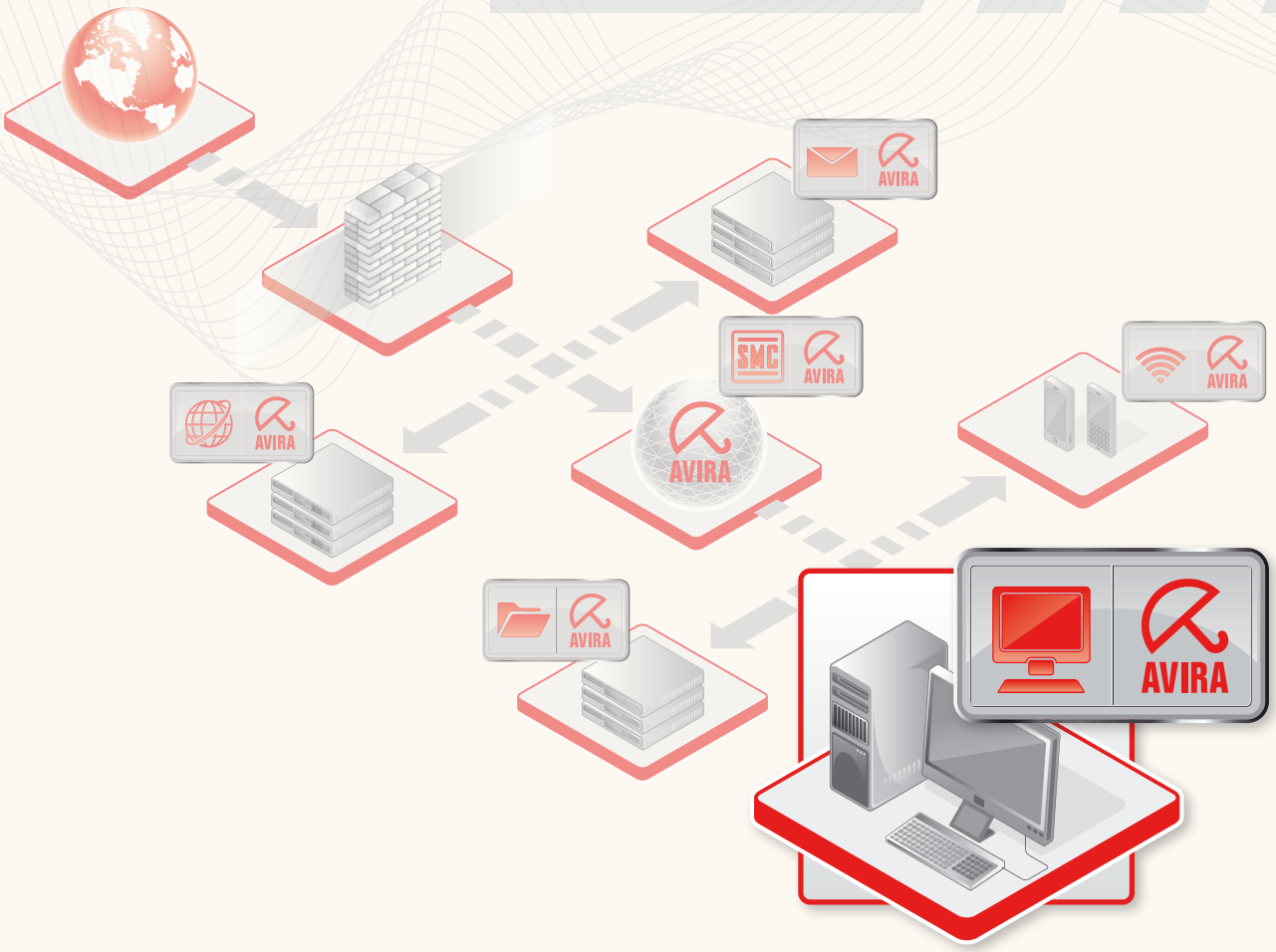
AVIRA
More Than Security

Руководство пользователя

Avira Premium Security Suite



www.avira.ru

Торговая марка и авторское право

Торговая марка

AntiVir является зарегистрированной торговой маркой Avira GmbH.
Windows является зарегистрированной торговой маркой Microsoft Corporation в США и других странах.
Все другие названия марок и продуктов являются товарными знаками или зарегистрированными товарными знаками, принадлежащими своим владельцам.
Защищенные товарные знаки не обозначены защищенными в этом руководстве. Это, однако, не означает, что они могут применяться свободно.

Информация об авторских правах

В Avira Premium Security Suite был использован код сторонних разработчиков. Мы благодарим обладателей авторских прав за предоставленный в наше распоряжение код. Подробную информацию об авторском праве Вы можете найти в разделе справки Avira Premium Security Suite TPL.

Содержание

1 Введение

Avira Premium Security Suite компании Avira GmbH защищает Ваш компьютер от вирусов, вредоносного и шпионского ПО, нежелательных программ и других опасностей. В настоящем руководстве дается краткая информация о вирусах и вредоносном ПО.

В руководстве описываются установка и обслуживание программы.

На нашем сайте http://www.avira.ru Вы можете загрузить руководство Avira Premium Security Suite как PDF-файл, Avira Premium Security Suite обновлять его или обновить Вашу лицензию.

Помимо этого, на нашем сайте Вы найдете такую информацию, как, например, телефон технической поддержки, а также наша рассылка новостей, на которую Вы можете подписаться.

С уважением, сотрудники Avira GmbH

2 Символы и выделения

Используются следующие символы:

Пиктограмма / Обозначение	Объяснение
✓	Обозначает условие, которое необходимо для выполнения действия.
▸	Обозначает этап действия, которое Вы выполняете.
→	Обозначает результат выполненного действия.
Предупреждение	Обозначает предупреждение о возможности потери данных.
Примечание	Обозначает примечание, содержащее важную информацию, или рекомендацию по использованию Avira Premium Security Suite.

Используются следующие выделения:

Выделение	Объяснение
Курсив	Имя или путь файла.
	Отображаемые элементы интерфейса (названия окон, области окон или поле опций).
Жирный	Выбранные элементы интерфейса (пункты меню, разделы или кнопки).

3 Информация о продукте

В этой главе Вы получите всю необходимую для приобретения и использования Avira Premium Security Suite информацию:

- см. главу: Производительность
- см. главу: Системные требования
- см. главу: Лицензирование
- см. главу: Управление лицензиями

Avira Premium Security Suite - мощный и гибкий инструмент, способный надежно защитить Ваш компьютер от вирусов, вредоносного ПО и иных угроз.

▶ Принимайте во внимание следующее:

Примечание
Потеря ценных данных может иметь серьезные последствия. Даже самая лучшая антивирусная программа не сможет защитить Вас на 100% от потери данных. Регулярно создавайте резервные копии Ваших данных.

Примечание
Программа, защищающая от вирусов, нежелательных или вредоносных программ, будет надежной и эффективной только при регулярном обновлении. Позаботьтесь об актуальности Avira Premium Security Suite с помощью автоматического обновления. Настройте программу соответственно.

3.1 Производительность

Avira Premium Security Suite предлагает Вам следующие функции:

- Центр контроля для мониторинга, администрирования и управления программами
- Централизованная настройка в стандартном и экспортном режимах с чувствительной к контексту Справкой.
- Scanner с управляемым профилем и настраиваемым поиском всех известных типов вирусов и вредоносных программ
- Интегрированный в Windows Vista модуль управления учетными записями пользователей (User Account Control) для выполнения задач, требующих прав администратора
- Guard для постоянного отслеживания попыток доступа к файлам
- MailGuard (POP3, IMAP-сканнер и SMTP сканер) для постоянной проверки писем на наличие в них вирусов и вредоносных программ. Включая проверку почтовых вложений
- WebGuard для мониторинга передаваемых через Интернет по HTTP-протоколу данных (Мониторинг портов 80, 8080, 3128)
- Резервирование для создания резервных копий Ваших данных
- Встроенный менеджер карантина для изоляции подозрительных файлов и работы с ними

- Защита от руткит-программ позволяет обнаружить ПО, скрыто установленное в системе (Руткит)
  (только для 32-битн. системы)
- Прямой доступ к подробной информации об обнаруженных вирусах и вредоносном ПО (Интернет)
- Простое и быстрое обновление программы, файла вирусных сигнатур (VDF), а также поискового ядра с помощью обновления одним файлом и инкрементного VDF-обновления с веб-сервера в Интернет
- Удобная система управления лицензиями
- Встроенный Планировщик для планирования единовременных или повторяющихся задач обновления, проверки и пр.
- Высочайший уровень обнаружения вирусов и вредоносных программ, гарантируемый новой технологией поиска (поисковое ядро) с применением эвристики
- Распознавание всех популярных типов архивов, включая вложенные, с применением списков опасных расширений файлов
- Высокая производительность многопоточной технологии (одновременное сканирование нескольких файлов)
- Firewall для защиты Вашего компьютера от попыток получения несанкционированного доступа из/в Интернет или локальные сети.

3.2 Системные требования

Для безупречной работы Avira Premium Security Suite необходимо, чтобы система соответствовала следующим требованиям:

- Минимум - Pentium 266 MHz
- Операционная система
- Windows 2000, SP4 и пакет обновлений 1 или
- Windows XP, SP2 (32 или 64 бит) или
- Windows Vista (32 или 64 бита, SP 1 рекомендуется)
- Не менее 100 Мб свободной памяти на жестком диске (при использовании Карантина и для временной памяти - больше)
- Минимум 192 Мб ОЗУ для Windows 2000/XP
- Минимум 512 Мб ОЗУ для Windows Vista
- Для установки Avira Premium Security Suite: Права администратора
- Для установки всех продуктов: Windows Internet Explorer 6.0 и выше
- При необходимости интернет-соединение (см. Установка)

Примечания для пользователей Windows Vista

В Windows 2000 и Windows XP многие пользователи работают с правами администратора. Это нежелательно по соображениям безопасности, так как значительно повышается опасность инфицирования системы вирусами и вредоносными программами.

По этой причине Microsoft вводит в Windows Vista "Управление учетными записями пользователей" (User Account Control). Таким образом пользователи, работающие с правами администратора, получают дополнительную защиту: в Windows Vista администратор обладает привилегиями обычного пользователя. Действия, для которых необходимы права администратора, Windows Vista четко выделяет специальным примечанием. Кроме того, пользователь должен явно подтверждать желаемое действие. Только после получения подтверждения производится повышение привилегий, и операционная система выполняет задание администратора.

Avira Premium Security Suite для выполнения некоторых действий в Windows Vista требует права администратора. Эти действия обозначаются следующими значками:  . Если этот символ отображается на кнопке, для выполнения данного действия требуются права администратора. Если Ваша учетная запись не имеет прав администратора, система управления учетными записями пользователей Windows Vista требует указания пароля. Если Вы не имеете пароля администратора, Вы не сможете выполнить требуемое действие.

3.3 Лицензирование

Для того, чтобы использовать Avira Premium Security Suite, Вам необходима лицензия. Вы соглашаетесь с лицензионными условиями Avira Premium Security Suite.

Лицензия предлагается в форме кода активации. Код активации - это код, состоящий из букв и цифр, который Вы получили при приобретении Avira Premium Security Suite. С помощью кода активации устанавливаются точные параметры Вашей лицензии - какая программа и на какой временной период лицензируется.

Код активации пересылается Вам в электронном письме, если Вы приобрели Premium Security Suite в Интернет-магазине, или размещен на упаковке продукта.

Чтобы лицензировать программу, укажите код активации в процессе активации Avira Premium Security Suite. Продукт может быть активирован в процессе установки. Вы можете активировать Avira Premium Security Suite и после установки с помощью Центр контроля в пункте Справка::Менеджер лицензий.

4 Установка и удаление

этой главы содержится информация об установке и удалении Avira Premium Security Suite:

- см. главу Установка: Предпосылки, Типы установки, Произвести установку
- см. главу Установочные модули
- см. главу Установка изменений
- см. главу Удаление: Выполнить удаление

4.1 Установка

Убедитесь перед установкой Avira Premium Security Suite в том, что Ваш компьютер соответствует Минимальным системным требованиям. Если Ваш компьютер отвечает всем требованиям, Вы можете установить Avira Premium Security Suite.

Примечание
Начиная с Windows XP Avira Premium Security Suite создает точку восстановления перед установкой Avira Premium Security Suite. Это позволит Вам безопасно удалить Avira Premium Security Suite в случае неудачной установки. Не забывайте, что для этого опция **Отключить восстановление системы** в: "Пуск | Настройка | Панель управления | Система | Восстановление системы" не должна быть включена.
Если Вы хотите определить более раннюю точку восстановления системы, Вы можете сделать это с помощью функции "Пуск | Программы | Стандартные | Служебные | Восстановление системы". Созданную программой Avira Premium Security Suite точку восстановления системы вы сможете определить по строке Premium Security Suite.

Типы установки

Во время установки Вы можете выбрать тип установки:

полная

Premium Security Suite устанавливается полностью со всеми компонентами. Программные файлы устанавливаются в стандартную папку `C:\Program Files`.

По выбору

У Вас есть возможность установить отдельные компоненты программы (см. главу Установка и удаление::Установочные модули). Можно выбрать папку, в которую будет произведена установка. Вы можете отключить создание иконок на рабочем столе и группы программ в меню Пуск.

Перед запуском процесса установки

- Закройте Вашу почтовую программу. Кроме того, рекомендуется завершить все работающие приложения.
- Убедитесь в том, что не установлены другие антивирусные решения. Автоматические функции защиты различных систем безопасности могут мешать друг другу.
- Установите Интернет-соединение. Интернет-соединение необходимо для выполнения следующих этапов установки:
- Загрузка актуальных программных файлов и поискового ядра, а также файл вирусных сигнатур через программу установки (при установке через интернет)
- Активация Avira Premium Security Suite
- Выполнение обновления Premium Security Suite по завершении установки
- Приобретите ключ лицензии Premium Security Suite, если Вы хотите активировать Premium Security Suite.

Примечание
Установка через интернет:
Для установки Avira Premium Security Suite через интернет Avira GmbH предлагает программу установки, которая перед выполнением установки загружает с сервера Avira GmbH актуальные программные файлы. Этот способ обеспечивает установку Premium Security Suite с актуальным файлом вирусных сигнатур.
Установка через пакет для инсталляции
Пакет для инсталляции содержит программу установки и необходимые программные файлы. При установке через пакет для инсталляции у Вас нет возможности выбора языка для Premium Security Suite. Рекомендуется после завершения установки выполнить обновление, чтобы обновить файл вирусных сигнатур.

Примечание
Для активации продукта Avira Premium Security Suite соединяется через HTTP-протокол по порту 80 (Web-коммуникация), а также через зашифрованный протокол SSL по порту 443 с серверами Avira GmbH. Если Вы используете брандмауэр, убедитесь в том, что входящий/исходящий трафик не блокируется им.

Произвести установку

Программа установки работает в диалоговом режиме. Каждое окно содержит ряд кнопок для управления процессом установки.

Важнейшие кнопки выполняют следующие функции:

- **ОК:** Подтвердить действие.
- **Отменить:** Отменить действие.
- **Далее:** Перейти к следующему шагу.
- **Назад:** Перейти к предыдущему шагу.

Так Вы установите Premium Security Suite:

Примечание
Приведенное ниже руководство по отключению Windows Firewall касаются только Windows XP.

- ▶ Запустите установщик двойным щелчком по установочному файлу, который Вы загрузили из Интернет, или находящемуся на CD.

Установка через интернет

→ Появится *окно приветствия*.

- ▶ Нажмите **Далее**, чтобы продолжить установку.

→ Появится диалоговое окно *Выбор языка*.

- ▶ Выберите язык для установки Premium Security Suite и подтвердите выбор, нажав **Далее**.

→ Появится диалоговое окно *Загрузить*. С сервера Avira GmbH будут загружены все файлы, необходимые для установки. По завершении загрузки окно *Загрузка* будет закрыто.

Установка через пакет для инсталляции

→ Откроется диалоговое окно ассистента установки *Avira Premium Security Suite*.

- ▶ Нажмите *Принять*, чтобы запустить установку.

→ Установочный файл распаковывается. Запускается процедура установки.

→ Появится *окно приветствия*.

- ▶ Нажмите **Далее**.

