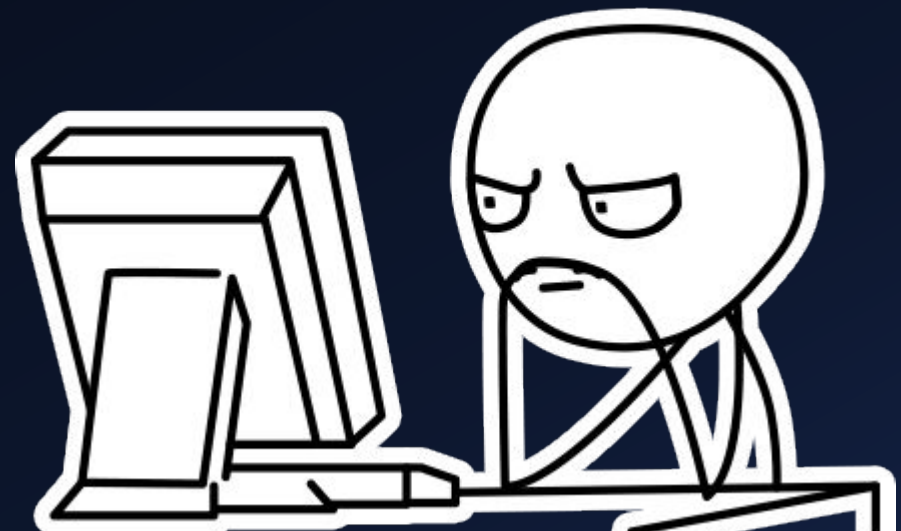
Антивирусные программы

ЕРМОЛЕНКО В.В.
ФАЗЛЫКАЕВ Р.
МОЛОДЦОВ П.
БУРДУКОВ А.

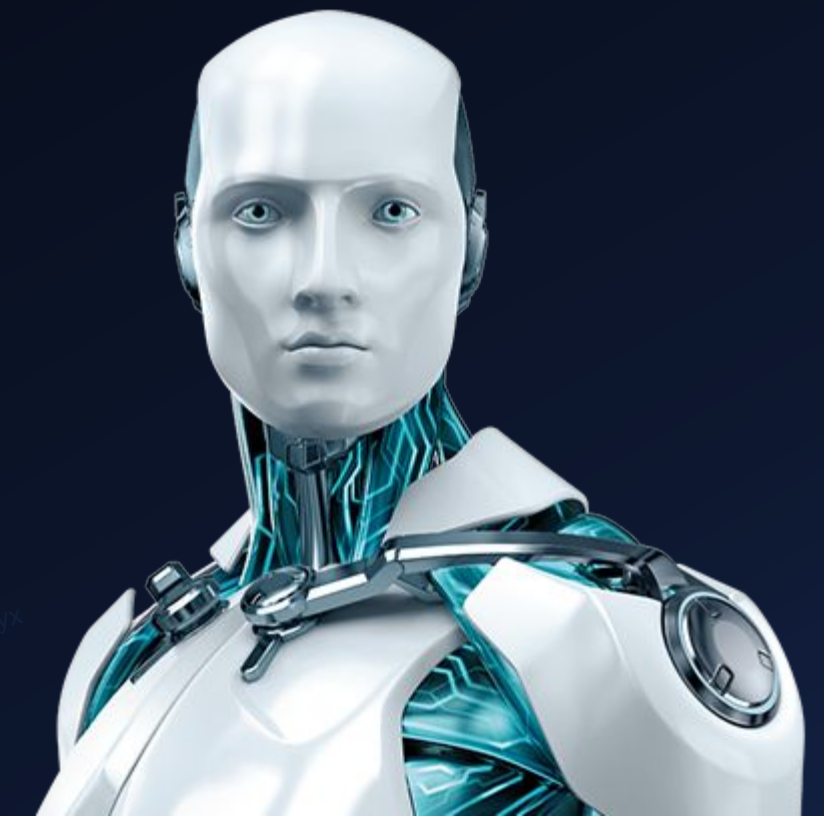
Оглавление

- Что такое антивирус?
  - История развития и структура.
- Что такое лжеантивирус?
  - История возникновения.
- Технологии антивирусной защиты.
  - Сигнатурный метод детектирования
  - Проактивные технологии защиты
- Заключение



Что такое антивирус?

- Антивирус – специальная программа для обнаружения вирусов в компьютере, а также для предотвращения заражения файлов и ОС вредоносным кодом. Антивирусы также могут снабжаться дополнительными функциями – фильтрация спама, шифрование, резервное копирование данных и пр.



Подробнее об антивирусах

Компьютер тормозит только в двух случаях:
1.Вирус.
2.Антивирус.

