Министерство образования и науки

Республики Казахстан

Карагандинский государственный технический университет

Кафедра

**КУРСОВАЯ РАБОТА**

на тему: Компьютерные вирусы и антивирусные программы

**Выполнил:**

**Проверил:**

**Караганда 2009 г.**

Содержание

Введение

1. Теоретическая часть

1.1 Антивирус NOD32

1.1.1 Основные плюсы

1.2 Модули и компоненты

1.3 Антивирус Dr. WEB

1.4 Антивирус Kaspersky Internet Security

1.4.1 Компоненты защиты

1.5 Задачи поиска вирусов

2. Практическая часть

2.1 Результаты тестирования диска

2.1.1 Антивирус NOD32

2.1.2 Антивирус Kaspersky Internet Security

2.1.3 Антивирус Dr. WEB

2.1.4 Антивирус AVZ

2.2 Сводные диаграммы по проверки диска

2.3 Результаты тестирования папки с вирусами

2.4 Сводная диаграмма

Вывод

## Введение

**Цель работы:**

1. Установка, настройка и использование антивирусных программ.

2. Определение скорости проверки файлов на наличие вирусов.

3. Проверка антивирусных программ на эффективность поиска зараженных файлов.

**Задачи работы:**

1. Установить 4 антивирусные программы;

2. Протестировать жесткий диск с настройками по умолчанию, максимальными, по оптимальному для каждой программы.

3. В результатах проверки отобразить время сканирования, количество проверяемых объектов, скорость тестирования. Свести полученные данные в сводные диаграммы.

4. Протестировать папку, где хранятся вирусы с максимальными настройками.

5. В результате проверки отобразить количество проверенных объектов, количество обнаруженных вирусов и для определения наилучшего антивируса свести все данные в сводную диаграмму.

## 1. Теоретическая часть

## 1.1 Антивирус NOD32

**NOD32** - антивирусный пакет, выпускаемый фирмой Eset. Возник в конце 1998 года. Название изначально расшифровывалось как Nemocnica na Okraji Disku ("Больница на краю диска").

NOD32 - это комплексное антивирусное решение для защиты в реальном времени от широкого круга угроз. Eset NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, phishing-атаки. В решении Eset NOD32 используется патентованная технология ThreatSense®. Эта технология предназначена для выявления новых возникающих угроз в реальном времени путем анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ.

Наравне с базами вирусов NOD32 использует эвристические методы. Считается, что среди других ведущих антивирусных пакетов NOD32 отличается малым использованием системных ресурсов.

## 1.1.1 Основные плюсы

**Дружественный интерфейс** Интерфейс программы лёгок и интуитивно понятен, настройка не вызывает проблем.

**Высокая производительность** Эффективное обнаружение вредоносных программ не обязательно должно замедлять работу компьютера. NOD32 по большей части написан на языке ассемблера и неоднократно выигрывал награды за высочайшую производительность среди антивирусных приложений. NOD32 в среднем в 2-5 раз быстрее, чем его конкуренты (источник: Virus Bulletin).

**Малое влияние на системные ресурсы** NOD32 экономит ресурсы жесткого диска и оперативной памяти, оставляя их для критических приложений. Установщик занимает всего 8,6 Мбайт, а приложению требуется менее 20 Мбайт оперативной памяти (это значение может варьироваться с изменением технологии обнаружения). Обновления технологии ThreatSense, включающие записи эвристической логики и вирусные сигнатуры, обычно имеют объем 20-50 Кбайт.

**Простота управления** Обновления программы и вирусной базы данных выполняются автоматически в фоновом режиме. Если NOD32 используется на личном или домашнем компьютере, можно просто включить функцию автоматического обновления и больше никогда об этом не вспоминать. Предприятия и организации с крупными распределенными сетями могут использовать мощный компонент удаленного администрирования (Remote Administrator), позволяющий разворачивать, устанавливать, наблюдать и контролировать тысячи рабочих станций и серверов NOD32.