Продолжение установки через интернет и через пакет для инсталляции

→ Появится диалоговое окно *Дополнительные категории угроз*. В диалоговом окне содержится информация о защитных функциях Premium Security Suite и указания по расширению защитных функций Premium Security Suite.

- ▶ Нажмите **Далее**.

→ Возникает окно с лицензионным соглашением.

- ▶ Подтвердите, что Вы принимаете условия лицензионного соглашения и нажмите кнопку **Дальше**.

→ Откроется окно *Тип установки*.

- ▶ Решите, желаете ли Вы произвести полную или выборочную установку.
- ▶ Выберите опцию **Полная** или **Выборочная**, нажмите **Дальше**.

Выборочная установка

→ Возникнет окно *выбора целевой папки*.

- ▶ Подтвердите выбранную папку нажатием кнопки **Дальше**.

  - ИЛИ -

  Выберите другую папку нажатием кнопки **Обзор**, а затем подтвердите кнопкой **Дальше**.

→ Откроется диалоговое окно *Установка компонентов*:

- ▶ Включите или отключите желаемые компоненты, а затем подтвердите кнопкой **Дальше**.

→ При установленном Windows Firewall возникает Примечание, предлагающее отключить его для того, чтобы избежать конфликтов с Avira Firewall.

- ▶ Подтвердите кнопкой **Да**.

→ Windows Firewall будет отключен.

→ В следующем окне Вы можете установить, необходимо ли создавать иконку на рабочем столе и/или новую группу программ в меню Пуск.

▶ Нажмите **Далее**.

▶ Пропустите раздел "Полная установка".

Полная установка

→ При установленном Windows Firewall возникает Примечание, предлагающее отключить его для того, чтобы избежать конфликтов с Avira Firewall.

▶ Подтвердите кнопкой **Да**.

→ Windows Firewall будет отключен.

Далее для полной и выборочной установки

→ Открывается ассистент лицензий.

Вы имеете на выбор следующие опции активации Premium Security Suite

– Ввод кода активации

Ввод кода активации активирует Avira Premium Security Suite с Вашей лицензией.

– Выбор опции **Тестировать продукт**

При выборе опции **Тестировать продукт** в процессе активации генерируется тестовая лицензия, с которой активируется Avira Premium Security Suite. Вы сможете некоторое время тестировать Avira Premium Security Suite со всеми функциями в полном объеме.

Примечание
Опция **Действующий файл лицензии hbedv.key** позволит Вам прочитать действующий файл лицензии. Файл лицензии создается в процессе активации продукта с действующим кодом активации и сохраняется в программной папке Avira Premium Security Suite. Используйте эту опцию, если Вы уже произвели активацию продукта и хотите заново установить Avira Premium Security Suite.

Примечание
В некоторых коммерческих версиях Avira Premium Security Suite код активации уже находится в продукте. В этом случае нет необходимости указывать код активации. Встроенный код активации будет отображаться с помощью ассистента лицензий.

Примечание
Для активации Premium Security Suite устанавливается соединение с серверами Avira GmbH. С помощью опции **Настройки прокси** Вы можете настроить Интернет-соединение через прокси-сервер.

▶ Выберите тип процедуры активации и подтвердите нажатием кнопки **Далее**

Активация продукта

→ Открывается диалоговое окно, в котором Вы можете указать Ваши персональные данные.

▶ Введите Ваши данные и нажмите **Далее**

→ Ваши данные будут переданы на серверы Avira GmbH и проверены. Avira Premium Security Suite будет активирован с Вашей лицензией.

→ В следующем диалоговом окне отображаются данные Вашей лицензии.

▶ Нажмите **Далее**.

▶ Вы можете пропустить раздел "Активация с помощью выбора опции **Действующий файл лицензии hbedv.key** ".

Выбор опции "Действующий файл лицензии hbedv.key"

→ Открывается диалог чтения файла лицензии.

▶ Укажите файл лицензии hbedv.key с Вашими данными Premium Security Suite и нажмите **Открыть**

→ В следующем диалоговом окне отображаются данные Вашей лицензии.

▶ Нажмите **Далее**

После завершения активации или загрузки файла лицензии нажмите Далее

→ Будут установлены компоненты программы. Этап установки будет отображен в диалоговом окне.

→ В следующем окне Вы можете выбрать, необходимо ли открыть файл Readme после завершения установки.

▶ При необходимости подтвердите и закройте окно установки, нажав *Готово*.

→ Ассистент установки будет закрыт.

→ Откроется файл readme.

→ Далее откроется ассистент конфигурирования. Ассистент конфигурирования позволяет настроить Premium Security Suite. Если Вы прервете конфигурацию, то Premium Security Suite запустится со стандартными настройками.

Предварительные настройки в ассистенте конфигурирования

→ В диалоговом окне *Настройка AHeAD*, Вы можете выбрать уровень для обнаружения для технологии AHead. Выбранный уровень обнаружения будет использован для установки технологии AHead-Scanner (прямая проверка) и Guard (проверка в реальном времени) .

▶ Выберите уровень обнаружения и нажмите **Дальше**.

→ В диалоговом окне *Дополнительные категории угроз*, Вы можете выбрать категории угроз и настроить функции защиты Premium Security Suite.

▶ При необходимости активируйте дополнительные категории угроз, нажмите *Дальше*.

→ В диалоговом окне *Уровень безопасности брандмауэра* Вы можете определить, разрешает ли Avira Firewall внешний доступ к ресурсам с общим доступом, а также сетевой доступ для приложений, созданных надежными производителями.

▶ Активируйте необходимые опции, нажмите *Далее*.

→ В окне *Стартовый режим проверки*Вы можете определить, необходимо ли задавать время начала проверки Guard. Guard при каждом запуске системы будет работать в заданном стартовом режиме.

Примечание
Заданный стартовый режим Guard фиксируется в реестре и не может быть изменен через Avira Premium Security Suite. Настройка.

▶ Активируйте необходимые опции, нажмите *Далее*.

→ В диалоговом окне *Проверка системы* можно включить или отключить быструю проверку системы. Быстрая проверка системы проводится после завершения конфигурации и перед перезагрузкой системы, будет произведена проверка запущенных программ и системных файлов.

▶ Активируйте или деактивируйте опцию *Быстрая проверка системы*, нажмите*Далее*.

→ Нажмите *Готово* для завершения конфигурации.

▶ Нажмите *Готово*.

→ Заданные и выбранные настройки будут сохранены.

→ Если Вы активировали опцию *Быстрая проверка системы*, то откроется окно Luke Filewalker. Scanner проведет быструю проверку системы.

→ Откроется окно *Завершить установку*.

→ Если Вы установили Premium Security Suite на Windows XP и при этом деактивировали Windows Firewall, то появится окно с предложением перезагрузить систему.

Примечание
В Windows XP/Vista при выключенном Windows Firewall перезапуск системы необходим по причине безопасности.

▶ Завершите установку, нажав **Готово**.

- ИЛИ -

▶ Подтвердите перезагрузку компьютера кнопкой **OK**.

→ Будет проведена перезагрузка системы.

После успешной установки Центр контроля рекомендует в *Обзор :: Статус* проверить актуальность Premium Security Suite.

▶ Обновите Premium Security Suite, для поддержания в актуальном состоянии файла вирусных сигнатур.

▶ Проведите полную проверку системы.

4.2 Установка изменений

У Вас есть возможность добавлять или удалять отдельные программные компоненты установленного Avira Premium Security Suite (см. главу Установка и удаление::Установочные модули)

Если Вы хотите добавить или удалить программные компоненты установленного Avira Premium Security Suite, Вы можете воспользоваться пунктом **Установка и удаление программ** для того, чтобы **Изменить/Удалить** программы в **Панели управления Windows**.

Выберите Avira Premium Security Suite и нажмите кнопку **Изменить**. В окне приветствия Avira Premium Security Suite выберите пункт **Изменить**. Вы пройдете через процедуру изменения установленной программы.

4.3 Установочный модуль

При выборочной установке или установке изменений могут быть выбраны, добавлены или удалены следующие модули :

- **Premium Security Suite**
  Этот модуль содержит все компоненты, необходимые для успешной установки Avira Premium Security Suite.
- **AntiVir Guard**
  AntiVir Guard работает в фоновом режиме. Он отслеживает файлы при открытии, записи и копировании в режиме реального времени, а также лечит их, если необходимо (On-Access = по требованию). Если пользователь производит операцию с файлом (загрузка, выполнение, копирование), Avira Premium Security Suite автоматически проверяет файл. При операции Переименования AntiVir Guard не проверяет файл.
- **AntiVir MailGuard**
  MailGuard это связующее звено между Вашим компьютером и почтовым сервером, с которого Ваш почтовый клиент загружает письма. MailGuard цепляется как Proxy между почтовым сервером и клиентом. Все входящие письма перенаправляются через этот Proxy, проверяются на наличие вирусов и вредоносных программ, а затем пересылаются на Вашу почту. Программа автоматически обрабатывает инфицированные письма и запрашивает пользователя о необходимых действиях. В MailGuard предусмотрена защита от спама.
- **AntiVir WebGuard**
  При открытии страниц' в Интернет Вы получаете данные с веб-сервера через Ваш веб-браузер. Переданные веб-сервером данные (HTML файлы, скрипты и картинки, флэш, видео и аудио потоки) обычно попадают из кэш браузера непосредственно на исполнение в браузер, делая невозможной проверку в режиме реального времени, как это делает AntiVir Guard. Так вирусы и вредоносные программы попадают в Вашу систему. WebGuard является т.н. HTTP-прокси, который использует для передачи данных порты (80, 8080, 3128), проверяет передаваемые данные на наличие вирусов и вредоносных программ. Программа автоматически обрабатывает инфицированные файлы и запрашивает пользователя о необходимых действиях.
- **Avira Firewall**
  Avira Firewall контролирует коммуникации Вашего компьютера с внешним миром. Он разрешает или запрещает соединение, основываясь на правилах безопасности.

- ***Защита от руткит-программ***
  Защита от руткит-программ проверяет, содержится ли на Вашем компьютере ПО, которое после проникновения в систему не может быть обнаружено обычными методами обнаружения вредоносного ПО.
- ***Shell Extension***
  Avira Premium Security Suite Shell Extension создает в контекстном меню Windows Explorer (правая кнопка мыши) строку Проверить выбранные файлы с помощью AntiVir. Эта строка позволяет проверить отдельные файлы или папки.
- ***Резервирование***

Компонент Резервирование позволит автоматически и вручную организовать зеркалирование ваших данных.

4.4 Удаление

Если Вы хотите удалить Avira Premium Security Suite, воспользуйтесь опцией **Установка и удаление программ** для **Изменения/Удаления** программ через Панель управления Windows.

Так Вы удалите Avira Premium Security Suite (описано на примере с Windows XP и Windows Vista):

- ▶ Откройте пункт меню Windows **Пуск**, **Панель управления**.
- ▶ Дважды щелкните по **Program Files** (Windows XP: **Установка и удаление программ**).
- ▶ Выберите **Avira Premium Security Suite** и нажмите **Удалить**.

→ Вы должны будете подтвердить, что действительно хотите удалить программу.

- ▶ Подтвердите кнопкой **Да**.

→ Вы должны будете указать, хотите ли включить Windows Firewall (т.к. Avira Firewall будет отключен).

- ▶ Подтвердите кнопкой **Да**.

→ Удаляются все компоненты программы.

- ▶ Нажмите **Готово** для завершения установки.

→ В некоторых случаях может отобразиться окно с предложением перегрузить компьютер.

- ▶ Подтвердите кнопкой **Да**.

→ Avira Premium Security Suite удален. Компьютер при необходимости требуется перезагрузить. При этом будут удалены все папки, файлы и записи реестра Avira Premium Security Suite.

5 Обзор Premium Security Suite

этой главы содержится обзор функций и особенности использования Premium Security Suite.

- См. главу Интерфейс и работа с программой
- См. главу Это делается так

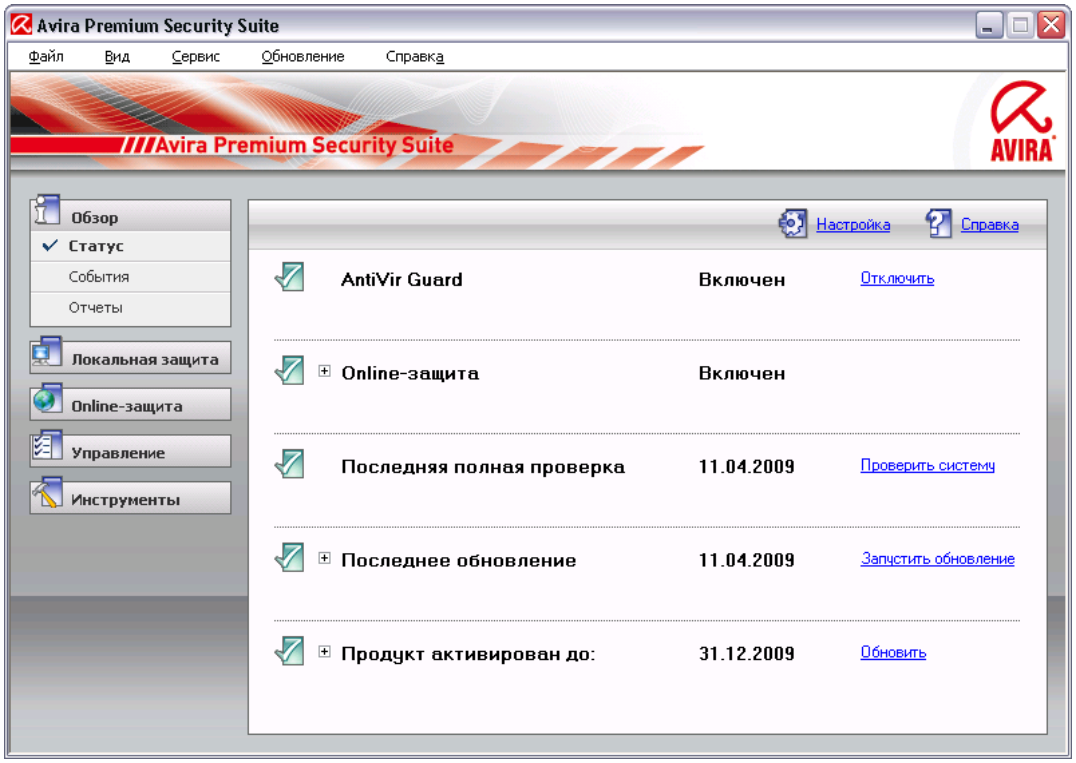
5.1 Интерфейс и работа с программой

Вы можете управлять Premium Security Suite с помощью трех элементов интерфейса программы:

- Центр контроля: Мониторинг и управление Premium Security Suite
- Avira Premium Security Suite. Настройка: Настройка Premium Security Suite
- Пиктограмма в системном трее на панели задач: Открытие Центр контроля и другие функции

5.1.1 Центр контроля

Центр контроля предназначен для наблюдения за статусом Вашего компьютера, для управления и пользования компонентами защиты и функциями Premium Security Suite.



Окно Центр контроля разделено на три области: **Меню**, **Строка меню** и основное окно **Вид**:

- **Меню:** Из пунктов меню Центр контроля Вы можете вызвать общие программные функции и информацию об Premium Security Suite.

- **Навигационное поле:** В разделе навигации Вы можете выбирать между различными вкладками Центр контроля. Отдельные вкладки содержат информацию и доступ к функциям программных компонентов Premium Security Suite, расположенных в строке меню по областям задач. Пример: Область задач *Обзор* - Раздел **Статус**.
- **Вид:** В этом окне отображается вкладка, которая была выбрана в навигационном поле. В зависимости от вкладки в верхней части основного окна находятся кнопки, предназначенные для выполнения функций / действий. В отдельных вкладках отображаются списки данных или объектов: Вы можете сортировать списки, щелкнув по полю, по которому желаете произвести сортировку.

Включение и выключение Центр контроля

Вы можете запустить Центр контроля следующими способами:

- Двойным щелчком по ярлыку на рабочем столе
- С помощью строки Premium Security Suite в меню Пуск | Программы.
- Через Avira Premium Security Suite Значок в трее.

Закрыть Центр контроля можно с помощью строки **Закрыть** в меню **Файл**. Можно также воспользоваться крестиком в правом верхнем углу окна Центр контроля.

