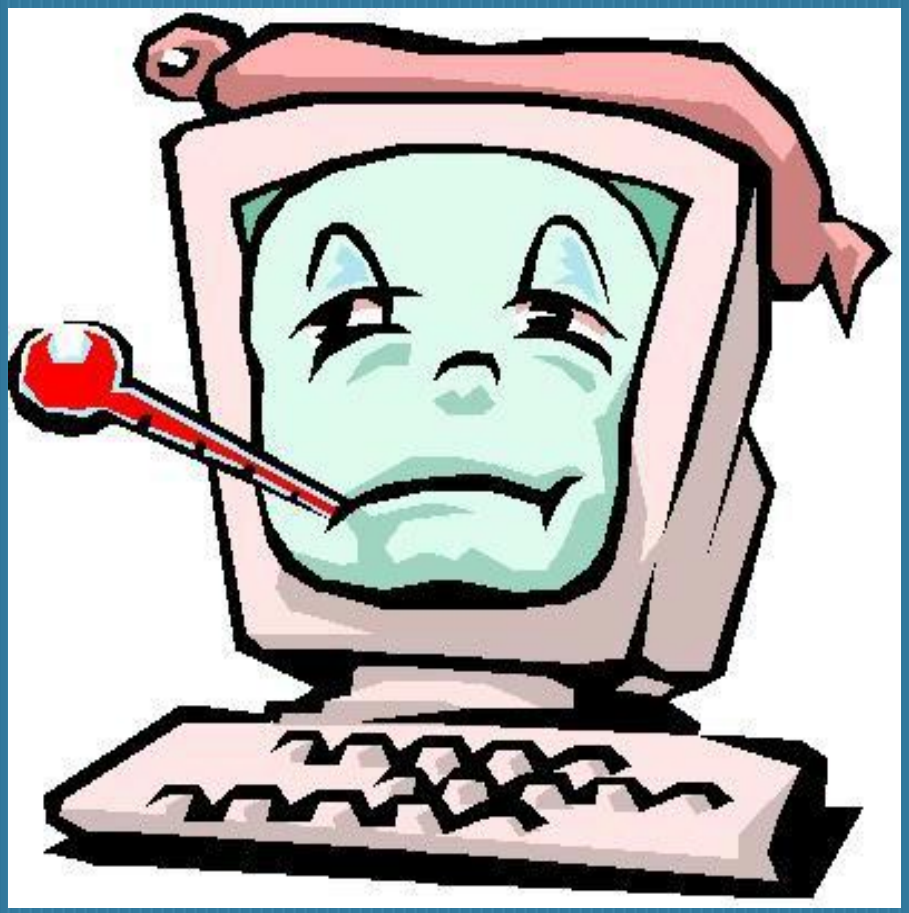
КОМПЬЮТЕРНЫЕ ВИРУСЫ

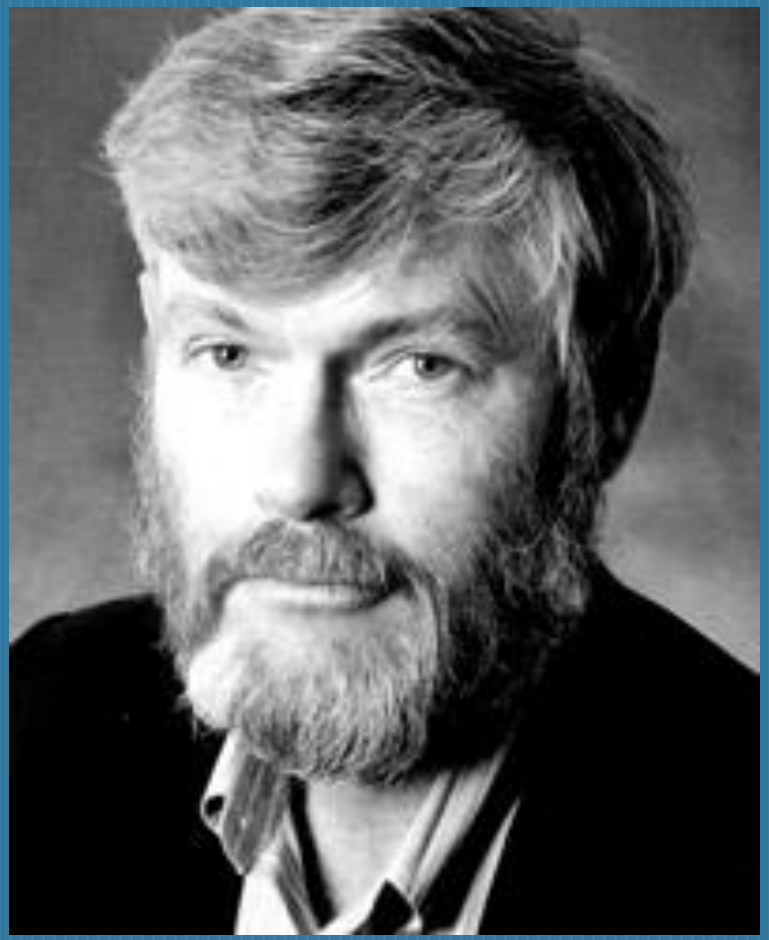
Что такое компьютерный вирус???

