

Антивирусные программы

ЕРМОЛЕНКО В.В.

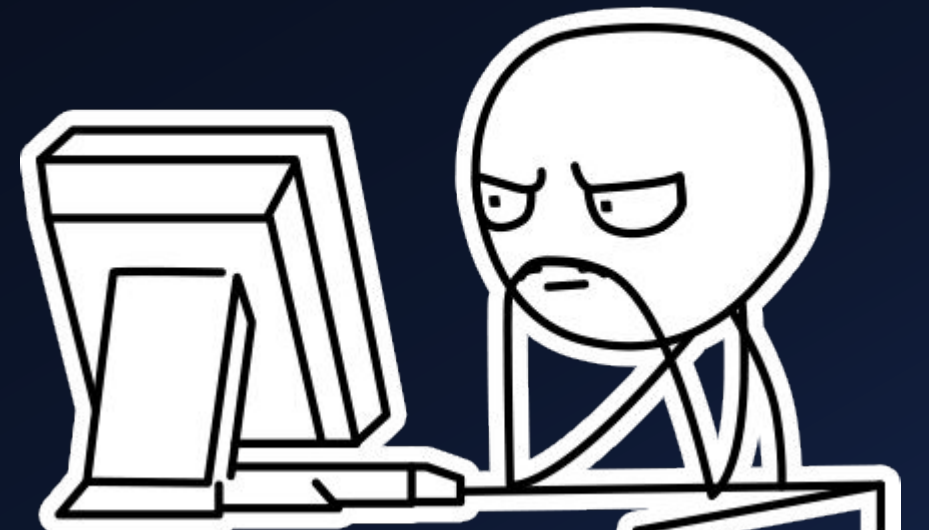
ФАЗЛЫКАЕВ Р.

МОЛОДЦОВ П.

БУРДУКОВ А.

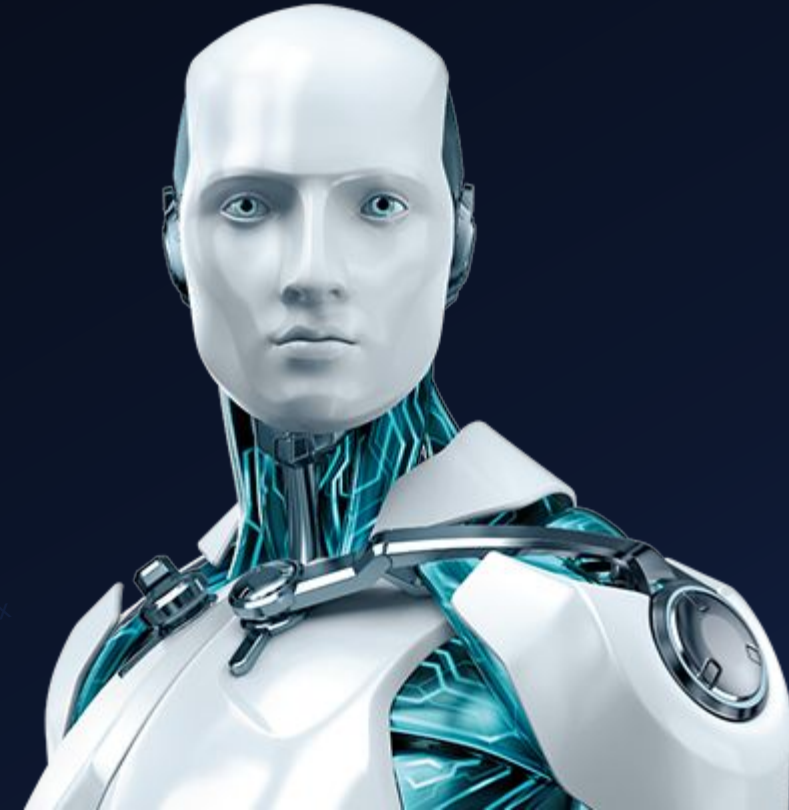
Оглавление

- 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.



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.



Эта картинка по размеру капец огромная.

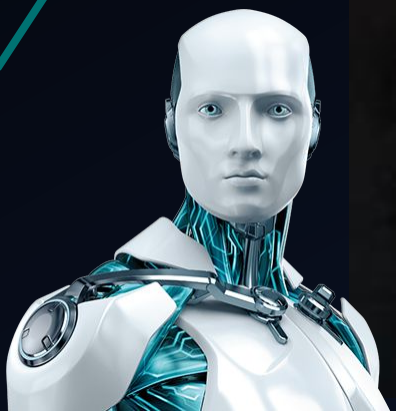
Вместо заключения:

- 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 – ~~паранейя~~ здравый смысл пользователя.