Центр контроля управление блоком

Так устроена навигация Центр контроля

▶ Выберите в строке меню область задач.

→ Откроется область задач, появятся дополнительные разделы. Выбран и отображается в основном окне первый раздел области задач.

▶ Для отображения в основном окне информации о другом разделе щелкните по нему.

- ИЛИ -

▶ Выберите раздел с помощью пункта меню *Вид*.

Примечание
Управление клавиатурой в меню Вы можете включить с помощью клавиши [Alt]. Если навигация включена, Вы можете перемещаться в меню с помощью клавиш курсора. Кнопкой Enter Вы можете выбрать выделенный пункт меню.
Для того, чтобы открыть, закрыть меню Центр контроля или для навигации по меню Вы можете использовать сочетание клавиш: [Alt] + подчеркнутая буква в меню или пункте меню. Удерживайте клавишу [Alt] нажатой, если Вы из меню хотите вызвать пункт меню или подменю.

Так Вы можете обработать данные или объекты, отображаемые в основном окне:

▶ Выделите данные или объекты, которые хотите обработать.

Чтобы выделить несколько элементов, удерживайте клавишу Ctrl или Shift (выбор нескольких расположенных друг под другом элементов) пока выбираете элементы.

▶ Щелкните по кнопке в верхней части основного окна, чтобы обработать объект.

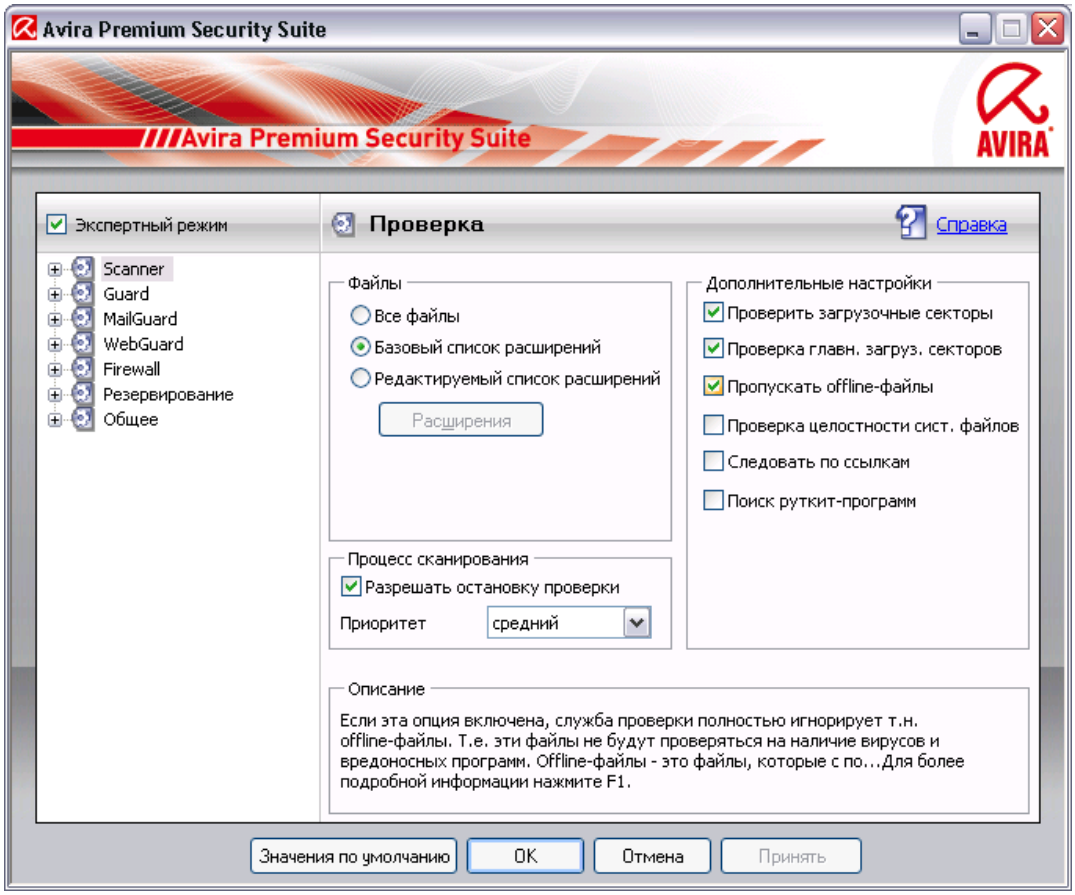
Обзор Центр контроля

- **Обзор**: В **Обзор** Вы найдете все вкладки, которые служат для наблюдения за функциями Avira Premium Security Suite.
- Раздел **Статус** показывает, какие модули Avira Premium Security Suite активны, предоставляет информацию о последних проведенных обновлениях. Можно видеть, обладает ли пользователь действующей лицензией.
- События. Здесь Вы можете увидеть, какие события были инициированы модулями Avira Premium Security Suite.
- Раздел Отчеты позволяет Вам получить информацию о результатах действий, выполненных Avira Premium Security Suite.
- **Локальная защита**: **Локальная защита** содержит компоненты, с помощью которых Вы можете проверить файлы на Вашем компьютере на наличие вирусов.
- Раздел Проверка дает Вам возможность довольно просто настроить и запустить сканирование. Предустановленный профиль позволит произвести проверку со стандартными настройками. Возможно также подстроить параметры проверки под Ваши индивидуальные задачи с помощью Выборочной проверки (настройка не сохраняется)или с помощью пользовательского профиля.
- Раздел Guard отображает информацию о проверенных данных, а также другие статистические данные, которые могут быть в любое время обнулены, позволяет открыть файл отчета. Подробная информация о последнем обнаруженном вирусе или вредоносной программе вызывается "одним щелчком".
- **Онлайн-защита**: В разделе **Онлайн-защита** Вы найдете компоненты, которые позволят защитить Вашу систему от вирусов, вредоносных программ и сетевых атак.
- Вкладка MailGuard показывает Вам проверенные MailGuard письма, их свойства и данные статистики. У Вас есть возможность тренировать фильтр антиспам и в будущем исключать из проверки Email-адреса на наличие вирусов или спама. Письма могут быть также удалены из буфера MailGuard.
- Вкладка WebGuard отображает информацию о проверенных URL, обнаруженных вирусах, а также другие статистические данные, которые в любой момент можно обнулить, предоставляет возможность вызвать файл отчета. Подробная информация о последнем обнаруженном вирусе или вредоносной программе вызывается "одним щелчком".
- Вкладка Firewall позволит Вам определить основные настройки Avira Firewall. Отображается также скорость передачи данных и все активные приложения, использующие сетевые соединения.
- **Управление**: С разделе **Управление** Вы найдете инструменты, которые позволят Вам изолировать подозрительные файлы, управлять ими, а также планировать регулярные задачи.
- Вкладка Карантин содержит элементы Менеджера карантина. Главное место для файлов на карантине или подозрительных файлов, которые Вы хотите поместить на карантин. Существует возможность отправить отдельный файл в вирусную лабораторию Центр исследования вредоносных программ.

- Вкладка Планировщик предоставляет возможность создавать, редактировать и удалять задачи проверки, обновления и резервирования, запускаемые в указанное время, а также задачи резервирования.
- **Инструменты**: В разделе **Инструменты** находятся инструменты для обеспечения безопасности данных.
- Вкладка Резервирование поможет Вам быстро и просто создать резервную копию Ваших данных и создать задачу резервирования.

5.1.2 Настройка

Avira Premium Security Suite. Настройка позволяет настраивать Premium Security Suite. После установки Premium Security Suite имеет стандартные настройки, позволяющие оптимально защитить Ваш компьютер. Premium Security Suite позволяет Вам настроить компоненты Premium Security Suite в соответствии с особенностями Вашего компьютера или Вашими требованиями.



Avira Premium Security Suite. Настройка имеет вид диалогового окна. Кнопки OK или Применить позволяют сохранить изменения в настройках, кнопка Отмена отменяет настройки, нажав кнопку Значения по умолчанию, Вы вернете стандартные настройки. В строке меню слева Вы можете выбрать различные разделы настроек.

Вызов блока Avira Premium Security Suite. Настройка

Вы можете запустить блок настроек несколькими способами:

- Через Управление Windows.
- Через Центр безопасности Windowsr - начиная с Windows XP SP 2.
- Через Avira Premium Security Suite Значок в трее.
- В Avira Premium Security Suite Центр контроля через пункт меню Сервис | Настройка.
- В Avira Premium Security Suite Центр контроля с помощью кнопки Настройка.

Примечание
При нажатии кнопки **Настройка** Центр контроля Вы попадаете в окно настройки раздела, который активен в Центр контроля. Для выбора отдельных пунктов настройки должен быть включен режим эксперта. В этом случае отображается диалоговое окно, в котором Вы должны включить режим эксперта.

Avira Premium Security Suite. Настройка управление блоком

Работа с окном навигации похожа на работу с Windows Explorer:

- ▶ Щелкните по строке в дереве каталогов для отображения этого раздела настроек в диалоговом окне.
- ▶ Щелкните по знаку плюс перед строкой для того, чтобы открылся раздел настроек и подразделы отобразились в виде дерева каталогов.
- ▶ Для того, чтобы скрыть подразделы, щелкните по знаку минус перед соответствующим разделом настроек.

Примечание
Для того, чтобы активировать, деактивировать функции в Avira Premium Security Suite. Настройка и нажимать кнопки, Вы можете использовать сочетания клавиш: [Alt] + подчеркнутая буква в имени функции или обозначении кнопки.

Примечание
Все разделы настройки отображаются только в режиме эксперта. Включите режим эксперта для отображения разделов блока настройки. Режим эксперта может быть защищен паролем, который необходимо указать при его включении.

Если Вы хотите сохранить созданные Вами настройки,

- ▶ нажмите кнопку **ОК**.

→ Окно настроек будет закрыто. Настройки будут сохранены.

- ИЛИ -

- ▶ Нажмите кнопку **Применить**.

→ Настройки будут сохранены. Окно настройки остается открытым.

Если Вы хотите закрыть окно настройки без сохранения изменений,

- ▶ нажмите кнопку **Отмена**.

→ Окно настройки будет закрыто. Изменения настроек не будут сохранены.

Если Вы хотите установить все настройки по умолчанию,

- ▶ нажмите кнопку **Значения по умолчанию**.

→ Все настройки примут значения по умолчанию. Изменения в списке и созданные пользователем строки в таком случае не сохраняются.

Обзор опций настройки

Вы располагаете следующими опциями настройки:

- **Scanner**: Настройка проверки

  Опции поиска

  Действия при обнаружении вируса

  Опции проверки архивов

  Исключения из проверки

  Эвристический поиск

  Настройка отчетов

- **Guard**: Настройка постоянной защиты

  Опции поиска

  Действия при обнаружении вируса

  Исключения постоянной защиты

  Эвристика постоянной защиты

  Настройка отчетов

- **MailGuard**: Настройка MailGuard

  Опции поиска: Активация контроля протоколов POP3 , IMAP, исходящих писем (SMTP)

  Действия при обнаружении вредоносной программы

  Эвристический поиск MailGuard

  Функция AntiBot: Разрешенный сервер SMTP, разрешенный отправитель

  Исключения из проверки MailGuard

  Настройка буфера памяти, очистка буфера

  Настройка учебной базы данных AntiSpam, очистить учебную базу данных

  Настройка отчетов

- **WebGuard**: Настройка WebGuard

  Опции поиска, активация и деактивация WebGuard

  Действия при обнаружении вируса

  Запрещенный доступ: Нежелательные типы файлов и MIME, Веб-фильтры для известных нежелательных URL (вредоносные программы, фишинг и т. д.)

  Исключения из проверки WebGuard: URL, типы файлов, MIME-типы

  Эвристика WebGuard

  Функция защиты детей: Ролевой доступ

  Настройка отчетов

- **Firewall**: Настройка Firewall

  Добавление правила адаптера

  Добавление индивидуальных правил адаптера

Список надежных производителей (исключения при доступе приложений к сети)

Расширенные настройки: Timeout для правил, блокирование Host-файла Windows, остановка брандмауэра Windows, оповещения

Настройка всплывающих окон (уведомления при доступе приложений к сети)

– **Резервирование**:

Добавление компонента Резервирование (Инкрементное резервирование, проверка на вирусы при резервировании)

Исключения: Настройка файлов для добавления к резервной копии

Настройка отчетов

– **Общее** :

Настройка отправки писем через SMTP

Дополнительные категории угроз для проверки и постоянной защиты

Защита паролем доступа к модулям Центр контроля и Avira Premium Security Suite. Настройка

Безопасность: Статус Обновить, статус Полная проверка системы, защита продукта

WMI: Активировать поддержку WMI

Настройка уведомления о событиях

Настройка функций отчетов

Настройка используемых папок

Обновление: Настройка подключения к серверу, настройка обновления продукта

Настройка акустических сигналов при обнаружении вируса

5.1.3 Значок в трее

После установки Вы увидите значок Premium Security Suite на панели задач системного трея:

Пиктограмма	Описание
	AntiVir Guard включен и Firewall включен
	AntiVir Guard отключен или Firewall отключен

Значок в трее отображает статус службы AntiVir Guard.

Через контекстное меню значка в трее доступны основные функции Avira Premium Security Suite. Для вызова контекстного меню необходимо щелкнуть правой кнопкой мыши по значку в трее.

Пункты контекстного меню

– **AntiVir Guard Включена**: Включает или отключает Avira AntiVir Guard.
– **Firewall**:

- Firewall включен: Включает или отключает Firewall
- Блокировать весь трафик: Включено: Блокирует любые передачи данных за исключением передачи собственной компьютерной системе (Local Host / IP 127.0.0.1).
- игровой режим включен: Включает или отключает режим: Включено: Применяются все установленные правила адаптера и приложений. Приложениям, для которых не определены правила, разрешены сетевые взаимодействия, при этом не появляются всплывающие окна.
- **Запустить AntiVir**: Открывает Avira Premium Security Suite Центр контроля.
- **Настроить AntiVir**: Открывает Avira Premium Security Suite. Настройка.
- **Запустить обновление**: Запускает Обновление.
- **Справка**: Открывает справочную онлайн-систему.
- **Avira в Internet**: Открывает веб-портал производителя Premium Security Suite. Для этого Вам необходимо иметь доступ к Интернет.

5.2 Это делается так

5.2.1 Активировать продукт

Для активации продукта Avira Premium Security Suite у Вас имеются следующие опции:

- Активация с помощью действующей полноценной лицензии

  Для активации Avira Premium Security Suite полноценной лицензией Вам необходим действующий активационный ключ, который содержит данные о Вашей лицензии. Код активации Вы могли получить от нас по Email или найти на упаковке продукта.

- Активация с помощью тестовой лицензии

  Avira Premium Security Suite активируется сознанной автоматически тестовой лицензией, которая позволяет Вам в течение определенного времени опробовать функции Avira Premium Security Suite в полном объеме.

Примечание
Для активации продукта или заказа тестовой лицензии Вам потребуется активное интернет-соединение.
Если не удается установить соединение с сервером Avira GmbH, проверьте настройки используемого брандмауэра: Для активации продукта используется соединение через HTTP-протокол и порт 80 (Web-коммуникация), а также через зашифрованный протокол SSL и порт 443. Убедитесь в том, что Ваш брандмауэр не блокирует входящие и исходящие данные. Сначала проверьте, можете ли Вы вызвать веб-страницу через Ваш браузер.

Так Вы активируете Premium Security Suite:

Если Вы еще не установили Avira Premium Security Suite:

- ▶ Установите Avira Premium Security Suite.
- ↪ Во время установки Вам потребуется выбрать способ активации
  - – *Активировать продукт*

    = Активация с помощью действующей полноценной лицензии
  - – *Тестировать продукт*

    = Активация с помощью тестовой лицензии
- ▶ Для активации полноценной лицензией введите активационный ключ.
- ▶ Подтвердите выбор способа активации нажатием кнопки **Далее**
- ▶ Укажите Ваши данные для регистрации и подтвердите их нажатием кнопки **Далее**.

↪ В следующем диалоговом окне отображаются данные Вашей лицензии. Активация Avira Premium Security Suite прошла успешно.

- ▶ Продолжите установку.

Если Вы уже установили Avira Premium Security Suite:

- ▶ В Центр контроля от Avira Premium Security Suite выберите пункт меню **Справка :: Менеджер лицензий**.

