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

Компьютерные вирусы. Антивирусы программы

Презентацию подготовил:
ученик 9 А класса
Повод Артем

В ряду технологический нововведений почти у каждого дома есть компьютер, содержащий важные файлы. Нужно защищать файлы от вирусов.

В презентации мы рассмотрим виды вирусов и как обезопасить свой компьютер от вирусов.

Что такое компьютерный вирус?

- **Компьютерный вирус** – вид вредоносного программного обеспечения, способный создавать копии самого себя и внедрятся в код других программ, системные области памяти, загрузочные секторы, а так же распространять свои копии по разнообразным каналам связи, с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера.

История создания вирусов

- Первый вирус появился в 1972 году, когда прекратила свое функционирование целая компьютерная сеть из состава «Эйрпанет». 19 апреля произошел сбой в работе устройств у нескольких тысяч пользователей. В этот день прекратилась любая передача данных, компьютеры выходили из строя.

Причины появления первого вируса

- Этот вирус стал результатом обычного розыгрыша от студента информационного отделения. Парень-практикант решил создать программу, с помощью которой хотел пошутить над своими коллегами. Он запланировал ее сделать так, чтобы она самостоятельно осуществляла запуск и имела возможность распространяться между отдельными компьютерами. Создавая эту программу, он даже не задумывался о последствиях, а именно о скорости распространения вируса. Он не предполагал, что скорость будет запредельной, а сама программа иметь способность уничтожать полезную информацию.

Люди после появления первого вируса

Виды вирусов

- **Загрузочные вирусы** проникают в загрузочные сектора устройств хранения данных .
- **Файловые вирусы** чаще всего внедряются в исполнительные модули программ (файлы с помощью которых производится запуск той или иной
- **Файлово-загрузочные вирусы** обедняют в себе возможности двух предыдущих групп, что позволяет им представлять серьезную угрозу работе компьютера.
- **Сетевые вирусы** распространяются посредством сетевых служб и протоколов. Таких как рассылка почты..
- **Документные вирусы** заражают файлы современных офисных систем через возможность использования в этих системах макросов.

Какие бывают вирусы и их степень опасности

- 1. **Вирусы-паразиты** – вирусы, работающие с файлами программ.Могут быть легко выявлены и уничтожены.
- 2. **Вирусы-репликаторы** – вирусы, основная задача которых как можно быстрее размножится всем возможным местам хранения данных и коммуникациям.
- 3. **Трояны -э**тот вид вирусов массирует свои модули под модули используемых программ, создавая файлы со схожими именами и параметрами
- 4. **Вирусы-невидимки** –наиболее сложны для обнаружения, так как имеют свои алгоритмы маскировки от сканирования.
- 5. **Самошифрующиеся вирусы** –хранится и распространяется в зашифрованном виде.
- 6. **Матирующиеся вирусы** – вирус постоянно меняет цепочки своего кода в процессе функционирования и размножения
- 7. "**Отдыхающие" вирусы** – являются очень опасными, так как могут очень продолжительное время находится в состоянии покоя.

Действие вируса

- 1. **Латентная стадия**. На этой стадии код вируса находится в системе, но никаких действий не предпринимает. Для пользователя не заметен. Может быть вычислен сканированием файловой системы и самих файлов.
- 2. **Инкубационная стадия**. На этой стадии код вируса активируется и начинает создавать свои копии, распространяя их по устройствам хранения данных компьютера, локальным и глобальным компьютерным сетям, рассылая в виде почтовых сообщений и так далее. Для пользователя может быть заметен, так как начинает потреблять системные ресурсы и каналы передачи данных, в результате чего компьютер может работать медленнее, загрузка информации из Интернет, почты и прочих данных может замедлятся.
- 3. **Активная стадия**. На этой стадии вирус, продолжая размножать свой код доступными ему способами, начинает деструктивные действия на которые ориентирован. Заметен пользователю, так как начинает проявляться основная функция вируса – пропадают файлы, отключаются службы, нарушается функционирование сети, происходит порча оборудования.

Что же такое антивирус?

- **Антивирусная программа** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ.

Первые антивирусы

- Появление первых вирусов привело к тому, что стало необходимостью создание антивирусной программы. Самая первая такая разработка принадлежала компании «Диалог-Наука». Ее антивирус выпускался на двух дискетах. Обновления выходили на таком же носителе каждую неделю. Удивительным фактом было то, что при обнаружении какого-либо вируса удаление не происходило. Для этого требовалось отослать результаты в лабораторию Москвы. Здесь уже разрабатывалось лекарство. Именно эта организация в последствие организовала известную во всем мире Лабораторию Касперского.

В чем заключается работа антивирусов?

- Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная *программа* объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.
- Из всех методов антивирусной защиты можно выделить две основные группы:
- **Сигнатурные методы** - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов
- **Эвристические методы** - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен

Сигнатурический анализ

- *Сигнатурный анализ* заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами.
- *Сигнатурой вируса* будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса.
- Задачу выделения сигнатур, как правило, решают люди - эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска.
- Практически в каждой компании, выпускающей антивирусы, есть своя *группа* экспертов, выполняющая *анализ* новых вирусов и пополняющая антивирусную базу новыми сигнатурами.
- Соотношение количества сигнатур и количества известных вирусов для каждой антивирусной базы свое и вполне может оказаться, что база с меньшим количеством сигнатур в действительности содержит информацию о большем количестве вирусов.Важное дополнительное свойство сигнатур - точное и гарантированное *определение* типа вируса. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вируса.

Эвристический анализ

- *Слово "эвристика"* происходит от греческого глагола "находить". Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок.

Какую же антивирусную программу выбрать?

Специалисты выделяют топ 5 :

- **Антивирус Касперского** - антивирус разработан "Лабораторией Касперского".
- **Symantec Norton AntiVirus** - продукт американской компании Symantec.
- **Dr. Web** - разработка ООО "Санкт-Петербургская антивирусная лаборатория Данилова".
- **NOD32** - компания ESET
- **Panda** - компания Panda

Антивирусные программы

Платные антивирусы

Kaspersky Internet Security 2015

- Плюсы: известный и авторитетный разработчик, отличная степень защиты.
- Минусы: сложности в обновлении , иногда не дает запустить точно «чистые» программы.

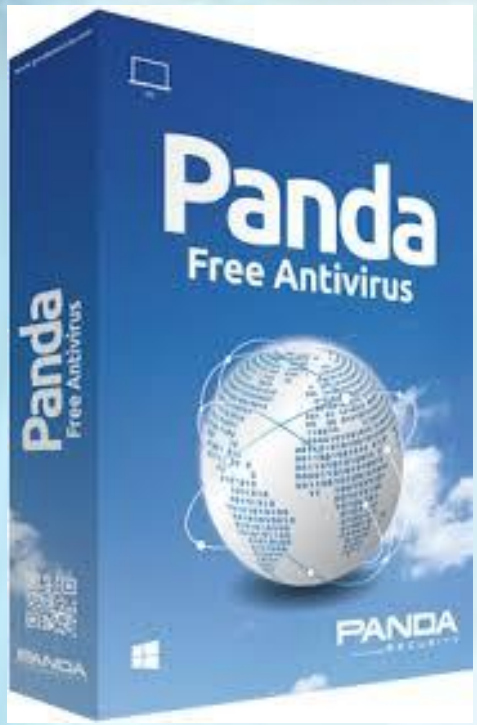
Norton 360

- Плюсы: высокая точность обнаружения вирусных угроз, удобный интерфейс.
- Минусы: излишняя самостоятельность.

Dr.Web Security Space

- Плюсы: известный и авторитетный разработчик, обширная антивирусная база, нет ложных реагирований, работает только с вирусами, отличное качество сканера.
- Минусы: относительно сложный интерфейс, долгое сканирование.

Бесплатные антивирусы



Panda Free Antivirus

Плюсы: Включает в себя облачный антивирус-антишпион, кроме этого, антивирус умеет блокировать подозрительные файлы, выдавая понятный любому пользователю подробный отчёт, позволяет работать без обновлений.

Минусы: в случае отсутствии интернета уровень защиты может быть значительно снижен.

ESET NOD 32

- **Плюсы:**
  - высокая производительность , антивирус практически не влияет на работу системы, интерфейс программы позволяет управлять защитой компьютера быстро и эффективно.

- **Минусы**
  - антивирусов: глубина его сканирования системы не всегда достаточна.

Если вдруг у вас появился вирус, то вот пару советов

- Установите антивирусную программу.
- Не открывайте сообщения электронной почты от незнакомых отправителей или вложения, которые вам неизвестны.
- Используйте функцию блокирования всплывающих окон в браузере.
- Регулярно обновляйте операционную систему.
- Используйте брандмауэр
- Используйте параметры конфиденциальности браузера.
- Включите контроль учетных записей.
- Очищайте кэш Интернета.

Источники информации

- http://wd-x.ru/history-of-the-first-virus/
- http://avdesk.kiev.ua/virus/83-virus.html
- http://informatika.sch880.ru/p16aa1.html
- https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0
- http://komputer-info.ru/luchshij-platnyj-antivirus-2014.html
- http://komputer-info.ru/luchshij-besplantniy-antivirus-2014.html

Будьте внимательны!