Министерство образования ХХХ

Государственное бюджетное профессиональное образовательное учреждение

ХХХ «ХХХХ»

09.02.07

ОТЧЕТ

По лабораторным работам

ОП 03 Информационные технологии

ККОО.ИТХХХХ.000

Студент

Преподаватель

Дата защиты_____ Оценка_____

2021

Лабораторная работа №5

1. Тема: вирусы и антивирусные программы

2. Цель: сформировать и закрепить навыки работы по работе с одной из антивирусных программ , научиться использовать антивирусную утилиту для выявления вредоносного ПО и уничтожения вируса на ПК

3. Оборудование: ПК

Профилактика

При использовании компьютера, особенно во время работы в Интернете, необходимо помнить о том, что ни одна система защиты от вирусов не способна снизить вероятность заражений до нуля. Для того чтобы достигнуть наивысшей степени безопасности и комфорта, следуйте нескольким простым правилам и используйте систему защиты от вирусов надлежащим образом.

Регулярно обновляйте систему защиты от вирусов.

Согласно статистическим данным, полученным от системы своевременного обнаружения ThreatSense.Net, тысячи новых уникальных вирусов появляются ежедневно. Они пытаются обойти существующие меры безопасности и приносят доход их авторам за счет убытков других пользователей. Специалисты лаборатории ESET ежедневно анализируют угрозы, создают и предоставляют к загрузке новые обновления для непрерывного усовершенствования защиты пользователей от вирусов. Неправильно настроенная система обновлений снижает эффективность программы. Дополнительную информацию о настройке процесса обновления см. здесь.

Загружайте пакеты обновлений операционной системы и других программ.

Авторы вредоносного кода используют различные уязвимости в системе для увеличения эффективности распространения злонамеренного кода. По этой

причине производители программного обеспечения внимательно следят за появлением отчетов о новых уязвимостях их программных продуктов и выпускают регулярные обновления, стараясь снизить вероятность появления новых угроз. Очень важно использовать эти обновления сразу после их выпуска. Примерами программных продуктов, регулярно нуждающихся в обновлениях, являются операционные системы семейства Windows или широко распространенный веб-браузер Internet Explorer.

Архивируйте важные данные.

Авторы злонамеренного программного обеспечения не заботятся о сохранности данных пользователей, и активность их продуктов зачастую ведет к полной потере функциональности компьютера и необратимому повреждению важной информации. Необходимо регулярно создавать резервные копии важных и уязвимых данных на внешних носителях (DVD-дисках или внешних накопителях на жестких дисках). Профилактические меры такого рода позволяют быстро и просто восстановить данных в случае их повреждения.

Регулярно сканируйте компьютер на вирусы.

Регулярное автоматическое сканирование компьютера с надлежащими настройками помогает устранять заражения, которые могут быть пропущены модулем защиты в режиме реального времени, например вследствие устаревшей на тот момент базы данных сигнатур вирусов.

Следуйте основным правилам безопасности.

Это наиболее эффективное и полезное правило из всех — всегда будьте осторожны. На данный момент огромное число злонамеренных программ требуют участия пользователя для установки и запуска. Если соблюдать элементарную осторожность при открытии новых файлов, можно значительно сэкономить время и силы, которые будут потрачены на поиск и устранение заражения. Некоторые полезные правила: не посещайте подозрительные веб-сайты с множеством всплывающих окон и анимированной рекламой;

будьте осторожны при установке свободно распространяемого ПО, пакетов кодеков и т. п.; используйте только безопасные программы и посещайте безопасные веб-сайты;

будьте осторожны при использовании вложений в сообщения электронной почты, особенно это касается сообщений, рассылаемых массово и отправленных неизвестными лицами;

не используйте учетную запись с правами администратора для повседневной работы на компьютере.

Страницы справочной системы

Мы рады приветствовать вас. И благодарим за то, что вы стали пользователем антивируса ESET NOD32. Эта справочная система поможет вам сделать работу на компьютере более удобной и безопасной.

С чего начать?

Перед запуском антивируса ESET NOD32 рекомендуется ознакомиться с различными типами заражений, с которыми вы можете столкнуться. Кроме того, ознакомьтесь с руководством по предотвращению. В нем находится важная информация о борьбе с угрозами безопасности.

Дополнительную информацию о новых функциях антивируса ESET NOD32 см. здесь. К вашим услугам также руководство по настройке и изменению основных параметров антивируса ESET NOD32.

Как использовать справочную систему антивируса ESET NOD32?

Информация страниц справки удобно распределена по главам и подразделам. Пользователь может найти необходимую информацию, просматривая структуру справочной системы.

Для того чтобы получить дополнительную информацию о любом окне программы, нажмите клавишу F1. Откроется страница справки, содержащая информацию о текущем окне.