Что такое лжеантивирус?

- Если антивирус защищает компьютер, то лжеантивирус пытается выдавать себя за настоящий антивирус, но на самом деле целью его создания является вымогание денег или распространение своего ПО.

Подробнее об лжеантивирусах

Технологии антивирусной защиты

- Антивирусы можно разделить по технологии защиты:

1. Классический (используется сигнатурный метод детектирования). Применяется в основном в бесплатных антивирусах(Avast, Panda, AVG и пр.);

2. Продукт проактивной защиты (используется проактивная технология антивирусной защиты);

3. Комбинированный.

AVG

NOD32

Эта картинка по размеру капец огромная.

Вместо заключения:

- Антивирусы на сегодня представляют собой целый комплекс различных модулей и программ, чтобы защитить компьютер от различных вирусных атак.
- Однако антивирусы неспособны на 100% защитить компьютер, т.к. мошенники постоянно пишут и изобретают новые методы обхода компьютерной защиты.
- Поэтому самый лучший антивирус – ~~паранойя~~ здравый смысл пользователя.

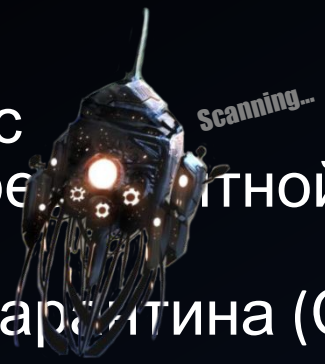

CONFIRMED
Спасибо
за
внимание!

История развития антивирусов

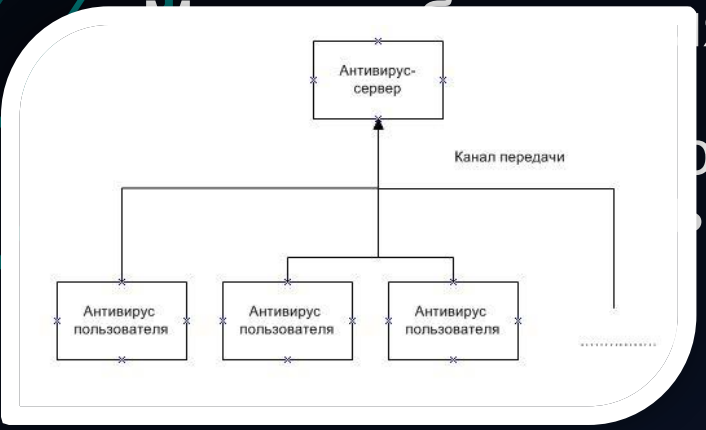
- Первые антивирусы появились 1984 году и назывались CHK4BOMB и BOMBSQAD. Как и последующие программы до начала 1990-х годов, они представляли собой набор из нескольких десятков сигнатур в теле программы. В 1992 году появилась программа-генератор полиморфного кода, что позволило значительно усложнить поимку вирусов. В итоге усложнились и антивирусы, начавшие использовать эмулятор кода (создатель – Евгений Касперский). Примерно в это же время появились такие системы защиты, как статистический анализ, эвристический анализатор и поведенческий блокиратор. С ростом популярности Windows повысились требования к разработчикам антивирусов, что сократило их количество. На данный момент антивирусное ПО разрабатывается более 60 компаниями по всему миру.

След.

Структура антивируса



- Антивирус
- Модуль ре тной защиты (Сканирует все файлы, проходящи П)
- Модуль ка тина (Специальное место для хранения подозрите айлов)
- Модуль «протектора» антивируса (защищает антивирус от посто вмешательства)
- я (отвечает за обновления антивирусной базы)
- у-антивирусу (позволяет объединять ко)
- по требованию пользователя)



Назад

Лжеантивирусы

- Лжеантивирусы начали активно распространяться в 2009 году и перестали быть серьезной угрозой только в 2011 году. Распространяются такие программы обычно через агрессивную рекламу и могут даже «отравить» поисковые результаты, в то числе и по темам, не относящимся к информационной безопасности.
- Выгоду мошенник получает разными путями:

  1. Обычное вредоносное поведение вроде кражи аккаунтов, блокировки ОС, эксплуатации вычислительной мощности компьютера и т.д.

  2. Антивирусная программа может быть самой настоящей, но ее цена будет завышена по сравнению с оригиналом.

