Практическое задание 15. Обеспечение безопасности в информационно-коммуникационных системах.

План.

15.1 Методы защиты информации
15.2 Работа с антивирусными программами
15.3 Информационная безопасность в компьютерах
15.4 Средства обеспечения информационной безопасности

Цель: В ходе данной практической работы студенты получат практические навыки по компьютерным вирусам, видам компьютерных вирусов и мерам защиты от них.

***Ключевые понятия, связанные с темой*: (https://nrm.uz/)**

компьютерный вирус- программа (набор исполняемых кодов), имеющая деструктивный характер, способная воспроизводить свою копию (которая может быть не полностью идентична оригиналу) и внедрять ее в различные ресурсы компьютерных систем, сетей и т. п. без ведома пользователя;

антивирусное программное обеспечение- антивирусное программное обеспечение для компьютеров, программа, предназначенная для обнаружения вирусов и могущая предлагать удалить или удалить их;

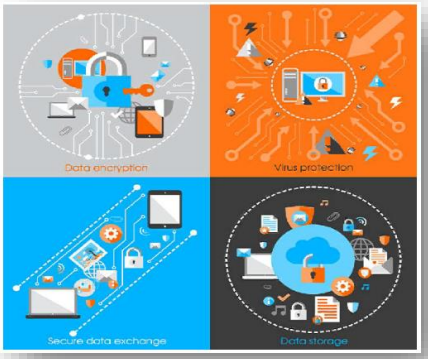
антивирусная защита- комплекс мер, направленных на предотвращение воздействия компьютерных вирусов, обнаружение и нейтрализацию вирусов с помощью антивирусных программ;

аутентификация- процедура проверки подлинности пользователя, приложения, устройства или данных;

информационный ресурс- информация в электронном виде, банк данных, база данных в составе информационной системы;

информационная система- организационно организованная совокупность информационных ресурсов, информационных технологий и средств связи, обеспечивающих сбор, хранение, поиск, обработку и использование информации;

информационная безопасность- защита информации и обеспечивающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут причинить неприемлемый ущерб субъектам информационных отношений;



инцидент информационной безопасности- единичный инцидент информационной безопасности или серия неблагоприятных или непредвиденных событий, которые могут привести к раскрытию информации и возникновению угроз информационной безопасности;

атака- уничтожение, раскрытие, изменение, блокирование, перехват, несанкционированный доступ к информационным активам или попытка несанкционированного использования информационных активов;

мониторинг- мониторинг состояния автоматизированных информационных систем;

серверная комната- помещение, в котором размещаются серверы предприятия, телекоммуникационное оборудование, источники бесперебойного питания и другое вычислительное оборудование;

сетевой экран- программа и (или) программное средство, осуществляющее управление поступлением и (или) выведением информации из автоматизированной системы;

хэш-сумма- контрольная сумма целостности файла, рассчитанная с использованием криптографического алгоритма;

персональная информация- сведения, относящиеся к определенному лицу или позволяющие его идентифицировать, зафиксированные в электронном виде, на бумажном носителе и (или) на ином материальном носителе;

автоматизированная система- информационная система, предназначенная для сбора, хранения, поиска, обработки и использования информации в сфере деятельности;

электронный архив- структурное подразделение банка, имеющее статус архива и осуществляющее сбор, учет, хранение и использование электронных банковских документов.

Источник:https://studfile.net/preview/7882776/

Что такое компьютерный вирус?

Защита от вирусов — одна из главных проблем, с которой сталкивается каждый пользователь компьютера. Ущерб, наносимый компьютерными вирусами, оценивается в миллиарды долларов.

Компьютерный вирус –Специально написанная программа, которая применяется к вычислительным системам, системным областям компьютера и файлам с целью создания всевозможных сбоев в работе компьютера, порчи файлов и каталогов, а также выведения из строя программ, имеет возможность создавать свои копии и присоединяться к другим программам.

Программа с вирусом внутри***поврежден***называется.

Когда такая программа начинает работать, вирус первым берет управление на себя.

Вирус находит и «повреждает» другие программы и выполняет какие-либо вредоносные действия (например, портит файлы или таблицу расположения файлов на диске, замедляет работу оперативной памяти и т. д.).

Скажем, заражение и повреждение других программ с целью маскировки вируса не всегда возможно, если выполняются определенные условия.

После завершения своей задачи вирус передаёт управление программе, в которой он установлен, и эта программа начинает работать нормально. При этом заражённая программа выглядит неповреждённой.

Большинство типов вирусов устроены таким образом, что при запуске зараженной программы вирус навсегда остается в памяти компьютера, периодически заражая программы и выполняя вредоносные действия на компьютере.

Все действия вируса могут выполняться довольно быстро и без каких-либо уведомлений, поэтому пользователю очень сложно заметить, что на компьютере происходит что-то необычное.

Если на вашем компьютере заражено относительно немного программ, присутствие вируса будет практически незаметно. Однако со временем на вашем компьютере начнут происходить странные вещи, например:

- некоторые программы перестают работать или работают некорректно;
- на экране появляются посторонние сообщения или символы;
- производительность компьютера снижается;
- некоторые файлы повреждаются и т.п.

К этому времени, как правило, уже достаточно много (или даже большинство) программ, с которыми работает пользователь, заражены вирусами, а некоторые файлы или диски считаются неисправными.

Кроме того, зараженные программы на компьютере пользователя могли быть переданы на компьютеры его коллег и друзей через дискеты или по локальной сети.

Некоторые типы вирусов более опасны своим подходом. Они изначально без предупреждения заражают большое количество программ или дисков, а затем наносят серьёзный ущерб, например, форматируя весь жёсткий диск компьютера.

Программа – вирус – не должна быть большой, чтобы её невозможно было обнаружить. Поэтому, как правило, вирусы пишутся достаточно квалифицированными программистами.***Ассемблер***написанный на этом языке.

Причины возникновения и распространения компьютерных вирусов, с одной стороны, кроются в психике человеческой личности и ее дурных качествах (страстях, мстительности, карьеризме непризнанных творцов, неумении конструктивно использовать свои способности), а с другой — связаны с отсутствием аппаратной защиты и противодействия со стороны операционной системы персонального компьютера.

Основные пути проникновения вирусов в компьютер — через съёмные диски (дискеты и лазерные) и компьютерные сети. Жёсткий диск может быть заражён вирусами при загрузке компьютера с дискеты, содержащей вирус.

Такое повреждение может быть случайным, например, если дискета не была извлечена из дисковода А и компьютер был перезагружен, в этом случае дискета может оказаться несовместимой с системой. Повредить дискету гораздо проще. Вирус может попасть на неё даже при вставке дискеты в дисковод заражённого компьютера и чтении её содержимого.

Поврежденный дискЭто программа в загрузочном секторе –***Диск, на котором находится вирус.***

После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Загрузочный сектор диска с наибольшим количеством вирусов и ***.EXE, *.COM, *.SYS** или***летучая мышь***Файлы с расширением . повреждены.

Файлы с небольшим количеством текста и графики менее подвержены повреждению.

Вредоносное ПО — это программа, содержащая внедренный в нее вирус. Очень важно вовремя обнаружить заражение компьютера вирусом. Для этого необходимо знать основные признаки появления вирусов.

К ним могут относиться:

- ***программы, которые ранее успешно работали, перестают работать или работают со сбоями;***
- ***низкая производительность компьютера;***
- ***невозможность загрузки операционной системы;***
- ***потеря файлов и каталогов или повреждение их содержимого;***
- ***изменение даты и времени изменения файла;***
- ***количество файлов на диске неожиданно значительно увеличивается;***
- ***серьезное сокращение размера свободной оперативной памяти;***
- ***отображение на экране нежелательных сообщений или изображений;***
- ***передача непреднамеренных звуковых сообщений;***
- ***Частые зависания и сбои при работе на компьютере.***

Следует отметить, что вышеперечисленные явления не обязательно вызваны вирусами, но могут быть следствием и других причин. Поэтому всегда сложно правильно диагностировать состояние компьютера.

Компьютерный вирус может существенно изменить и повредить любой файл на дисках компьютера.

Однако некоторые типы файлов могут быть «заражёны» вирусом. Это означает, что вирус может быть «внедрён» в эти файлы, то есть он может изменить их таким образом, что они будут содержать вирус, и в некоторых случаях вирус может начать свою работу.

Следует отметить, что тексты программ и документов, файлы с информацией о базах данных, таблицы электронных таблиц и другие подобные файлы не могут быть заражены вирусом, однако вирусы могут повредить эти файлы.