## 1.2 Модули и компоненты

**Antivirus MONitor (AMON)** On-access (резидентный) сканер, который автоматически проверяет файлы перед осуществлением доступа к ним.

**NOD32** "On-demand" сканер, который можно запустить вручную для проверки отдельных файлов или сегментов диска. Этот модуль можно также запрограммировать на запуск в часы с наименьшей загрузкой.

**Internet MONitor (IMON)** Резидентный сканер, работающий на уровне Winsock и препятствующий попаданию зараженных файлов на диски компьютера. Данный модуль проверяет Интернет-трафик (HTTP) и входящую почту, полученную по протоколу POP3.

**E-mail MONitor (EMON)** Дополнительный модуль для проверки входящих/исходящих сообщений через интерфейс MAPI, например, в Microsoft Outlook и Microsoft Exchange.

**Document MONitor (DMON)** Использует запатентованный интерфейс Microsoft API для проверки документов Microsoft Office (включая Internet Explorer).

## 1.3 Антивирус Dr. WEB

Программа Dr. Web относится к классу антивирусных программных средств, называемых полифагами. Она предназначена для поиска и обезвреживания файловых, загрузочных и файлово-загрузочных вирусов. Cущественной особенностью Dr. Web, которая выделяет его среди других программ-полифагов, является использование оригинального эвристического анализатора наряду с традиционным методом обнаружения вирусов по их сигнатурам (определенной последовательности байтов в теле программы, которая однозначно идентифицирует конкретный вирус). Большинство существующих в настоящее время программ-полифагов используют только метод обнаружения вирусов по сигнатурам.

Тем самым возможности таких программ по обнаружению вирусов ограничены строго определенным набором, который известен автору программы. Использование эвристического анализатора позволяет выявлять также вирусы, сигнатура которых неизвестна автору программы. Алгоритмы, используемые в Dr. Web позволяют выявлять все известные в настоящее время типы вирусов.

Программы семейства Dr. WEB выполняют поиск и удаление известных им вирусов из памяти и с дисков компьютера, а также осуществляют эвристический анализ файлов и системных областей дисков компьютера. Эвристический анализ позволяет с высокой степенью вероятности обнаруживать новые, ранее неизвестные, компьютерные вирусы.

В 1999 году появилось новое поколение 32-битных антивирусных программ (DrWeb32). Оно включает в себя набор программ для Windows 95-XP, DOS/386, OS/2 и Novell NetWare, к которым несколько позже присоединились программы для Linux, FreeBSD и Solaris x86.

В комплект программ для Windows 95-XP входит полифаг Dr. WEB и резидентный сторож SpIDer Guard. Программа-полифаг обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системных областях дисков компьютера.

Резидентный сторож (называемый также монитором), находясь в памяти компьютера, постоянно контролирует вирусоподобные ситуации, производимые различными программами с диском и памятью.

Начиная с версии 4.20, в комплект программ для Windows входит Планировщик Dr. WEB, позволяющий производить запуск антивирусных программ и проверку устройств хранения информации, а также осуществлять обновление вирусных баз и компонентов программы по графику, задаваемому пользователем.

Антивирусные программы семейства Dr. WEB для DOS, DOS/386, OS2 и Novell NetWare являются полифагами. В составе программ для Linux и FreeBSD присутствуют как полифаги, так и демоны. (Демон DrWebD может использоваться практически в любых схемах обработки данных в качестве подключаемого внешнего антивирусного фильтра. Например, почтовые системы (такие как sendmail, qmail и др.) могут быть достаточно легко и гибко настроены на использование демона DrWebD для проверки проходящих через почтовый сервер сообщений e-mail).

Программа представляет собой классический полифаг и предназначена для использования в 32-битных операционных системах семейства Windows (т.е. Windows 95/98/2000/ME/XP, а также Windows NT 4.0 и выше). Программа производит сканирование файлов и системных областей дисков компьютера на наличие в них компьютерных вирусов и, при нахождении последних, производит их лечение. Кроме того в составе программы имеется эвристический анализатор, позволяющий находить новые, неизвестные вирусы.