  3. Лжеантивирус может специально мешать работе ОС и сообщать об заражении, чтобы потом требовать деньги за очистку.
- Простейшие признаки лжеантивируса:

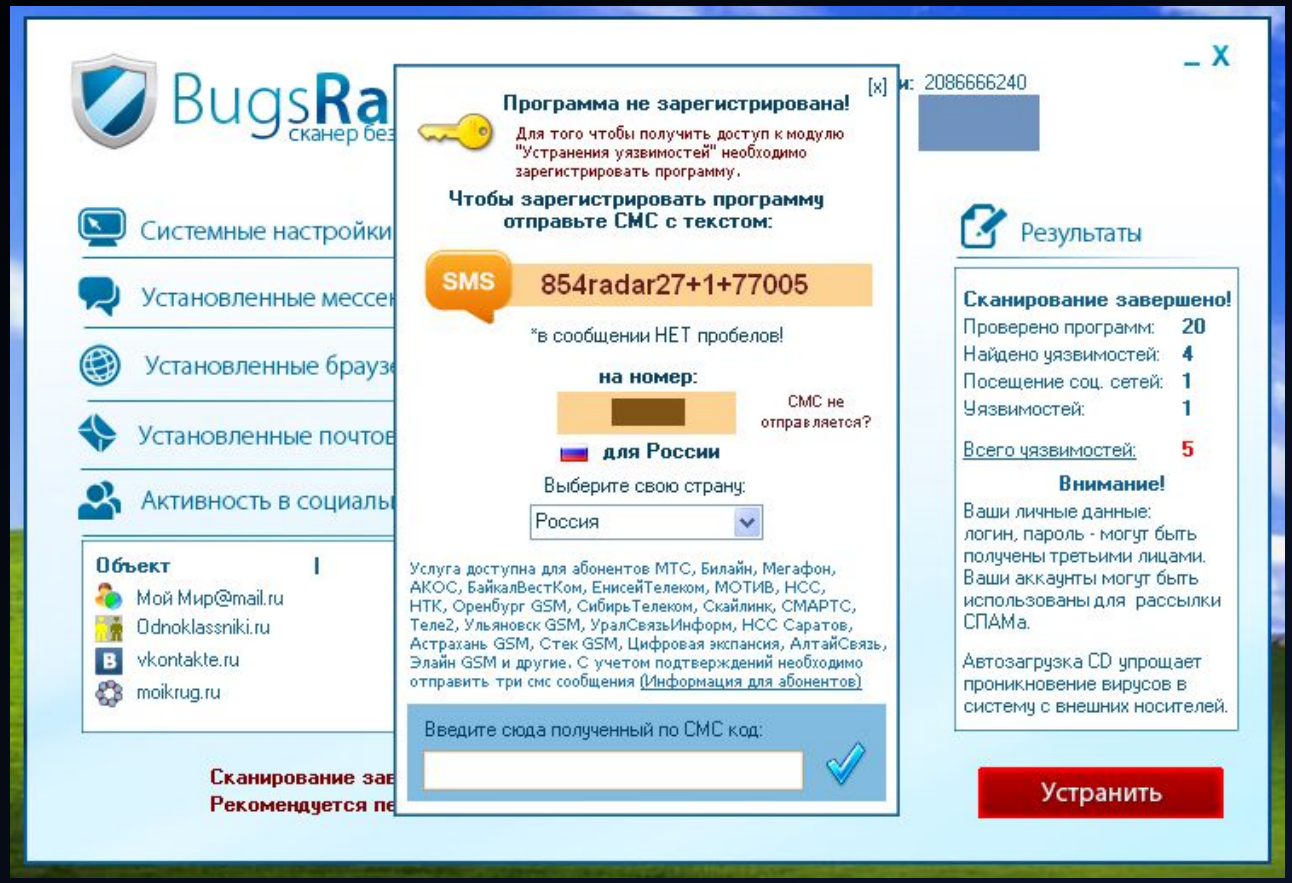
  1. Антивирус не будет гарантировать 100%-ое излечение, т.к. самым новейшим вирусам нужно время, чтобы они попали в антивирусную базу.