Типы файлов, которые могут быть «заражены» вирусом:

1.***Исполняемые файлы***, то есть**.COM** и**.YeXE** Файлы с расширением .exe представляют собой дублирующие (повторяющиеся) файлы, загружаемые при запуске других программ. Вирус в заражённых исполняемых файлах начинает свою работу при запуске программы, содержащей вирус. Самый опасный способ заражения вирусом**ДОС**командный процессор**COMMAND.COM** программа повреждена, потому что этот вирус**ДОС**Он запускается при выполнении любой команды и заражении любой исполняемой программы (если вирус может ее заразить).

Антивирусные программы

В настоящее время разработано множество методов борьбы с вирусами, и программы, использующие эти методы, называются антивирусами. По способу использования антивирусы можно разделить на следующие группы:***детекторы, фаги, вакцины, прививки, аудиторы, мониторы***.

Детекторы–Обнаруживает известные вирусы и сообщает об их наличии, сканируя оперативную память и файлы на основе вирусной сигнатуры (последовательности байтов, связанных с вирусом). Недостаток детекторов заключается в том, что они не способны обнаруживать новые вирусы.

Фаг – или врачи, выполняя работу, типичную для детекторов, удаляет вирусы из зараженного файла и восстанавливает файл в предыдущее состояние.

Вакцина-В отличие от предыдущих, он устанавливается на защищаемую программу. В результате программа считается заражённой и не модифицирована вирусом. Его недостатком является то, что он защищён только от определённых вирусов. Поэтому такие антивирусы не получили широкого распространения.

Привиговка- оставляет на файлах след, как будто они заражены вирусом. В результате вирусы не приживаются в зараженном файле.

Фильтры– в виде программ безопасности они работают в резидентном состоянии и уведомляют пользователя о выполнении специфических для вирусов процессов.

Аудиторы– это самое надежное средство защиты, сохраняющее в памяти начальное состояние диска и постоянно отслеживающее последующие его изменения.

Программы детектора Он сканирует память компьютера и файлы на наличие вирусов и выдает отчеты об обнаруженных вирусах.

Докторские программы не только находит зараженные вирусами файлы, но и лечит их, возвращая в исходное состояние.

Примерами таких программ являются Aidstest и Doctor Web. Учитывая постоянное появление новых вирусов, необходимо регулярно обновлять программы Doctor Web.

https://www.softmagazin.ru/blog/dr_web/- Dr.Web - функции, возможности и преимущества

Программы-фильтры используются для обнаружения подозрительного поведения, характерного для вирусов, во время работы компьютера.

Такими действиями могут быть:

- изменение атрибутов файла;
- запись данных на диски по постоянным адресам;
- запись данных в загрузочные сектора диска.

Программы аудита являются самым надёжным средством защиты от вирусов. Они сохраняют в памяти состояние программ, каталогов и системной области диска, когда компьютер не был заражён, и постоянно или по усмотрению пользователя сравнивают текущее и исходное состояния компьютера. Примером такой программы является программа ADINF.

Антивирусные меры

Чтобы защитить свой компьютер от вирусов и обеспечить безопасное хранение информации, необходимо соблюдать следующие правила:

- оснащение компьютера современными антивирусными программами;
- всегда проверяйте дискеты перед их использованием;
- Всегда сохраняйте копию ценной информации в сети в виде архивных файлов.

Существуют следующие виды защиты от компьютерных вирусов:

- наличие программ, восстанавливающих файлы при попадании на компьютер компьютерных вирусов;
- доступ к компьютеру по паролю, дисководы заблокированы;
- защита дисков от записи;
- использовать лицензионное программное обеспечение и не использовать пиратские программы;
- проверка загруженных программ на наличие вирусов;
- широкое использование антивирусных программ;
- периодическая проверка компьютеров на вирусы с помощью антивирусных программ.

Методы обнаружения и лечения вирусов

В настоящее время появились компании, специализирующиеся на борьбе с компьютерными вирусами. Они создают антивирусные программы, которые ежедневно и ежечасно обнаруживают и уничтожают вирусы на компьютерах клиентов.

В настоящее время наиболее популярными антивирусными программами, борющимися с компьютерными вирусами, являются:Основные из них:

KasperskyAnti-Virus (AVP) ScriptChecker, NortonAntivirus, DrWeb, Adinf, AVPрассматриваются.

Антивирус КасперскогоВ настоящее время программа обнаруживает и лечит более 100 000 видов компьютерных вирусов.

Способы защиты от компьютерных вирусов

Существует три уровня защиты от компьютерных вирусов:

- предотвращение проникновения вирусов;
- устранить вирусную атаку, если вирус все же проник в компьютер;
- для устранения разрушительных последствий, если бы нападение все же произошло.

Существует три способа реализации защиты:

- методы защиты программного обеспечения;
- аппаратные методы защиты;
- организационные методы защиты.

Когда речь идет о защите конфиденциальной информации, часто применяется здравый подход: «Профилактика лучше лечения».

К сожалению, именно он вызывает наиболее разрушительные последствия. Воздвигнув баррикады на пути проникновения вирусов в компьютер, не стоит бояться их силы и быть готовым к последующим действиям в случае разрушительной атаки. Вместе с тем, вирусная атака — не единственная и даже не самая распространённая причина потери важных данных. Существуют программные сбои, способные вывести операционную систему из строя, и аппаратные, способные вывести жёсткий диск из строя. Всегда существует вероятность потери компьютера вместе с важными данными в результате кражи, пожара или других чрезвычайных ситуаций.

Поэтому создание системы безопасности следует в первую очередь начинать «с конца» — с устранения разрушительных последствий любого воздействия, будь то вирусная атака, взлом помещения или физический выход из строя жесткого диска.

Надежная и безопасная работа с данными достигается только в том случае, если любое непредвиденное событие, включая полное физическое выключение компьютера, не приведет к негативным последствиям.

Задачи для завершения работы

1. Предоставьте информацию о типах вирусов, заражающих компьютеры.
2. Предоставьте информацию об используемых в настоящее время антивирусах.
3. Объясните пути проникновения вирусов в компьютер.
4. Объясните различия между типами антивирусных программ.

Контрольные вопросы

1. Что такое компьютерный вирус?
2. Проверка файлов и дисков на наличие компьютерных вирусов.
3. Проверка элементов, узлов и устройств на наличие компьютерных вирусов.
4. Что такое вирус и каковы его действия?
5. Как вирусы появляются на компьютере?
6. Какие типы вирусов вы знаете?
7. Как определить наличие вирусов на компьютере?
8. Какие типы антивирусных программ вы знаете?
9. Какие меры предосторожности необходимы для защиты от компьютерных вирусов?

Дополнительные (интернет) материалы:

Носители информации:флешка,компакт-дискиDVDдиски:

- Флеш-накопители — это устройства памяти, изготовленные из полупроводниковых элементов, которые могут хранить очень большие объемы информации.
- Размер флэш-памяти сегодня**64 ГБ** Он может хранить до 100 000 единиц информации.
- Флэш-память очень компактна и удобна в использовании. Скорость записи данных**6700**достигает до килобайт/сек.
- Скорость чтения данных достигает 18 000 кбайт/сек.
- Флэш-память является одним из важнейших носителей данных сегодня.
- **компакт-диск**Компакт-диски — это диски, получившие свое название по первым буквам слова «компактный диск», и используемые для хранения информации.состоит из оптической поверхности дляКомпакт-диск — это круглый носитель информации в форме диска. Ёмкость компакт-дисков составляет 700 МБ. Информация на них записывается и считывается с помощью лазерного луча, подаваемого устройством для чтения дисков.
- **DVD**DVD — это диски, название которых расшифровывается как Digital Video Disc (цифровой видеодиск). Ёмкость этих дисков составляет 4,5 ГБ, что в 7 раз больше, чем у CD.

О компьютерных вирусах и их типах

- Сегодня все пользователи компьютеров знакомы с понятием вируса. Они не раз сталкивались с этой небольшой программой. Во многих случаях они даже терпели поражение. Если вы знаете, то эта статья будет посвящена вирусам.
- ***Вирус***– это программа, созданная программистом, которая нарушает бесперебойную работу компьютера и в конечном итоге делает его невозможным включение. Такие программы в основном загружаются на компьютер пользователя через Интернет.
- Конечно, эти программы появляются на компьютере без ведома пользователя интернета. Программа, которая с ними борется, называется антивирусом (подробнее об этом в следующих статьях).
- ***Вирусы ведут себя на компьютерах по-разному.***Некоторые из них засоряют ваш компьютер ненужными файлами, другие занимают много оперативной памяти и замедляют работу компьютера, а некоторые вирусы удаляют необходимые файлы или системные файлы, причиняя вред. Чтобы избежать их, необходимо знать типы вирусов, то есть, что делает каждый вирус и как с ним бороться. Ниже приведены их типы (типы взяты с сайта ref.uz):
- ***Троянские кони***– Название происходит от трюка, использованного древними греками во время похода на Трою, когда они воспользовались любовью троянцев к лошадям и подарили им большого деревянного коня, что привело к поражению троянцев. Сегодня термин «троянский конь» означает «дар без цели». В компьютерном и интернет-мире троянов правильнее называть «программой без цели». Трояны обычно распространяются через интернет. Трояны устанавливаются на ваш компьютер и изначально представляются полезной программой, но их истинное предназначение остаётся неизвестным пользователю. Они скрытно выполняют действия, заданные их создателем (взломщиком – злобным хакером). Трояны не размножаются, но ставят под угрозу безопасность вашего компьютера:

трояны могут удалять ваши важные данные, отправлять данные с вашего компьютера по назначению и устанавливать несанкционированные соединения с вашим компьютером из интернета.