Dr. WEB для Windows выпущена в двух вариантах: с графическим интерфейсом (DrWeb32w) и без него (DrWebwcl). Оба варианта поддерживают одинаковый набор параметров (ключей) командной строки. Но для варианта с графическим интерфейсом все настройки могут производиться из диалоговых панелей. Вариант без графического интерфейса требует несколько меньших ресурсов.

Оба варианта программы используют один и тот же конфигурационный файл и одну и ту же группу настроек в этом файле, что дает возможность попеременного использования данных программ с настройкой требуемых режимов наиболее удобным способом.

## 1.4 Антивирус Kaspersky Internet Security

Защита Kaspersky Internet Security строится исходя из источников угроз, то есть на каждый источник предусмотрен отдельный компонент приложения, обеспечивающий его контроль и необходимые мероприятия по предотвращению вредоносного воздействия этого источника на данные пользователя. Такое построение системы защиты позволяет гибко настраивать приложение под нужды конкретного пользователя или предприятия в целом.

Kaspersky Internet Security включает:

Компоненты защиты, обеспечивающие защиту вашего компьютера на всех каналах поступления и передачи информации.

Задачи поиска вирусов, посредством которых выполняется проверка компьютера или отдельных файлов, каталогов, дисков или областей, на присутствие вирусов.

Сервисные функции, обеспечивающие информационную поддержку в работе с приложением и позволяющие расширить ее функциональность.

## 1.4.1 Компоненты защиты

Защита вашего компьютера в реальном времени обеспечивается следующими компонентами защиты:

**Файловый Антивирус.**

Файловая система может содержать вирусы и другие опасные программы. Вредоносные программы могут годами храниться в вашей файловой системе, проникнув однажды со съемного диска или из интернета, и никак не проявлять себя. Однако стоит только открыть зараженный файл, вирус тут же проявит себя.

Файловый Антивирус - компонент, контролирующий файловую систему компьютера. Он проверяет все ОТКРЫВАЕМЫЕ, ЗАПУСКАЕМЫЕ И СОХРАНЯЕМЫЕ файлы на вашем компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается приложением, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен Антивирусом. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище, или помещен на карантин.

**Почтовый Антивирус.**

Электронная почтовая корреспонденция широко используется злоумышленниками для распространения вредоносных программ. Она является одним из основных средств распространения червей. Поэтому крайне важно контролировать все почтовые сообщения.

Почтовый Антивирус - компонент проверки всех входящих и исходящих почтовых сообщений вашего компьютера. Он анализирует электронные письма на присутствие вредоносных программ. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

**Веб-Антивирус.**

Открывая в интернете различные веб-сайты, вы рискуете заразить компьютер вирусами, которые будут установлены на компьютер при помощи скриптов, содержащихся на веб-страницах, а также загрузить опасный объект на свой компьютер.

Веб-Антивирус специально разработан для предотвращения подобных ситуаций. Данный компонент перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Строгому контролю также подвергается весь http-трафик.

**Проактивная защита.**

С каждым днем вредоносных программ становится все больше, они усложняются, комбинируя в себе несколько видов, методы распространения становятся все более сложными для обнаружения.

Для того чтобы обнаружить новую вредоносную программу еще до того, как она успеет нанести вред, "Лабораторией Касперского" разработан специальный компонент - Проактивная защита. Он основан на контроле и анализе поведения всех программ, установленных на вашем компьютере. На основании выполняемых действий Kaspersky Internet Security принимает решение: является программа потенциально опасной или нет. Таким образом, ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.

**Анти-Шпион.**

В последнее время широкое распространение получили программы, производящие несанкционированный показ материалов рекламного характера (баннеры, всплывающие окна), программы несанкционированного дозвона на платные интернет-ресурсы, различные средства удаленного администрирования и мониторинга, программы-шутки и т.д.

