Сравнительный анализ антивирусных программных средств

Исследовательский проект

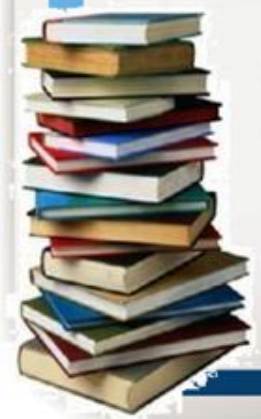
Автор проекта: Плаксина Н.,

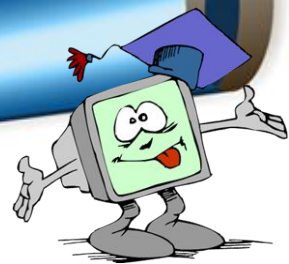
Студентка группы «Технологическая №1».,

Руководитель: Сорокина Е.А., преподаватель информатики

Актуальность:

- Компьютерные вирусы во всем мире наносят громадный ущерб, как большим компаниям, так и отдельным пользователям, на меры профилактики и защиты затрачиваются огромные денежные средства. Рядовые пользователи имеют возможность придерживаться мер безопасности и использовать антивирусное программное обеспечение.





Цель проекта:

выяснить какое антивирусное программное обеспечение обладает наиболее высокой степенью защиты.

Задачи проекта:

- Дать определение понятию «компьютерный вирус», рассмотреть классификации вирусов
- Изучить типы антивирусных программ;
- Привести обзор популярных антивирусных программ;
- Проанализировать причины использования того или другого вида антивируса.

Объект исследования	современное антивирусное программное обеспечение
Предмет исследования	анализ рынка современного антивирусного программного обеспечения в России и за рубежом

Компьютерный вирус – это небольшая программа, обладающая способностью саморазмножения (то есть добавления своей точной или несколько видоизмененной копии к другим программам, документам, системной области диска, загрузочному сектору или оперативной памяти), а также выполняющая без ведома пользователя различные действия, обычно нежелательные. При этом копии сохраняют способность дальнейшего распространения.

Классификация вирусов

Загрузочные вирусы

- заражают загрузочный сектор гибкого диска или винчестера. При заражении дисков загрузочный вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не программному коду загрузчика операционной системы, а коду вируса.

Файловые вирусы

- при своем размножении тем или иным способом используют файловую систему операционной системы. Файловые вирусы могут поражать исполняемые файлы различных типов (EXE, COM, BAT, SYS).