- ***Черви***– Черви, как следует из их названия, – это вирусы, которые очень быстро размножаются. Эти вирусы обычно распространяются через интрасети в Интернете. Для этого они используют электронную почту или другие быстродействующие механизмы. Они наносят серьёзный ущерб данным и безопасности вашего компьютера. Черви могут проникнуть на ваш компьютер, используя уязвимости операционной системы или открывая заражённые электронные письма.
- ***БотинокВирусы загрузочного сектора***– Эти вирусы отключают специальную часть жёсткого диска, используемую для запуска компьютера (загрузки). После заражения компьютер может стать неработоспособным. Обычно вирус распространяется через дискеты.
- ***Макровирусы***– Макровирусы – это вирусы, использующие для своего распространения язык макропрограммирования других программ. Обычно они заражают документы Microsoft Word или Excel.
- ***Резидентные вирусы памяти —*** Эти вирусы находятся в оперативной памяти (ОЗУ) компьютера и выполняют свои вредоносные действия. Обычно их запускает другой вирус. Они остаются в памяти компьютера даже после того, как вирус, их запустивший, завершает работу, отсюда и название.
- ***РуткитРуткит-вирусы – Руткит-вирусы*** Среди них они отличаются чрезвычайной опасностью и способностью скрываться. Руткиты используются злоумышленниками для захвата вашего компьютера. Некоторые руткиты не обнаруживаются даже антивирусами, поскольку они выдают себя за файлы операционной системы. Руткиты обычно устанавливаются на ваш компьютер троянами.
- Полиморфные вирусы – эти вирусы не только копируют себя, но и изменяют свой код в процессе репликации. Полиморфные вирусы также могут быть труднообнаружимы некоторыми антивирусами.
- ***Бомбы замедленного действия или логические бомбы***– Это вирусы, активирующиеся в определённую дату или время, или при определённом действии пользователя. Например, в День смеха (1 апреля) или в Новый год они могут сделать вам «подарок», удалив данные с вашего компьютера.

https://www.texnoman.uz/post/kompyuter-viruslari-haqida-va-ularing-turlari.html-О компьютерных вирусах и их типах

Программы детектора

Средства защиты информации операционной системы

- позволяет обнаружить файлы, зараженные несколькими известными вирусами.
- проверяет указанный пользователем диск на наличие определенной комбинации байтов, связанных с вирусом.
- Если в конкретном файле будут обнаружены подобные случаи, пользователь будет уведомлен об этом..
- Например:**Norton AntiVirus или AVSP**

- **Полифаг, сканер – антивирусная программа.**Принцип работы основан на сканировании файлов, загрузочных секторов дисков и оперативной памяти и обнаружении в них известных и новых вирусов.
- **Антивирусный блокировщик– сторожевые (мониторные) программы**Они находятся в оперативной памяти компьютера, перехватывают репликацию и вредоносные вызовы вирусов и оповещают о них пользователя. К «вирусоопасным» относятся следующие случаи, характерные для момента спонтанного размножения вирусов: вызовы открытия исполняемых файлов на запись, Записывает данные в загрузочный сектор дисков или жёстких дисков. Пользователь может разрешить или запретить выполнение текущей операции.
- **Врачи — «терапевтические антивирусы».**
- **Вакцина-** Он создаёт видимость того, что файлы, не заражённые вирусом, заражены. Вирусные программы воспринимают такие файлы как «заражённые» при заражении.

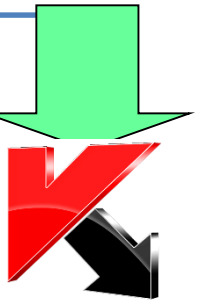
Программы

- Работа программы состоит из двух этапов. На первом этапе программа запоминает начальное состояние программ и системного сектора диска (загрузочных секторов и секторов таблицы разделов жёсткого диска). На этом этапе программы и сектора диска считаются незаражёнными вирусами.
- В таких случаях в любой момент можно сравнить начальное и текущее состояние программ и системных секторов диска с помощью программы-аудитора, после чего пользователь получает уведомление об обнаруженных несоответствиях.
- Например, AdInf (Advanced Diskinfoscope), который встроен в Касперский, IDSMonitor

Врач-аудитор

- Эти программы не только обнаруживают изменения в файлах и секторах диска операционной системы, но и автоматически восстанавливают их в исходное состояние при возникновении изменений. Такие программы являются в некоторой степени универсальными, выполняя операции восстановления на основе ранее сохранённой информации о состоянии файлов и секторов диска.
- Однако эти программы лечат компьютерные вирусы, механизм заражения файлов которых известен на момент лечения.
- **Например: AVP, Aidstest, Scan, Norton AntiVirus, Doctor Web.**

Возможности антивирусного программного обеспечения



- Защита от вирусов, троянов и червей;
- защита от спама, рекламного ПО и потенциально опасных вирусов;
- Сканирование файлов, электронной почты и интернет-трафика в режиме реального времени;
- проактивная защита от новых и неизвестных атак;
- антивирусная проверка внешних носителей любого типа;
- проверка и обработка архивных файлов;

•Контролировать выполнение опасных макросов в документах Microsoft Office;

•система восстановления поврежденных секторов диска.

Антивирус,DrWeb, Nod 32, Антивирус Касперского, Avast, Антивирус Панда

ДОКТОР ВЕБ

После запуска «Доктор Веб» антивирусная программа автоматически сканирует файлы системы. Окно «Доктор Веб» состоит из заголовка, строки меню, области сканирования, статистики и рабочих областей (рисунок 9).