Анти-Шпион отслеживает данные действия на вашем компьютере и блокирует их выполнение. Например, компонент блокирует показ баннеров и всплывающих окон, мешающих пользователю при работе с веб-ресурсами, блокирует работу программ, пытающихся осуществить несанкционированный пользователем дозвон, анализирует веб-страницы на предмет фишинг-мошенничества.

**Анти-Хакер.**

Для вторжения на ваш компьютер хакеры используют любую возможную "лазейку", будь то открытый порт, передача информации с компьютера на компьютер и т.д.

Анти-Хакер - компонент, предназначенный для защиты вашего компьютера при работе в интернете и других сетях. Он контролирует исходящие и входящие соединения, проверяет порты и пакеты данных.

**Анти-Спам.**

Не являясь источником прямой угрозы, нежелательная корреспонденция (спам) увеличивает нагрузку на почтовые серверы, засоряет почтовый ящик пользователя, ведет к потере времени и тем самым наносит значительный финансовый урон.

Компонент Анти-Спам встраивается в установленный на вашем компьютере почтовый клиент и контролирует все поступающие почтовые сообщения на предмет спама. Все письма, содержащие спам, помечаются специальным заголовком. Предусмотрена также возможность настройки Анти-Спама на обработку спама (автоматическое удаление, помещение в специальную папку и т.д.).

## 1.5 Задачи поиска вирусов

Помимо защиты всех источников проникновения вредоносных программ крайне важно периодически проводить проверку вашего компьютера на присутствие вирусов. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты из-за, например, установленного низкого уровня защиты или по другим причинам.

Для поиска вирусов в состав Kaspersky Internet Security включены три задачи:

**Критические области.**

Проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные сектора дисков, системные каталоги Windows. Цель задачи - быстрое обнаружение в системе активных вирусов, без запуска полной проверки компьютера.

**Мой Компьютер.**

Поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.

**Объекты автозапуска.**

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы, а также оперативной памяти и загрузочных секторов дисков.

Также предусмотрена возможность создавать другие задачи поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых баз раз в неделю или задачу поиска вирусов в каталоге **Мои документы**.

**Антивирус AVZ.**

Антивирусная утилита AVZ предназначена для поиска и удаления:

SpyWare, AdvWare программ и модулей (это одно из основных назначений утилиты);

Сетевых и почтовых червей;

Троянских программ (включая все их разновидности, в частности Trojan-PSW, Trojan-Downloader, Trojan-Spy) и Backdoor (программ для скрытного удаленного управления компьютером);

Троянских программ-звонилок (Dialer, Trojan. Dialer, Porn-Dialer);

Клавиатурных шпионов и прочих программ, которые могут применяться для слежения за пользователем;

Утилита является прямым аналогом программ Trojan Hunter и LavaSoft Ad-aware 6. Первичной задачей программы является удаление AdWare, SpyWare и троянских программ.

Сразу следует отметить, что программы категорий SpyWare, AdWare по определению не являются вирусами или троянскими программами. Они шпионят за пользователем и загружают информацию и программный код на пораженный компьютер в основном из маркетинговых соображений (т.е. передаваемая информация не содержит критических данных - паролей, номеров кредитных карт и т.п., а загружаемая информация является рекламой или обновлениями). Однако очень часто грань между SpyWare и троянской программой достаточно условна и точная классификация затруднительна. Моя методика классификации и критерии описаны в данной справочной системе.

Особенностью программы AVZ является возможность настройки реакции программы на каждую из категорий вредоносных программы - например, можно задать режим уничтожения найденных вирусов и троянских программ, но заблокировать удаление AdWare.

Другой особенностью AVZ являются многочисленные эвристические проверки системы, не основанные на механизме поиска по сигнатурам - это поиск RootKit, клавиатурных шпионов, различных Backdoor по базе типовых портов TCP/UDP. Подобные методы поиска позволяют находить новые разновидности вредоносных программ.