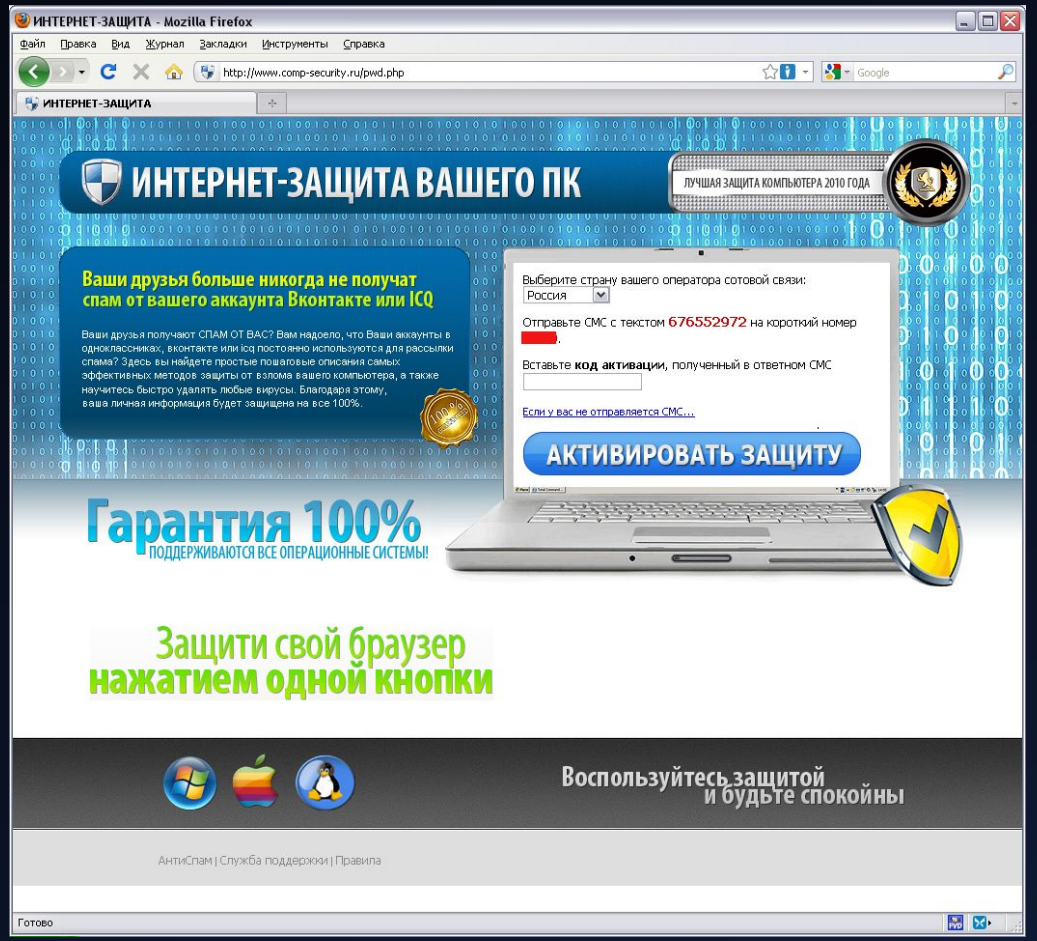
  2. Настоящие антивирусы просят деньги только за дополнительные функции, удаление вирусов они делают бесплатно.

  3. Антивирус не может лечить и сканировать через веб-браузер – сайты не имеют доступа к файлам компьютера.

След.

Примерно так это выглядит:



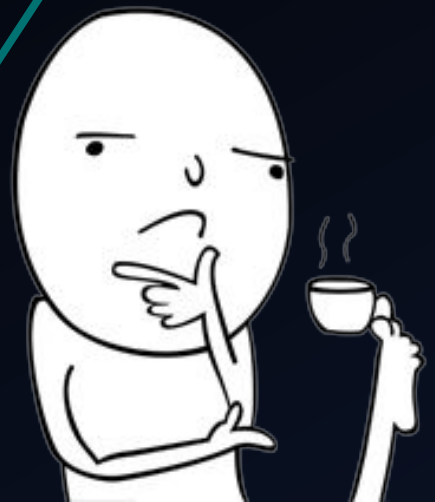


Назад

Сигнатурный метод детектирования

Метод работы антивируса, при котором программа сканируя файл или пакет данных, обращается к словарю с вирусами и если было найдено какое-либо соответствие, антивирус удаляет, отправляет в карантин или пытается «вылечить» файл/пакет, удалив часть вредоносного кода. Такой метод требует частого обновления базы сигнатур, иначе даже из-за незначительного изменения вирус может остаться незамеченным.

Нельзя просто так взять, и не заполнить пустое пространство глупыми картинками



Назад

Проактивная технология антивирусной защиты

Совокупность технологий и методов, используемых в антивирусе с целью предотвращения заражения, а не поиска уже известного вредоносного ПО. Используемые технологии:

- Эвристический анализ - позволяет находить полиморфные и сложношифрованные вирусы(возможны частые ложные срабатывания);
- Эмуляция кода - запуск неизвестного ПО в условиях эмуляции работы ОС и центрального процессора(работает медленно);
- Анализ поведения - отслеживание активности пользователя и анализ единичных или целой цепочки действий;
- Песочница – ограничение привилегий выполнения - аналог эмуляции кода, запуск неизвестного ПО в ограниченной среде – нет доступа к критическим системным файлам, веткам или реестру(нужно понимание пользователя для правильной оценки программы);
- Виртуализация рабочего окружения - запуск неизвестного ПО в буфере (возможна потеря важной информации, т.к. доступ к жесткому диску сохраняется).



Назад