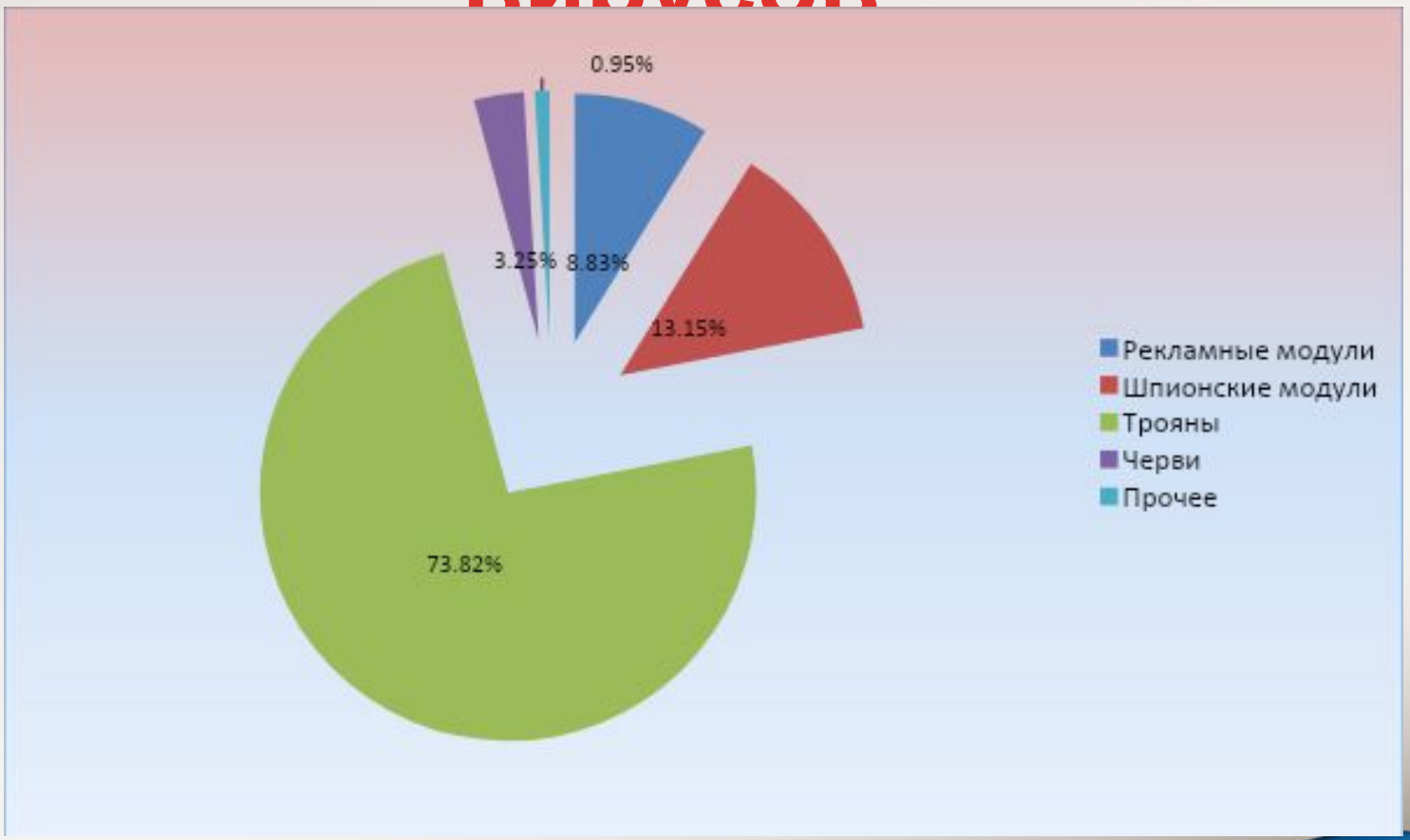
Макро-вирусы

- являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Сетевые вирусы

- для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей. Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.

Распространенные виды вирусов



Каналы распространения

Флеш-накопители

Электронная почта

Веб-страницы

Системы обмена мгновенными сообщениями

Антивирусные программы

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

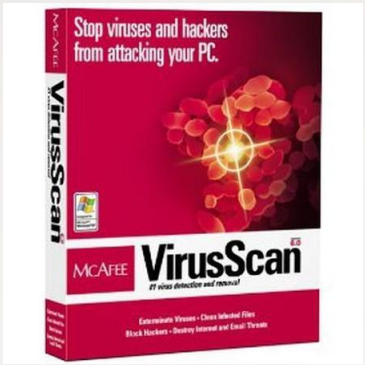
Типы антивирусных программ

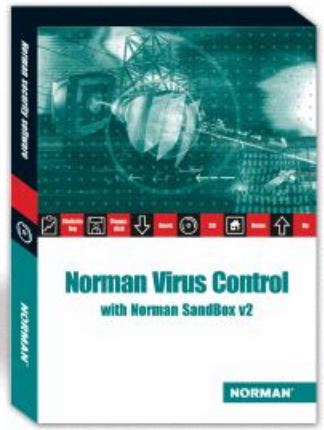
Программы – сканнеры (или полифаги)