Кроме типового для программ данного класса поиска файлов по сигнатурам в AVZ встроена база с цифровыми подписями десятков тысяч системных файлов. Применение данной базы позволяет уменьшить количество ложных срабатываний эвристики и позволяет решать ряд задач. В частности, в системе поиска файлов есть фильтр для исключения известных файлов из результатов поиска, в диспетчере запущенных процессов и настроек SPI производится цветовое выделение известных процессов, при добавлении файлов в карантин производится блокировка добавления известных AVZ безопасных файлов.

Как показала моя практика, очень часто программа типа SpyWare может быть классифицирована как AdWare и наоборот (причины просты - целью шпионажа в большинстве случаев является целевая реклама). Для таких случаев в своей классификации я ввел обобщающую категорию Spy, которая грубо может трактоваться как AdWare+SpyWare. Термин Spy переводится как "шпион", "тайный агент", "следить", "подглядывать", "совать нос в чужие дела". Этот термин достаточно хорошо подходит к программам подобного класса.

## 2. Практическая часть

## 2.1 Результаты тестирования диска

## 2.1.1 Антивирус NOD32

**Статистика:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | По умолчанию | Оптимальная защита | Максимальная зашита |
| Проверено | 2311 | 2326 | 3492 |
| Обнаружено | 0 | 0 | 0 |
| Длительность | 00: 00: 29 | 00: 00: 31 | 00: 00: 55 |
| Скорость проверки | 514 Kb/s | 511 Kb/s | 502 Kb/s |

## 2.1.2 Антивирус Kaspersky Internet Security

**Статистика:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | По умолчанию | Оптимальная защита | Максимальная зашита |
| Проверено | 2311 | 2330 | 3513 |
| Обнаружено | 0 | 0 | 0 |
| Длительность | 00: 00: 48 | 00: 01: 02 | 00: 01: 29 |
| Скорость проверки | 492 Kb/s | 488 Kb/s | 484 Kb/s |

## 2.1.3 Антивирус Dr. WEB

**Статистика:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | По умолчанию | Оптимальная защита | Максимальная зашита |
| Проверено | 2311 | 2323 | 3305 |
| Обнаружено | 0 | 0 | 0 |
| Длительность | 00: 00: 35 | 00: 00: 56 | 00: 01: 03 |
| Скорость проверки | 504 Kb/s | 499 Kb/s | 490 Kb/s |

## 2.1.4 Антивирус AVZ

**Статистика:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | По умолчанию | Оптимальная защита | Максимальная зашита |
| Проверено | 2311 | 2319 | 3203 |
| Обнаружено | 0 | 0 | 0 |
| Длительность | 00: 00: 42 | 00: 00: 59 | 00: 01: 12 |
| Скорость проверки | 493 Kb/s | 491 Kb/s | 486 Kb/s |

## 2.2 Сводные диаграммы по проверки диска



## 2.3 Результаты тестирования папки с вирусами

Для данной лабораторной работы была взята папка с **85 вирусами.**

Названия данных вирусов:

обнаружено: вредоносная программа Constructor. DOS. DarkBomb.11Файл: E: \disk\_2\VIRI\A-BOMB11. RAR/A-BOMB. EXE // ExePack

обнаружено: вредоносная программа Constructor. DOS. DarkBomb. 20Файл: E: \disk\_2\VIRI\ANSI20B. RAR/ANSIB20. EXE

обнаружено: вредоносная программа Constructor. DOS. AdusterФайл: E: \disk\_2\VIRI\ANSIMAKE. RAR/ANSIMAKE. EXE // ExePack

обнаружено: троянская программа Trojan. DOS. Antilame. aФайл: E: \disk\_2\VIRI\ANTI. RAR/ANTICOMM. RAR/ANTICOMM.com

обнаружено: вирус Virus. BAT. Vir94.comФайл: E: \disk\_2\VIRI\BATCHCOL. ZIP/VIRUSES. ZIP/BATCH. ZIP/BATCH.com