- Компью́терный ви́рус — компьютерная программа или вредоносный код, отличительным признаком которых является способность к размножению. В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру.



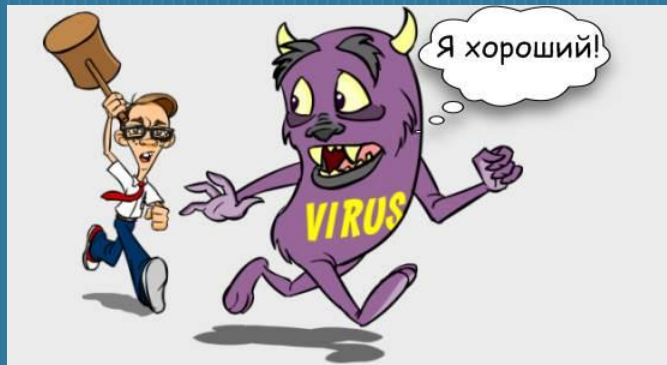
Почему именно «вирус»?

- Достоверно неизвестно, кто и когда первым употребил слово вирус по отношению к компьютеру. Это **Грегори Бенфорд** (на фото справа) — астрофизик и, по совместительству, писатель-фантаст из США. Многие считают, что именно в его рассказе **«Человек в шрамах»** (1970) слово «вирус» было впервые использовано по отношению к компьютерной программе.



Все ли вирусы приносят вред?

- Однако, не все **вирусы для компьютеров** столь враждебны. Некоторые из них просто выводят на экран монитора безобидные сообщения юмористического, рекламного или политического содержания. Никакого вреда для компьютера при этом не наблюдается. Чего не скажешь о пользователе, нервная система которого подвергается определённому испытанию. Испытанию, с которым далеко не все из нас могут справиться. Оторванные мышки, изуродованные клавиатуры и разбитые мониторы в роликах на YouTube — тому яркое подтверждение.



Классификация компьютерных вирусов:

- **Сетевой червь** — вид «враждебного» ПО, который способен самостоятельно распространяться с помощью локальных или глобальных компьютерных сетей. Первым представителем является уже упомянутый Morris worm.
- **Троянский конь, троян** — вид компьютерного вируса, распространяемого (загружаемого в ПК) непосредственно человеком. В отличие от червя, троян не может самопроизвольно захватывать тот или иной компьютер. Первым «троянским конём» в 1989 году стал компьютерный вирус AIDS.

Основные источники вирусов:

дискета, на которой находятся зараженные вирусом файлы;

компьютерная сеть, в том числе система электронной почты и Internet;

жесткий диск, на который попал вирус в результате работы с зараженными программами;

вирус, оставшийся в оперативной памяти после предшествующего пользователя.

Признаки вирусов

Основные ранние признаки заражения компьютера вирусом:

уменьшение объема свободной оперативной памяти;

замедление загрузки и работы компьютера;