↪ Откроется ассистент лицензий, где Вы можете выбрать способ активации. Активируйте продукт, следуя приведенной выше схеме.

5.2.2 Avira Premium Security Suite обновить автоматически

Примечание
По умолчанию устанавливается задача обновления, при которой Avira Premium Security Suite обновляется при установленном интернет-соединении 2 часа и при создании интернет-соединения.

С помощью AntiVir Планировщик Вы определяете задачу автоматического обновления Avira Premium Security Suite:

- ▶ Выберите в Центр контроля раздел **Управление ::Планировщик**.
- ▶ Выберите символ  . *Создать новую задачу, используя мастер*.
- ↪ Появится диалоговое окно *Имя и описание задачи*.
- ▶ Введите имя и описание задачи.
- ▶ Нажмите **Далее**.
- ↪ Появится диалоговое окно *Тип задачи*.
- ▶ Выберите **Обновление** из списка.
- ▶ Нажмите **Далее**.
- ↪ Появится диалоговое окно *Время выполнения задачи*.
- ▶ Выберите время проведения обновления.
  - – **Немедленно**
  - – **Ежедневно**
  - – **Еженедельно**
  - – **Интервал**
  - – **Однажды**
  - – **Логин**

Примечание
Рекомендуется регулярно обновлять Avira Premium Security Suite, например, с интервалом все 2 часа.

- ▶ В зависимости от выбора задайте время.
- ▶ При необходимости выберите дополнительные опции(в зависимости от типа задачи):
  - – **Дополнительно запускать задачу при Интернет-соединении:**

    Помимо выполнения задач с установленной частотой осуществляется дополнительный запуск задач при каждом установленном Интернет-соединении.
  - – **Повторно запускать задачу, если определенное для нее время прошло:**

    Выполняются задачи, срок выполнения которых уже прошел, но они не могли быть запущены в назначенное время, например, если компьютер был выключен.
- ▶ Нажмите **Далее**.

→ Появится диалоговое окно *Выбор режима отображения*.

- ▶ Выберите режим отображения задачи:
  - – **Минимизировано:** только прогресс выполнения
  - – **Максимизировано:** все окно задачи.
  - – **Скрытый режим**: нет окна задачи
- ▶ Нажмите кнопку **Готово**.

→ Новое установленное задание будет отмечено галочкой как активированное на стартовой странице раздела **Управление :: Проверка**.

- ▶ Деактивируйте задачи, которые не должны выполняться.

Используя следующие символы, Вы можете обработать задания:

 Просмотреть свойства задания

 Изменение задачи

 Удаление задачи

 Запустить задачу

 Остановить задачу

5.2.3 Запустить обновление вручную

Существует несколько способов запустить обновление Avira Premium Security Suite вручную. При выполнении обновления вручную производится обновление файла вирусных сигнатур и поискового движка. Обновление продукта возможно, если в настройках Общее :: Обновление включена опция **Загрузить и автоматически установить обновление продукта**.

Запустить обновление Avira Premium Security Suite вручную:

- ▶ Щелкните правой кнопкой мыши по значку Avira Premium Security Suite в трее на панели задач.

→ Появится контекстное меню.

▶ Выберите пункт **Обновить сейчас**.

→ Отображается диалоговое окно *Программа обновлений*..

- ИЛИ -

▶ Выберите в Центр контроля раздел **Обзор :: Статус**.

▶ Нажмите в поле *Последнее обновление* на ссылку **Запустить обновление**.

→ Появится диалоговое окно Программа обновлений..

- ИЛИ -

▶ Выберите в Центр контроля в меню **Обновление** команду *Запустить обновление*.

→ Появится диалоговое окно Программа обновлений..

Примечание
Рекомендуется регулярно обновлять Avira Premium Security Suite, например, все 2 часа.

Примечание
Вы можете выполнить обновление вручную через Центр безопасности Windows.

5.2.4 Прямая проверка: Искать с помощью профиля поиска вирусы и вредоносное ПО

Профиль поиска включает в себя все диски и папки, которые необходимо проверить.

Существует несколько способов проведения проверки через профиль поиска:

– Использовать предустановленный профиль поиска

Если предустановленные профили соответствуют Вашим требованиям.

– Адаптация и использование профиля поиска (выбор вручную)

Создать индивидуальный профиль поиска.

– Создание и использование нового профиля поиска

Если Вы хотите создать собственный профиль поиска.

В зависимости от операционной системы для запуска профиля поиска доступны различные символы.

– Windows XP и 2000:

 С помощью этого символа запускается проверка через профиль поиска.

– Windows Vista:

В Microsoft Windows Vista через Центр управления доступны ограниченные права, например, для доступа к папкам и файлам. Определенные действия и доступ к файлам доступны через Центр управления при наличии расширенных прав администратора. Расширенные права администратора выдаются профилем поиска при каждом запуске.

 С помощью этого символа запускается ограниченная проверка через профиль поиска. Проверяются только те папки и файлы, доступ к которым разрешен Windows Vista.

 С помощью этого символа запускается проверка с расширенными правами администратора. После подтверждения будут проверены все папки и файлы выбранного профиля поиска.

Проверка с помощью профиля поиска на вирусы и вредоносное ПО

- ▶ Выберите в Центр контроля раздел **Локальная защита :: Проверка**.
- ↪ Появятся предустановленные профили поиска.
- ▶ Выберите один из предустановленных профилей поиска.

  - ИЛИ -
- ▶ Используйте профиль поиска *Выбор вручную*.

  - ИЛИ -
- ▶ Создайте новый профиль поиска.
- ▶ Выберите символ (Windows XP:  или Windows Vista: ).
- ▶ Появится окно *Luke Filewalker*, запустится прямая проверка.
- ↪ По окончании проверки будут показаны результаты.

Если Вы хотите запустить профиль поиска:

- ▶ В профиле поиска **Выбор вручную** разверните дерево каталогов настолько, чтобы были открыты все дисководы и папки , которые необходимо проверить.
  - – Нажмите на значок **+**: Отобразится следующий уровень каталогов.
  - – Нажмите на значок **-**: Следующий уровень каталогов будет скрыт.
- ▶ Отметьте узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле необходимого уровня каталогов.

  Существует несколько способов выбора папок:
  - – Каталог с подкаталогами (черный флажок)
  - – Каталог без подкаталогов (зеленый флажок)
  - – Только подкаталоги в каталоге (серый флажок, у подкаталогов флажок черный)
  - – Не выделять (галочка отсутствует)

Если Вы хотите создать новый профиль поиска.

- ▶ Выберите символ  . **Создать новый профиль.**
- ↪ Среди имеющихся профилей появится новый *Новый профиль*.
- ▶ При необходимости переименуйте профиль поиска, нажав на символ  .

- ▶ Отметьте узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле.

  Существует несколько способов выбора папок:

  - Каталог с подкаталогами (черный флажок)
  - Каталог без подкаталогов (зеленый флажок)
  - Только подкаталоги в каталоге (серый флажок, у подкаталогов флажок черный)
  - Не выделять (галочка отсутствует)

5.2.5 Прямая проверка: Поиск вирусов и вредоносного ПО с помощью Drag&Drop

Поиск вирусов и вредоносного ПО с помощью Drag&Drop:

✓ Центр контроля от Avira Premium Security Suite открыт.

- ▶ Выделите файл или папку, который/которую необходимо проверить.
- ▶ Удерживая нажатой левую кнопку мыши, перетащите отмеченный файл или отмеченную папку в *Центр контроля*.

→ Появится окно *Luke Filewalker*, запустится прямая проверка.

→ По окончании проверки будут показаны результаты.

5.2.6 Прямая проверка: Искать с помощью контекстного меню вирусы и вредоносное ПО

Искать с помощью контекстного меню вирусы и вредоносное ПО:

- ▶ Щелкните правой кнопкой мыши (например, в проводнике Windows, на рабочем столе иил в открытой папке Windows) по файлу или папке, который/которую Вы хотите проверить.

→ Появится контекстное меню проводника Windows.

- ▶ В контекстном меню выберите **Проверить выбранные файлы с помощью AntiVir**.

→ Появится окно *Luke Filewalker*, запустится прямая проверка.

→ По окончании проверки будут показаны результаты.

5.2.7 Прямая проверка: Автоматический поиск вирусов и вредоносного ПО

Вы определяете задачу, с помощью которой Вы устанавливаете автоматический поиск вирусов и вредоносных программ:

- ▶ Выберите в Центр контроля раздел **Управление :: Планировщик**.
- ▶ Выберите символ  . .

→ Появится диалоговое окно *Имя и описание задачи*.

- ▶ Введите имя и описание задачи.
- ▶ Нажмите **Далее**.

→ Появится диалоговое окно *Тип задачи*.

- ▶ Выберите строку **Проверка**.
- ▶ Нажмите **Далее**.

→ Появится диалоговое окно *Выбор профиля*.

- ▶ Выберите профиль для проверки.
- ▶ Нажмите **Далее**.

→ Появится диалоговое окно *Время выполнения задачи*.

- ▶ Выберите время проведения проверки.
  - – **Немедленно**
  - – **Ежедневно**
  - – **Еженедельно**
  - – **Интервал**
  - – **Однажды**
  - – **Логин**
- ▶ В зависимости от выбора задайте время.
- ▶ При необходимости выберите дополнительную опцию из следующих (в зависимости от типа задачи):
  - – **Повторно запускать задачу, если определенное для нее время прошло:**

    Выполняются задачи, срок выполнения которых уже прошел, но они не могли быть запущены в назначенное время, например, если компьютер был выключен.
- ▶ Нажмите **Далее**.

→ Появится диалоговое окно *Выбор режима отображения*.

- ▶ Выберите режим отображения задачи:
  - – **Минимизировано:** только прогресс выполнения
  - – **Максимизировано:** все окно задачи.
  - – **Скрытый режим**: нет окна задачи
- ▶ Нажмите кнопку **Готово**.

→ Новое установленное задание будет отмечено галочкой как активированное на стартовой странице раздела *Управление :: Планировщик*.

- ▶ Деактивируйте задачи, которые не должны выполняться.

Используя следующие символы, Вы можете обработать задания:

 Просмотреть свойства каждого задания

 Изменение задачи

 Удаление задачи

 Запустить задачу

 Остановить задачу

5.2.8 Прямая проверка: Прямой поиск активных руткит-программ

Для поиска активных руткит-программ, используйте предустановленный профиль поиска *Поиск программ-руткитов*.

Прямой поиск активных руткит-программ:

- ▶ Выберите в Центр контроля раздел **Локальная защита :: Проверка**.
- → Появятся предустановленные профили поиска.
- ▶ Выберите предустановленный профиль поиска **Поиск программ-руткитов**.
- ▶ Отметьте дополнительные узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле.
- ▶ Выберите символ (Windows XP:  или Windows Vista: ).
- → Появится окно *Luke Filewalker*, запустится прямая проверка.
- → По окончании проверки будут показаны результаты.

5.2.9 Реагировать на найденные вирусы и вредоносное ПО

Для отдельных компонентов защиты Premium Security Suite в разделе *Действия при обнаружении* Вы можете определить действия Premium Security Suite при обнаружении вируса или вредоносной программы:

Опции Scanner

- **Интерактивно**

В интерактивном режиме об обнаружении вирусов при проверке Scanner сообщается в диалоговом окне. Настройка определена по умолчанию. При поиске **программ-руткит**, **загрузочных вирусов** и при **проверке активных процессов** появляется диалоговое окно, в котором Вы можете выбрать действие для инфицированных объектов.
При **проверке файлов** оповещение и выбор действия для инфицированных файлов зависит от выбранного режима уведомления:
Режим уведомления: Комбинированный

В комбинированном режиме уведомления при завершении проверки файлов Вы получите уведомление со списком обнаруженных инфицированных файлов. У Вас нет возможности выбора действий над инфицированным файлом. Вы можете выполнить стандартное действие Scanner для всех инфицированных файлов или прервать Scanner.

Режим уведомления: Комбинированный (экспертный)

В экспертном режиме уведомления при завершении проверки файлов Вы получите уведомление со списком обнаруженных инфицированных файлов. Вы можете выбрать действие над инфицированным файлом в контекстном меню. Вы можете выполнить выбранное действие для всех инфицированных файлов или завершить Scanner

Режим уведомления: Индивидуальный

В индивидуальном режиме уведомлений при проверке файлов о каждом обнаруженном вирусе сообщается отдельно. Вы можете выбрать, что делать с зараженным файлом.

- **Автоматический**

В автоматическом режиме при обнаружении вируса или вредоносной программы автоматически выполняется действие, которое Вы предварительно выбрали. Если опция *Выводить уведомление* включена, то при обнаружении вируса Вы получите предупреждение с предложением выбора действий.

Опции при Guard, MailGuard, WebGuard:

– **Интерактивный**

В интерактивном режиме при обнаружении вируса или вредоносной программы отображается диалоговое окно, предлагающее на выбор несколько действий над инфицированными объектами. Настройка определена по умолчанию.

– **Автоматический**

В автоматическом режиме при обнаружении вируса или вредоносной программы автоматически выполняется действие, которое Вы предварительно выбрали. Если опция *Выводить уведомление* включена, то при обнаружении вируса Вы получите предупреждение с предложением выбора действий.

В интерактивном режиме при обнаружении вирусов или вредоносных программ в уведомлении Вы можете выбрать, что делать с инфицированными объектами и подтвердить свой выбор. Вы можете выбрать одно из следующих действий:

Примечание
Предлагаемые действия зависят от операционной системы, от защитных компонентов (AntiVir Guard, AntiVir Scanner, AntiVir MailGuard, AntiVir WebGuard), которые сообщают об обнаруженных вирусах и вредоносных программах.

Действия Scanner и Guard:

– **Лечить**

Файл будет вылечен.

Эту опцию можно выбрать, если лечение файла возможно.

– **Поместить на карантин**

Файл упаковывается в специальный формат (**.qua*) и перемещается в папку карантина *INFECTED* на Вашем жестком диске, чтобы исключить прямой доступ. Файлы из этой папки могут быть позже вылечены или, в случае необходимости, отправлены компании Avira GmbH.

– **Удалить**

Файл удаляется, но при необходимости может быть восстановлен с помощью соответствующих утилит (например, *Avira UnErase*). Вирусная сигнатура может быть обнаружена повторно. Этот процесс значительно быстрее, чем *переписать и удалить*. При обнаружении установочного вируса удаляется загрузочный сектор. Записывается новый загрузочный сектор.

– **Переписать и удалить**

Файл переписывается, заменяется шаблоном и удаляется. Он не может быть восстановлен.

– **Переименовать**

*переименует файл в *.VIR*. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Файлы могут быть позже вылечены и переименованы обратно.

– **Пропустить**

Avira Premium Security Suite не выполняет дальнейших действий. Инфицированный файл все еще активен в Вашей системе!

Предупреждение
Опасность потери информации и нанесения вреда операционной системе! Используйте опцию *Пропустить* в исключительных случаях.

– **Запретить доступ**

Действия при обнаружении Guard: Доступ к инфицированным файлам блокируется. В файл отчета вносятся данные об обнаружении вируса (если опция включена).

– **Копировать в карантин**

Действия при обнаружении руткит-программы: Вирус копируется в папку Карантина.

– **Завершить программу**

Действия при обнаружении подозрительного процесса: Процесс завершается. Откроется следующее диалоговое окно, в котором Вы можете выбрать, что делать с зараженным файлом.

Действия MailGuard: Входящие письма

– **Поместить на карантин**

Письмо со всеми приложениями помещается на карантин. Инфицированное письмо удаляется. Тело письма и приложения к нему (если есть) заменяются стандартным текстовым шаблоном.

– **Удалить**

Инфицированное письмо удаляется. Тело письма и возможные приложения заменяются стандартным текстовым шаблоном.

– **Удалить приложение**

Инфицированное приложение заменяется стандартным текстовым шаблоном. Если поврежден текст письма, то оно удаляется и заменяется стандартным текстовым шаблоном. Письмо доставляется адресату.

– **Поместить приложение на карантин**

Инфицированное приложение помещается на карантин, а затем удаляется (заменяется стандартным текстовым шаблоном). Текст письма доставляется адресату. Инфицированное приложение может быть позже доставлено адресату из Менеджера карантина.

– **Пропустить**

Инфицированное письмо доставляется адресату.