обнаружено: вирус Virus. BAT. DittyФайл: E: \disk\_2\VIRI\BATCHCOL. ZIP/VIRUSES. ZIP/DITTY. ZIP/WINSTART. BAT

обнаружено: вирус Virus. BAT. Fret.1023Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/VIRUSES. ZIP/FRET102. ZIP/FRET102. BAT

обнаружено: вирус Virus. BAT. IBBM. Bug. aФайл: E: \disk\_2\VIRI\BATCHCOL. ZIP/VIRUSES. ZIP/IMABUG. ZIP/IMABUG. TXT

обнаружено: вирус Virus. BAT. Lame.874Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/VIRUSES. ZIP/LAME. ZIP/LAME. TXT

обнаружено: вирус Virus. BAT. Winstart.296Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/VIRUSES. ZIP/WINSTART. ZIP/WINST296. ZIP/WINSTART. BAT

обнаружено: вирус Virus. BAT. Winstart.297Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/VIRUSES. ZIP/WINSTART. ZIP/WINST297. ZIP/WINSTART. BAT

обнаружено: вирус Virus. BAT. Batalia6Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/TOOLS. ZIP/BATALIA. ZIP/BATALIA6. ZIP/RULZ

обнаружено: вирус Virus. BAT. Batalia6Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/TOOLS. ZIP/BATALIA. ZIP/BATALIA6. ZIP/BATALIA6. BAT

обнаружено: вирус Virus. BAT. Batalia6Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/TOOLS. ZIP/BATALIA. ZIP/BATALIA6. ZIP/PACK. BAT

обнаружено: вредоносная программа Constructor. BAT. BVGenФайл: E: \disk\_2\VIRI\BATCHCOL. ZIP/TOOLS. ZIP/BVGEN. ZIP/BVGEN. BAT

обнаружено: вирус Type\_BAT (модификация) Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/TUTORIAL. ZIP/BVTUTOR1. TXT

обнаружено: вирус Virus. BAT. PifVФайл: E: \disk\_2\VIRI\BATCHCOL. ZIP/TUTORIAL. ZIP/BVTUTOR2. TXT

обнаружено: вирус Type\_BAT (модификация) Файл: E: \disk\_2\VIRI\BATCHCOL. ZIP/TUTORIAL. ZIP/BVTUTOR3. TXT

обнаружено: троянская программа Trojan. DOS. Bomb\_ACKФайл: E: \disk\_2\VIRI\BOMB. RAR/BOMB. TRO

обнаружено: вредоносная программа Constructor. DOS. G2Файл: E: \disk\_2\VIRI\G2. RAR/G2. EXE

обнаружено: вредоносная программа Constructor. DOS. IVP\_17Файл: E: \disk\_2\VIRI\IVP. RAR/IVP. RAR/IVP. EXE

обнаружено: вирус Virus. DOS. IVP-basedФайл: E: \disk\_2\VIRI\IVP. RAR/IVP. RAR/EXAMPLES. RAR/BUBBLES2.com

обнаружено: вредоносная программа Constructor. DOS. NRLGФайл: E: \disk\_2\VIRI\NRLG. RAR/NRLG. EXE // Tinyprog

обнаружено: вредоносная программа Constructor. DOS. SpamacidalФайл: E: \disk\_2\VIRI\SPMACIDL. RAR/SPMACID. EXE // ExePack

обнаружено: троянская программа Trojan. BAT. SpamФайл: E: \disk\_2\VIRI\SPMACIDL. RAR/TROJAN. RAR/SPAM. BAT

обнаружено: троянская программа Trojan. BAT. SpamФайл: E: \disk\_2\VIRI\SPMACIDL. RAR/TROJAN. RAR/SPAM.com

обнаружено: троянская программа Trojan. DOS. THCK. aФайл: E: \disk\_2\VIRI\THCK200. RAR/THCK-FP. EXE

обнаружено: троянская программа Trojan. DOS. THCK. aФайл: E: \disk\_2\VIRI\THCK200. RAR/THCK-TBC. EXE