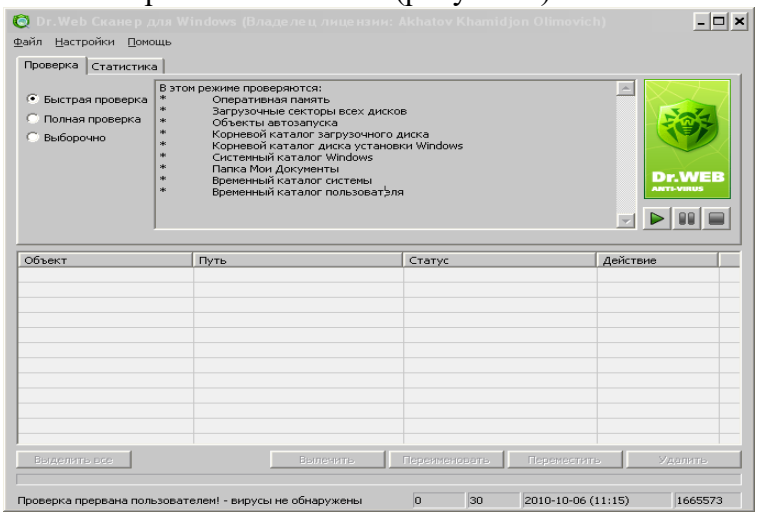


Рисунок 9

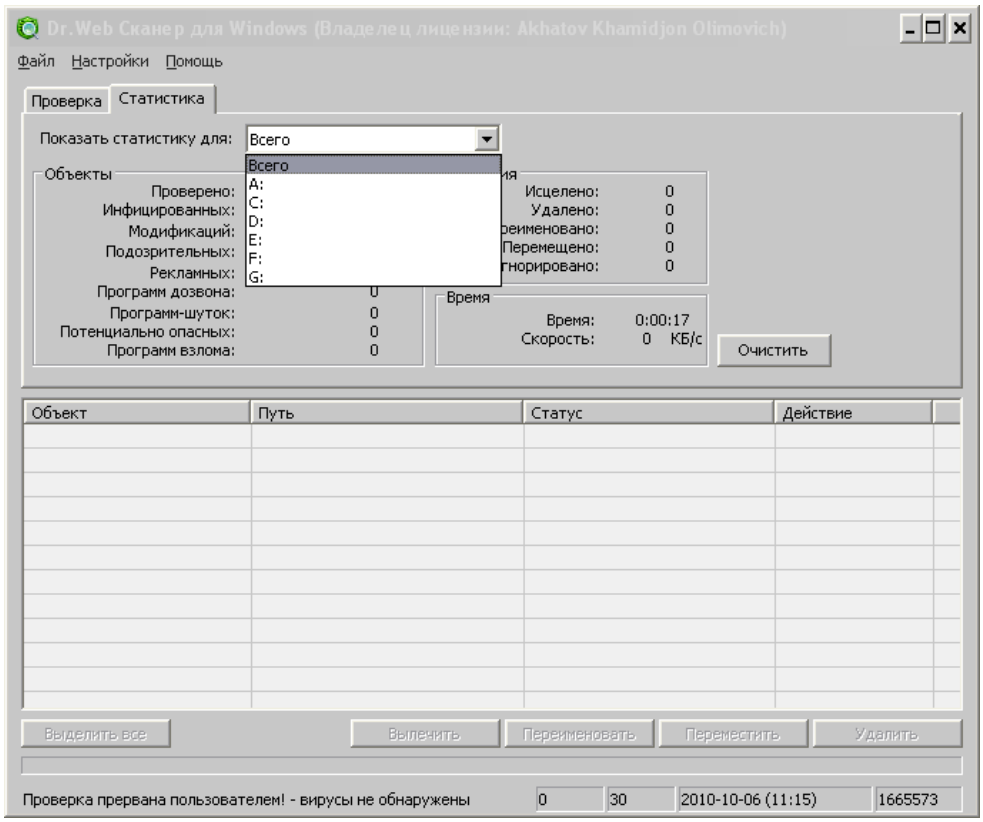
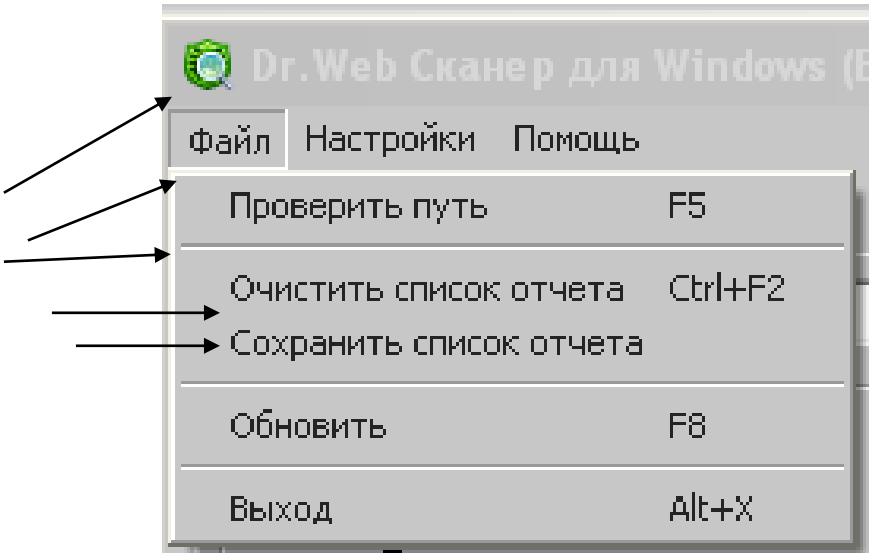


Рисунок 10

Панель меню

Меню Файл состоит из следующих разделов:



Проверьте путь

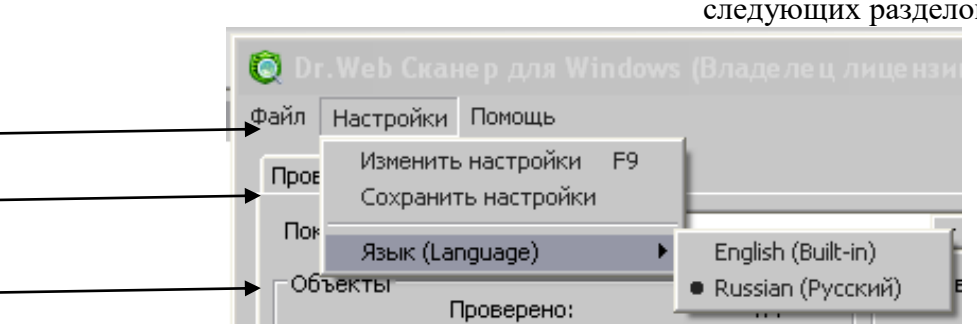
Очистить список в отчете

Сохранить список в отчете

Обновить

Выйти из программы

Меню «Настройки» состоит из следующих разделов:

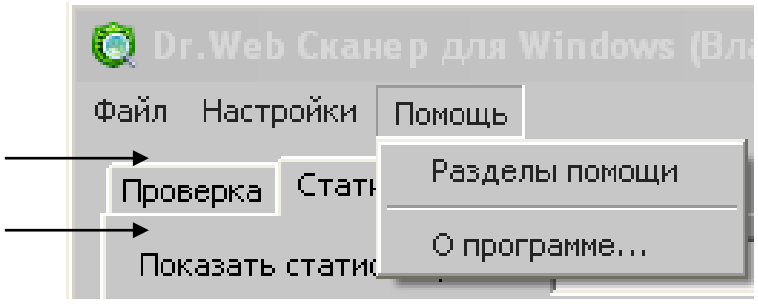


Настройка параметров программы

Сохраните измененный параметр

Выбор языка (русский и Английский язык)

Меню «Справка» состоит из следующих разделов:



Полезная информация

О программе

В меню «Настройки» нажмите «Готово» (Раздел «Действия» позволяет автоматически очищать заражённые файлы и документы, удалять файлы, которые невозможно вылечить, и вирусы, изменять архивные и почтовые файлы, а также удалять другие файлы, которые считаются вредоносными и опасными (рис. 11). После изменения раздела «Действия» необходимо выбрать раздел «Сохранить настройки» в меню настроек и сохранить их.

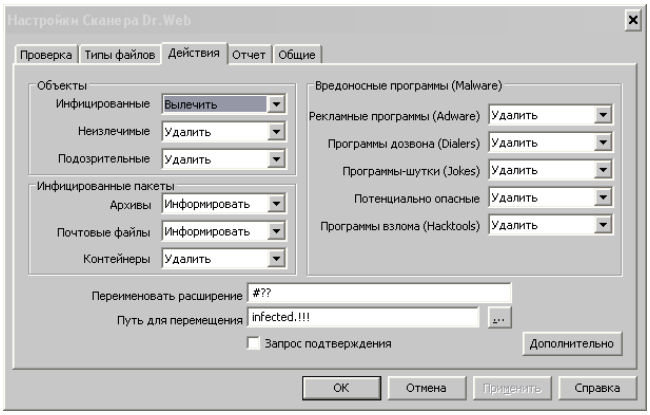


Рисунок 11

Сканирование на вирусы состоит из 3 частей:

- Быстрая проверка (Быстрый поиск) (9-картина)

- Полная проверка (Full check) (12-картина)
- Выборочно (проверка выборочно) (Рисунок 13)

Быстрый поиск позволяет быстро искать файлы в оперативной памяти и во всех секторах диска, элементы автозапуска, системные файлы, запускающие операционную систему Windows, файлы в папке «Мои документы», а также временные каталоги и файлы.

Полное сканирование позволяет полностью проверить файлы на всех секторах диска, на всех основных и дополнительных смонтированных дисках.

Выборочное сканирование (сканирование по выбору) позволяет сканировать один или несколько дисков по вашему усмотрению.

После того, как пользователь выберет одну из дополнительных проверок,  Нажата кнопка «Начать проверку». Чтобы временно приостановить проверку,  Нажата кнопка «Пауза сканирования». Чтобы приостановить сканирование,  Нажата кнопка «Остановить проверку».