Предупреждение
Таким образом в Вашу систему могут проникнуть вирусы и вредоносные программы. Выбирайте опцию **Пропустить** в исключительных случаях. Выключите предварительный просмотр в Microsoft Outlook.

Действия MailGuard: Исходящие письма

– **Поместить письмо на карантин (не отправлять)**

Письмо со всеми вложениями помещается на Карантин и не отправляется. Копия письма остается в папке с исходящими письмами. Вы получите на Ваш электронный адрес уведомление об ошибке. При каждой последующей отправке с Вашего адреса письма будут проверяться на вирусы.

– **Блокировать почту (не отправлять)**

Письма не будут отправляться, оставаясь в папке с исходящей корреспонденцией. Вы получите на Ваш электронный адрес уведомление об ошибке. При каждой последующей отправке с Вашего адреса письма будут проверяться на вирусы.

– **Пропустить**

Инфицированное письмо будет отправлено.

Предупреждение
Так вирусы и вредоносные программы могут попасть в компьютер получателя письма.

Действия WebGuard:

– **Запретить доступ**

Запрошенная веб-сервером страница или переданные данные и файлы не будут перенаправлены Вашему браузеру. В окне веб-браузера отображается информация об отказе в доступе.

– **Поместить на карантин**

Запрошенная веб-сервером страница или переданные данные и файлы будут помещены на карантин. Инфицированный файл может быть восстановлен из менеджера карантина, если в этом возникнет необходимость. Его также можно отправить в наш адрес и им займется Центр исследования вредоносных программ.

– **Пропустить**

Запрошенная веб-сервером страница или переданные данные и файлы отправляются модулем WebGuard Вашему веб-браузеру.

Предупреждение
Таким образом в Вашу систему могут проникнуть вирусы и вредоносные программы. Выбирайте опцию **Пропустить** в исключительных случаях.

Примечание
Мы рекомендуем помещать на карантин подозрительные файлы, которые невозможно вылечить.

Примечание
Отправьте нам для проверки файлы, отмеченные эвристикой.
Вы можете загрузить их на наш вэб-сервер:http://www.avira.ru/file-upload
Файлы, обнаруженные эвристикой, отмечены обозначением *HEUR/* или *HEURISTIC/* перед именем файла, напр.: *HEUR/testdatei.**.

5.2.10 Карантин: Обращение с файлами (*.qua) на карантине

Обращение с файлами, помещенными на карантин:

▶ Выберите в Центр контроля раздел **Управление :: Карантин** .

- Проверьте тип файлов, чтобы Вы могли обратно загрузить на Ваш компьютер их оригиналы.

Если Вам необходима более подробная информация:

- Выберите файл и нажмите  . .

→ Появится диалоговое окно *Свойства* с дополнительной информацией о файле.

Если Вы хотите провести повторную проверку файла:

Проверка файла необходима, если файл вирусных сигнатур Avira Premium Security Suite был обновлен и существует подозрение о ложном срабатывании. При повторной проверке Вы можете подтвердить ложное срабатывание и восстановить файл.

- Выберите файл и нажмите  . .

→ При настройке прямого поиска файл проверяется на вирусы и вредоносные программы.

→ После проверки появится диалог *Статистика проверки*, который показывает статистику о состоянии файла перед повторной проверкой и после нее.

Если Вы хотите удалить файл:

- Выберите файл и нажмите  . .

Если Вы хотите отправить файл на вэб-сервер Центр исследования вредоносных программ:

- Отметьте файл, который Вы хотите загрузить.
- Нажмите  . .

→ Откроется диалог с формуляром для Ваших контактных данных.

- Введите полные данные.
- Выберите тип: **Подозрительный файл** или **Ложное срабатывание**.
- Нажмите **OK.**.

→ Заархивированный файл загружается на вэб-сервер Центр исследования вредоносных программ.

Примечание
Проверка Центр исследования вредоносных программ рекомендуется в следующих случаях:
Эвристика (подозрительный файл): При проверке Premium Security Suite распознала файл как подозрительный и отправила его на карантин: В диалоговом окне обнаружения вируса или файла отчета проверки рекомендуется анализ файла Центр исследования вредоносных программ .
Подозрительный файл: Вы определили файл как подозрительный и поэтому поместили его на карантин, однако проверка файла на вирусы говорит об обратном.
Ложное срабатывание: Вы исходите из того, что обнаружение вируса является ложным срабатыванием: Premium Security Suite обнаружила вирус в файле, который с высокой вероятностью не инфицирован.

Примечание
Вы можете отправить незаархивированный файл размером до 20 Мб или заархивированный файл размером до 8 Мб.

Примечание
Вы можете отправить только один файл.

Файлы, помещенные на карантин, могут быть восстановлены:

– см. раздел: Карантин: Восстановление файлов из карантина

5.2.11 Карантин: Восстановление файлов в карантине

В зависимости от операционной системы для восстановления файла доступны различные символы.

– Windows XP и 2000:

 С помощью этого символа Вы восстановите файл в первоначальную папку.

 С помощью этого символа Вы восстановите файл в указанную папку.

– Windows Vista:

В Microsoft Windows Vista через Центр управления доступны ограниченные права, например, для доступа к папкам и файлам. Определенные действия и доступ к файлам доступны через Центр управления при наличии расширенных прав администратора. Расширенные права администратора выдаются профилем поиска при каждом запуске.

 С помощью этого символа Вы восстановите файл в указанную папку.

 С помощью этого символа Вы восстановите файл в первоначальную папку. Если для доступа к папке необходимы расширенные права администратора, то появится соответствующий запрос.

Восстановление файлов из карантина:

Предупреждение
Опасность потери информации и нанесения вреда операционной системе! Используйте функцию *Восстановить выбранный объект* в исключительных случаях. Восстанавливайте только те файлы, которые могут быть вылечены при повторной проверке.

✓ Повторно проверить и вылечить файл.

► Выберите в Центр контроля раздел **Управление :: Карантин** .

Примечание

Письма и приложения могут быть восстановлены при помощи опции  с расширением **.eml*.

Если Вы хотите восстановить файл в его прежнюю папку:

► Отметьте файл и нажмите кнопку с символом (Windows 2000/XP: 

,Windows Vista ).

Эта функция недоступна для электронных писем.

Примечание

Письма и приложения могут быть восстановлены при помощи опции  с расширением **.eml*.

→ Появится вопрос, хотите ли Вы восстановить файл в его прежнюю папку.

▶ Нажмите **Да**

→ Файл будет восстановлен в папку, из которой он был помещен на карантин.

Если Вы хотите восстановить файл в определенную папку:

▶ Выберите файл и нажмите . .

→ Появится вопрос, хотите ли Вы восстановить файл в его прежнюю папку.

▶ Нажмите **Да**

→ Появится стандартное окно выбора папки Windows.

▶ Выберите папку, в которую необходимо восстановить файл, подтвердите выбор.

→ Файл будет восстановлен в указанную папку.

5.2.12 Карантин: Поместить подозрительный файл на карантин

Вы можете поместить подозрительный файл на карантин вручную:

▶ Выберите в Центр контроля раздел **Управление :: Карантин** .

▶ Нажмите . .

→ Появится стандартное окно выбора файлов Windows.

▶ Выберите необходимый файл и подтвердите свой выбор.

→ Файл переместится в папку карантина.

Файлы, помещенные на карантин, могут быть проверены AntiVir Scanner:

- см. раздел : Карантин: Обращение с файлами (*.qua) на карантине

5.2.13 Профиль поиска: Добавить или удалить тип файла из профиля поиска

Определите, какие типы файлов необходимо добавить в проверку или исключить из проверки (возможно при выборе вручную и самоопределяющихся профилях поиска):

✓ Выберите в Центр контроля раздел **Локальная защита ::** *Проверка*.

▶ Щелкните правой кнопкой мыши по профилю поиска, который Вы хотите обработать.

→ Появится контекстное меню.

▶ Выберите строку **Файловый фильтр**.

▶ Разверните контекстное меню, нажав на маленький треугольник на правой стороне контекстного меню.

→ Появятся пункты *По умолчанию*, *Проверить все файлы* и *По выбору*.

▶ Выберите строку **По выбору**.

→ Появится диалоговое окно *Расширения* со списком всех типов файлов, которые будут проверятся через профиль поиска.

Если Вы хотите исключить тип файлов из проверки:

- ▶ Выберите тип файлов и нажмите **Удалить**.

Если Вы хотите добавить тип файлов в проверку:

- ▶ Отметьте тип файлов.
- ▶ Нажмите **Добавить** и введите расширение типа файлов.

  Максимальная длина расширения не может превышать 10 символов, не ставьте точку перед расширением. В качестве заменителей допускаются групповые символы (`*` и `?`) .

5.2.14 Профиль поиска: Создание ярлыка для профиля поиска

Создав ярлык для профиля поиска, Вы можете запускать проверку прямо с рабочего стола, не вызывая Центр контроля от Avira Premium Security Suite.

Создать ярлык к выбранному профилю на рабочем столе:

- ✓ Выберите в Центр контроля раздел **Локальная защита ::** *Проверка*.
- ▶ Выберите профиль поиска, для которого Вы хотите создать ярлык.
- ▶ Выберите символ 
- → Появится ярлык на рабочем столе.

5.2.15 События: Фильтровать события

В Центр контроля в меню **Обзор :: События** отображаются события, созданные программными компонентами Premium Security Suite. (аналогично списку событий Вашей операционной системы Windows). В программные компоненты входят:

- – Программа обновлений
- – Guard
- – MailGuard
- – Scanner
- – Планировщик
- – Firewall

Отображаются следующие типы событий:

- – Информация
- – Предупреждение
- – Ошибка
- – Обнаружение

Фильтрация отображаемых событий:

- ▶ Выберите в Центр контроля раздел **Обзор :: События** .
- ▶ Отметьте флажком программные компоненты, чтобы отобразить события активных компонентов.

  - ИЛИ -

  Снимите флажок с программных компонентов, чтобы скрыть события деактивированных компонентов.

- ▶ Отметьте флажком типы событий, чтобы отобразить их.

  - ИЛИ -

Снимите флажок с типов событий, которые необходимо скрыть.

5.2.16 MailGuard: Исключить адреса из проверки

Вы можете составить список адресов (отправитель), которые необходимо исключить из проверки модулем MailGuard (белый список):

- ▶ Выберите в Центре управления раздел **Онлайн-защита :: MailGuard**.
- → В списке Вы увидите входящие письма.
- ▶ Отметьте письма, которые Вы хотите исключить из проверки MailGuard.
- ▶ Нажмите на необходимый символ, чтобы исключить письмо из проверки MailGuard.

   Выделенный Email в дальнейшем не будет проверяться на наличие вирусов и вредоносных программ.

   Выделенный адрес в дальнейшем не будет проверяться на наличие спама.

→ Выделенный адрес в электронном письме вносится в список исключений в дальнейшем не будет проверяться на наличие вирусов и вредоносных программ или спама.

Предупреждение
Поэтому исключайте из проверки MailGuard только надежные адреса.

Примечание
В конфигурации MailGuard :: Общее :: Исключения Вы можете внести дополнительные адреса в список исключений или удалить оттуда адреса.

5.2.17 MailGuard: Тренировать модуль Антиспам

Модуль Антиспам содержит учебную базу данных. В этой базе данных находятся Ваши критерии разделения на категории. Таким образом со временем можно установить внутренние фильтры, алгоритмы и критерии оценки для спама на основании Ваших личных критериев.

Сортировка электронных писем для учебной базы данных:

- ▶ Выберите в Центре управления раздел **Онлайн-защита :: MailGuard**.
- → В списке Вы увидите входящие письма.
- ▶ Отметьте письма, которые Вы хотите сортировать.
- ▶ Нажмите на необходимый символ, чтобы отметить письмо, например, как спам  или как "хорошее" письмо 

→ Письмо будет сохранено в учебной базе данных и в следующий раз будет использовано для распознавания спама.

Примечание
Вы можете отменить учебную базу данных здесь: MailGuard :: Общее :: Удалить антиспам.

5.2.18 Firewall: Выбрать уровень безопасности для Firewall

Вы можете выбрать уровень безопасности. В зависимости от этого у Вас появятся различные возможности конфигурации для правил адаптера.

Доступны следующие уровни безопасности:

- **Низкий**
- Распознается сканирование портов и флудинг.
- **Средний**
- Запрещаются подозрительные TCP- и UDP-пакеты.
- Предотвращается сканирование портов и флудинг.
- **Высокий**
- Компьютер невидим в сети.
- Блокируются соединения из вне.
- Предотвращается сканирование портов и флудинг.
- **Пользовательский**
- Правила, установленные пользователем: Программа автоматически переключается на этот режим, если Вы изменили правила адаптера.

Примечание
Стандартная настройка уровня безопасности для всех предопределенных правил Avira Firewall - **Высокий**.

Для Firewall можно установить следующие уровни безопасности:

▶ Выберите в Центр контроля раздел **Защита :: Брандмауэр**.

▶ Установите ползунковый регулятор на необходимый уровень безопасности.

→ Уровень безопасности становится активным.

5.2.19 Резервирование: Создание резервной копии вручную

С помощью инструмента резервирования в Центр контроля Вы можете быстро и просто создать резервную копию своих личных файлов. Резервирование Avira поможет создать т.н. зеркалирование, позволяющее сохранять текущее состояние Ваших данных, не загружая ресурсы. При резервировании с помощью модуля Резервирование Avira резервируемые данные проверяются на вирусы. Инфицированные файлы не сохраняются.

Примечание
Зеркальное обновление в отличие от регулярного не создает различных версий файла резервной копии. Зеркалирование сохраняет состояние файлов на момент последнего резервирования. Если некоторые файлы больше не требуется резервировать, при следующем резервировании не происходит выравнивания, т.е. старые версии ранее сохраненных файлов не удаляются.

Примечание
Резервирование Avira со стандартными установками добавляет в резерв только измененные файлы, проверяя их при этом на вирусы и вредоносное ПО. Вы можете изменять эту настройку здесь: Резервирование::Установки.

Так можно создать резервную копию при помощи инструмента резервирования:

- Выберите в Центр контроля раздел **Инструменты ::Резервирование**.

→ Появятся предустановленные профили резервирования.

- Выберите один из предустановленных профилей резервирования.

  - ИЛИ -

- Примените профиль резервирования *Выбор вручную*.

  - ИЛИ -

- Создайте новый профиль резервирования.
- Для выбранного профиля в поле *Целевая папка* задайте место хранения.

  Вы можете указать в качестве папки для резервирования папку на Вашем компьютере, сетевой диск или сменный носитель, например, USB.

- Выберите символ . .

→ Появится диалоговое окно *Резервирование Avira*, запустится резервирование. Состояние и результаты резервирования отобразятся в окне резервирования.

Если Вы хотите запустить профиль резервирования.

- В поисковом профиле *Выбор вручную* разверните дерево каталогов настолько, чтобы были открыты все дисководы и папки, для которых Вы хотите создать резервные копии:
  - Нажмите на значок +. Отобразится следующий уровень каталогов.
  - Нажмите на значок -: Следующий уровень каталогов будет скрыт.
- Отметьте узлы и папки, для которых Вы создаете резервную копию, поставив флажок в соответствующем поле:

  Существует несколько способов выбора папок:
  - Каталог с подкаталогами (черный флажок)
  - Каталог без подкаталогов (зеленый флажок)
  - Только подкаталоги в каталоге (серый флажок, у подкаталогов флажок черный)
  - Не выделять (галочка отсутствует)

Если Вы хотите создать новый профиль резервирования.

- Выберите символ . **Добавление нового профиля**

→ Среди имеющихся профилей появится новый *Новый профиль*.

- При необходимости переименуйте профиль резервирования, нажав на символ .
- Отметьте узлы и папки, для которых Вы создаете резервную копию, поставив флажок в соответствующем поле.