Программа позволяет искать справочную информацию по ключевым словам или по словам и фразам. Разница между двумя способами состоит в том, что ключевое слово, характеризующее содержимое справочной страницы, может отсутствовать в тексте этой страницы. Поиск по словам и фразам осуществляется в содержимом всех страниц. В результате отображаются все страницы, содержащие именно эти слова и фразы.

Классификация компьютерных вирусов

По среде обитания:

- Сетевые – распространяются по различным компьютерным сетям
- Файловые – внедряются в исполняемые модули (COM, EXE)
- Загрузочные – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
- Фалово-загрузочные – внедряются и в загрузочные сектора и в исполняемые модули

По способу заражения:

- Резидентные – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
- Нерезидентные – не заражают оперативную память и активны ограниченное время

По воздействию:

- Неопасные – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
- Опасные – приводят к различным нарушениям в работе компьютера
- Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

- Паразиты – изменяют содержимое файлов и секторов, легко обнаруживаются

- Черви – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
- Стелсы – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
- Мутанты – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
- Трояны – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

Основные меры по защите от вирусов

- оснастите свой компьютер одной из современных антивирусных программ: Doctor Weber, Norton Antivirus, AVP
- постоянно обновляйте антивирусные базы
- делайте архивные копии ценной для Вас информации (гибкие диски, CD)

Классификация антивирусного программного обеспечения

- Сканеры (детекторы). Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.
- Мониторы. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распостранение вируса на самой ранней стадии.
- Ревизоры. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.

Требования к системе:

Для корректной работы антивируса ESET NOD32 система должна соответствовать следующим аппаратным и программным требованиям:

- операционная система Windows 2000, XP, 2003
- процессор 400 МГц, 32-разрядный (x86) или 64-разрядный (x64);
- 128 Мб оперативной памяти;
- 35 Мб свободного места на диске;
- Super VGA (800 x 600).
- операционная система Windows Vista
- процессор 1 ГГц, 32-разрядный (x86) или 64-разрядный (x64);
- 512 Мб оперативной памяти;
- 35 Мб свободного места на диске;
- Super VGA (800 x 600).

Удаление программы

Если в системе уже установлен антивирус ESET NOD32, мастер установки предложит удалить его.

Выберите «Удалить», если нужно удалить антивирус ESET NOD32 с компьютера.

Антивирусная защита

Защита от вирусов и шпионских программ предназначена для ограждения системы от вредоносных атак с помощью проверки содержимого файлов, сообщений электронной почты и обмена данными через Интернет. Если вредоносный код обнаружен, модуль защиты от вирусов и шпионских программ обезвреживает его, сначала блокируя его исполнение, а затем очищает, удаляет или перемещает на карантин

Обновление программы

Регулярные обновления системы являются основой для обеспечения максимально возможного уровня безопасности, который предоставляется антивирусом ESET NOD32. Модуль обновления предназначен для получения регулярных обновлений программы. При этом обновляются как базы данных сигнатур вирусов, так и компоненты системы ESET Smart Security.

Примечание

Имя пользователя и пароль предоставляются компанией ESET после приобретения антивируса ESET NOD32.

Информацию о текущем состоянии обновлений можно получить в разделе «Обновление». Этот раздел содержит данные о версии базы данных сигнатур вирусов и информацию о необходимости ее обновления. Там же можно запустить процесс обновления немедленно с помощью функции «Обновить базу данных сигнатур вирусов». Эта функция доступна среди других параметров, таких как имя пользователя и пароль для доступа к серверам обновлений.

Информационная часть содержит такие полезные данные, как дата и время последнего удачного обновления и количество вирусов, информация о которых содержится в базе данных сигнатур. Числовой индикатор является активной ссылкой на список всех сигнатур, добавленных в базу в текущем обновлении. Этот список расположен на веб-сайте компании ESET.

Рекомендации

Как обновить антивирус ESET NOD32?

Как запланировать выполнение задачи (каждые 24 часа)?

Как удалить вирус с компьютера?

Если вашей проблемы нет в списке, воспользуйтесь поиском по ключевому слову или фразе по страницам справочной системы антивируса ESET NOD32.

Если решение не удалось найти методом поиска по содержимому справочной системы, обратитесь к регулярно обновляемой базе знаний компании ESET.

При необходимости свяжитесь напрямую со службой технической поддержки, опишите свою проблему или задайте вопрос. Контактная информация находится непосредственно в программе на вкладке «Справка и поддержка».

Вирусы

При заражении компьютера вирусами происходит порча файлов. Название категории возникло вследствие сходства таких программ с биологическими вирусами, так как они используют сходную технику для передачи своего кода с компьютера на компьютер.

Компьютерные вирусы атакуют в основном исполняемые файлы и документы. Для размножения вирус присоединяет свое «тело» к концу заражаемого файла. Вот краткое описание цикла размножения: после запуска зараженного файла вирус активируется (это происходит перед активацией самого приложения) и выполняет атакующие действия. После этого происходит запуск самого приложения. Вирус не может заразить компьютер, пока пользователь (по ошибке или намерено) собственноручно не запустит злонамеренную программу.