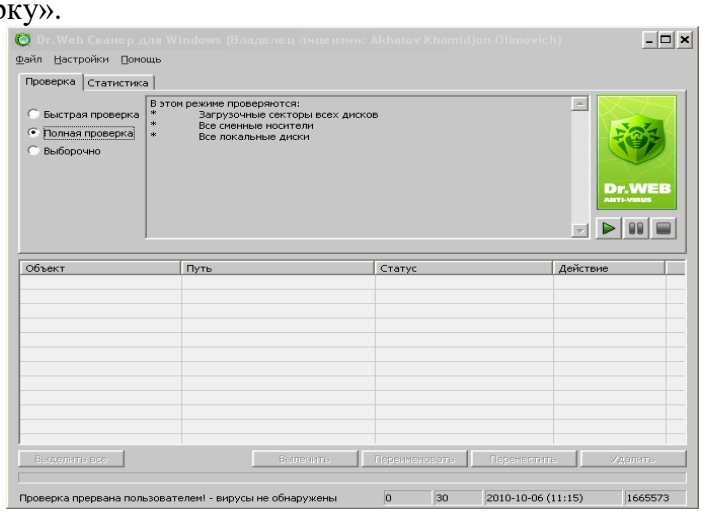


Рисунок 12

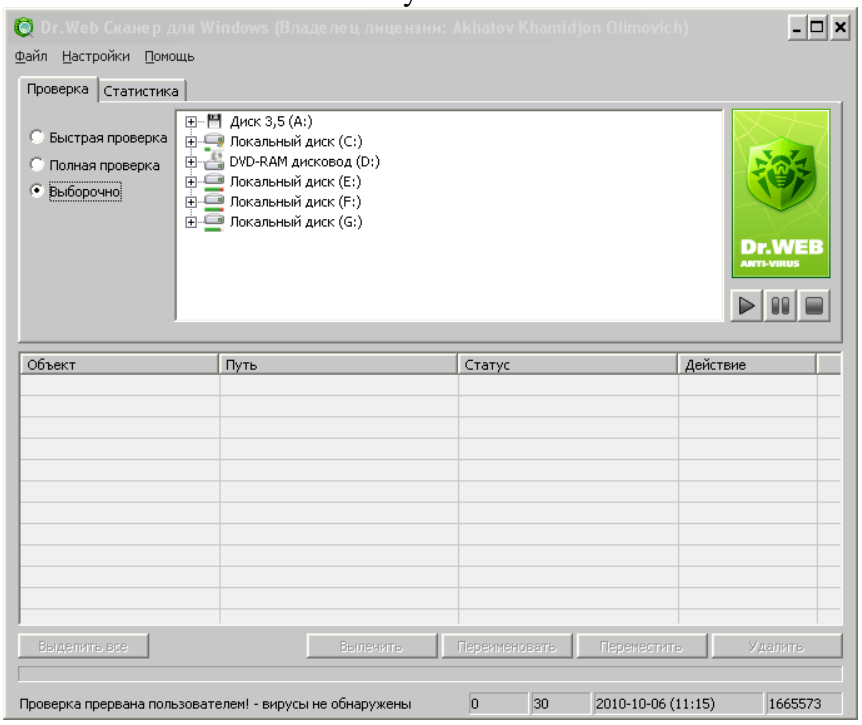


Рисунок 13

После сканирования на вирусы программа автоматически очищает зараженные файлы и удаляет файлы, которые не удалось очистить. Количество проверенных,

зараженных, вылеченных, удаленных, заархивированных и измененных файлов отображается в окне «Статистика» (Отчет) (рисунок 14).

Если в меню настроек не предусмотрены команды автоматической очистки и удаления, то можно выделить найденные вирусные программы с помощью мыши или кнопки «Выделить все», вылечить зараженные файлы с помощью кнопки «Лечить», переименовать их с помощью кнопки «Переименовать», переместить в безопасное место с помощью кнопки «Переместить» и удалить файлы, которые не удалось вылечить, с помощью кнопки «Удалить».

В нижней части окна отображается количество найденных вирусов, количество проверенных документов, время и дата сканирования.

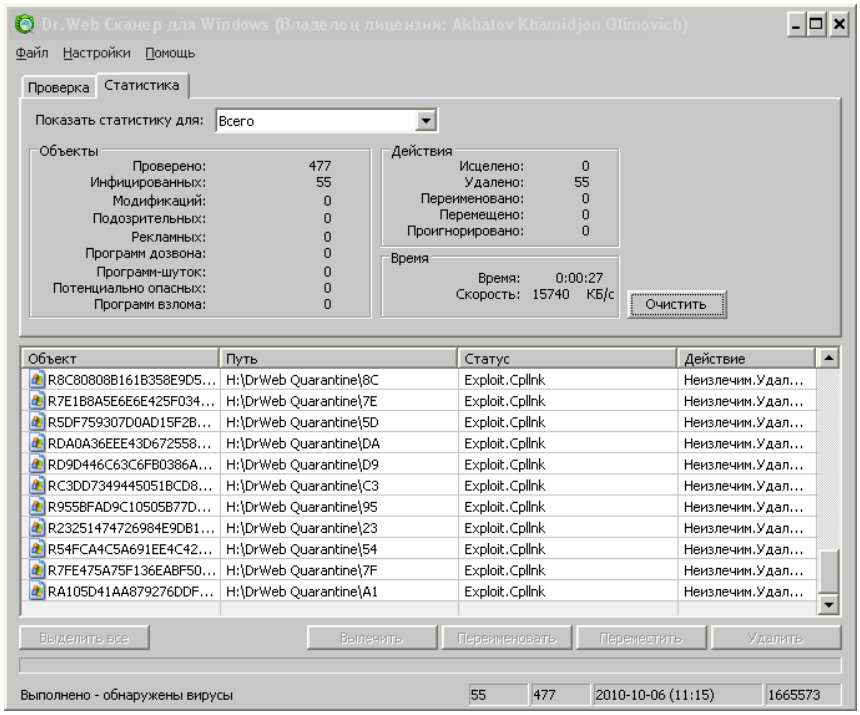


Рисунок 14

АНТИВИРУС КАСПЕРСКОГО

После запуска антивирусной программы «Лаборатория Касперского» перейдите в раздел «Настройки» и установите автоматический режим обнаружения и лечения вирусов, а также удаления файлов, лечение которых невозможно (рисунки 16, 17).

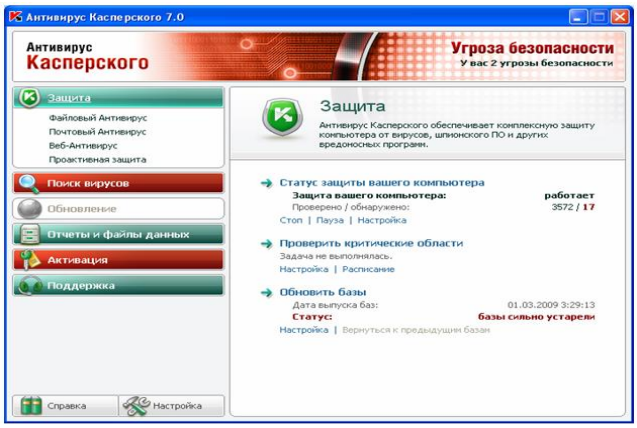


Рисунок 15

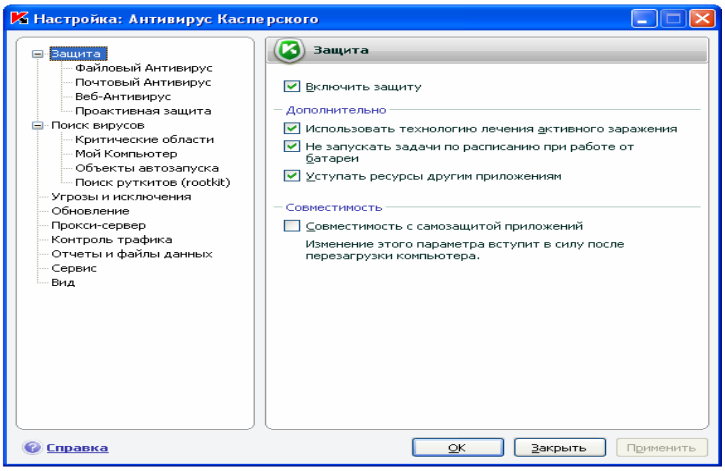


Рисунок 16

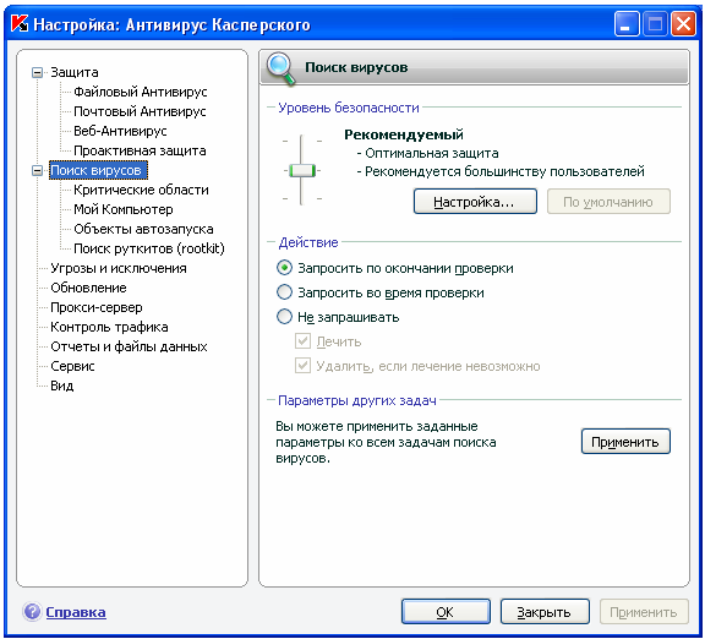


Рисунок 17

Для обновления базы данных программного обеспечения перейдите в раздел «Настройки» и выберите необходимые команды в разделе «Обновление». Раздел «Обновление» содержит следующие команды:

- Автоматически
- Каждый день
- Вручную

Команда «Автоматически» обновляет базу данных автоматически при каждом запуске программы. Команда «Каждый 1 день» обновляет базу данных ежедневно. Команда «Вручную» позволяет пользователю обновлять базу данных в любое время (рисунок 18).