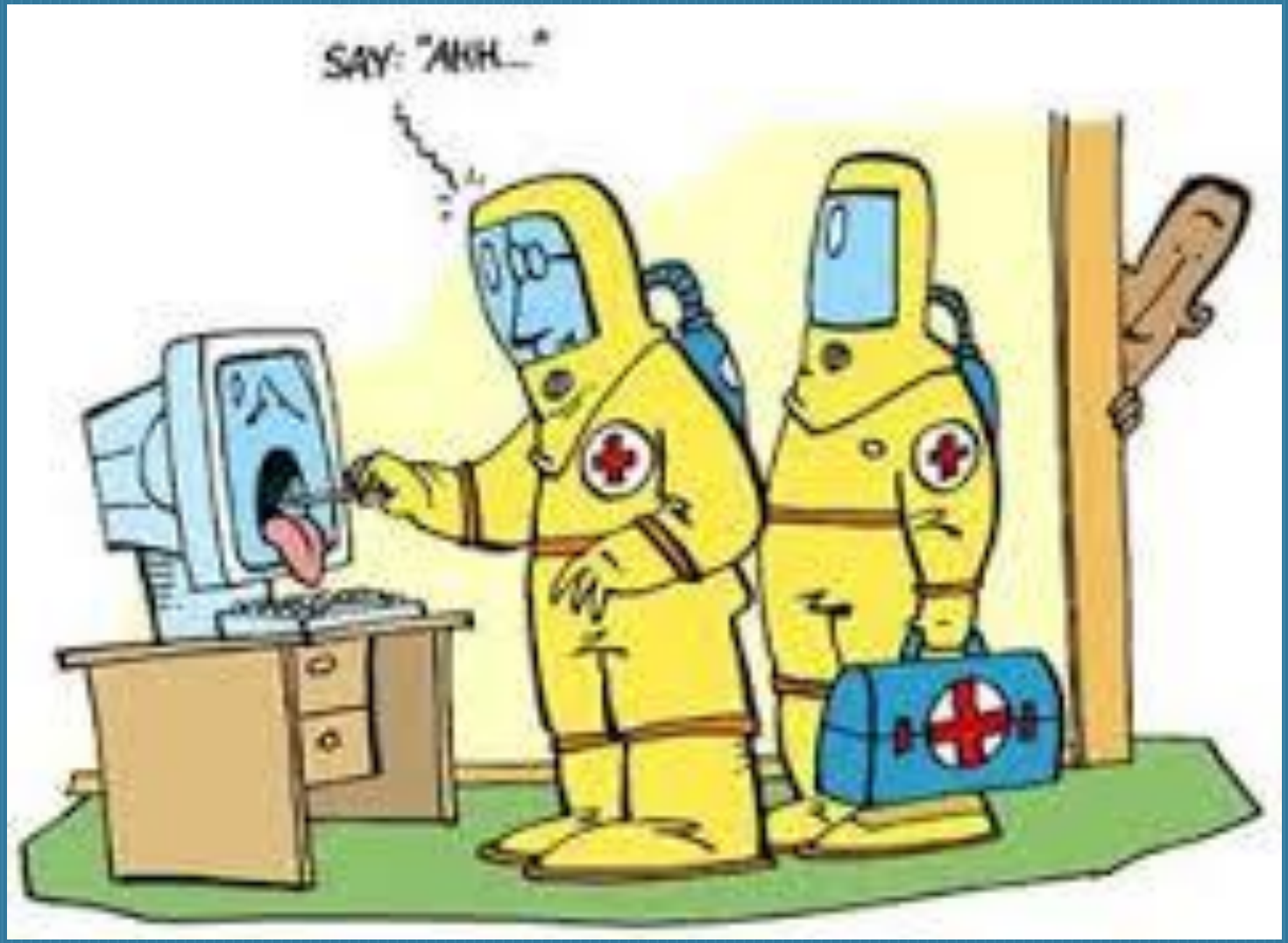
непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;

ошибки при загрузке операционной системы;

невозможность сохранять файлы в нужных каталогах;

непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

Как же лечить компьютер?



Антивирусные программы

- 1) программы-детекторы: предназначены для нахождения зараженных файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать зараженные файлы. Существуют специализированные, то есть предназначенные для борьбы с одним вирусом детекторы и полифаги, которые могут бороться с многими вирусами;
- 2) программы-лекари: предназначены для лечения зараженных дисков и программ. Лечение программы состоит в изъятии из зараженной программы тела вируса. Также могут быть как полифагами, так и специализированными;
- 3) программы-ревизоры: предназначены для выявления заражения вирусом файлов, а также нахождение поврежденных файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера. В случае несоответствия данных выводится сообщение о возможности заражения;
- 4) лекари-ревизоры: предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.

- 5) программы-фильтры: предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции. Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.
- 6) программы-вакцины: используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).
- Следует заметить, что выбор одного "наилучшего" антивируса крайне ошибочное решение. Рекомендуется использовать несколько разных антивирусных пакетов одновременно. Выбирая антивирусную программу следует обратить внимание на такой параметр, как количество распознающих сигнатур (последовательность символов, которые гарантированно распознают вирус). Второй параметр - наличие эвристического анализатора неизвестных вирусов, его присутствие очень полезно, но существенно замедляет время работы программы. На сегодняшний день существует большое количество разнообразных антивирусных программ. Рассмотрим коротко, распространенные в странах СНГ.

Как не допустить образование вируса? Что же нужно что бы обезопасить свой компьютер от вируса?

