Антивирусная программа Доктор Web

Dr.Web для Windows

Dr.Web для Windows включает в себя следующие компоненты:

- **Dr.Web Сканер для Windows – антивирусный сканер с графическим интерфейсом. Программа запускается по запросу пользователя или по расписанию и производит антивирусную проверку компьютера.**
- **SpIDer Guard для Windows – антивирусный сторож (называемый также монитором). Программа постоянно находится в оперативной памяти, осуществляя проверку файлов "на лету", а также обнаруживая проявления вирусной активности.**
- **SpIDer Mail для рабочих станций Windows – почтовый антивирусный сторож. Программа перехватывает обращения любых почтовых клиентов компьютера к почтовым серверам по протоколам POP3/SMTP, обнаруживает и обезвреживает почтовые вирусы до получения писем почтовым клиентом с сервера или до отправки письма на почтовый сервер.**
- **Dr.Web Модуль автоматического обновления для Windows – позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов комплекса, а также производит их автоматическую установку.**
- **В состав Dr.Web для рабочих станций входят также Планировщик заданий для Windows, сканер для среды DOS и ряд вспомогательных программ.**

Лицензионный ключевой файл

- Права пользователя на использование антивируса регулируются при помощи специального файла, называемого ключевым файлом. В ключевом файле содержится, в частности, следующая информация:

- перечень компонентов, которые разрешено использовать данному пользователю
- период, в течение которого разрешено использование антивируса
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать антивирус)

- Ключевой файл имеет расширение key и при работе программ по умолчанию должен находиться в каталоге установки.

- Ключевой файл имеет формат, защищенный от редактирования. Редактирование файла делает его недействительным. Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

- Коммерческие пользователи, приобретающие Dr.Web у законных поставщиков продукта, получают лицензионный ключевой файл. Параметры этого ключевого файла, регулирующие права пользователя, установлены в соответствии с пользовательским договором. В такой файл также заносится информация о пользователе и продавце антивируса.

- Для целей ознакомления с антивирусом также могут поставляться демонстрационные ключевые файлы. Такие ключевые файлы обеспечивают полную функциональность основных антивирусных компонентов, но имеют ограниченный срок действия и не предполагают оказания поддержки пользователю.

- Ключевой файл может поставляться в виде файла с расширением key или в виде zip-архива, содержащего этот файл, а также в виде файла специального формата с расширением dwz, используемого для распространения дополнений к пакету.

Ключевой файл может быть получен пользователем одним из следующих способов:

Получен в процессе регистрации продукта на сайте ООО ”Доктор Веб”. На основании введенного пользователем регистрационного серийного номера, полученного от продавца, формируется соответствующий лицензионный ключевой файл. При отсутствии серийного номера пользователь при регистрации может получить только демонстрационный ключевой файл. Сформированный ключевой файл высылается по электронной почте, а также может быть загружен со страницы регистрации.

Получен из Интернета на завершающей стадии процесса установки или при первом обновлении программного комплекса при помощи модуля автоматического обновления. Модуль производит регистрацию программного комплекса на сайте ООО ” Доктор Веб”, получает и устанавливает сформированный при регистрации ключ. Данный метод можно использовать только для варианта Dr.Web для рабочих станций.

Включен в состав дистрибутива продукта при его комплектации.

Передан пользователю по электронной почте в виде файла с расширением dwz . В этом случае для установки ключевого файла следует дважды щелкнуть по значку файла, присоединенного к письму.

Передан на отдельном носителе в виде файла с расширением key. В этом случае его необходимо скопировать в каталог установки Dr.Web.