После выбора одной из команд нажмите кнопку «Настроить…», и будет отображен путь к базе данных. Если компьютер подключен к Интернету, база данных обновится автоматически. Если база данных находится на самом компьютере, нажмите кнопку «Добавить…», чтобы указать местоположение базы данных, и нажмите кнопку «ОК» (рисунок 19). После отображения базы данных нажмите кнопку «Обновить» в окне программы, и база данных будет обновлена.

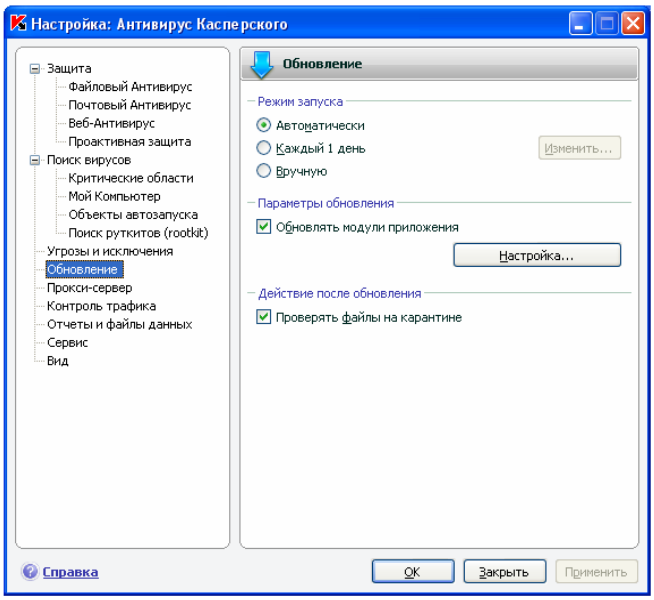


Рисунок 18

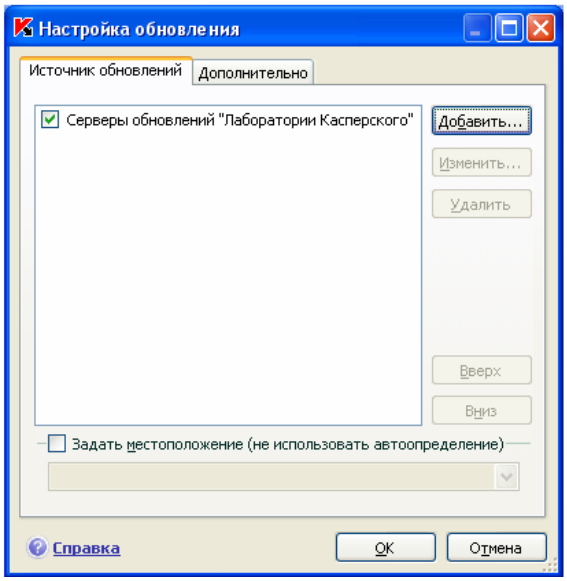


Рисунок 19

Для поиска программ, зараженных вирусами, перейдите в раздел «Поиск вирусов», выберите нужную команду и нажмите кнопку «Начать сканирование» (рисунки 20, 21, 22, 23).

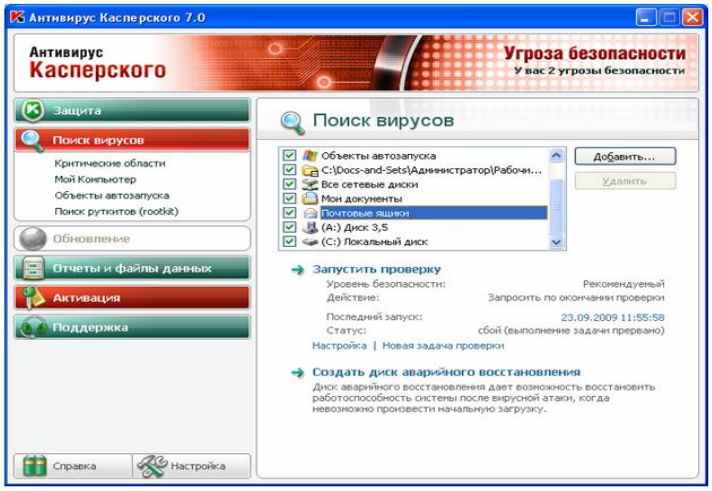


Фото 20

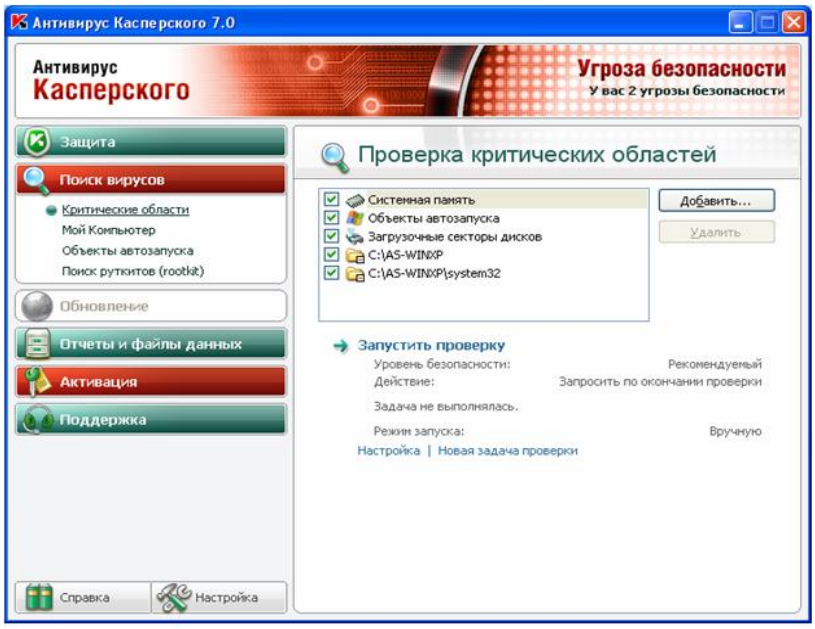


Фото 21

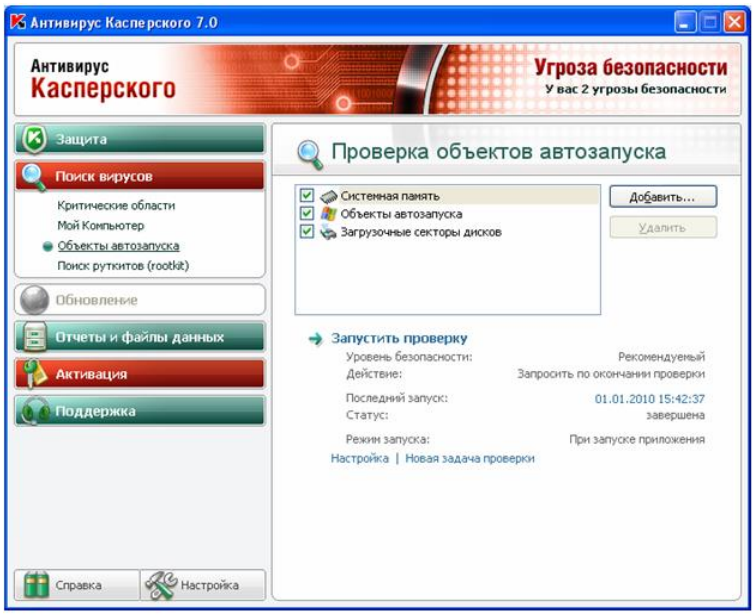


Фото 22

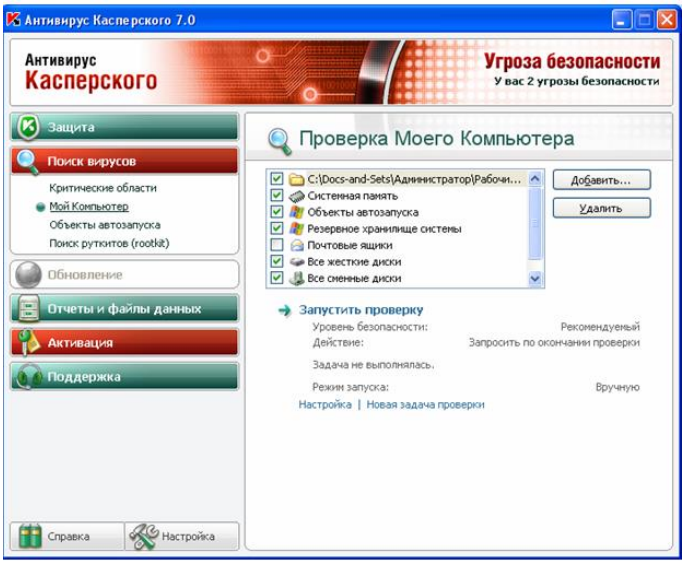


Фото 23

РАБОТА С АНТИВИРУСОМ ESET NOD32

Рабочее окно антивирусной программы ESET NOD32 содержит следующие разделы.