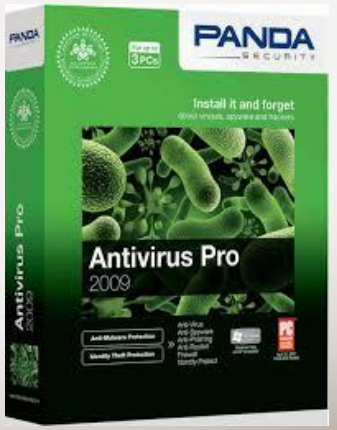
Программы – ревизоры

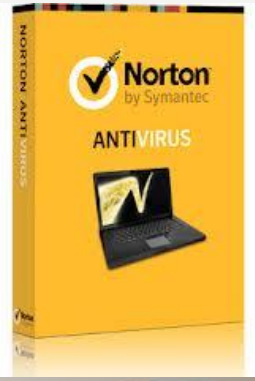
Программы – фильтры

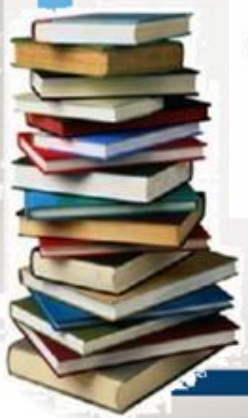
Обзор популярных антивирусных программ











Eset NOD32 (Словакия)

NOD 32 Antivirus System от Eset Software обеспечивает хорошо сбалансированную безупречную защиту персональных компьютеров и корпоративных систем, работающих на платформах Microsoft Windows /2000/2003/XP/7/Vista, UNIX/Linux, а также для почтовых серверов Microsoft Exchange Server, Lotus Domino и других. Главным преимуществом NOD32 является его быстрая работа, невероятное низкое потребление системных ресурсов и не раз доказанная способность ловить 100% вирусов.

Norman Virus Control (Норвегия)

Разработанная компанией Symantec программа Norman Virus Control ™ позволяет предотвратить попадание ненужных сообщений в почтовый ящик пользователя. Программа, совместимая с любым почтовым клиентом POP3, производит многоуровневую фильтрацию входящих сообщений электронной почты, выявляя и помечая "макулатурные" письма; при этом вся нужная корреспонденция доставляется без задержки. Кроме того, Norman Virus Control отсекает рекламные заголовки и всплывающие окна, делая прогулку по Интернету куда более приятной.

Kaspersky Anty-Virus (Россия)

Антивирус Касперского® является последним технологическим достижением "Лаборатории Касперского" в области защиты домашнего компьютера от вирусных угроз. Помимо обычных антивирусных функций, в Антивирус Касперского® встроены уникальные технологические компоненты, позволяющие пользователю отслеживать все происходящие на компьютере изменения и контролировать поведение документов в формате MS Office, обеспечивая эти документы дополнительным уровнем безопасности. Антивирус Касперского® представляет собой уникальный набор компонентов, некоторые из которых были ранее были доступны только для корпоративных пользователей программных продуктов компании. Теперь все эти средства антивирусной борьбы доступны для домашнего использования.

Avast!
(Россия)

Основные характеристики Avast!: Высокий уровень выявления вирусов, троянов и червей. Резидентный (в режиме реального времени) и обычный сканер. Сканирование архивов. Проверка входной и исходной электронной почты. Глубокая интеграция в систему. Проверить тот или иной файл можно непосредственно из проводника Windows, щелкнув по нему правой кнопкой мыши и выбрав надпись "Сканировать...". Карантин Avast! изолирован от операционной системы, что обеспечивает большую безопасность работы. Ни один файл, сохраняемый в карантине не может быть запущен. Бесплатное распространение.

McAfee VirusScan (США)

McAfee Anti-Spyware Enterprise - это простое в установке, управлении и мониторинге средство, специально разработанное в соответствии с уникальными требованиями компаний любого размера. Данный продукт поддерживается одной из ведущих антивирусных исследовательских организаций в мире - McAfee® AVERTTM, и обеспечивает всестороннюю защиту от шпионского ПО.

Norton Antivirus (США)

Приложение Norton AntiVirus – также очень популярная в настоящее время антивирусная программа. Ее разработчиком является всемирно известная фирма Symantec. По сравнению с программами «Антивирус Касперского Personal» и Dr.Web для отечественного пользователей этот антивирус обладает одним существенным недостаткам - он не поддерживает русский язык.