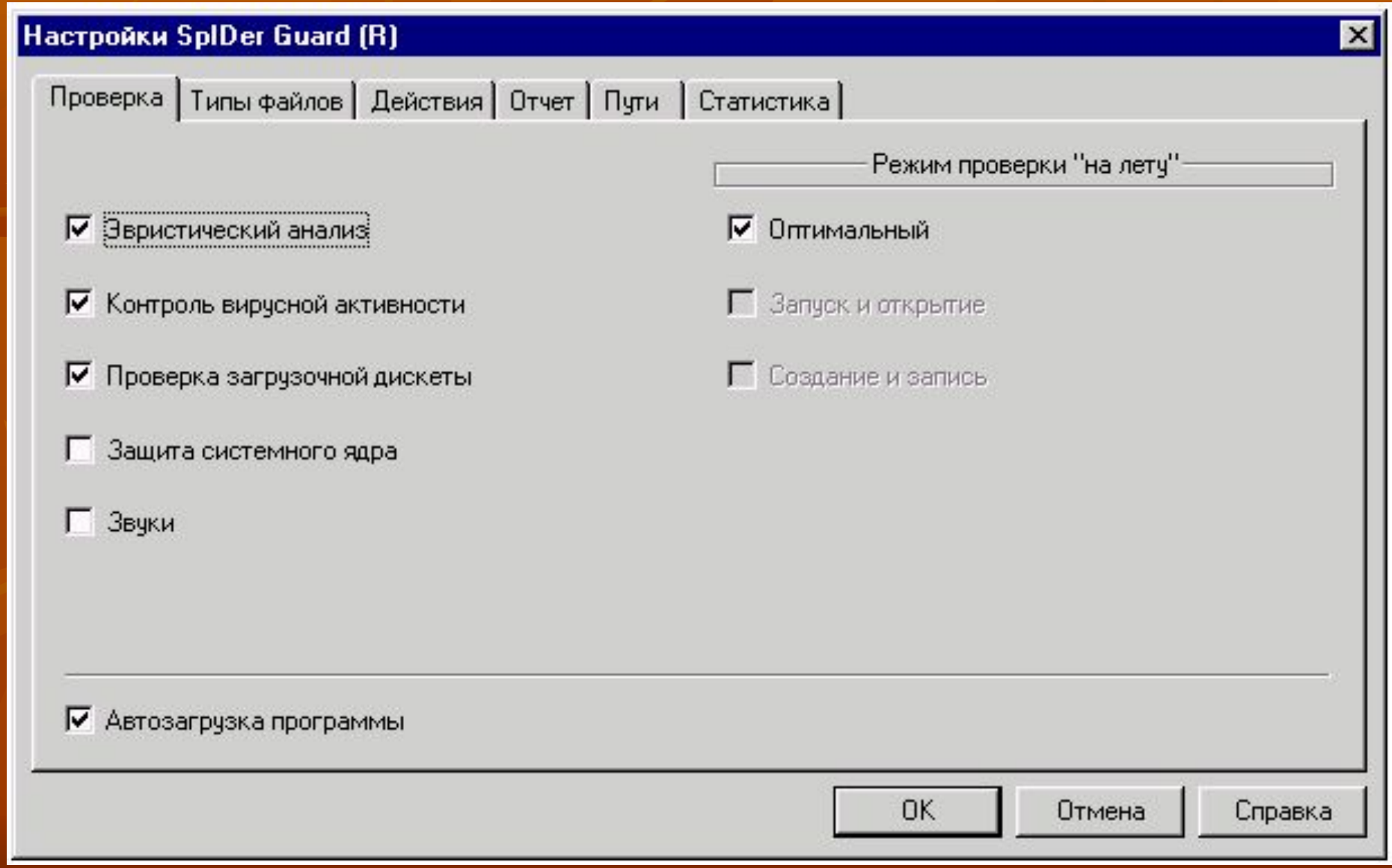
Передан в виде zip-архива, содержащего файл с расширением key. Извлеките файл при помощи архиватора данного формата (например, WinZip или Pkunzip) и поместите его в каталог установки.

Рекомендуется сохранять лицензионный ключевой файл до истечения срока его действия. При переустановке антивируса или в случае установки на несколько компьютеров повторная регистрация серийного номера не требуется. Используйте ключевой файл, полученный при первой регистрации. Повторная регистрация может потребоваться в случае утраты ключевого файла. При повторной регистрации укажите те же персональные данные, что были введены при первой регистрации; может измениться только адрес электронной почты – в таком случае лицензионный ключевой файл будет выслан по новому адресу.