Компьютерные вирусы могут различаться по активности и степени опасности. Некоторые из вирусов особо опасны, так как могут уничтожать файлы на компьютере. С другой стороны, некоторые из вирусов не приводят к серьезным повреждениям. Они просто досаждают пользователю своей деятельностью, которая призвана демонстрировать навыки их разработчиков.

Важно заметить, что вирусы постепенно становятся редкостью по сравнению с троянскими программами или шпионским ПО, так как они коммерчески малоэффективны для авторов злонамеренных программ. Таким образом, термин «вирус» зачастую неверно используется для других типов

заражений. В настоящее время он постепенно выходит из употребления, и на смену ему приходит более точный термин «злонамеренное ПО». Если компьютер заражен вирусом, необходимо восстановить зараженные файлы в их исходное состояние, т. е. очистить их с помощью антивирусной программы.

Примеры вирусов: OneHalf, Tenga и Yankee Doodle

Обновление компонента программы

Обновления компонентов программы предоставляет новые функции или вносит изменения в уже существующие. Это действие может выполняться как в автоматическом режиме без вмешательства пользователя, так и с уведомлением. После установки обновления компонентов программы может бепотребоваться перезагрузка.

«Никогда не обновлять компоненты программы»

Обновление компонентов программы выполняться не будет. Этот выбор подходит для серверной установки, поскольку серверы обычно перезапускаются во время технического обслуживания.

«Всегда обновлять компоненты программы»

Обновления компонентов программы будут загружаться и устанавливаться автоматически. Обратите внимание на то, что может потребоваться перезагрузка компьютера.

«Запросить подтверждение перед загрузкой компонентов»

Программа будет отображать диалоговое окно с предложением загрузить обновления всякий раз, когда обновления доступны.

«Перезапустить после обновления компонентов программы»

Для правильного функционирования программы после выполнения обновления компонентов система должна быть перезагружена.

«Никогда не перезапускать компьютер»

Запрос на перезагрузку не будет отображаться даже в тех случаях, когда это необходимо. Этот выбор не рекомендуется, так как компьютер может функционировать некорректно до следующей перезагрузки.

«Предложить перезапуск компьютера, если необходимо»

После обновления компонентов программы будет предложено перезагрузить компьютер.

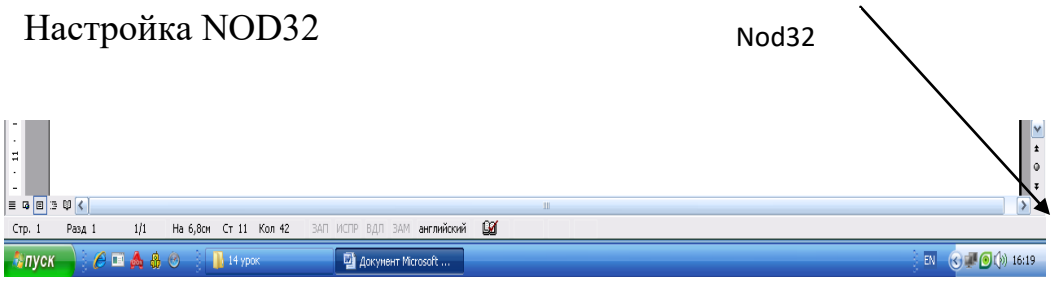
«Если необходимо, перезапустить компьютер без уведомления»

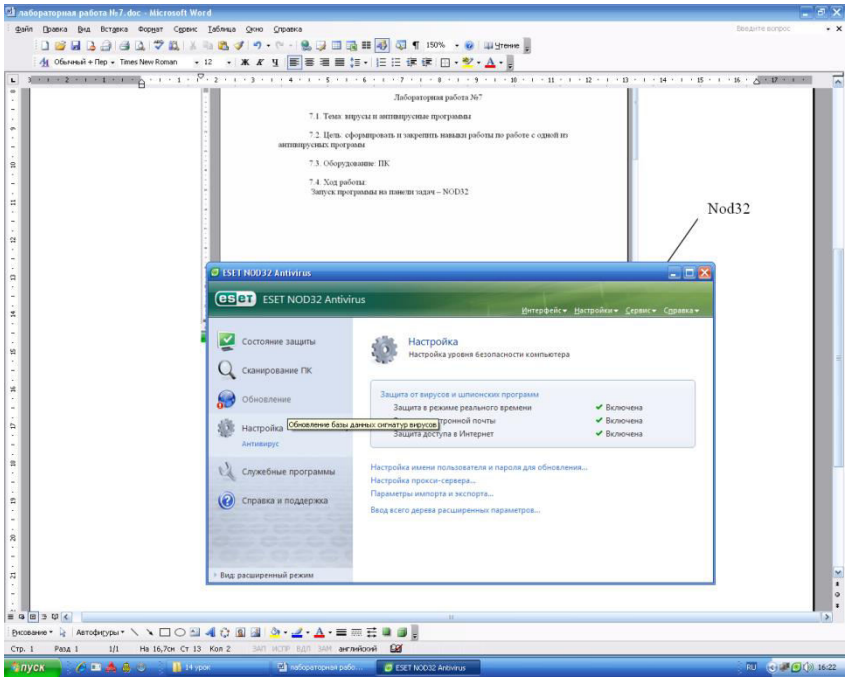
После обновления компонентов программы компьютер, если это необходимо, будет перезагружен.

