Исследовательская работа на тему:

Вирусы и защиты от них

Работу выполнил
Студент 3 курса
специальности «ПОВТ и АС»
Группы А
Латыпов Айнур Марсельевич

Руководитель:
Деревяшкина Елена Ивановна

Цель: выяснить какие антивирусы наиболее популярны и при помощи анализа выявить их достоинства и недостатки

ПЛАН:

- Введение
- Вирусы и их разновидности
- Основные методы защиты от компьютерных вирусов
- Результаты социологического опроса
- Рассматриваем возможности Касперского 2010
- Рассматриваем возможности Avast
- Рассматриваем возможности NOD_32
- Рассматриваем возможности Dr. Web

ВВЕДЕНИЕ

На сегодняшний день всё большие темпы принимает процесс компьютеризации. Многие люди уже не читают простые книги – вместо них они читают электронные книги, используют разные компьютерные программы и играют в различные компьютерные игры.

поэтому стоят серьезные вопросы:

- *«как защитить их компьютеры от вирусов?»*
- *«какой способ защиты наиболее оптимальный?»*

Поэтому я решил сделать анализ, который бы позволил ответить на эти вопросы.

Для начала я провел социологический опрос, чтобы узнать какие антивирусные программы являются наиболее распространенными.

Используя результаты этого социологического опроса, произвел анализ преимуществ и недостатков наиболее распространенных антивирусных программ.

На основе полученных данных сделал вывод, отвечающий на оба поставленных вопроса.

Что такое «компьютерный вирус»?

Компьютерный вирус - это специально написанная, как правило, небольшая по размерам программа, которая может записывать (внедрять) свои копии (возможно, измененные) в компьютерные программы, расположенные в исполнимых файлах, системных областях дисков, драйверах, документах и т. д., причем эти копии сохраняют возможность к “размножению”.

Процесс внедрения вирусом своей копии в другую программу (системную область диска и т. д.) называется **заражением**, а программа или иной объект, содержащий вирус - **зараженным**.

Разновидности вирусов

- вирусы
  - ***файловые***
  - ***Загрузочные***
  - ***DIR - вирусы***
  - ***Драйверные***
  - ***Макровирусы***

Описание действия этих вирусов

Вирусы, заражающие файлы, называются ***файловыми* вирусами**. Вирус в зараженных исполнимых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те файловые вирусы, которые после своего запуска остаются в памяти резидентно - они могут заражать файлы и вредить до следующей перезагрузки компьютера. А если они заразят любую программу, запускаемую из файла AUTOEXEC.BAT или CONFIG.SYS, то и при запуске с жесткого диска вирус снова начнет свою работу.

***Загрузочными* вирусами** или бутовыми (от слова boot-загрузчик), называются вирусы, поражающие загрузочную запись операционной системы и главную загрузочную запись жесткого диска. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера.

Для заражения компьютера загрузочным вирусом достаточно иметь всего один раз зараженную дискету в дисководе А: в момент перезагрузки компьютера.

Вирусы, меняющие файловую систему на диске, обычно называют ***DIR - вирусами***. Такие вирусы прячут свое тело в некоторый участок диска (обычно - в последний кластер диска) и помечают его в таблице размещения файлов (FAT) как конец файла. Для всех .COM и .EXE-файлов, содержащихся в соответствующих элементах каталога, указатели на первый участок файла заменяются ссылкой на участок диска, содержащий вирус, а правильный указатель в закодированном виде прячется в неиспользуемой части элемента каталога. Поэтому при запуске любой программы в память загружается вирус, после чего он остается в памяти резидентно, подключается к программам ОС для обработки файлов на диске и при всех обращениях к элементам каталога выдает правильные ссылки.

Драйверные вирусы заражают драйверы устройств, т. е. файлы, указываемые в приложении Devise файла CONFIG.SYS. Вирус, находящийся в этих файлах, начинает свою работу при каждом обращении к соответствующему устройству.