Спасибо
за
внимание!



История развития антивирусов

- Первые антивирусы появились в 1984 году и назывались СНК4ВОМВ и ВОМBSQAD. 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 реального времени защиты (Сканирует все файлы, проходящие в систему)
- Модуль карантина (Специальное место для хранения подозрительных файлов)
- Модуль «протектора» антивируса (защищает антивирус от постоянного вмешательства)



...я (отвечает за обновления антивирусной базы)

...ру-антивирусу (позволяет объединять ко

... по требованию пользователя)



You shall not pass!



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.



Примерно так это ВЫГЛЯДИТ:

BugsRadar сканер безвредных уязвимостей

Системные настройки
Установленные мессенджеры
Установленные браузеры
Установленные почтовые клиенты
Активность в социальных сетях

Объект

- Мой Мир@mail.ru
- Odnoklassniki.ru
- vkontakte.ru
- moikrug.ru

Программа не зарегистрирована!

Для того чтобы получить доступ к модулю "Устранения уязвимостей" необходимо зарегистрировать программу.

Чтобы зарегистрировать программу отправьте СМС с текстом:

SMS 854radar27+1+77005

*в сообщении НЕТ пробелов!

на номер: [input type="text"] СМС не отправляется?

для России

Выберите свою страну:
Россия

Услуга доступна для абонентов МТС, Билайн, Мегафон, АКОС, БайкалВестКом, ЕнисейТелеком, МОТИВ, НСС, НТК, Оренбург GSM, СибирьТелеком, Скайлинк, SMARTC, Теле2, Ульяновск GSM, УралСвязьИнформ, НСС Саратов, Астрахань GSM, Стек GSM, Цифровая экспансия, АлтайСвязь, Элайн GSM и другие. С учетом подтверждений необходимо отправить три смс сообщения (Информация для абонентов)

Введите сюда полученный по СМС код: [input type="text"]

Результаты

Сканирование завершено!

Проверено программ: 20
Найдено уязвимостей: 4
Посещение соц. сетей: 1
Уязвимостей: 1

Всего чязвимостей: 5

Внимание!

Ваши личные данные: логин, пароль - могут быть получены третьими лицами.
Ваши аккаунты могут быть использованы для рассылки СПАМа.

Автозагрузка CD упрощает проникновение вирусов в систему с внешних носителей.

Устранить

Сканирование за...
Рекомендуется пе...

ИНТЕРНЕТ-ЗАЩИТА - Mozilla Firefox

http://www.comp-security.ru/pwd.php

ИНТЕРНЕТ-ЗАЩИТА ВАШЕГО ПК

ЛУЧШАЯ ЗАЩИТА КОМПЬЮТЕРА 2010 ГОДА

Ваши друзья больше никогда не получат спам от вашего аккаунта Вконтакте или ICQ

Ваши друзья получают СПАМ ОТ ВАС? Вам надоело, что Ваши аккаунты в одноклассниках, вконтакте или icq постоянно используются для рассылки спама? Здесь вы найдете простые пошаговые описания самых эффективных методов защиты от взлома вашего компьютера, а также научитесь быстро удалять любые вирусы. Благодаря этому, ваша личная информация будет защищена на все 100%.

Выберите страну вашего оператора сотовой связи:
Россия

Отправьте СМС с текстом **676552972** на короткий номер [input type="text"]

Вставьте код активации, полученный в ответном СМС
[input type="text"]

Если у вас не отправляется СМС...

АКТИВИРОВАТЬ ЗАЩИТУ

Гарантия 100%
ПОДДЕРЖИВАЮТСЯ ВСЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ!

Защити свой браузер нажатием одной кнопки

Воспользуйтесь защитой и будьте спокойны

АнтиСпам | Служба поддержки | Правила

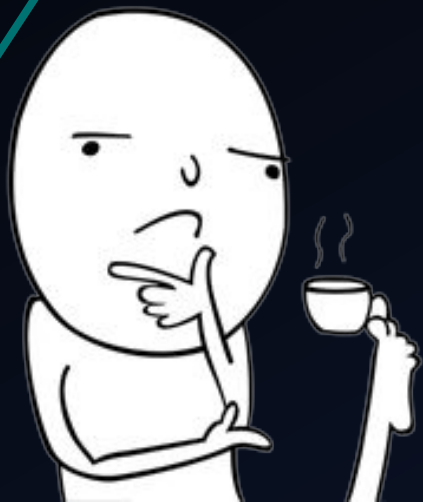
Готово

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

Д

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

Д