Презентация подготовлена для конкурса «Интернешка» http://interneshka.org/

Компьютерные вирусы и Антивирусные программы

Работа Лепинских Анны 9«Б»
Г. Новоуральск
МАОУ «СОШ № 54»

КОМПЬЮТЕРНЫЕ ВИРУСЫ

- **Компьютерные вирусы –** программы, которые создают программисты специально для нанесения ущерба пользователям ПК. Их создание и распространение является преступлением.
- Вирусы могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков и до кументы. Активизация вируса может вызвать уничтожение программ и данных.. Первая эпидемия произошла в 1986г (вирус «Brain» - мозг по англ.) Всемирная эпидемия заражения почтовым вирусом началась 5 мая 2000г, когда компьютеры по сети Интернет получили сообщения «Я тебя люблю» с вложенным файлом, который и содержал вирус.

ПО МАСШТАБУ ВРЕДНЫХ ВОЗДЕЙСТВИЙ

- ***Безвредные*** – не влияют на работу ПК, лишь уменьшают объем свободной памяти на диске, в результате своего размножения
- ***Неопасные*** – влияние, которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами;
- ***Опасные*** – приводят к сбоям и зависаниям при работе на ПК;
- ***Очень опасные*** – приводят к потери программ и данных (изменение, удаление), форматированию винчестера и тд.

ПО СРЕДЕ ОБИТАНИЯ

- **Файловые вирусы** - способны внедряться в программы и активизируются при их запуске. Из ОП вирусы заражают другие программные файлы (com, exe, sys) меняя их код вплоть до момента выключения ПК. Передаются с нелегальными копиями популярных программ, особенно компьютерных игр. Но не могут заражать файлы данных (изображения, звук)
- **Загрузочные вирусы** - передаются через зараженные загрузочные сектора при загрузке ОС и внедряется в ОП, заражая другие файлы. Правила защиты:1)Не рекомендуется запускать файлы сомнительного источника (например, перед загрузкой с диска А – проверить антивирусными программами); 2) установить в BIOS ПК (Setup) защиту загрузочного сектора от изменений
- **Макровирусы** - заражают файлы документов Word и Excel. Эти вирусы являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов. Угроза заражения прекращается после закрытия

АНТИВИРУСНАЯ ПРОГРАММА

Антивирусная программа - програма, предназначенная для борьбы с компьютерными вирусами.

В своей работе эти программы используют различные принципы для поиска и лечения зараженных файл ов.

Для нормальной работы на ПК каждый пользователь должен следить за обновлением антивирусов.

Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

Имеются различные типы антивирусных программ – полифаги, ревизоры, блокировщики, сторожа, вакцины и пр.

ТИПЫ АНТИВИРУСНЫХ ПРОГРАММ

- **Антивирусные сканеры –** после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса
- **Антивирусные сторожа (мониторы) –** постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП
- **Полифаги –** самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов. Занимают много места, работают не быстро
- **Ревизоры –** проверяют изменение длины файла. Не могут обнаружить вирус в новых файлах (на дискетах, при распаковке), т.к. в базе данных нет сведений о этих файлах
- **Блокировщики –** способны обнаружить и остановить вирус на самой ранней стадии его развития (при записи в загрузочные сектора дисков). Антивирусные блокировщики могут входить в BIOS Setup.

СПИСОК НЕКОТОРЫХ АНТИВИРУСНЫХ ПРОГРАММ

- **AVG Anti-Virus Free** - (русский) - популярный антивирус, в случае домашнего применения используется бесплатно. Основные преимущества, быстрой, простой, не требователен к ресурсам.
  Dr.Web CureIt! - Бесплатная утилита Dr.Web CureIt! Лучшее средство для проверки Вашего компьютера и лечения от вирусов реальном времени.
- **NOD32 On-DemandScanner** - антивирусный сканер бесплатная версия антивируса NOD32, может быстро и легко обнаружить и удалить вирусы, интернетовские черви, троянских коней и другие вредные программы.

СПИСОК НЕКОТОРЫХ АНТИВИРУСНЫХ ПРОГРАММ

- **Avast! AntivirusHome** - бесплатный антивирусный сканер. Использует резидентный и обычный сканеры, сканирует архивов, проверяет почту, интегрируется в систему Windows, русский.
  Norton Internet Security - бесплатная подписка в течении месяца на один год. NIS-360 имеет антивирус, файрвол и нужные инструменты от всех видов угроз.
- **Immunet Protect** - бесплатный облачный антивирус. Преимущества перед коллегами: не конфликтует с другим антивирусным, не большие размеры, высокая скорость, постоянные обновления базы.
- **Microsoft Security Essentials** - бесплатная антивирусная программа, имеет все необходимые средства защиты компьютера. Простая в использовании

Как правильно выбрать антивирусную программу?