Вирусы, заражающие драйверы устройств, очень мало распространены, поскольку драйверы редко переписывают с одного компьютера на другой.

Так как сейчас редакторы Word для Windows более всего распространены, то в 1995 г. появилась новая разновидность вируса, заражающая файлы документов, созданные этими редакторами - ***макровирусы***. Это стало возможным, поскольку в Word для Windows встроен мощный язык макрокоманд WordBasic. Запуск вируса происходит при открытии на редактирование зараженных документов. При этом макрокоманды вируса записываются в глобальный шаблон NORMAL.DOT, так что при новых сеансах работы с Word для Windows вирус будет автоматически активирован. При наличии вируса при сохранении редактируемых документов или записи документов на диск под новым именем (командой Save As) вирус копирует свои макрокоманды в записываемый на диск документ, так что тот оказывается зараженным.

КАК ЗАЩИТИТЬСЯ ОТ ВИРУСОВ?

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо и применение специализированных программ для защиты от вирусов - *антивирусов*

Разновидности антивирусов

- Антивирусы
  - ***Программы-детекторы***
  - ***Программы-доктора***
  - ***Программы-ревизоры***
  - ***Доктора-ревизоры***
  - ***Программы-фильтры***
  - ***Программы-вакцины***

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.

Программы-доктора, или фаги, “лечат” зараженные программы или диски, “выкусывая” из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.

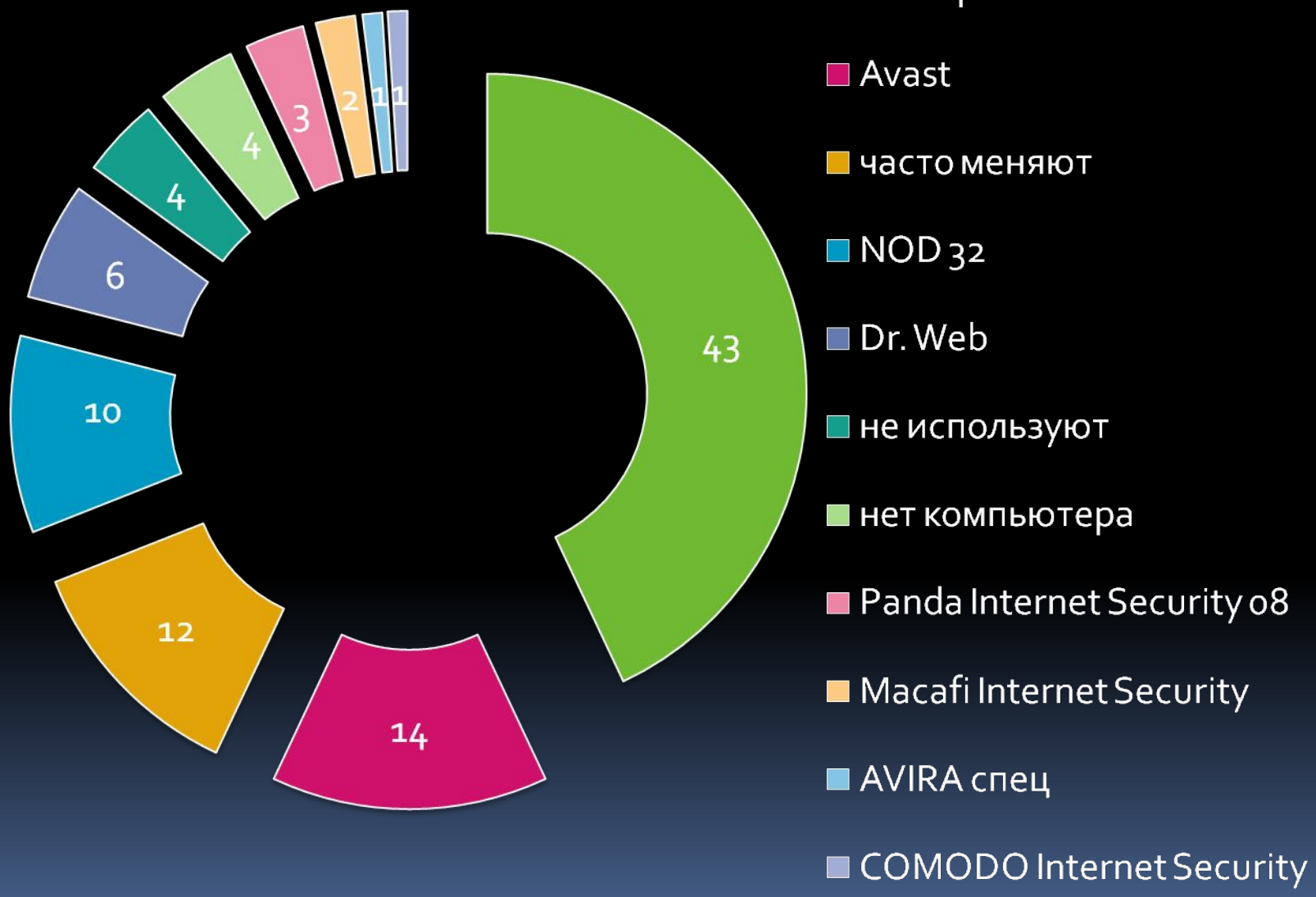
Программы-ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.