- Количество запросов на получение ключевого файла ограничено – регистрация с одним и тем же регистрационным серийным номером допускается не более 25 раз. Если это число превышено, ключевой файл не будет выслан. В этом случае обратитесь в службу технической поддержки http://support.drweb.com/request/ (в запросе следует подробно описать ситуацию, указать персональные данные, вводимые при регистрации, и регистрационный серийный номер). Ключевой файл будет выслан вам службой технической поддержки по электронной почте.

Вкладка Проверка

На этой вкладке задается режим проверки файлов и процессов защищаемого компьютера.

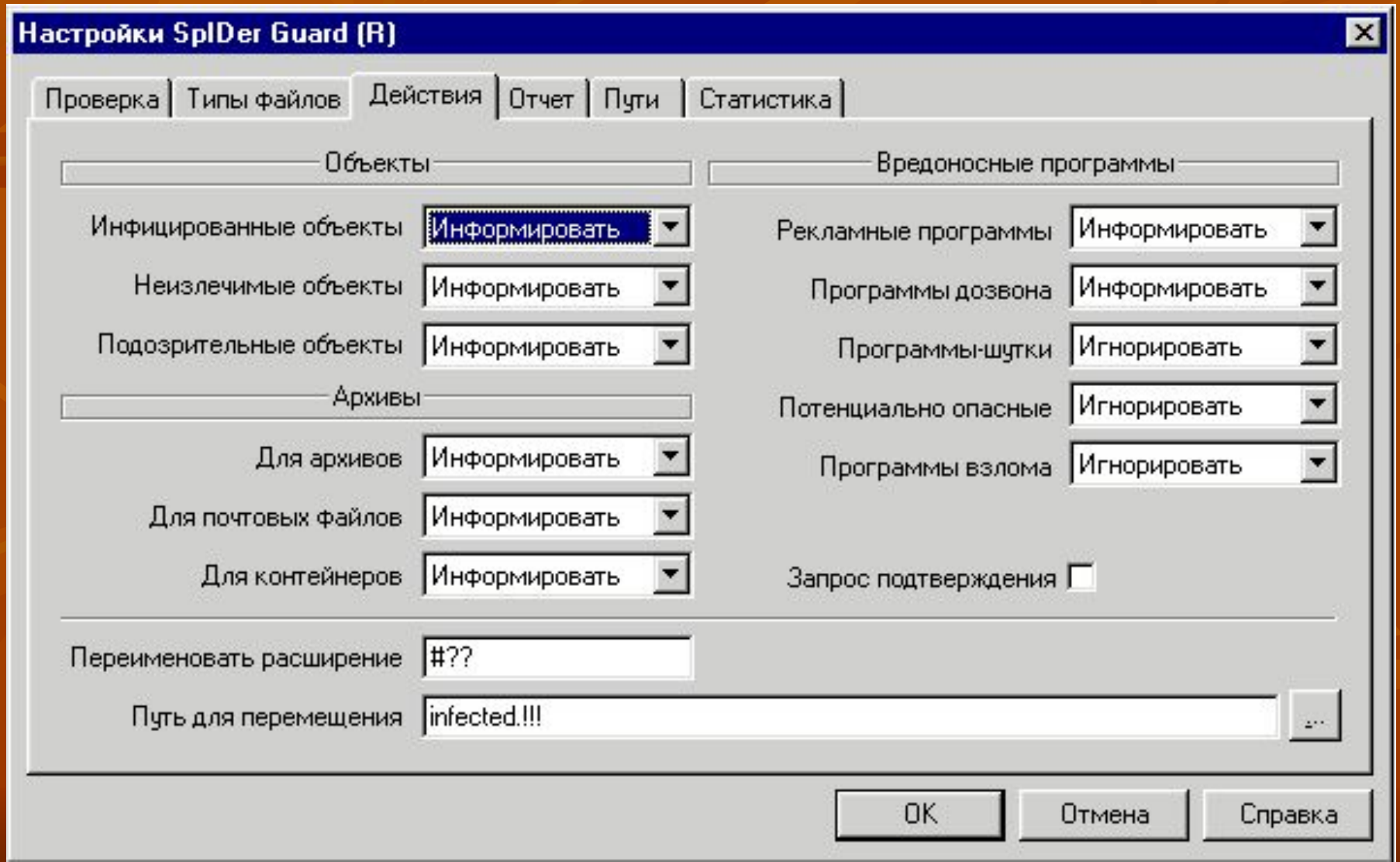


В группе флажков Режим проверки "на лету" задается действие с объектом, при котором производится его проверка "на лету".
По умолчанию установлен флажок Оптимальный. В этом режиме файлы и загрузочные сектора жестких дисков компьютера проверяются только при попытке создания файла или записи в существующий файл (загрузочный сектор), а файлы и загрузочные сектора сменных устройств - также при открытии на чтение или запуск программы. Этот режим рекомендуется использовать после тщательной проверки всех жестких дисков при помощи Dr.Web Сканер для Windows. При этом будет исключено проникновение на компьютер новых вирусов через сменные устройства, а повторной проверки заведомо "чистых" объектов не происходит.