обнаружено: троянская программа Trojan. DOS. THCK. aФайл: E: \disk\_2\VIRI\THCK200. RAR/THCK-TC. EXE

обнаружено: вредоносная программа Constructor. DOS. TBTRФайл: E: \disk\_2\VIRI\TSR\_TB. RAR/TSR\_TB. EXE

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-ENGL. RAR/VCS. BIN

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-ENGL. RAR/VCS2. BIN

обнаружено: вредоносная программа Constructor. DOS. VCSФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-ENGL. RAR/VCS\_ENGL. EXE

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-GERM. RAR/VCS. BIN

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-GERM. RAR/VIRUS. CYY

обнаружено: вредоносная программа Constructor. DOS. VCSФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-GERM. RAR/VCS. EXE

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-TURD. RAR/VCS-TURD.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCS-VDV. RAR/VCS-VDV.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSBPOEM. RAR/VCSBPOEM.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSCATAN. RAR/VCSCATAN.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSCONFG. RAR/VCSCONFG.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSDARKS. RAR/VCSDARKS.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSDR-NO. RAR/VCSDR-NO.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSLOSER. RAR/VCSLOSER.com

обнаружено: вирус Virus. DOS. VCS. MantaФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSMANTA. RAR/VCSMANTA.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSPARAN. RAR/VCS.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSPARAN. RAR/VCSPARAN.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSPUSSY. RAR/VCSPUSSY.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSSTTS1. RAR/VCSSTTS1.com

обнаружено: вирус Virus. DOS. VCS. dropperФайл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSSTTS2. RAR/VCSSTTS2.com

обнаружено: вирус Virus. DOS. Vdv.853Файл: E: \disk\_2\VIRI\VCS-COLL. RAR/VCSVD853. RAR/VCSVD853.com

обнаружено: вредоносная программа VirTool. DOS. HtcappФайл: E: \disk\_2\VIRI\VLC. RAR/HTCAPP. EXE // PkLite

обнаружено: вредоносная программа Constructor. DOS. VLab.11Файл: E: \disk\_2\VIRI\VLC. RAR/VLAB. EXE

обнаружено: вирус Virus. DOS. AntiWin.633Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/ANTIWIN. ZIP/ANTIWIN. EXE

обнаружено: вирус Virus. DOS. DWI.1051Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/DWI. ZIP/DWI.com

обнаружено: вирус Virus. DOS. DWI.1051Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/DWI. ZIP/DWI. EXE // Com2Exe

обнаружено: вирус Virus. DOS. Trivial. Winex.113Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/EXE2WIN. ZIP/E2WIN113.com

обнаружено: вирус Virus. DOS. Trivial. Exe2Win.116Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/EXE2WIN. ZIP/E2WIN116.com

обнаружено: вирус Virus. DOS. Trivial. Winex.132Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/EXE2WIN. ZIP/E2WIN132.com

обнаружено: вирус Virus. DOS. Trivial. Winex.214Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/EXE2WIN. ZIP/E2WIN214.com

обнаружено: вирус Virus. DOS. BetaBoys.459Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINAIMED. ZIP/WHY-WIND. ZIP/WHY-WIND.com

обнаружено: вирус Virus. Win9x. Boza. cФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/BIZATCH. ZIP/BIZATCH. EXE

обнаружено: троянская программа Trojan. DOS. CreateФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/KBWIN. ZIP/CREATE.com

обнаружено: вирус Virus. DOS. Jerusalem. KbWin.1349Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/KBWIN. ZIP/KBWIN95. EXE

обнаружено: вирус Virus. Multi. Ph33rФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/PH33R. ZIP/PH33R.com

обнаружено: вирус Virus. Win16. Tentacle. 1958Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/TENTACLE. ZIP/TENTACLE. EXE

обнаружено: вирус Virus. Win16. TwitchФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/TWITCH. ZIP/TWITCH. EXE