- 1)Ни в коем случае нельзя устанавливать два и более, каждый из них борется за свое единственное существование в системе компьютера, а другие определяет как вредоносную программу.
- 2) Для правильного выбора антивируса играет роль и мощность вашего компьютера. Если компьютер слабоват – лучше пробовать антивирусы с небольшим потреблением оперативной памяти, чтобы не нагружать систему. Если компьютер постоянно подключен к Интернету – необходимо выбирать антивирус, содержащий в себе сетевой экран, защищающий от вплывающих окон и попадания на вредоносные сайты.
  3) В выборе антивирусной программы можно руководствоваться рейтингами антивирусов, которые проводятся независимыми лабораториями.
- 4) При выборе платного или бесплатного варианта антивирусной программы следует для себя определиться, насколько важна информация на компьютере. Если вы платите деньги за антивирус, то вправе требовать оперативной поддержки и решения возникших проблем при форс-мажорных обстоятельствах.
- 5) Можно дать только один совет, как правильно выбрать антивирус для защиты системы. Попробовать в пользовании каждый антивирус в течение месяца. На это уйдет продолжительное время, но для себя вы сможете определиться, какой антивирус больше всего вам понравился в работе. Кроме этого, при использовании постоянных антивирусов периодически пробуйте дополнительно проверять компьютер другими бесплатными антивирусными утилитами. Так вы сможете самостоятельно убедиться в эффективности установленного антивируса и сделать соответствующие выводы.

ВИРУСЫ МОБИЛЬНОГО ТЕЛЕФОНА

- **Мобильные вирусы** — это небольшие программы, предназначенные для вмешательства в работу мобильного телефона, смартфона, коммуникатора, которые записывают, повреждают или удаляют данные и распространяются на другие устройства через SMS и Интернет.

ПРОИСХОЖДЕНИЕ МОБИЛЬНЫХ ВИРУСОВ

- Впервые о мобильных вирусах заговорили ещё в 2000 году. Вирусами назвать их было тяжело, так как это был набор команд, исполняемый телефоном, который передавался через SMS. Такие сообщения забивали соответствующие ячейки памяти и при удалении блокировали работу телефона. Наибольшее распространение получили команды для таких телефонов, как Siemens и Nokia.
- Тенденция такова, что: чем функциональнее телефон, тем большему количеству угроз он подвержен. Любые команды, функции и возможности, позволяющие создавать программы и приложения для мобильных телефонов, могут стать инструментом для создания вирусов. Наиболее перспективной платформой для написания вирусов является Java 2ME, так как подавляющее большинство современных телефонов поддерживает данную платформу.
- Основной целью мобильных вирусов, как и в случае с компьютерными вирусами, является получение персональной информации, которую можно продать или использовать в личных нуждах. К такой информации могут относиться личные данные владельца телефона, данные самого устройства, личные сообщения, иногда номера кредитных карт.

МОБИЛЬНЫЙ ВИРУС

- На данный момент самым распространенным способом заражения мобильного телефона вирусом считается загрузка файлов с компьютера или интернета, хотя многие считают, что в дальнейшем больше всего вирусов будут передаваться от телефона к телефону.
- На сегодняшний день больше всего вирусов передается на телефоны, работающие под управлением операционной системы Symbian. Однако, большинство операционных систем для мобильного телефона изначально защищены от массовой атаки вирусов.
- Зараженные файлы обычно маскируются под игры, программы безопасности, спам и, конечно, порнографические файлы. Некоторые вирусы иногда маскируются под сообщения от ваших друзей или знакомых, которые вы, конечно же, захотите прочитать. Но для того, чтобы вирус из сообщения проник в саму систему, недостаточно просто открыть это сообщение. Необходимо установить ту программу, которую вы получаете в сообщение, но до настоящего времени еще никто не придумал, как создать самораспаковывающийся телефонный вирус.

РАСПРОСТРАНЕНИЕ ВИРУСОВ

- через Интернет - вирус распространяется также, как и обычный компьютерный вирус. Пользователь загружает инфицированный файл на телефон через компьютер или мобильный интернет. Инфицированными могут быть загрузочные файлы, всплывающая реклама, рингтоны, игры и различные программы.
- через Bluetooth – вирусы могут передаваться во время передачи данных с одного телефона на другой через Bluetooth. Его может послать любой человек, находящийся в зоне действия Bluetooth, поэтому рекомендуется всегда ставить ограничение доступа других устройств к вашему мобильному телефону. В данном случае вирус распространяется также, как любая инфекция.
- через мультимедийные сообщения MMS - вирус прикрепляется к текстовому сообщению MMS точно также, как и компьютерный вирус, переданный по электронной почте. Пользователь должен открыть само приложение и установить его в телефон, только тогда вирус сможет проникнуть в систему телефона и начать действовать. Как правило, вирус, переданный по MMS, проникает в список контактов и сам рассылается по всем телефонным номерам.