4. Ход работы:

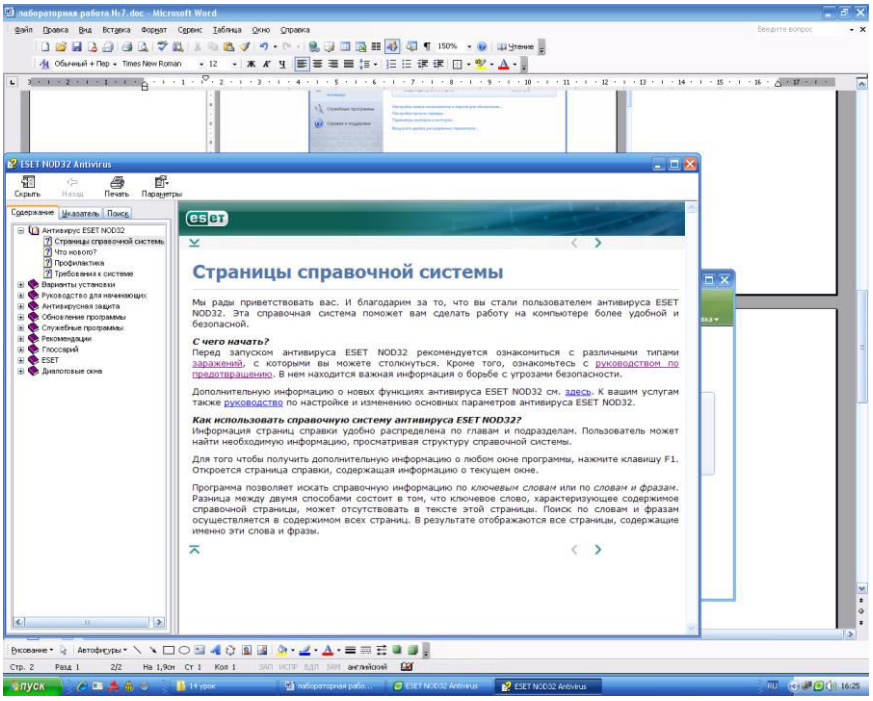
1) Запуск программы на панели задач – NOD32