обнаружено: вирус Virus. Win16. StalkerX.1241Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/W31V. ZIP/W31V. EXE

обнаружено: вирус Virus. Win16. StalkerX.1241Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/W31V. ZIP/W31V. OBJ // ObjectModule

обнаружено: вирус Virus. Win16. WinLamer2.1734Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WINLAMER. ZIP/WINLAME2. EXE

обнаружено: вирус Virus. Win16. Winsurf. aФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WINSURFR. ZIP/WINSURFR. SCR // DebugScript

обнаружено: вирус Virus. Win16. Winsurf. aФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WINSURFR. ZIP/WINSURFR.com

обнаружено: вирус Virus. Win16. Wintiny. bФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WINTINY. ZIP/WINTINY. EXE

обнаружено: вирус Virus. Win16. AEP. aФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WINVIK. ZIP/WINVIKA. ZIP/WINVIR.com

обнаружено: вирус Virus. Win16. AEP. aФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WINVIK. ZIP/WINVIKA. ZIP/WINVIKA. EXE

обнаружено: вирус Virus. Win16. AEP. bФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WINVIK. ZIP/WINVIKB. ZIP/WINVIKB. EXE

обнаружено: вирус Virus. Win16. Vir\_1\_4Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WVIR14. ZIP/WVIR14. EXE

обнаружено: вирус Virus. Win16. Vir\_1\_4Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINMADEF. ZIP/WVIR14. ZIP/WVIR14A. EXE

обнаружено: вредоносная программа VirTool. Win16. PMEФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINTOOLS. ZIP/PMEW00. ZIP/PMEW. OBJ // ObjectModule

обнаружено: вирус Virus. Win16. StalkerX.650Файл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINTOOLS. ZIP/VKIT100. ZIP/DATA. BIN

обнаружено: вредоносная программа Constructor. DOS. VkitФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINTOOLS. ZIP/VKIT100. ZIP/VKIT. EXE

обнаружено: вредоносная программа Constructor. DOS. WVEФайл: E: \disk\_2\VIRI\WINVCOLL. ZIP/WINTOOLS. ZIP/WVE100. ZIP/WVE. EXE

Далее были протестированы все имеющиеся антивирусы, результаты тестирования приведены в сводных таблицах 1,2. Все данные, полученные при тестировании были сведены в общую сводную диаграмму.

**Таблица 1** - Количество найденных вирусов для каждого антивируса

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Типы вирусов | Антивирус NOD32 | Kaspersky Internet Security | Dr. WEB | AVZ |
| Вредоносная программа | 15 | 16 | 14 | 11 |
| Троянская программа | 8 | 9 | 6 | 5 |
| Вирус | 52 | 55 | 49 | 52 |

**Таблица 2** - Процент обнаружения вирусов для каждого антивируса

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Антивирус | % обнаружения | Проверено | Тел вирусов | Подозрительных файлов |
| Антивирус NOD32 | 91% | 85 | 75 | 3 |
| Kaspersky Internet Security | 98% | 85 | 80 | 0 |
| Dr. WEB | 84% | 85 | 69 | 2 |
| AVZ | 83% | 85 | 68 | 1 |

## 2.4 Сводная диаграмма

**Процент обнаружения каждого антивируса**



## Вывод

В результате выполнения данной лабораторной работы, я ознакомилась с пятью различными антивирусами, изучила их характеристики. В ходе этой работы были протестированы жесткие диски, а также специально взятая папка с вирусами. В результате мы можем сравнить производительность и эффективность каждого антивируса.

Таким образам, по данным работы я пришла к выводу, что антивирус **Kaspersky Internet Security** является более эффективным при нахождении различного рода вирусов (процент нахождения здесь выше), но по производительности и по скорости обработки файлов лучшим является Антивирус **NOD32.** Другие же антивирусы имеют еще более низкие результаты.

Мне кажется, в плане обеспечения безопасности компьютера лучшим является более эффективный антивирус **Kaspersky Internet Security.**