных червей.

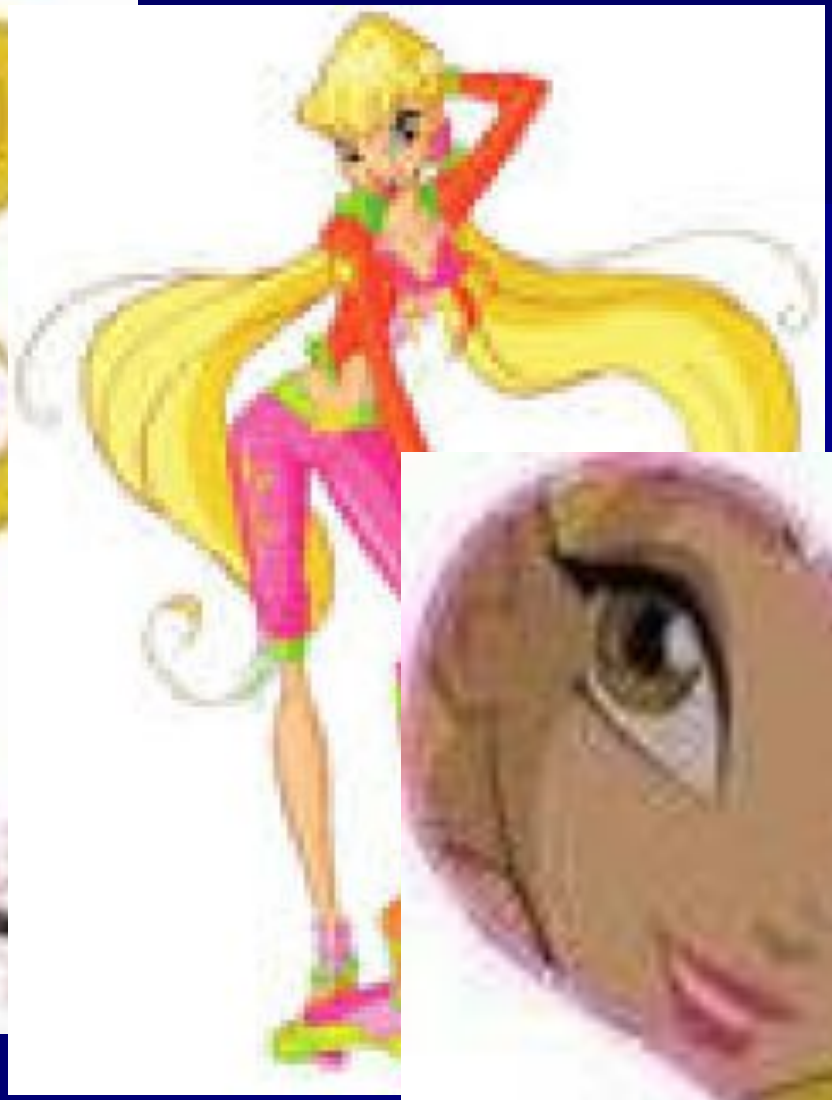


Список некоторых известных компьютерных червей

▪Из средств массовой информации

Май 2000 года

- Появился червь «I love you» - один из самых вредоносных за всю историю.
- По некоторым оценкам, он обошёлся пользователям ПК по всему миру больше чем в 10 млрд $.



▪Из средств массовой информации

6 июня 2001 г.

За фотографиями
«победительниц конкурсов красоты»
скрывался опасный Интернет-червь.

"Лаборатория Касперского", российский лидер в области разработки систем информационной безопасности, предупреждает пользователей об обнаружении нового и опасного Интернет-червя "I-Worm. MsWorld".

Во избежание его дальнейшего распространения компания рекомендует пользователям внимательно ознакомиться с описанием этого Интернет-червя, что позволит предотвратить его проникновение на компьютеры:

а) Данный Интернет-червь является Windows-программой размером около 130 килобайт.

б) Червь распространяется при помощи вложенных файлов в сообщениях электронной почты, для чего использует популярную почтовую программу Microsoft Outlook.

в) Рассылаемые червем письма выглядят следующим образом:

Заголовок: Miss World
Текст: Hi, %имя получателя%
Enjoy the latest pictures of Miss World from various Country

г) Имя файла-носителя червя может изменяться.

д) При открытии вложенного файла червь последовательно выводит несколько изображений Мисс мира.

После этого Интернет-червь получает доступ к программе Microsoft Outlook, считывает из адресной книги первые 50 адресов и рассылает по этим адресам свои копии, а затем форматируют все системные диски.

Из средств массовой информации

Декабрь **2004** года

- Запущен червь SantyЗапущен червь Santy — первый червь, использующий для распространения веб-сайты.
- Этот червь использует для нахождения своих жертв поисковую систему Google.

Из средств массовой информации

Май 2004 года

- Появляется червь Sasser, эксплуатировавший операционную систему Microsoft Windows и вызвавший многочисленные проблемы в сети.
- Иногда этот червь парализуя работу целых организаций.

Почта

Календарь

Заметки

Список папок

Домашнее задание.

п. 1.6.3.

Сетевые черви и защита от них.

Контрольные вопросы.

Тест.