Настройка NOD32

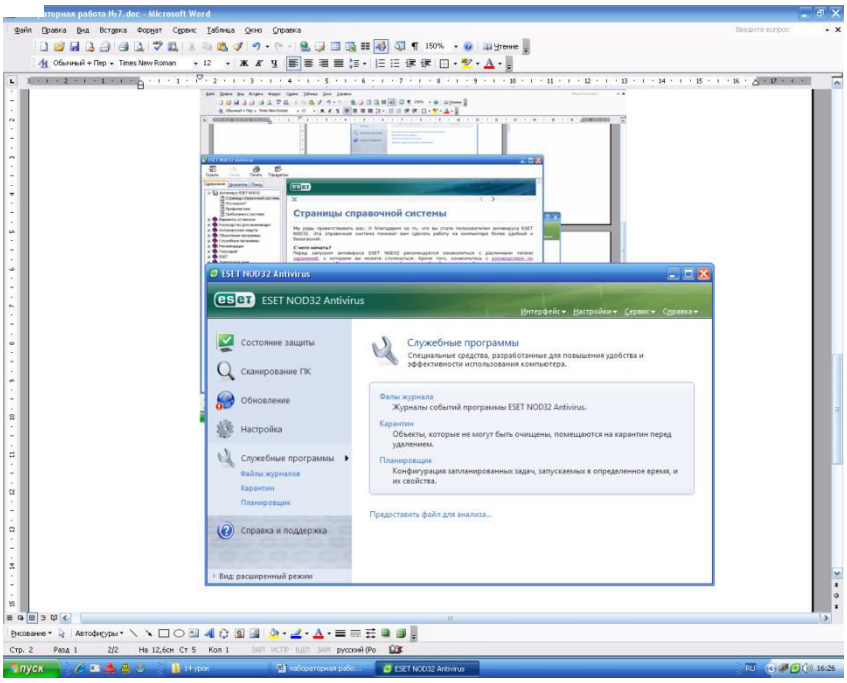




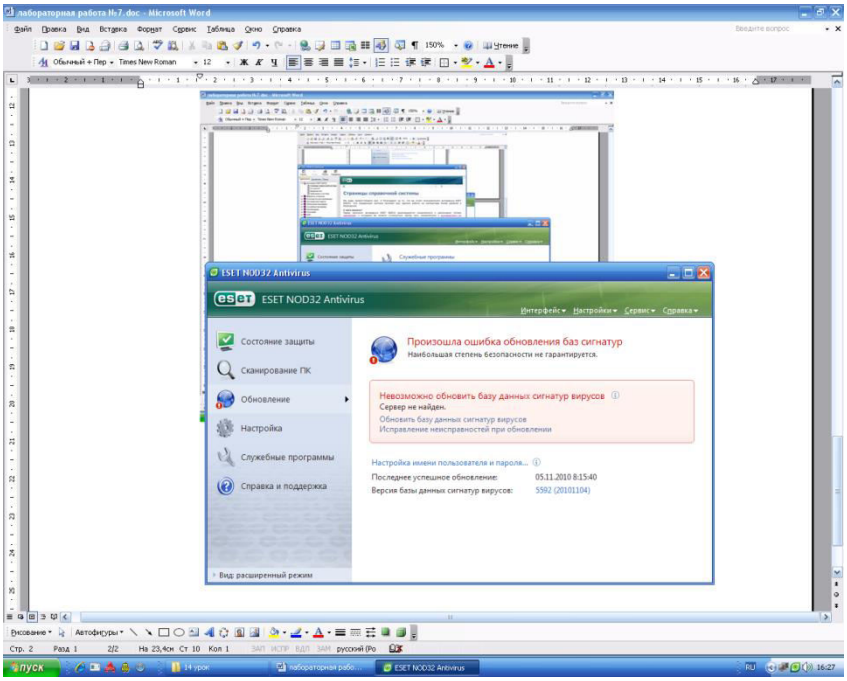
Страница справочной системы



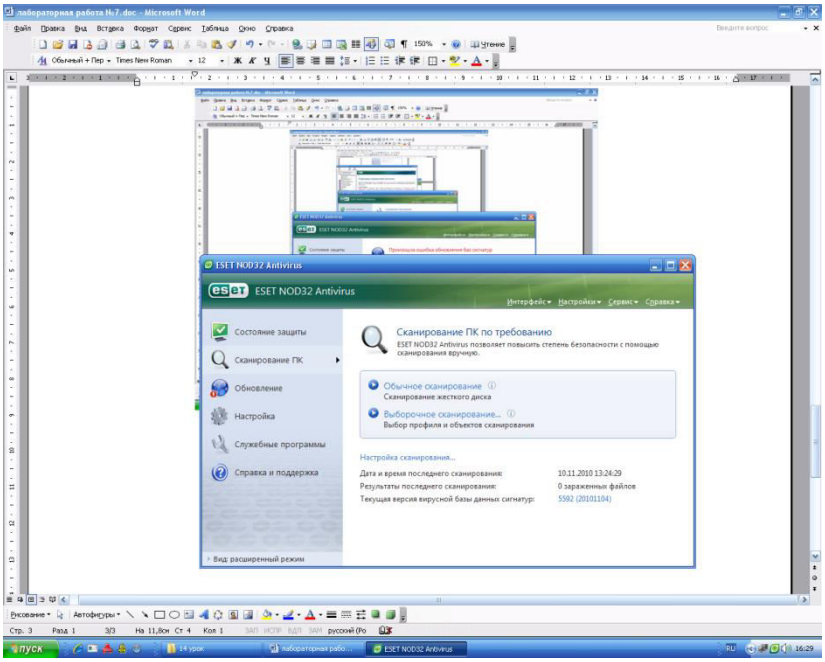
Служебные программы



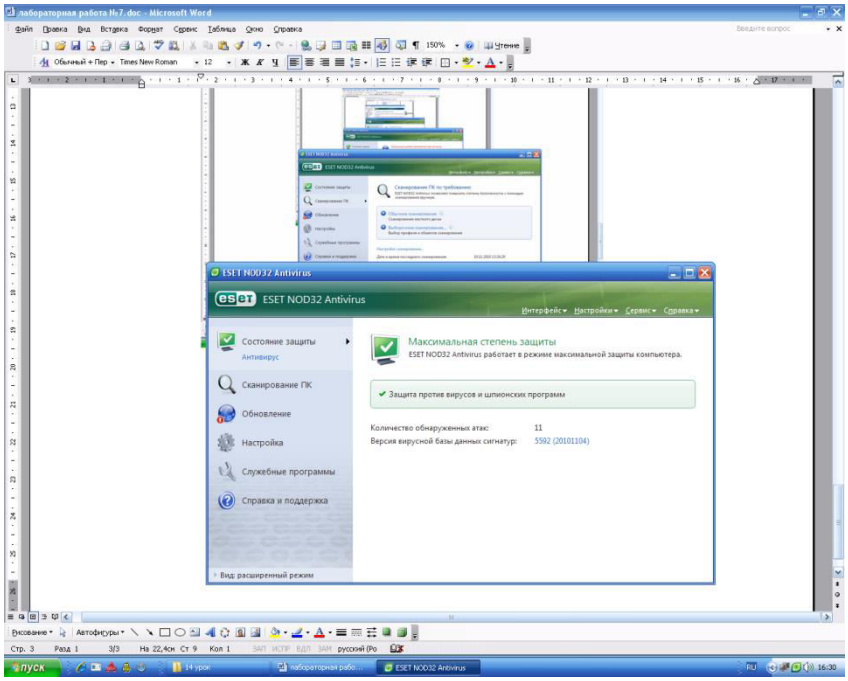
Обновление



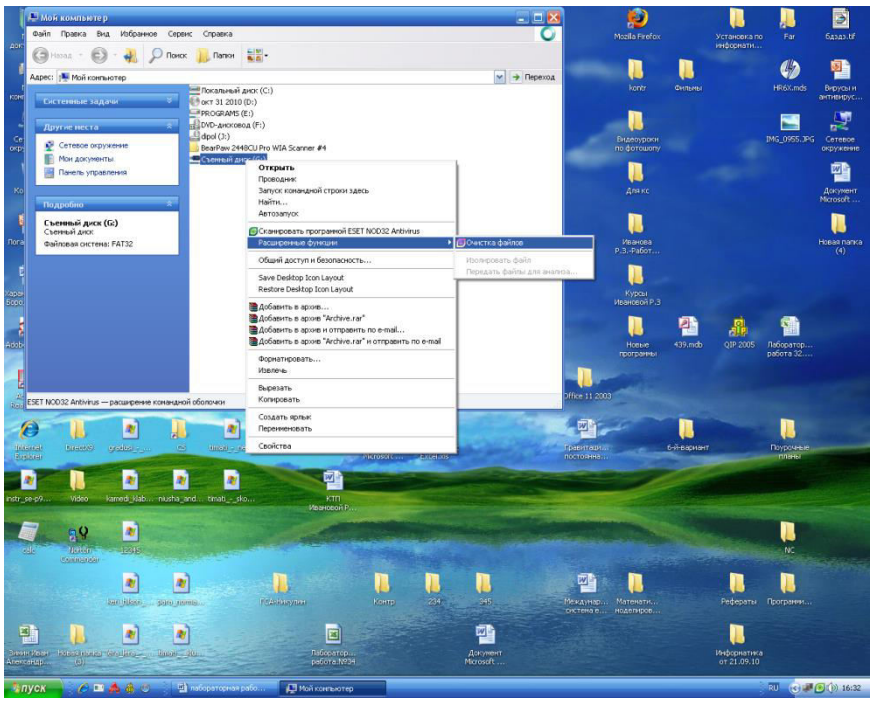
Сканирование ПК , удаление или изолирование вирусной программы



Состояния защиты



Очистка вирусов



2) Антивирусная утилита Dr. Web Curelt.

1. Обновить антивирусные базы

2. Познакомиться с возможностями программы

3. Проверить ПК на наличие вирусов.

Ход работы:

1 определение последовательности в запуске и обнаружении вредоносного ПО на проверяемых объектах:

- Запустить утилиту на Windows XP-7.
- Дождаться загрузки базы, отменить обновление базы.
- Ознакомиться с вкладками окна программы: Область, Объекты, Действия, Настройки.
- Установить Область сканирования – диск D:, Объекты – программы по расширению, Действия – запрос на лечение, Настройки - файл отчета.
- Запустить сканирование.
- После окончания сканирования проанализировать результаты (вкладка Статистика).

2 законспектировать этапы по обнаружению вредоносного ПО.

Вопросы:

1. Что такое антивирусная утилита?
2. Дайте классификацию вирусов.
3. Для чего нужны антивирусные программы?
4. Как запустить Dr. Web Curelt в безопасном режиме?
5. Средства антивирусной защиты.
6. Примеры антивирусных программ ПК.