Доктора-ревизоры - это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

Программы-фильтры располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Программы-вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны и далее не рассматриваются.

статистика использования антивирусов



как обновляют свои антивирусы пользователи

Преимущества и недостатки Касперского 2010

Плюсы:

- Легко установить
- Удобный интерфейс
- Возможность детальной настройки антивируса
- Используется принцип многоуровневой защиты
- возможность провести анализ уязвимости программ и их устранение при обнаружении
- возможность составить список доверенных программ
- если нет интернета чтобы установить хотя бы пробную версию – есть возможность обновить антивирусные базы один раз без лицензии
- отдельно уделена проблема проверки USB-накопителей

минусы:

- она очень ресурсоемка
- нет возможности сканирования системы при загрузке ОС
- загружается только через 25-30с после загрузки ОС

Преимущества и недостатки Avast

плюсы

- Легко установить
- Удобный интерфейс
- Возможность детальной настройки антивируса (возможностей настройки меньше чем у Касперского 2010)
- При запуске программы производится процесс проверки памяти и загруженных программ
- Возможность создания файлов, предупреждающих о зараженности компьютера вирусом других пользователей. Это ограничивает дальнейшее распространение вирусов.
- Можно спланировать сканирование компьютера после перезагрузки. При сканировании указанным методом вирусы не успевают скрыться от антивирусной программы.
- Можно использовать длительное время демо-лицензию
- Является мощным сканером

минусы

- В большинстве случаев может только удалять зараженный файл
- Используется для защиты только мощный сканер. В этом случаи компьютер защищен только на 30%, если БД не обновлять каждый день

Преимущества и недостатки Nod_32

плюсы

- Легко установить
- Удобный интерфейс
- Возможность детальной настройки
- Если нет ключа - работают все функции кроме функции обновления
- В диалоговых окнах используются только успокаивающие цвета
- Не надоедает сообщениями об устаревших базах данных

минусы

- Нет принципа многоуровневой защиты, используется для защиты только один компонент
- Нет функции обновления хотя бы один раз без лицензии

Преимущества и недостатки Dr.Web

плюсы

- Легко установить
- Удобный интерфейс
- Возможность настройки по своему усмотрению (эти возможности невелики)
- Если нет ключа - работают все функции кроме функции обновления
- В диалоговых окнах используются только успокаивающие цвета
- Не надоедает сообщениями об устаревших базах данных
- сканирует память при запуске

минусы

- Нет принципа многоуровневой защиты, используется для защиты только один компонент
- Нет функции обновления хотя бы один раз без лицензии
- В большинстве случаев сканирование работает от ручного запуска

Спасибо за внимание!!!