  Существует несколько способов выбора папок:
  - Каталог с подкаталогами (черный флажок)
  - Каталог без подкаталогов (зеленый флажок)
  - Только подкаталоги в каталоге (серый флажок, у подкаталогов флажок черный)
  - Не выделять (галочка отсутствует)

5.2.20 Резервирование: Автоматическое создание резервных копий

Вы определяете задачу, с помощью которой Вы устанавливаете автоматическое создание резервных копий файлов:

- ▶ Выберите в Центр контроля разделе **Управление ::Планировщик**.
- ▶ Выберите символ  . .
- ↪ Появится диалоговое окно *Имя и описание задачи*.
- ▶ Введите имя и описание задачи.
- ▶ Нажмите **Далее**.
- ↪ Появится диалоговое окно *Тип задачи*.
- ▶ Выберите строку **Задача резервирования**.
- ▶ Нажмите **Далее**.
- ↪ Появится диалоговое окно *Выбор профиля*.
- ▶ Выберите профиль для проверки.

Примечание
Отобразятся профили резервирования, для которых задавалась папка резервирования.

- ▶ Нажмите **Далее**.
- ↪ Появится диалоговое окно *Время выполнения задачи*.
- ▶ Выберите время проведения проверки.
  - **Немедленно**
  - **Ежедневно**
  - **Еженедельно**
  - **Интервал**
  - **Однажды**
  - **Логин**
  - **Plug&Play**

    При событии Plug&Play резервирование происходит тогда, когда сменный носитель, выбранный в качестве хранилища профиля резервирования, подключается к компьютеру. Для события Plug&Play необходимо, чтобы в качестве места хранения резервной копии было указано USB-устройство.
- ▶ В зависимости от выбора задайте время.
- ▶ При необходимости выберите дополнительную опцию из следующих (в зависимости от типа задачи):
  - **Повторно запускать задачу, если определенное для нее время прошло:**

    Выполняются задачи, срок выполнения которых уже прошел, но они не могли быть запущены в назначенное время, например, если компьютер был выключен.
- ▶ Нажмите **Далее**.
- ↪ Появится диалоговое окно *Выбор режима отображения*.
- ▶ Выберите режим отображения задачи:
  - **Минимизировано:** только прогресс выполнения

- **Максимизировано:** все окно резервирования.
- **Скрытый режим**: нет окна резервирования.

▶ Нажмите кнопку **Готово**.

→ Новое установленное задание будет отмечено галочкой как активированное на стартовой странице раздела *Управление :: Планировщик*.

▶ Деактивируйте задачи, которые не должны выполняться.

Используя следующие символы, Вы можете обработать задания:

 Просмотреть свойства каждого задания

 Изменение задачи

 Удаление задачи

 Запустить задачу

 Остановить задачу

6 Scanner

С помощью Scanner Вы можете проводить проверку на вирусы и вредоносные программы (прямая проверка). Существует несколько способов проведения проверки на вирусы:

- **Проверка через контекстное меню**
  Проверка через контекстное меню (правая кнопка - пункт **Проверить выбранные файлы с помощью AntiVir**) рекомендуется, если Вы, например, хотите проверить отдельные файлы и папки в проводнике Windows. Другое преимущество заключается в том, что для проверки через контекстное меню нет необходимости сначала запускать Avira Premium Security Suite Центр контроля.
- **Проверка с помощью Drag & Drop**
  Перетащите файл или папку в программное окно Avira Premium Security Suite Центр контроля, и будет осуществлена Scanner этого файла или папки со всем содержимым. Эта процедура рекомендуется, если Вы хотите проверить отдельные файлы и папки, которые, например, находятся на Вашем рабочем столе.
- Проверка через профиль
  Эта процедура рекомендуется, если Вы хотите проверить отдельные файлы и папки, которые, например, находятся на Вашем рабочем столе. Вы не должны выбирать эти папки и диски перед каждой проверкой.
- **Прямая проверка через Планировщик**
  Планировщик дает возможность провести проверку в установленное время.

При поиске программ-руткитзагрузочных вирусов и при проверке активных процессов необходимы специальные методы. Вы располагаете следующими опциями настройки:

- Поиск руткит-программ через профиль поиска *Поиск руткит-программ*
- Проверка активных процессов через профиль поиска **Активные процессы**
- Поиск загрузочных вирусов через команду **Проверка загрузочных записей** в меню **Сервис**

7 Обновления

Эффективность антивирусного ПО напрямую зависит от актуальности состояния программы, особенно VDF-файла и движка. Для выполнения обновления в Premium Security Suite встроен компонент Программа обновлений. Программа обновлений обеспечивает, чтобы Avira Premium Security Suite находилась постоянно на самом современном уровне и была в состоянии, обнаруживать ежедневно новые вирусы. Программа обновлений актуализирует следующие компоненты:

- VDF-файл:

  VDF-файл содержит образцы вредоносных кодов, используемых Premium Security Suite при проверке на вирусы или лечении файлов.

- Поисковый движок:

  Поисковый движок Premium Security Suite применяет различные методы обнаружения вирусов.

- Программные файлы (Обновление продукта):

  Пакеты обновлений продукта предоставляют в распоряжение отдельные программные компоненты.

При выполнении обновлений актуализируется VDF-файл и поисковый движок. В зависимости от настроек Программа обновлений дополнительно выполняет обновление продукта или сообщает о доступных для загрузки обновлениях. После обновления Premium Security Suite необходима перезагрузка.

Примечание
Из соображения безопасности Программа обновлений проверяет, был ли изменен хост-файл Windows так, что ссылка для обновления Avira Premium Security Suite была заменена на ложную, чтобы Программа обновлений перенаправлялась бы на чужую страницу. Если хост-файл Windows был изменен, Программа обновлений поместит информацию об этом в файл отчета.

В Центр контроля / Планировщик Вы можете создавать задачи обновления, которые Программа обновлений выполняет в определенные интервалы. По умолчанию после установки Premium Security Suite создана задача обновления. У Вас есть возможность вручную запустить обновление:

- В Центр контроля: В меню Обновление и разделе Статус
- С помощью контекстного меню значка в трее

Вы закачиваете обновления из интернет с веб-сервера разработчика. По умолчанию используется существующее сетевое соединение с сервером Avira GmbH. Здесь Вы можете определить стандартную установку Avira Premium Security Suite. Настройка: Общее :: Обновление

8 Avira Firewall :: Обзор

Avira Firewall контролирует и регулирует входящий и исходящий обмен данными Вашей системы и защищает ее от атак и угроз из Интернет: На основании правил безопасности разрешается или запрещается входящий и исходящий обмен данными или прослушивание порта. Если Avira Firewall запрещает сетевую активность и блокирует сетевое соединение, то Вы получите уведомление в виде всплывающего окна. Вы можете настроить Avira Firewall следующими способами:

- через установку уровня безопасности в Центр контроля

  В Центр контроля Вы можете устанавливать уровень безопасности. Уровень безопасности *Низкий*, *Средний* и *Высокий* охватывают несколько дополняющих друг друга правил безопасности, основанных на фильтрах пакетов. Правила безопасности устанавливаются как предустановленные правила адаптера в Avira Premium Security Suite. Настройка в Firewall::Правила адаптера.

- сохранением действий в окне Сетевое событие

  Если приложение будет устанавливать сетевое или Интернет-соединение, то появится всплывающее окно *Сетевое событие*. В окне *Сетевое событие* пользователь может выбрать, разрешить сетевую активность приложению или запретить. Если опция **Сохранять действие для приложения** включена, то действие определяется как правило приложения и устанавливается в настройках Firewall::Определить правила приложения. При сохранении действий в окне Сетевое событие у Вас появится набор правил для сетевой активности приложений.

Примечание
Приложениям надежных производителей сетевой доступ разрешается по умолчанию, правило адаптера запрещает доступ к сети. Вы можете удалить производителя из списка надежных разработчиков.

- создав правила адаптера и приложений в Avira Premium Security Suite. Настройка

  В Avira Premium Security Suite. Настройка Вы можете изменить предустановленные правила адаптера или установить новые. Уровень безопасности Firewall автоматически устанавливает значение *Пользователь*, если Вы добавляете или изменяете правила адаптера.
  С помощью правил приложения Вы можете определить правила мониторинга, рассчитанные для приложений:
  С помощью простых правил приложений Вы можете установить, запретить или разрешить сетевую активность приложению программы или управлять ими интерактивно при помощи всплывающего окна *Сетевое событие* .
  В расширенной конфигурации раздела *Правила приложения* Вы можете определить различные фильтры пакетов для приложения, которые определены специально для правил приложения.

Примечание
В правилах приложения различают два режима: *Привилегированные* и *Отфильтрованные*. Для правил приложения в режиме *Отфильтрованные* наивысшим приоритетом наделяются соответствующие правила адаптера, т.е. соответствующее правило адаптера выполняется после правила приложения. Возможно, что доступ к сети разрешенных приложений вследствие высокого уровня защиты или соответствующего правила адаптера будет запрещен. При правилах приложения в режиме *Привилегированные* правила адаптера игнорируются. Если приложения в режиме *Привилегированные* разрешено, то доступ приложения к сети в любом случае разрешается.

9 Резервирование

У Вас есть различные возможности создать резервную копию Ваших файлов:

С помощью инструмента резервирования

С помощью этого инструмента Вы можете выбрать профиль резервирования или создать новый для резервирования.

С помощью задачи резервирования модуля Планировщик

Планировщик дает возможность создавать временные или реагирующие на событие задачи резервирования. Планировщик автоматически выполняет задачи резервирования. Эта технология удобна, если Вам необходимо резервировать определенные файлы регулярно.

10 FAQ, советы

Здесь Вы найдете часто задаваемые вопросы об Avira Premium Security Suite, справку по проблемам, советы и рекомендации по работе с Avira Premium Security Suite.

См. главу Помощь в сложных случаях

См. главу Горячие клавиши

См. главу Центр безопасности Windows

10.1 Помощь в случае возникновения проблем

Здесь Вы найдете информацию о причинах возникновения и способах решения возможных проблем.

- Появляется уведомление об ошибке *открытия файла лицензии*.
- AntiVir MailGuard отключена.
- В виртуальной машине невозможно воспользоваться сетевым окружением, если Avira Firewall установлен на Вашей базовой ОС, а уровень безопасности Avira Firewall установлен как средний или высокий.
- VPN-соединение блокируется, если уровень безопасности Avira Firewall установлен как средний или высокий.
- Письмо, отправленное через TSL-соединение, было заблокировано MailGuard.
- Не работает чат: не отображаются сообщения пользователей чата

Появляется сообщение о том, что *файл лицензии не открывается*.

Причина: файл зашифрован.

▶ Для активации лицензии Вы не должны открывать файл. Достаточно сохранить его в программной директории Avira Premium Security Suite.

При попытке запустить обновление появляется сообщение о том, что *соединение было разорвано при загрузке файла ….*

Причина: Ваше Интернет-соединение неактивно. Поэтому Avira Premium Security Suite не может найти веб-сервер в Интернет.

▶ Проверьте, работают ли другие Интернет-службы (напр., WWW или Email). Если они не работают, восстановите интернет-соединение.

Причина: Прокси-сервер недоступен.

▶ Проверьте, не изменился ли логин для регистрации на прокси-сервере, установите в случае необходимости Ваши настройки.

Причина: файл update.exe блокируется Вашим персональным межсетевым экраном.

▶ Убедитесь в том, что файл update.exe не блокируется Вашим персональным межсетевым экраном.

Иначе:

▶ Проверьте в Avira Premium Security Suite. Настройка (Режим эксперта) Ваши настройки в пункте Общее :: Обновить.

Вирусы и вредоносные программы невозможно удалить или переместить.

Причина: Файл загружается Windows и находится в активном состоянии.

▶ Обновите Avira Premium Security Suite.

▶ Если Вы используете операционную систему Windows XP, отключите восстановление системы.

▶ Запустите компьютер в безопасном режиме.

▶ Запустите Avira Premium Security Suite и Avira Premium Security Suite. Настройка (Режим эксперта).

▶ Выберите Scanner :: Поиск :: Файлы:: Все файлы и закройте окно с помощью кнопки **ОК**.

▶ Запустите проверку всех локальных дисков.

▶ Запустите компьютер в нормальном режиме.

▶ Проверьте систему в нормальном режиме.

▶ Если другие вирусы не обнаружены, включите восстановление системы, если Вы им пользуетесь.

Иконка показывает, что программа отключена.

Причина: AntiVir Guard отключена.

▶ В Центр контроля в разделе Обзор :: Статус в поле AntiVir Guard щелкните по ссылке **Активировать**.

Причина: AntiVir Guard блокируется межсетевым экраном.

▶ Установите в настройках Вашего файрвола разрешение для AntiVir Guard. AntiVir Guard функционирует только с адресом 127.0.0.1 (local host). Не устанавливается соединение с Интернет. Это действует и применительно к AntiVir MailGuard.

Иначе:

▶ Проверьте способ запуска службы AntiVir Guard. Запустите службу: Выберите на панели задач "Пуск | Настройка | Панель управления". Запустите ярлык "Службы" (в Windows 2000 и Windows XP он находится в поддиректории "Администрирование"). Найдите строку "Avira AntiVir Guard". Должен быть определен тип запуска "Авто" и состояние "Работает" Запустите службу вручную. Выбрав соответствующую строку, нажмите кнопку "Пуск" При возникновении уведомления об ошибке проверьте его. Если возникает сообщение об ошибке, проверьте то, что предложено системой.

Компьютер работает очень медленно, когда я выполняю резервное копирование данных.

Причина: AntiVir Guard проверяет во время процесса резервного копирования все файлы, с которыми работает backup система.

▶ Выберите в Avira Premium Security Suite. Настройка (Режим эксперта) Guard :: Поиск:: Исключения и добавьте в список объектов, исключенных из проверки, программу резервного копирования данных.

Мой брандмауэр сообщает об AntiVir Guardи о программе AntiVir MailGuard, как только они становятся активными.

Причина: Соединение с программой AntiVir Guard и AntiVir MailGuard производится через протокол TCP/IP. Брандмауэр отслеживает все соединения, производящиеся по этому протоколу.

▶ Установите разрешение для AntiVir Guard и программы AntiVir MailGuard. AntiVir Guard функционирует только с адресом 127.0.0.1 (local host). Не устанавливается соединение с Интернет. Это действует и применительно к AntiVir MailGuard.

AntiVir MailGuard отключена.

Проверьте работоспособность программы AntiVir MailGuard по контрольной таблице, если возникают проблемы со службами AntiVir MailGuard.

Контрольная таблица

▶ Проверьте, связывается ли Ваш почтовый клиент с сервером через IMAP. Этот протокол в настоящее время не поддерживается.

▶ Проверьте, связывается ли почтовый клиент с сервером через Kerberos, APOP или RPA. Эти методы аутентификации в настоящее время не поддерживаются.

▶ Проверьте, регистрируется ли Ваш почтовый клиент на сервере через SSL (часто его называют TSL - Transport Layer Security). AntiVir MailGuard поддерживает SSL, но без проверки зашифрованных писем на наличие вирусов и вредоносных программ. Причиной тому является тот факт, что соединение производится через порт 995, а не через обычный для POP3 порт 110. Часто этот порт называется "альтернативным". Большинство почтовых серверов поддерживают SSL и через этот порт.

▶ Включена ли AntiVir MailGuard (служба)? Запустите службу: Выберите на панели задач "Пуск | Настройка | Панель управления". Запустите ярлык "Службы" (в Windows 2000 и Windows XP он находится в поддиректории "Администрирование"). Найдите строку "Avira AntiVir MailGuard". Должен быть определен тип запуска "Авто" и состояние "Работает" Запустите службу вручную. Выбрав соответствующую строку, нажмите кнопку "Пуск" При возникновении уведомления об ошибке проверьте его. Если возникает сообщение об ошибке, проверьте то, что предложено системой. Если возникает сообщение об ошибке, проверьте список событий. Если не удалось исправить положение, необходимо полностью удалить Avira Premium Security Suite через "Пуск | Настройка | Панель управления | Установка и удаление программ", перезагрузить компьютер и вновь установить Avira Premium Security Suite.

Общее

▶ AntiVir MailGuard в настоящее время не поддерживает IMAP (Internet Message Access Protocol). Если Ваша почтовая программа использует этот протокол для связи с почтовым сервером, Вы не защищены от вирусов и вредоносных программ.

▶ Зашифрованные с помошью SSL (Secure Sockets Layer) POP3 соединения (часто называемые также TLS (Transport Layer Security) не могут быть защищены и будут игнорироваться.

- Аутентификация на почтовом сервере возможна только с помощью "пароля". "Kerberos" и "RPA" в настоящее время не поддерживаются.
- Avira Premium Security Suite не проверяет письма на наличие в них вирусов и вредоносных программ.