Если вы снимете флажок Оптимальный, станут доступными флажки Запуск и открытие (предписывает проверять все файлы и загрузочные сектора при открытии на чтение или запуск программы) и Создание и запись (проверять при попытке создания файлов или записи в существующие). С помощью этих флажков вы можете самостоятельно установить уровень защиты компьютера. Установка обоих флажков обеспечивает максимальный уровень защиты, но значительно увеличивает нагрузку на компьютер.

Вкладка Действия

На этой вкладке задается реакция программы на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов.



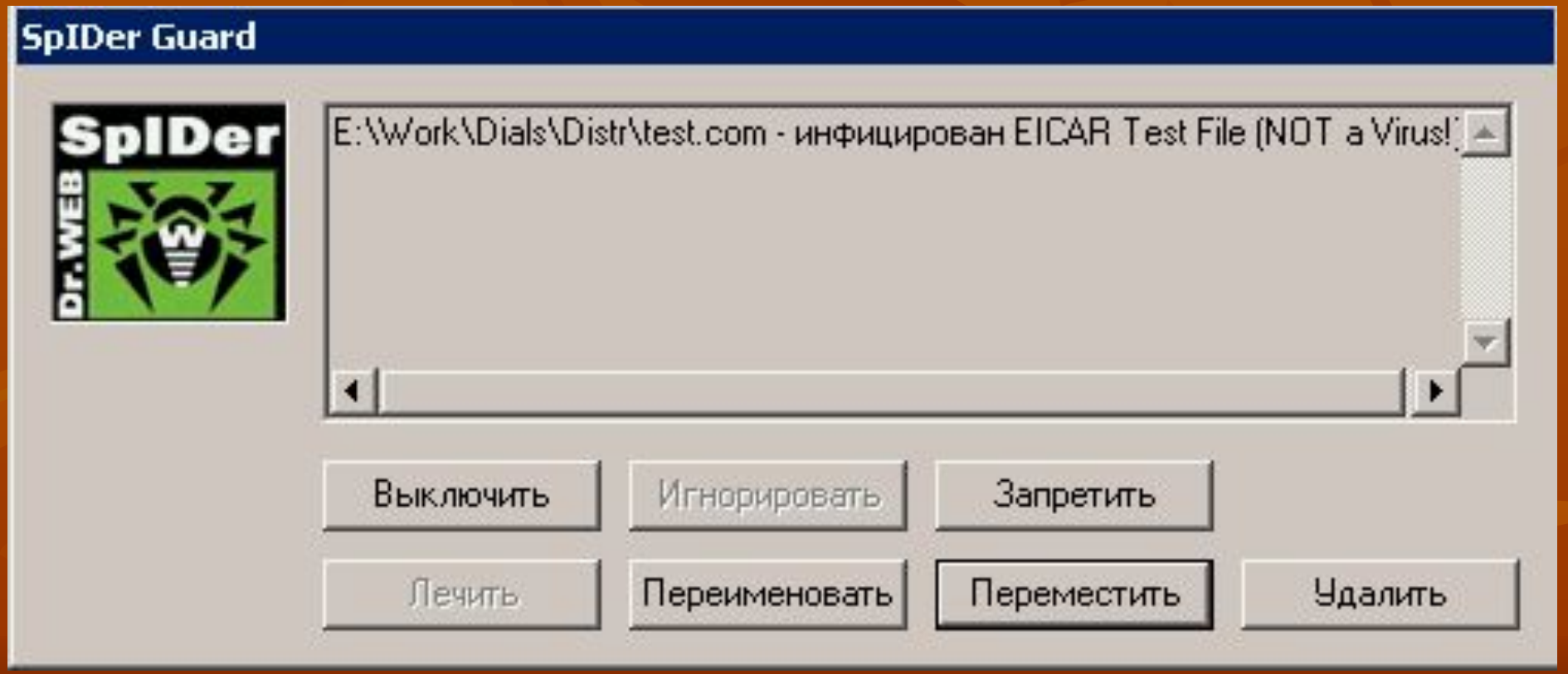
Реакция задается отдельно для объектов, зараженных известным и (предположительно) излечимым вирусом, для зараженных неизлечимым вирусом и для предположительно зараженных (подозрительных), а также для отдельных видов вредоносных программ и отдельных типов архивов.
По умолчанию сторож в пакете Dr.Web для рабочих станций лишь информирует пользователя обо всех зараженных и подозрительных объектах. При этом сведения об обнаруженных инфекциях выводятся в окно Запрос пользователю, в котором вы можете в дальнейшем предписать программе необходимые действия вручную.