Задание 2

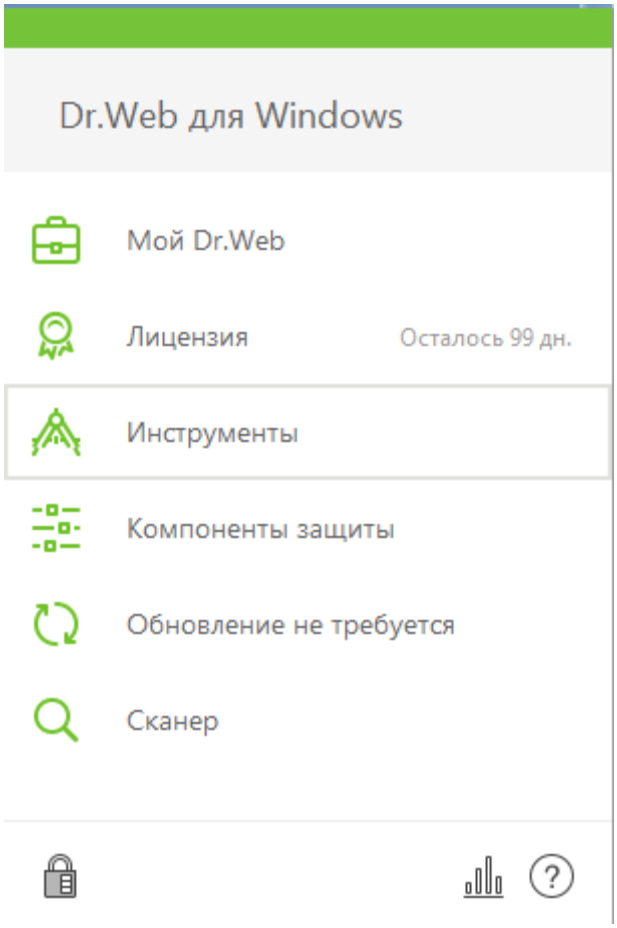


Figure 1

Задание 3

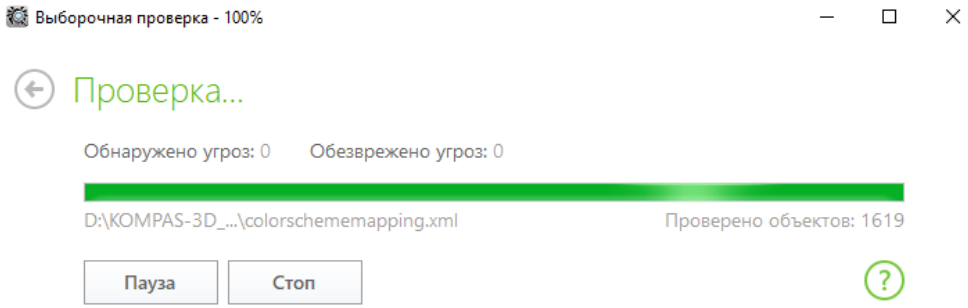


Figure 2

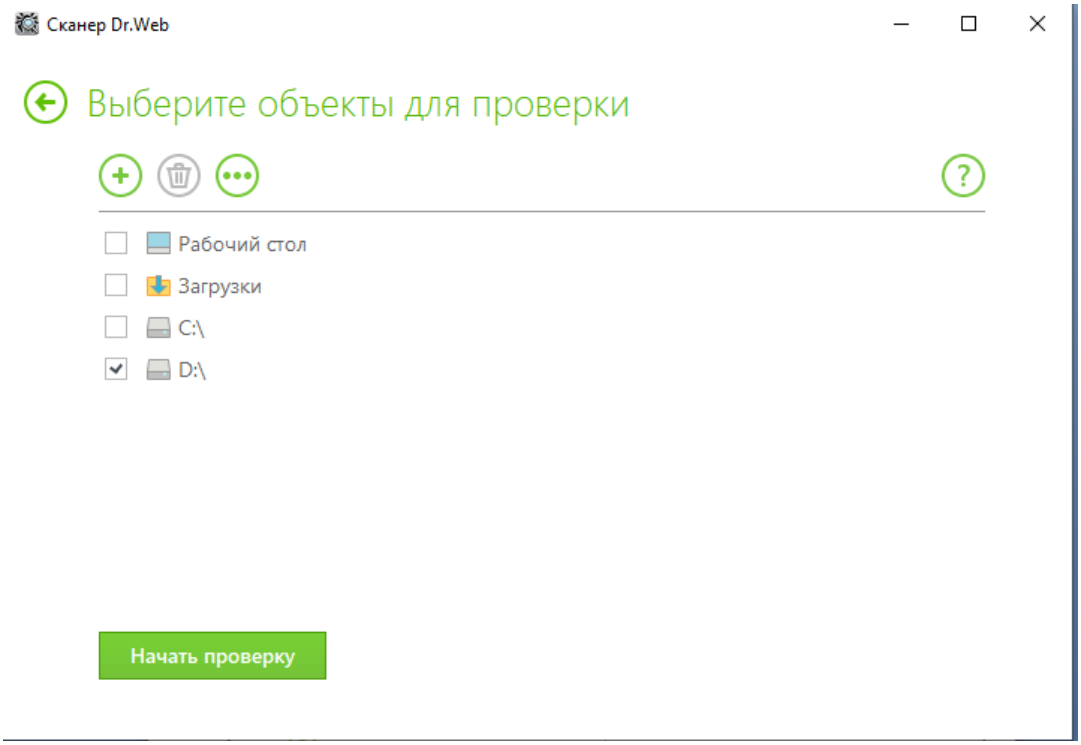


Figure 3

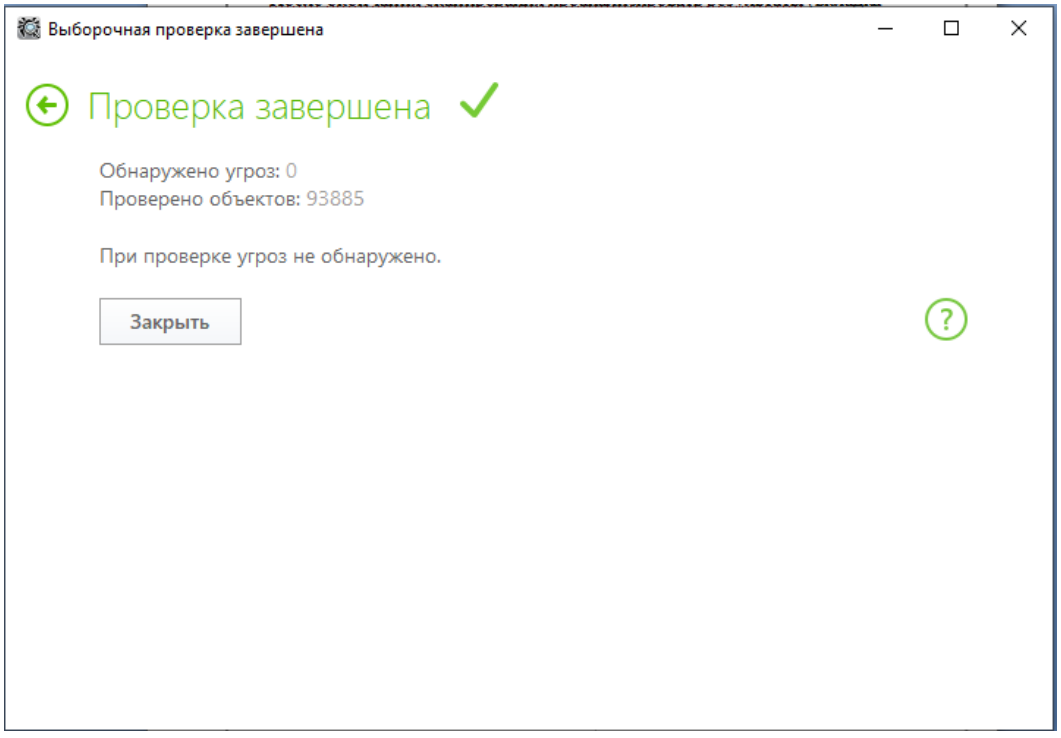


Figure 4

Вирусов на данном ПК не обнаружено.

1. Что такое антивирусная утилита?

Антивирусные утилиты – это программы, которые ищут и удаляют вирусы, и другие вредоносные программы на более глубоком уровне, чем обычные антивирусы.

2. Дайте классификацию вирусов.

По среде обитания:

- Сетевые – распространяются по различным компьютерным сетям
- Файловые – внедряются в исполняемые модули (COM, EXE)
- Загрузочные – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
- Фалово-загрузочные – внедряются и в загрузочные сектора и в исполняемые модули

По способу заражения:

- Резидентные – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
- Нерезидентные – не заражают оперативную память и активны ограниченное время

По воздействию:

- Неопасные – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
- Опасные – приводят к различным нарушениям в работе компьютера
- Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

- Паразиты – изменяют содержимое файлов и секторов, легко обнаруживаются
- Черви – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
- Стелсы – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области

- Мутанты – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую

- Трояны – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

3. Для чего нужны антивирусные программы?

   Антивирус — это программный комплекс, который защищает компьютер или другое устройство от вирусов и внешних воздействий.

4. Как запустить Dr. Web Curelt в безопасном режиме?

Для этого необходимо перезагрузить компьютер и во время звукового сигнала нажать на клавишу F8, пока на экране не появится меню запуска Windows. Если оно не появилось, тогда нажимайте на F8 с периодичностью в 1-2 секунды, пока не появится. После нужно будет выбрать — Безопасный режим (Safe Mode), далее Enter. Теперь можете запускать Dr.Web.

5. Средства антивирусной защиты.

   Если вредоносный код обнаружен, модуль защиты от вирусов и шпионских программ обезвреживает его, сначала блокируя его исполнение, а затем очищает, удаляет или перемещает на карантин

6. Примеры антивирусных программ ПК
   - Dr.Web
   - AVAST
   - ESET NOD32
   - Kaspersky