Примечание
Мы рекомендуем Вам регулярно производить обновление продуктов Microsoft для того, чтобы закрыть возможные бреши в безопасности.

В виртуальной машине недоступно сетевое окружение, если Avira Firewall установлен на базовой ОС, а уровень безопасности Avira Firewall определен как средний или высокий.

Если Avira Firewall установлен на компьютере, на котором также работает виртуальная машина (например, VMWare, Virtual PC и т.п.), система блокирует все сетевые окружения виртуальной машины, если уровень безопасности Avira Firewall определен как средний или высокий. При установленном низком уровне безопасности Firewall работает в нормальном режиме.

Причина: Виртуальная машина эмулирует программными средствами сетевую карту. С помощью такой эмуляции пакеты данных гостевой системы собираются в специальный UDP-пакет и переправляются через внешний шлюз обратно к хост-системе. Avira Firewall блокирует эти входящие пакеты при уровне безопасности от среднего и выше.

Чтобы этого избежать, проделайте следующее:

- Выберите в Центр контроля раздел **Онлайн-защита :: Firewall**.
- Воспользуйтесь ссылкой **Настройка**.
- Отображается диалоговое окно *Avira Premium Security Suite. Настройка*. Вы находитесь в разделе настройки *правил приложений*.
- Включите **Экспертный режим**.
- Выберите раздел настроек **Правила адаптера**.
- Нажмите кнопку **Добавить**.
- Выберите во *Входящих правилах* **UDP**.
- Укажите имя правила в поле **Имя**.
- Нажмите кнопку **OK**.
- Проверьте, расположено ли данное правило над правилом **Запрещать все IP-пакеты**.

Предупреждение
Это правило является потенциально опасным, так как оно принципиально разрешает UDP-пакеты. Вернитесь после работы с виртуальной машиной к исходным настройкам.

VPN-соединение блокируется, если уровень безопасности Avira Firewall определен как средний или высокий.

Причина: Проблема заключается в последнем правиле в цепочке **Запрещать все IP-пакеты**. Правило вступает в силу, если пакет не соответствует ни одному из расположенных выше правил. Отправленные через VPN-софт пакеты проверяются на соответствие этим правилам, так как на основании их типов (т.н. GRE-пакеты) они не подходят под другие категории.

Замените правило **Запрещать все IP-пакеты** двумя новыми правилами, регулирующими прохождение TCP- и UDP-пакетов. Таким образом, есть возможность, что допускаются также пакеты, проходящие по другим протоколам.

Письмо, отправленное через TSL-соединение, было заблокировано MailGuard.

Причина: Transport Layer Security (TLS: зашифрованный протокол передачи данных в интернет) не поддерживается MailGuard. У Вас есть несколько возможностей отправить письмо:

- Используйте другой порт, но не используемый SMTP порт 25. Так Вы сможете избежать проверки модулем MailGuard
- Откажитесь от защищенного TSL-соединения и отключите поддержку TSL в Вашем почтовом клиенте.
- Отключите проверку исходящих писем с помощью MailGuard в настройках MailGuard::Поиск

Не работает чат: не отображаются сообщения пользователей чата, браузер загружает данные.

Этот феномен может возникать в чатах, работающих по HTTP-протоколу с 'transfer-encoding= chunked'.

Причина: WebGuard проверяет данные на вирусы до того, как они будут загружены веб-браузером. В процессе передачи данных с ’transfer-encoding= chunked' WebGuard не может определить длину сообщений или объем данных.

- Укажите в настройках URL чата для исключения его из проверки (см. Avira Premium Security Suite. Настройка: WebGuard::Исключения).

10.2 Горячие клавиши

Горячие клавиши дают возможность использовать альтернативную навигацию по Avira Premium Security Suite, вызывать отдельные модули и запускать действия.

Ниже приводится список команд (горячие клавиши), доступных в Avira Premium Security Suite. Подробную информацию о функциях Вы найдете в соответствующих разделах справочной системы.

10.2.1 В диалоговых полях

Горячие клавиши	Описание
Ctrl + Tab Ctrl + Page Down	Перейти к следующему разделу.
Ctrl + Shift + Tab Ctrl + Page up	Перейти к предыдущему разделу.
Tab	Переход к следующей опции / группе опций.
Shift + Tab	Переход к предыдущей опции / группе опций.
← ↑ → ↓	Переключение между опциями в списке или в одной группе опций.
Пробел	Включение / выключение опции, обозначенной чек-боксом (поле с галочкой).
Alt + подчеркнутая буква	Выбор опции или выполнение команды.
Alt + ↓ F4	Открывает раскрывающийся список.
Esc	Закрывает раскрывающийся список. Отмена команды и закрытие окна.
Enter	Выполнение команды активной опции или кнопки.

10.2.2 В справке

Горячие клавиши	Описание
Alt + Пробел	Отображение системного меню.
Alt + Tab	Переключение между открытыми окнами.
Alt + F4	Закрытие окна.
Shift + F10	Отображение контекстного меню справки.
Ctrl + Tab	Перейти к следующему разделу в навигационном окне.
Ctrl + Shift + Tab	Перейти к предыдущему разделу в навигационном окне.
Page up	Переход к теме, расположенной в содержании или списке выше текущей.
Page down	Переход к теме, расположенной в содержании или списке ниже текущей.
F6	Переключение между окнами навигации и тематическими окнами.
Page up	Перемещение внутри темы.

Page down	

10.2.3 В Центр контроля

Общее

Горячие клавиши	Описание
F1	Вызов Справки
Alt + F4	Закрытие Центр контроля
F5	Обновить вид
F8	Открыть меню настройки
F9	Запустить обновление

Вкладка Проверка

Горячие клавиши	Описание
F2	Переименование выбранного профиля
F3	Запуск проверки с выбранным профилем
F4	Создание ярлыка на рабочем столе для выбранного профиля
Ins	Добавление нового профиля
Del	Удаление выбранного профиля

Вкладка Firewall

Горячие клавиши	Описание
Enter	Свойства

Раздел Карантин

Горячие клавиши	Описание
F2	Повторная проверка объекта
F3	Восстановление объекта
F4	Отправка объекта
F6	Восстановление объекта в...
Enter	Свойства
Ins	Добавление файла
Del	Удаление объекта

Вкладка Планировщик

Горячие клавиши	Описание
F2	Изменение задачи
Enter	Свойства
Ins	Добавление новой задачи
Del	Удаление задачи

Раздел Отчет

Горячие клавиши	Описание
F3	Показать файл отчета
F4	Печать файла отчета
Enter	Отображение отчета
Del	Удаление отчета(ов)

Вкладка События

Горячие клавиши	Описание
F3	Экспортировать событие(я)
Enter	Показать событие
Del	Удалить событие(я)

10.3 Центр безопасности Windows XP

- от Windows XP SP 2 -

10.3.1 Общее

Центр безопасности Windows проверяет статус компьютера применительно к аспектам безопасности.

Если обнаруживается проблема в одном из этих важных пунктов (напр., антивирусные базы устарели), Центр Управления отправляет уведомление об этом и дает рекомендации для более качественной организации защиты системы.

10.3.2 Центр безопасности Windows и Avira Premium Security Suite

Брандмауэр

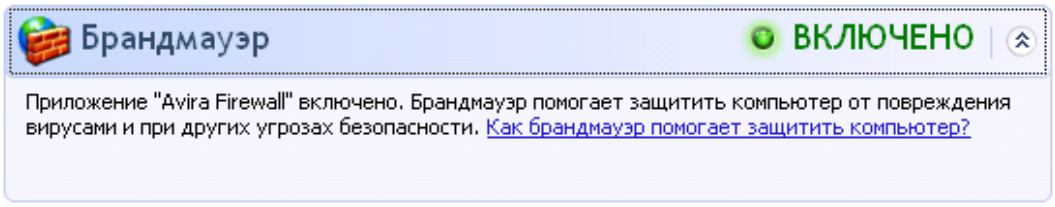
Вы можете получить следующую информацию от Центра обеспечения безопасности со ссылкой на свой брандмауэр:

- Брандмауэр АКТИВИРОВАН / Брандмауэр включен

– Брандмауэр ДЕАКТИВИРОВАН / Брандмауэр выключен

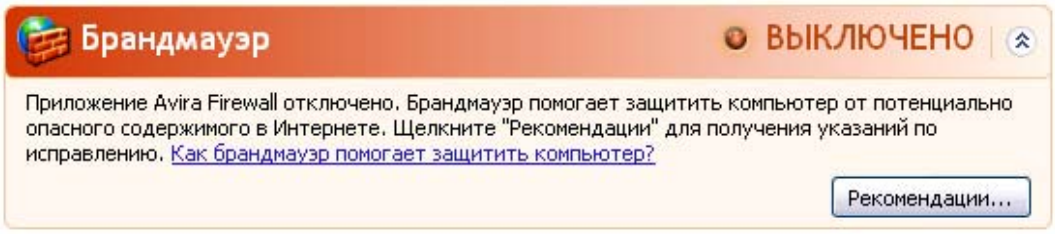
Брандмауэр АКТИВИРОВАН / Брандмауэр выключен

После установки Avira Premium Security Suite и отключения брандмауэра Windows Вы получите следующее уведомление:



Брандмауэр ДЕАКТИВИРОВАН / Брандмауэр выключен

Вы получите следующее сообщение, если отключите Avira Firewall:



Примечание
Вы можете включить или отключить Avira Firewall через вкладку Статус в разделе Avira Premium Security Suite Центр контроля.

Предупреждение
Если Вы отключили Avira Firewall, Ваш компьютер больше не защищен от неавторизованного доступа по ЛВС или через Интернет.

Антивирусное ПО / Защита от вредоносных программ

Вы можете получить от Центра Управления следующую информацию, касающуюся защиты от вирусов.

Антивирусных программ НЕ ОБНАРУЖЕНО

Антивирусные базы УСТАРЕЛИ

Защита от вирусов ВКЛЮЧЕНА

Защита от вирусов ВЫКЛЮЧЕНА

Защита от вирусов НЕ КОНТРОЛИРУЕТСЯ

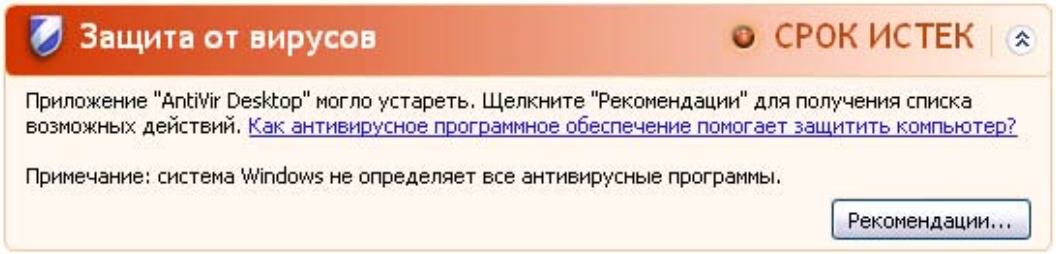
Защита от вирусов НЕ ОБНАРУЖЕНА

Это сообщение отправляется Центром обеспечения безопасности Windows, если на компьютере не было обнаружено антивирусных программ.

Примечание
Установите Avira Premium Security Suite на Ваш компьютер для того, чтобы защитить его от вирусов и иных вредоносных программ.

Антивирусные базы УСТАРЕЛИ

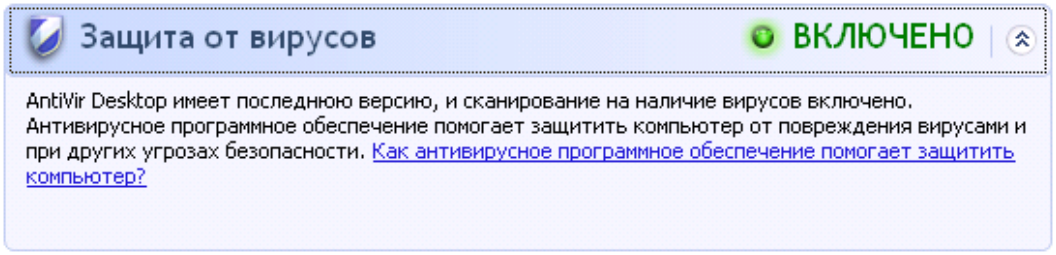
Если Вы уже установили Windows XP Service Pack 2 или Windows Vista, а теперь устанавливаете Avira Premium Security Suite, в процессе установки Вы получите следующее сообщение:



Примечание
Чтобы Центр обеспечения безопасности Windows посчитал Avira Premium Security Suite актуальным, после установке программы обязательно необходимо произвести обновление. Вы можете актуализировать Вашу систему, произведя Обновление Avira Premium Security Suite.

Защита от вирусов ВКЛЮЧЕНА

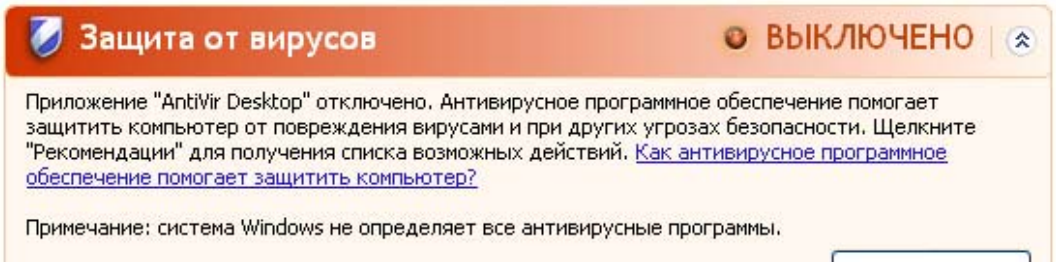
После установки Avira Premium Security Suite и последующего за ней обновления программы Вы получаете следующую информацию:



Avira Premium Security Suite теперь находится в актуальном состоянии, а AntiVir Guard включена.

Защита от вирусов ОТКЛЮЧЕНА

Следующее уведомление Вы получите, если AntiVir Guard будет отключена или служба Guard будет остановлена.



Примечание
Вы можете включить или отключить AntiVir Guard в разделе Обзор :: Статус Avira Premium Security Suite Центр контроля. Если AntiVir Guard включен, на панели задач появится открытый красный зонтик.

Защита от вирусов НЕ КОНТРОЛИРУЕТСЯ

Если Вы получите следующую информацию от Центра обеспечения безопасности Windows, значит Вы решили самостоятельно контролировать Ваше антивирусное ПО.

Примечание
Функция Windows Vista не поддерживается.

Примечание
Центр обеспечения безопасности Windows поддерживается Avira Premium Security Suite. Вы можете включить эту опцию в любое время с помощью кнопки "Рекомендации...".

Примечание
Даже если Вы установили на Вашей системе Windows XP Service Pack 2 или Windows Vista, Вам все же требуется антивирусная система, например, Avira Premium Security Suite. Хотя Windows XP SP 2 контролирует Ваше антивирусное ПО, Центр обеспечения безопасности Windows не имеет функций антивирусной защиты. Без дополнительных специальных средств защиты от вирусов Ваша система не защищена.

11 Вирусы и другое

11.1 Дополнительные категории угроз

Программы дозвона на платные номера (DIALER)

Определенные услуги, предлагаемые в Интернет, являются платными. Оплата в Германии осуществляется через программы коммутируемого доступа с номерами 0190/0900 (в Австрии и Швейцарии через номера 09x0; в Германии среднесрочно устанавливается на 09x0). Будучи установленными на Вашем компьютере, программы-дайлеры устанавливают соединения с абонентами, имеющими коммерческие номера, звонки на которые тарифицируются по премиум-разряду.

Предоставление online-контента с выставлением телефонного счета является законным и может быть полезно пользователям. Качественные дайлеры работают так, что пользователь всегда отдает себе отчет в том, какими услугами он пользуется и сколько за них платит. Они устанавливаются на компьютер только в том случае, если пользователь дает на это свое согласие. Факт согласия должен быть однозначно и четко определен. Установление соединения программ-дайлеров отображается корректно. Кроме того, надежные дайлеры четко информируют о размере суммы.

К сожалению, существуют дайлеры, которые с целью обмана незаметно устанавливаются на компьютеры. Они заменяют, например, стандартное соединение через модем пользователя интернет на ISP (Internet-Service-Provider) и при каждом соединении вызывают дорогостоящие номера 0190/0900. Только при следующем телефонном счете пользователь замечает, что программа-дайлер 0190/0900 на его компьютере при каждом подключении к интернет набирал номера-премиум, что привело к соответствующим счетам.