- Защитный статус (Состояние защиты)
- PC scan (Сканирование ПК)
- Обновление базы данных (Обновление)
- Настройка (Настройка)
- Вспомогательная информация (Spravka i podderjka) (рис. 24)

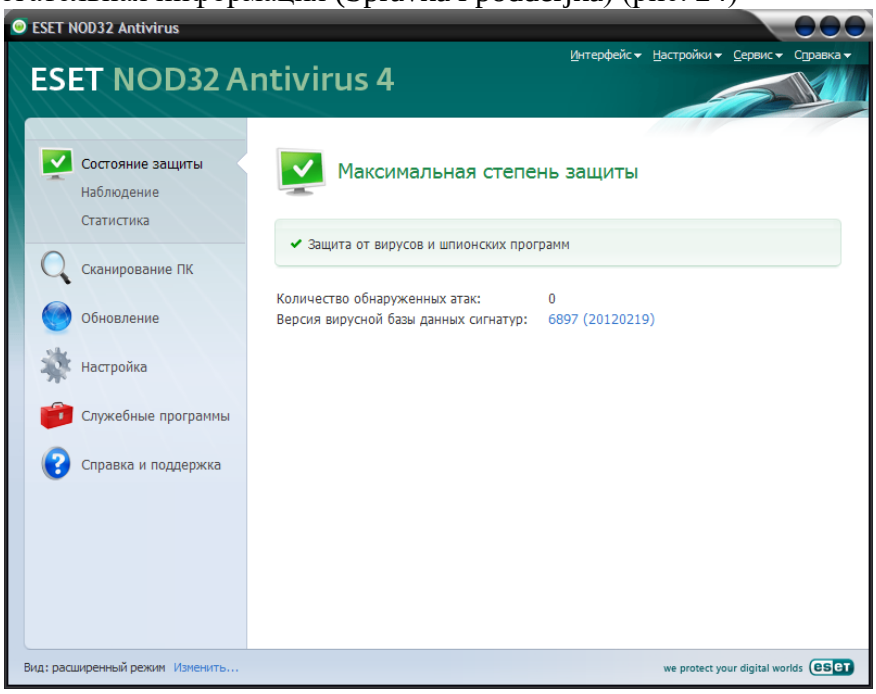


Фото 24

СТАТУС ЗАЩИТЫ(Состояние защиты) – в этом разделе представлена полная информация о состоянии, типах и количестве вирусных программ, обнаруженных на компьютере. (Рисунки 25, 26)

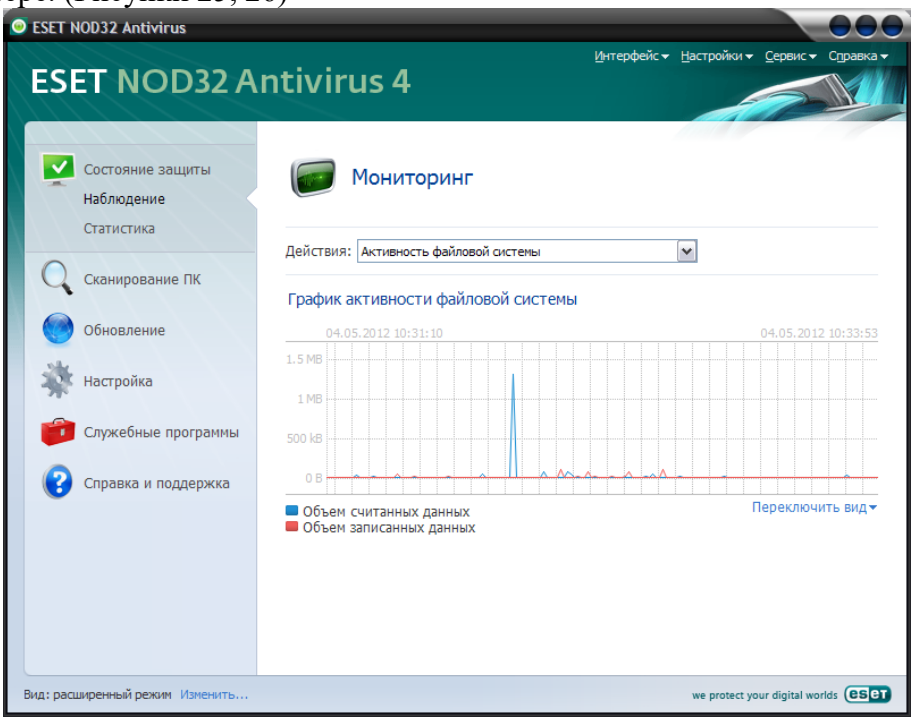


Фото 25

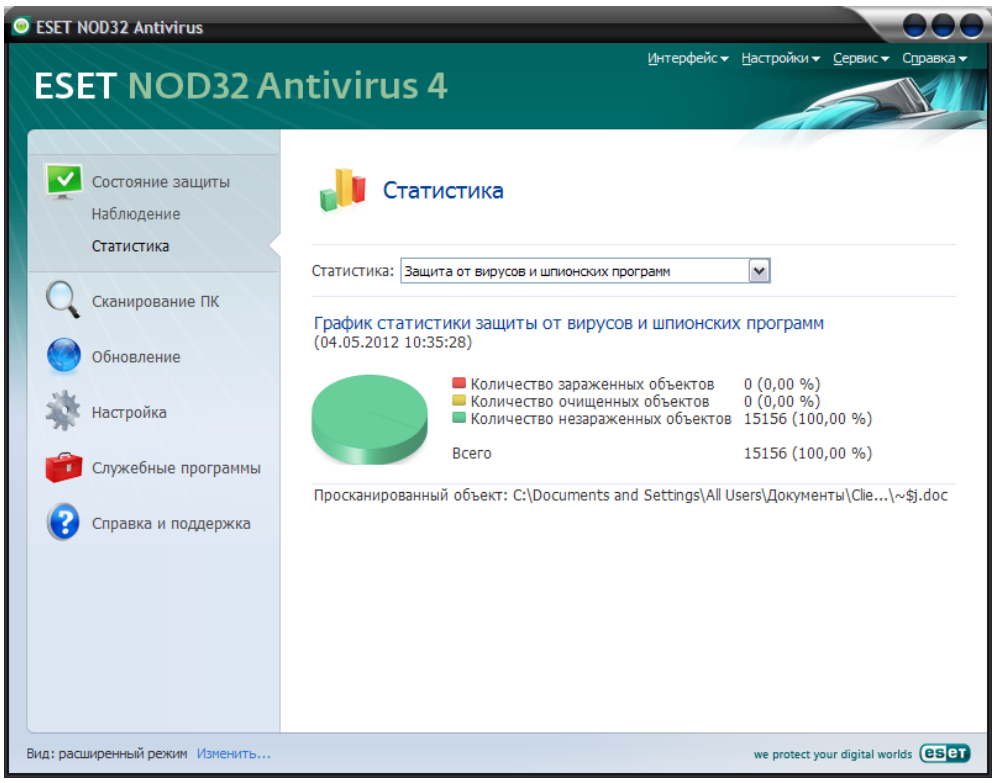


Фото 26

КОМПЬЮТЕРНАЯ ПРОВЕРКА (Сканирование ПК) –Этот раздел позволяет заражать диски компьютера вирусами. (Рисунок 27)