ДЕЙСТВИЕ ВИРУСОВ

- Первый известный вирус мобильного телефона Cabir был абсолютно безвреден. Он просто забирался в телефон и пытался проникнуть как можно дальше. Однако, другие мобильные вирусы не такие уж и небезопасные. Вирус может проникать в телефонную книгу и удалять всю информацию о контактах или удалять заметки в вашем телефоне. Мобильный вирус также может разослать инфицированные сообщения на любой телефонный номер, записанный в вашей записной книге. Мало того, что он просто проникает в систему, он еще тратит деньги с вашего счета на рассылку всех своих сообщений вашим же друзьям, родственникам и деловым партнерам. Самое худшее, на что способен вирус, так это удалить или закрыть некоторые приложения или же полностью вывести ваш мобильный телефон из строя. Ниже приводится список всех самых распространенных мобильных вирусов и их воздействие на телефон.

СПИСОК ВИРУСОВ МОБИЛЬНОГО ТЕЛЕФОНА

- **Cabir. A** Дата появления - июнь 2004 Цель для поражения: мобильные телефоны с операционной системой Symbian 60
  Способ распространения: через Bluetooth
  Вред: никакого
- **Skulls.A** Дата появления - ноябрь 2004
  Цель для поражения: мобильные телефоны с операционной системой Symbian
  Способ распространения: через интернет
  Вред: блокирование всех функций телефона, кроме приема и совершения звонков
- **Commwarrior. A** Дата появления – январь 2005
  Цель для поражения: мобильные телефоны с операционной системой Symbian 60
  Способ распространения: через Bluetooth и MMS
  Вред: отсылает дорогие MMS сообщения на все номера телефонов, записанных в записной книжке
- **Locknut.B** Дата появления – март 2005
  Цель поражения: мобильные телефоны с операционной системой Symbian 60
  Способ распространения: через интернет
  Вред: разрушает память ROM, блокирует все функции телефона, активирует другие вредоносные программы
- **Fontal.A** Дата появления – апрель 2005
  Цель поражения: мобильные телефоны с операционной системой Symbian 60
  Способ распространения: через интернет
  Вред: полностью выводит телефон из строя.

ЗАЩИТА МОБИЛЬНОГО ТЕЛЕФОНА

- **1.** Выключите Bluetooth или закройте доступ для других пользователей.

- **2.** Проверьте свою систему безопасности, попытайтесь отыскать в своих папках любой незнакомый для вас файл с подозрительным названием . Правда, это помогает не всегда, поскольку, например, вирус Commwarrior выбирает любое название для всех своих зараженных файлов. Однако, в большинстве случаев вирус все же можно вычислить по имени файла. В интернете можно также отыскать сайты, которые борются с распространением вирусов. Вы можете сделать заявку на одном из таких сайтов, и на ваш телефон пришлют полное описание вируса и способы борьбы с ним. Наиболее популярными считаются сайты - F-Secure, McAfee и Symantec.
- **3.** Установите на мобильный телефон любой антивирусник. Многие компании разрабатывают программные средства защиты данных мобильных телефонов, некоторые из них можно бесплатно загрузить в интернете, другие можно только купить, также есть специальные программы, предназначенные только для мобильных операторов. Сразу после установления такие программы могут выявить и удалить вирус, и в дальнейшем защитить ваш телефон от проникновения некоторых видов вирусов. Компания Symbian специально разработала версию антивирусника для защиты своей операционной системы, которая принимает только надежные файлы.

КАК ЗАЩИТИТЬ ФЛЕШКУ ОТ ВИРУСОВ

- Часто ли вам приходится очищать flash-накопитель (флешку) от вирусов, которые распространяются через файл autorun.inf? Особенно смешно смотреть на лица пользователей ПК, у которых после успешной работы с флешкой на одном компьютере и открытии её потом на своём, исчезают все файлы. И что самое интересное, никто не желает предпринимать никаких действий для защиты своих флеш-накопителей, так и бегают к своим сисадминам с просьбой вернуть файлы. А ведь существуют несколько способов,...

ПРОГРАММЫ ДЛЯ ЗАЩИТЫ USB НАКОПИТЕЛЯ

- Как уже было сказано, все бесплатные программы, помогающие защитить флешку от вирусов действуют примерно одинаково, внося изменения и записывая собственные файлы autorun.inf, устанавливая права на доступ к этим файлам и предотвращая запись вредоносного кода на них (в том числе, когда вы работаете с Windows, используя аккаунт администратора). Отмечу наиболее популярные из них.
- Bitdefender USB Immunizer
- Бесплатная программа от одного из ведущих производителей антивирусов не требует установки и очень проста в использовании. Просто запустите ее, и в открывшемся окне вы увидите все подключенные USB накопители. Кликните по флешке, чтобы защитить ее.

ЗАЩИТА ФЛЕШКИ ВРУЧНУЮ

- Защита флешки вручную
- Все, что нужно для предотвращения заражения флешки вирусами можно проделать и вручную без использования дополнительных программ.