К недостаткам рассматриваемого антивируса можно отнести то, что процесс сканирования компьютера (или указанных объектов) требует слишком много ресурсов компьютера, в результате чего заметно замедляется его быстродействие или работа вообще становится невозможной. Однако высокое качество сканирования с лихвой компенсирует этот недостаток.

DoctorWeb (Россия)

В последнее время стремительно растет популярность антивирусной программы – Doctor Web, которая относится к классу детекторов - докторов, но в отличие от многих других антивирусных программ имеет так называемый "эвристический анализатор" - алгоритм, позволяющий обнаруживать неизвестные вирусы. Важной функцией является контроль заражения тестируемых файлов резидентным вирусом(ключ /V). При сканировании памяти нет стопроцентной гарантии, что "Лечебная паутина" обнаружит все вирусы, находящиеся там.

Тестирование винчестера Dr.Web-ом занимает много времени, поэтому не каждый пользователь может себе позволить тратить столько времени на ежедневную проверку всего жесткого диска. Таким пользователям можно посоветовать более тщательно (с опцией /S2) проверять принесенные извне дискеты.

Panda (Испания)

Panda Antivirus — это антивирусное решение, отлично адаптированное к потребностям небольших организаций и профессионалов. Программа защищает компьютер и от вирусов, и от хакеров. Благодаря таким встроенным функциям, как межсетевой экран и блокиратор скриптов, Panda гарантирует защиту от вирусов, хакеров и других опасностей, связанных с сетью Интернет, в рамках единого и простого в использовании продукта