Известные антивирусные программы

- Популярные :
- • Антивирус Касперского 2016
  • ESET NOD32 Antivirus
  • Антивирус Dr.Web для Windows
  • Emsisoft Anti-Malware
  • Avast Pro Antivirus 2016
  • McAfee AntiVirus Plus
  • Panda Antivirus Pro 2016
  • Symantec Endpoint Protection
  • Kaspersky Small Office Security
  • AVG AntiVirus 2016

Как защитить компьютер от вирусов

- **Установите антивирусную программу.** Установка антивирусной программы и ее постоянное обновление позволяют защитить компьютер от вирусов. Антивирусные программы проверяют наличие вирусов в сообщениях электронной почты, операционной системе и файлах. Новые вирусы могут появляться ежедневно, поэтому необходимо постоянно проверять обновления на веб-сайте изготовителя антивирусной программы. Некоторые антивирусные программы продаются на условиях годовых подписок, которые могут быть обновлены при необходимости, однако многие из них доступны бесплатно. Корпорация Microsoft предлагает Microsoft Security Essentials, бесплатную антивирусную программу, которую можно загрузить с веб-сайта **Microsoft Security Essentials**. Кроме того, можно посетить веб-страницу **поставщиков программ по обеспечению безопасности Windows** для поиска антивирусной программы стороннего изготовителя.
- **Не открывайте сообщения электронной почты от незнакомых отправителей или вложения, которые вам неизвестны.** Многие вирусы содержатся во вложениях электронной почты и начинают распространяться сразу после открытия вложения. Настоятельно не рекомендуется открывать вложения без предварительной договоренности о его получении. Программы Microsoft Outlook и Почта Windows помогают блокировать потенциально опасные вложения.
- **Используйте функцию блокирования всплывающих окон в браузере.** Всплывающие окна — это небольшие окна веб-браузера, которые появляются поверх просматриваемой страницы веб-сайта. Несмотря на то что большая их часть создается рекламодателями, они также могут содержать вредоносный или небезопасный код. Функция блокирования всплывающих окон может предотвратить отображение некоторых или всех подобных окон.

- Блокирование всплывающих окон в веб-браузере Internet Explorer включено по умолчанию. Дополнительные сведения об изменении параметров этой функции, а также о ее включении и отключении см. в разделе **Блокировка всплывающих окон в Internet Explorer: вопросы и ответы**.
- **Регулярно обновляйте операционную систему Windows.** Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа. Убедитесь, что Windows получает данные обновления, включив функцию автоматического обновления Windows. Дополнительные сведения см. в разделе **Включение и выключение автоматического обновления**.
- **Используйте брандмауэр.** Брандмауэр Windows или другие брандмауэры оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также запрещает вирусам, вирусам-червям и злоумышленникам загружать потенциально опасные программы на компьютер. Дополнительные сведения о брандмауэре Windows см. в разделе **Параметры брандмауэра Windows**.
- **Используйте параметры конфиденциальности браузера.** Важно знать, как веб-сайты могут использовать личную информацию, чтобы предотвратить целевую рекламу, мошенничество и кражу личных данных. При использовании Internet Explorer можно в любой момент настроить параметры конфиденциальности или восстановить параметры по умолчанию. Дополнительные сведения см. в разделе **Изменение параметров конфиденциальности Internet Explorer**.
-

- **Включите контроль учетных записей (UAC).** При попытке внесения изменений, требующих разрешения администратора, функция контроля учетных записей выводит соответствующее уведомление и предоставляет возможность принятия изменений. Контроль учетных записей помогает предотвратить внесение вирусами нежелательных изменений. Дополнительные сведения о включении функции контроля учетных записей и настройке параметров см. в разделе **Включение и выключение контроля учетных записей**.
- **Очищайте кэш Интернета и журнал просмотров веб-страниц.** Большинство браузеров хранит сведения о посещаемых веб-сайтах, а также информацию, которую им, возможно, потребуется предоставить (например, имя и адрес пользователя). Несмотря на то что сохранение этих сведений на компьютере может быть полезно, существуют ситуации, когда их необходимо удалить частично или полностью. Например, это требуется, если пользователь работает на общедоступном компьютере и не хочет оставлять на нем свои личные сведения. Сведения о процедуре очистки журнала Internet Explorer см. в разделах **Удаление журнала веб-страниц** и **Удаление файлов cookie**.
-

Спасибо за внимание!

Работу выполняли:

Учащиеся 10 класса МБОУ «СОШ №21» НМР РТ

Загидуллина Л.Р, Хуснуллина Д.Р.