Dr.Web для серверов Windows в случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом по умолчанию предпринимает автоматические действия по предотвращению вирусной угрозы.

Запрос пользователю в случае обнаружения инфекции

Данное окно открывается при обнаружении сторожем зараженного или подозрительного объекта, если в настройках реакции программы задано информирование.

назад



Вы можете выбрать другие реакции:

Вылечить – (доступна только при настройке реакции Для инфицированных) предписывает сторожу пытаться излечить объект, зараженный известным вирусом. Если вирус неизлечим или попытка лечения не была успешной, будет отработана реакция, заданная для неизлечимых вирусов.

Удалить – предписывает удалить зараженный или подозрительный файл (для загрузочных секторов никаких действий производиться не будет).

Состав доступных кнопок зависит от типа обнаруженной инфекции и типа зараженного объекта (для архивов, почтовых файлов и файловых контейнеров часть реакций также недоступны).

Кнопка Лечить (доступна только при обнаружении предположительно излечимого вируса, недоступна для архивов любого типа) предписывает сторожу пытаться излечить объект, зараженный известным вирусом. Если вирус неизлечим или попытка лечения не была успешной, окно откроется снова в виде, предусмотренном для обнаружения неизлечимых вирусов.

Кнопка Удалить предписывает удалить зараженный или подозрительный файл (для загрузочных секторов никаких действий производиться не будет). При настройках по умолчанию недоступна для архивов любого типа.

Кнопка Переименовать предписывает переименовать расширение имени зараженного или подозрительного файла в соответствии с настройками по умолчанию.

Кнопка Переместить предписывает переместить зараженный или подозрительный файл в каталог карантина, заданный по умолчанию.

Кнопка Запретить предписывает запретить доступ к файлу, проверка которого вызвала реакцию сторожа. Блокировка доступа к файлу снимается только после перезагрузки компьютера.

Кнопка Выключить предписывает немедленно завершить работу Windows при обнаружении объекта (в ряде случаев из-за действия вируса корректное завершение будет невозможно). В дальнейшем рекомендуется удалить вирус при помощи Dr.Web для DOS, запущенного с защищенного диска.

Кнопка Игнорировать предписывает не предпринимать каких-либо действий при обнаружении подозрительного объекта.

Автор: Аверкина Т.П., учитель МОУ «Тархановская СОШ» Ичалковского района РМ