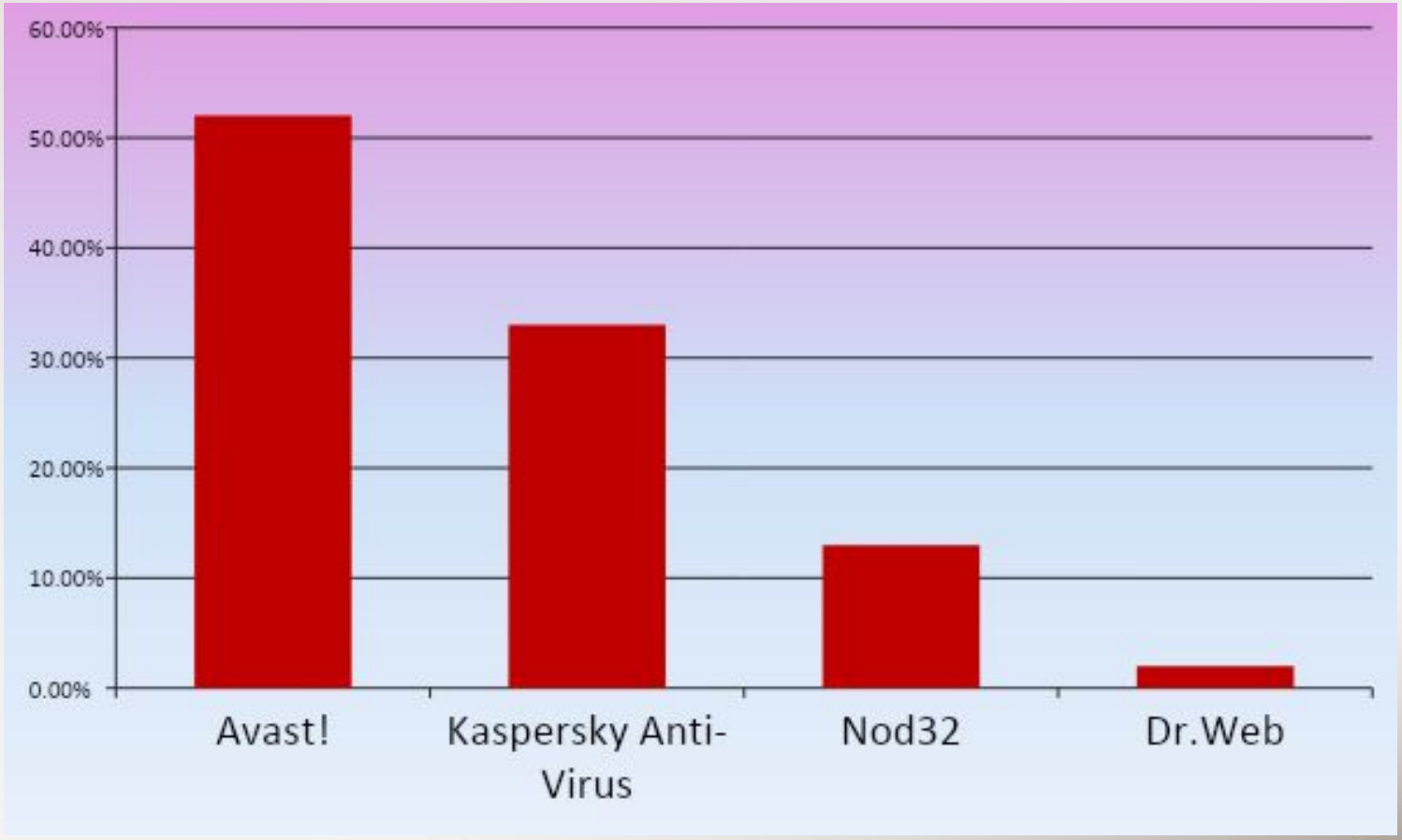
Анализ антивирусных программ

Регулярные серьезные тесты антивирусных программ проводится журналом **Virus Bulletin (**Бюлютень Вирусов**).** Для этого журналом **Virus Bulletin** были разработаны собственные методики тестирования и собрана коллекция различных вирусов для проведения тестов.

Антивирусные продукты тестируются на неком наборе зараженных файлов (так называемый ITW-набор, ITW = «In The Wild»), по результатам прогонов затем делается вывод: заслуживает продукт 100% сертификата безопасности или нет. Данная награда свидетельствует о том, что данный продукт прекрасно справляется с ITW-коллекцией VirusBulletin.

Рейтинг антивирусных

Процент использования программ студентами



Выводы

- Проведя анализ антивирусных программ и рассмотрев литературные источники, я выяснила, какие из них имеют более удобный интерфейс и отвечают системным требованиям. Выбирая антивирусную программу, нужно учесть её возможности, цену и необходимую операционную систему для работы с этой программой и возможности компьютера. К сожалению, на данный момент нет такой антивирусной программы, которая гарантировала бы защиту от всех разновидностей вирусов и прочей нежелательной информации на 100%. Защищенность от вирусов зависит и от грамотности пользователя. Применение в совокупности всех видов защит позволит достигнуть высокой безопасности компьютера, и соответственно, информации.
- Для исследования я выбрала четыре антивирусные программы. Это Avast!, Kaspersky Anty-Virus, Dr.web и NOD32.
- Самой удобной для работы программой оказалась Avast! Как показал опрос студентов она экономически выгодна (главное преимущество), имеет удобный интерфейс и может регулярно обновляться через Интернет.

Информационные ресурсы

- Донцов Д. Как защитить компьютер от ошибок, вирусов, хакеров. Питер, 2008
- Касперский Е. Компьютерные вирусы в MS-DOS. - М.: Эдель, 2012.
- Сычев Ю.Н. Информационная безопасность: учебное пособие, руководство по изучению дисциплины, практикум, тесты, учебная программа. - М.: АЛЛАНА, 2009.
- Филин С.А. Информационная безопасность: Учебное пособие. - М.: Альфа-Пресс, 2009.
- http://drweb.ru/
- http://school.bakai.ru/inform/inform.htm
- http://www.kaspersky.ru/
- httphttp://http://wwwhttp://www.http://www.viruslisthttp://www.viruslist.http://www.viruslist.comhttp://www.viruslist.com/

Спасибо за внимание!