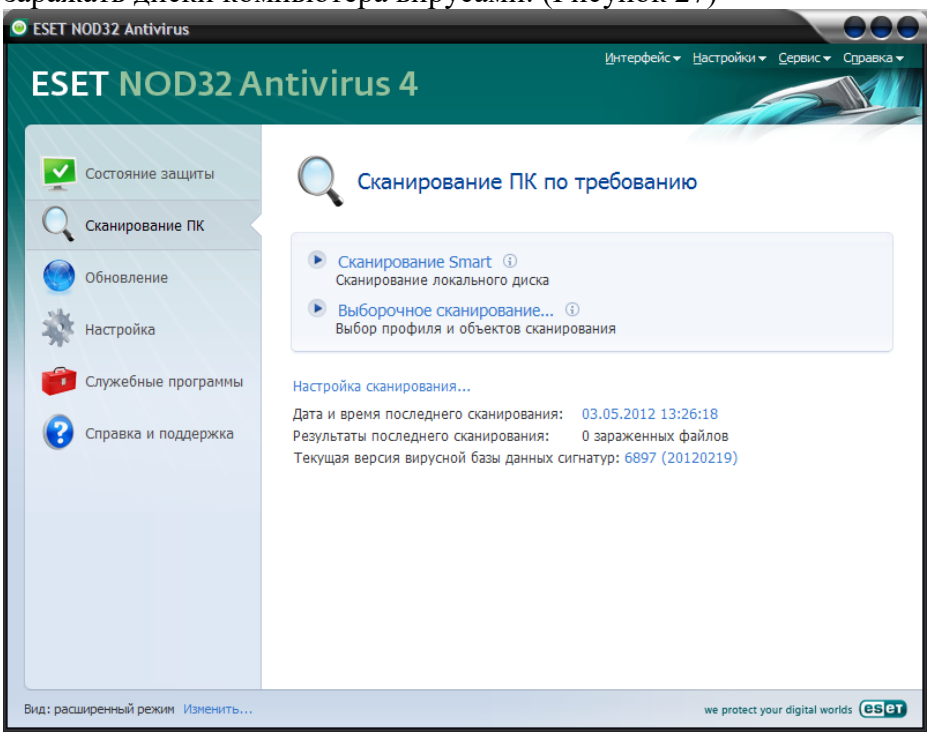


Фото 27

ОБНОВИТЬ БАЗУ ДАННЫХ (Обновление) –Раздел позволяет обновить базу данных антивирусной программы. (Рисунок 28)

НАСТРОЙКИ (Настройки)– раздел позволяет настраивать и изменять параметры программы, а также настраивать режим работы защиты. (Рисунок 29)

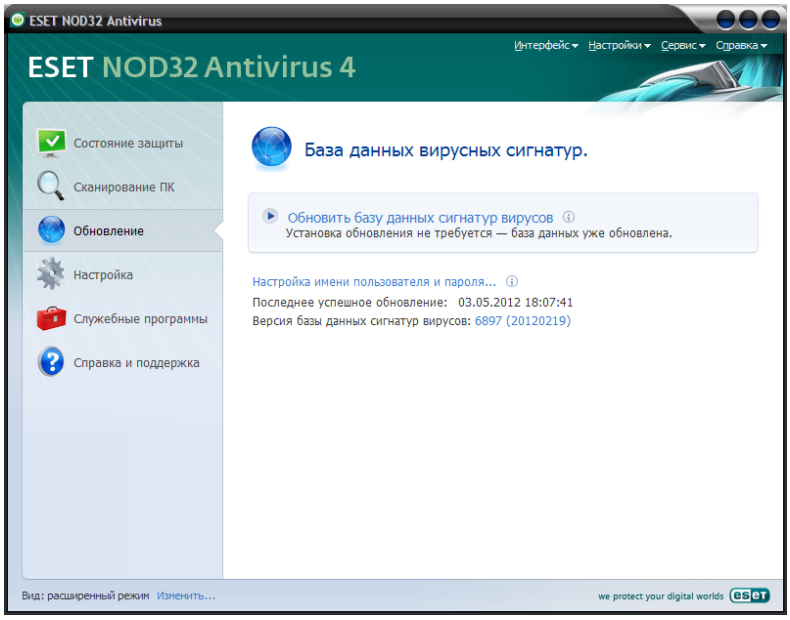


Фото 28

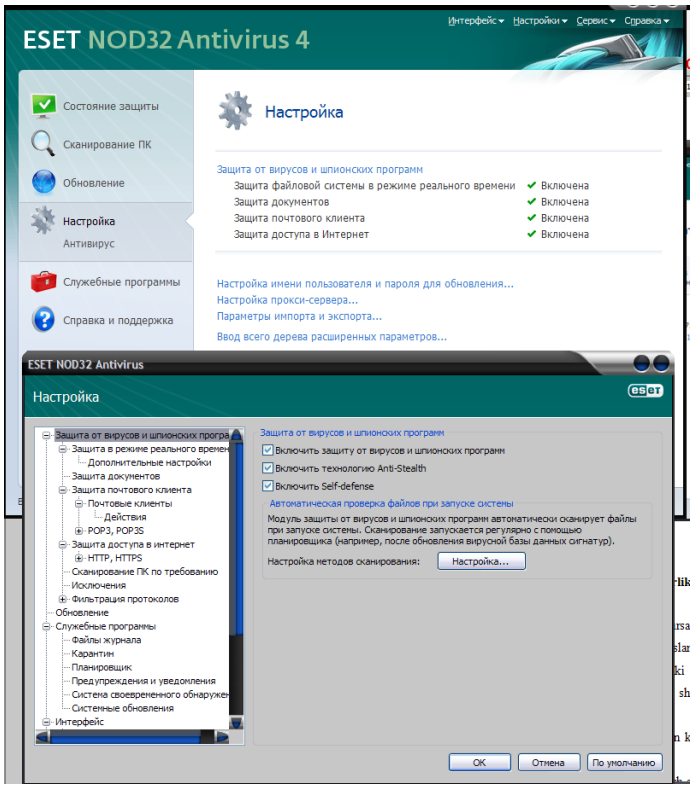


Фото 29

КАК ПРЕДОТВРАТИТЬ КОМПЬЮТЕРНЫЕ ВИРУСЫМЕРЫ ПРЕДОСТОРОЖНОСТИ

Примеры ущерба, причиненного вирусом:

•заражение жёсткого диска или оперативной памяти компьютера — в процессе своего размножения вирусная программа может заполнить весь жёсткий диск своими точками или другими символами. Она также может записывать их в оперативную память, тем самым уменьшая её объём;

•Повреждение таблицы размещения файлов. Если она повреждена, невозможно будет прочитать нужный файл и каталог с диска;

•Повреждение данных в загрузочном секторе. Загрузочный сектор — это специальная программа на диске, повреждение которой приводит к сгоранию диска и его выходу из строя.

•переформатирование диска — вся информация на диске будет полностью стерта;

•Он может вывести сообщение на диск или воспроизвести мелодию. В большинстве случаев это сообщение непонятно;

•автоматическая загрузка карт компьютера;

•комплект кнопок перестает работать и перегорает;

•Изменение содержимого программ и файлов данных. Вирус случайным образом перемешивает и сжигает данные и т.д.

Простую вирусную инфекцию можно легко обнаружить с помощью антивирусного программного обеспечения. Полиморфные вирусы (со сложной структурой) обнаружить этим методом сложнее, поскольку они меняют свой внешний вид в процессе размножения.

Приложения, использующие макросы, могут быть заражены макровирусами. Макровирусы — это инструкции, вставляемые в файлы вместе с данными. Примерами таких приложений являются интерпретаторы Word, Excel и PostScript. Они заражаются макровирусами при открытии файла данных.

Раньше вирусами заражались только диски. Поскольку вирусы передавались с компьютера на компьютер через диски, новые вирусы BBS распространялись через модемы. Появление Интернета привело к появлению ещё одного канала, где традиционные методы борьбы с вирусами оказались неэффективны.

Вероятность заражения вирусами возрастает пропорционально частоте появления новых файлов и приложений на компьютере. Чем важнее данные на компьютере, тем выше должны быть меры защиты от вирусов. Равнодушие к этим факторам может не только привести к значительному материальному ущербу, но и поставить под угрозу дальнейшую деятельность организации или компании.

Не стоит забывать, что вирусы обычно появляются в результате каких-либо действий пользователя (например, установка приложений, чтение файлов из сети, чтение электронных сообщений и т.д.). Поэтому необходимо устанавливать специальные фильтры на точках входа данных, специальные программы, ограничивающие загрузку зараженных файлов и программ. Одним из таких устройств является продукт корпорации Symantec (партнером является компания Nuron DC в Ташкенте). Symantec выдвигает идею комплексной защиты всей корпоративной сети, а не отдельно взятой машины. Точка входа вируса в корпоративную сеть может быть любой — от браузера до рабочей станции. Поэтому контроль осуществляется на всех уровнях. Антивирусное программное обеспечение Symantec реализовано с использованием технологии корпорации Dynamic Document Review и также борется с почтовыми вирусами.

Отличительной особенностью антивирусного программного обеспечения является необходимость своевременного обновления репозитория антивирусного ПО.