Для качественной защиты от нежелательных дайлеров, мы рекомендуем поместить используемые ими номера в черный список.

По умолчанию Avira Premium Security Suite обнаруживает наиболее распространенные программы-дайлеры.

Если в настройках в разделе Дополнительные категории угроз включена опция **Программы дозвона на платные номера (DIALER)**, Вы получите уведомление об обнаружении активности такой программы. Теперь у Вас появляется возможность, легко удалять нежелательные программы дозвона. Если Вы все же хотите использовать какую-либо программу дозвона, поместите ее в список, исключаемых из проверки объектов.

Игры (GAMES)

Мы совсем не против компьютерных игр, но совсем не обязательно играть в них в рабочее время (может быть, исключая обеденные перерывы). Тем не менее, многие сотрудники посвящают массу своего рабочего времени различным компьютерным играм и развлечениям. Через Интернет можно загрузить целую массу игр. Существует огромное количество игр по электронной почте: Популярны различные игры от шахмат до "морского боя": Игры отправляются партнеру по электронной почте, затем партнер должен ответить на письмо.

Исследования показали, что совокупное время, потраченное сотрудниками на игры, достигло в денежном выражении довольно внушительной величины. Поэтому совершенно понятно стремление все большего числа работодателей оградить рабочие станции от игрового и развлекательного ПО.

Avira Premium Security Suite обнаруживает компьютерные игры. Если в настройках в разделе Дополнительные категории угроз включена опция **Игры (GAMES)**, Вы получите соответствующее уведомление, если Avira Premium Security Suite обнаружит подобные объекты. После чего игры, в прямом смысле слова, заканчиваются, так как у Вас появляется возможность удалять их очень легко.

Программы-шутки (JOKES)

Программы-шутки разрабатываются, например, для поднятия настроения. Они, как правило, не могут самостоятельно размножаться и не наносят вреда. После запуска такой программы компьютер демонстрирует что-нибудь необычное на мониторе, сопровождая это звуком. В качестве примеров программ-шуток можно назвать Стиральную машину в дисководе (DRAIN.COM) и Пожирателей экрана (BUGSRES.COM).

Но, внимание! Все симптомы таких развлекательных программ могут быть также имитированы вирусами или троянами. В конце концов, эти программы могут просто испугать пользователя, или могут помочь ему самому стать инициатором действий, причиняющих вред.

Avira Premium Security Suite в состоянии распознавать и уничтожать такие программы, благодаря встроенным расширенным поисковым и идентификационным функциям. Если в настройках в разделе Дополнительные категории угроз включена опция **Программы-шутки (JOKES)**, пользователь извещается об обнаружении таких объектов.

Риск вторжения в приватную сферу (SPR)

Программы, влияющие на безопасность Вашей системы, вызывающие нежелаемую программную активность, вторгающиеся в приватную сферу, могут быть опасными и являются нежелательными.

Avira Premium Security Suite распознает программы, "несущие риск вторжения в приватную сферу". Если в настройках в разделе Дополнительные категории угроз включена опция **Security Privacy Risk (SPR)**, вы получите уведомление от Avira Premium Security Suite, если будут обнаружены такие программы.

Backdoor-программы (BDC)

Для организации хищения данных или манипуляции с компьютером, backdoor-программа удаленного администрирования проникает в систему через "черный ход", о чем пользователь, как правило, даже не догадывается. Через Интернет или ЛВС клиентская часть такой программы может управляться третьими лицами.

Avira Premium Security Suite распознает "backdoor-утилиты удаленного администрирования". Если в настройках в разделе Дополнительные категории угроз включена опция **Backdoor-клиент (BDC)**, Вы получите уведомление, если Avira Premium Security Suite обнаружит подобный объект.

Рекламные и шпионские программы (ADSPY)

Программа, демонстрирующая рекламные материалы, или передающая личные данные пользователя без его согласия и уведомления третьим лицам, может быть нежелательной.

Avira Premium Security Suite распознает рекламные и шпионские программы "Adware/Spyware". Если в настройках в разделе Дополнительные категории угроз включена опция **Adware/Spyware (ADSPY)**, пользователь получает уведомление об обнаружении Avira Premium Security Suite рекламных и шпионских программ.

Необычные средства сжатия данных (PCK)

Файлы, сжатые при помощи необычных программ-паковщиков, могут быть отнесены к подозрительным.

Avira Premium Security Suite распознает деятельность "необычных паковщиков". Если в настройках в разделе Дополнительные категории угроз включена опция **Необычные паковщики (PCK)**, пользователь получает предупреждение в случае, если Avira Premium Security Suite обнаружит подобные объекты.

Файлы с двойным (скрытым) расширением (HEUR-DBLEXT)

Исполняемые файлы, скрывающие настоящие расширения файлов. Этот метод сокрытия часто используется вредоносным ПО.

Avira Premium Security Suite распознает "Файлы с двойным расширением". Если в настройках в разделе Дополнительные категории угроз включена опция **Файлы с двойным расширением (Double Extension files)**, пользователь получает уведомление в случае обнаружения Avira Premium Security Suite подобных объектов.

Фишинг

Фишинг, известный как *brand spoofing*, является специфической формой хищения данных, нацеленной на реальных или потенциальных клиентов Интернет-провайдеров, банков, различных служб и учреждений.
Через передачу своего электронного адреса в интернет, заполнение формулятор онлайн, вступление в новые группы Ваши данные через "Internet crawling spiders" могут быть использованы без Вашего разрешения для совершения неправомерных действий.

Avira Premium Security Suite распознает "Фишинг". Если в настройках в группе Дополнительные категории угроз включена опция **Фишинг (Phishing)**, пользователь получает уведомление при обнаружении Avira Premium Security Suite таких объектов.

Приложение (APPL)

Под APPL обозначены приложения, запуск которых может быть связан с определенным риском, или источник их происхождения не внушает доверия.

Avira Premium Security Suite распознает "Приложение (APPL)". Если в настройках в пункте Дополнительные категории угроз включена опция **Приложение (APPL)** , Вы получаете соответствующее предупреждение, если Avira Premium Security Suite замечает подобное поведение.

11.2 Вирусы и вредоносные программы

Рекламные программы

Под рекламными программами понимаются такие программы, которые, выполняя свою основную функцию, еще и демонстрируют пользователю рекламные баннеры и всплывающие рекламные окна. Эти рекламные сообщения иногда бывает очень сложно отключить или скрыть. Программы в своей работе основываются на поведении пользователей и являются проблематичными по соображениям безопасности.

Утилиты администрирования (Backdoor)

С помощью утилит администрирования (Задняя дверь, черный ход) можно, обходя системы защиты от НСД, получить компьютер под свой контроль.

Программа, работающая в скрытом режиме, дает пользователю практически неограниченные права. С помощью backdoor-программ можно получить доступ к персональным данным пользователя. Однако, чаще всего эти программы используются для инфицирования системы компьютерными вирусами и установки на нее вредоносных программ.

Загрузочные вирусы

Загрузочный и главный загрузочный сектор жесткого диска заботливо инфицируются загрузочными вирусами. Эти вирусы изменяют важную информацию, необходимую для запуска системы. Одно из последствий: невозможность загрузки операционной системы...

Bot-сеть

Под Bot-сетью понимается удаленно управляемая сеть (в Интернет), состоящая из отдельных персональных компьютеров, коммуницирующих между собой. Контроль сети достигается с помощью вирусов или троянских программ, инфицирующих компьютер. Они ожидают дальнейших указаний злоумышленника, не принося вреда инфицированным компьютерам. Эти сети могут применяться для рассылки СПАМа или организации DDoS атак. Пользователи участвующих компьютеров могут и не догадываться о происходящем. Основной потенциал bot-сетей заключается в том, что такие сети могут достигать численности в несколько тысяч элементов, чья совокупная пропускная способность может поставить под угрозу любую систему обработки запросов.

Эксплойт

Эксплойт (брешь в безопасности) – это компьютерная программа или скрипт, использующий специфические уязвимости операционной системы или программы. Эксплойт (брешь в безопасности) - это компьютерная программа или скрипт, использующий специфические уязвимости операционной системы или программы. Так в систему могут проникать программы, с помощью которых могут быть получены расширенные права доступа.

Hoax (обман, ложь, мистификация, шутка)

Уже несколько лет пользователи Интернет получают сообщения о вирусах, распространяющихся якобы с помощью электронной почты. Эти предупреждения рассылаются с просьбой отправить их как можно большему числу друзей и коллег для того, чтобы защитить от этой "угрозы" все человечество.

Ловушки

Honeypot (Горшочек меда) - сетевая служба, (программа или сервер). Эта служба имеет задачу наблюдать за сетью и фиксировать атаки. Обычный пользователь не знает имени этой службы, поэтому никогда к ней не обращается. Если злоумышленник исследует сеть на наличие уязвимостей, он может воспользоваться услугами, предложенными ловушкой, о чем моментально будет сделана запись в лог-файлы, а также сработает сигнализация.

Макровирусы

Макровирусы - это маленькие программы, написанные на макроязыке приложений (напр., WordBasic для WinWord 6.0), которые распространяются только среди документов, созданных для этого приложения. Поэтому они еще называются документными вирусами. Для того, чтобы они стали активными, требуется запуск соответствующего приложения и выполнение инфицированного макроса. В отличие от "нормальных" вирусов, макровирусы инфицируют не исполняемые файлы, а документы, созданные определенным приложением-хозяином.

Фарминг

Фарминг - это манипуляция хост-файлом веб-браузера для перенаправления запроса на фальшивый сайт. Это производная от классического фишинга. Фарминг-мошенники содержат сервера больших объемов, на которых хранятся фальшивые веб-страницы. Фарминг можно назвать общим понятием различных типов DNS-атак. При манипуляции хост-файлом с помощью троянской программы или вируса производится манипуляция системой. В результате система способна загружать только фальсифицированные веб-сайты, даже если Вы правильно вводите адрес.

Фишинг

Phishing означает "выуживание" личной информации о пользователе интернет. Злоумышленник отправляет своей жертве письмо, в ответ на которое необходимо ввести личную информацию, прежде всего это имя пользователя, пароли, PIN и TAN для доступа к банковским счетам онлайн. С помощью похищенных данных мошенник может выдать себя за свою жертву и осуществлять действия от имени ничего не подозревающего лица. Понятно, что: банки и страховые компании никогда не просят клиентов прислать номер кредитной карты, PIN, TAN или другие пароли по Email, SMS или по телефону.

Полиморфные вирусы

Полиморфные вирусы - истинные мастера маскировки и перевоплощения. Они изменяют свой собственный программный код, а поэтому их довольно сложно обнаружить.

Программные вирусы

Компьютерный вирус - это программа, обладающая способностью после своего запуска самостоятельно прикрепляться к другим программам, инфицируя их таким образом. Вирусы размножаются самостоятельно, что отличает их от логических бомб и троянских программ. В отличие от червя, вирусу всегда необходима программа, внутри которой он может записать свой вредоносный код. Обычно вирус не изменяет работоспособность программы, к которой прикрепляется.

Руткит

Руткит - набор программных средств, которые устанавливаются в систему, обеспечивая сокрытие логина злоумышленника, процессов и делая копии данных: то есть, делают их администратора невидимым. Вы пытаетесь обновить уже установленную шпионскую программу или установить удаленное шпионское ПО.

Скрипт-вирусы и черви

Эти вирусы очень просты в написании и распространяются по электронной почте глобально в течение нескольких часов.

Скриптовые вирусы и черви используют скриптовые языки (Javascript, VBScript и др.), чтобы добавлять себя к новым скриптам или распространяться через вызов функций операционной сети. Зачастую инфицирование происходит по электронной почте или в результате обмена файлами (документами).

Червем называется программа, размножающаяся самостоятельно, но не инфицирующая другие программы. Черви не могут стать частью других программ. Очень часто в системах с рестриктивной политикой безопасности черви являются единственной возможностью обеспечить проникновение внутрь вредоносных программ.

Шпионское ПО

Шпионские программы пересылают персональные данные пользователя без его ведома и разрешения производителю ПО или третьим лицам. Шпионские программы анализируют поведение пользователя Интернет, а основываясь на этих данных, демонстрируют рекламные баннеры или всплывающие окна, которые могут заинтересовать этого пользователя.

Троянские программы (Троянцы)

Троянские программы в последнее время встречаются довольно часто. Так обозначаются программы, которые должны выполнять определенные функции, но после запуска демонстрирующие свое истинное лицо, выполняя совершенно другие действия (обычно разрушительного характера). Троянские программы не могут размножаться самостоятельно, что отличает их от вирусов и червей. Большинство из них имеют интересные имена (SEX.EXE или STARTME.EXE), которые провоцируют пользователя на запуск троянских программ. Непосредственно после запуска они становятся активными и, например, запускают форматирование жесткого диска. Дроппер является специальным видом троянской программы. Эта программа рассаживает вирусы в системе.

Зомби

Зомби-ПК - это компьютер, инфицированный вредоносными программами, позволяющий злоумышленникам, преследующим криминальные цели, удаленно администрировать систему. Инфицированный ПК запускает, например, Denial-of-Service- (DoS) атаку или рассылает спам/фишинг письма.

12 Информация и сервис

этой главы размещены контактные данные для связи с нами.

См. главу Контакты

См. главу Техническая поддержка

См. главу Подозрительный файл

См. главу Уведомление о ложном срабатывании

См. главу Обратная связь

12.1 Контактный адрес

Мы с удовольствием поможем Вам, если у Вас есть вопросы и пожелания по линии продукции Avira Premium Security Suite. Наши контакты Вы найдете здесь: Центр контроля в Справка :: О Avira Premium Security Suite.

12.2 Техническая поддержка

Служба техподдержки Avira Premium Security Suite всегда готова помочь, если у Вас есть вопросы или технические проблемы.

На нашем сайте http://www.avira.ru/premium-suite-support Вы можете получить всю необходимую информацию, касающуюся техподдержки.

Для более быстрой и качественной помощи мы просим Вас предоставлять нам следующую информацию:

- **Информация о лицензии**. Вы найдете ее в Avira Premium Security Suite Центр контроля в пункте меню Справка :: О Premium Security Suite :: Информация о лицензии
- **Информация о версии**. Вы найдете ее в Avira Premium Security Suite Центр контроля в пункте меню Справка :: О Premium Security Suite :: Информация о версии.
- **Версия операционной системы** и информация об установленных сервис-паках.
- **Установленные программы**, например, антивирусное ПО сторонних производителей.
- **Точный текст сообщения** программы или файла отчета.

12.3 Подозрительный файл

Вирусы, которые пока не обнаруживаются нашими продуктами, а также подозрительные файлы Вы можете высылать нам. Мы предоставляем Вам несколько возможностей связаться с нами.

- Выберите в менеджере карантина Центр контроляфайл и отправьте его, воспользовавшись пунктом Отправить файл контекстного меню.
- Отправьте требуемый файл в архиве (WinZIP, PKZip, Arj и т.д.) в приложении к письму по адресу virus-premium-suite@avira.ru. Т.к. некоторые почтовые шлюзы работают с антивирусным ПО, защитите файл(ы) паролем и не забудьте сообщить его нам.

У Вас есть также возможность отправить подозрительные файлы через наш сайт.

12.4 Сообщить о ложном срабатывании

Если Вы считаете, что Avira Premium Security Suite обозначил заведомо "чистый", по Вашему мнению, файл инфицированным, отправьте этот файл в запакованном (WinZIP, PKZIP, Arj etc.) виде на адрес virus-premium-suite@avira.ru. Т.к. некоторые почтовые шлюзы работают с антивирусным ПО, защитите файл(ы) паролем и не забудьте сообщить его нам.

12.5 Обратная связь для вашей безопасности

Avira считает безопасность клиентов самой главной своей задачей. У нас работает собственная команда экспертов, придирчиво тестирующая все решения Avira и каждый файл обновления перед их опубликованием. Само собой разумеющимся является для нас серьезное отношение к возможным уязвимостям системы, быстрая и открытая реакция на них.

Если Вы обнаружили уязвимость в одном из наших программных продуктов, отправьте, пожалуйста, нам сообщение об этом на адрес vulnerabilities-premium-suite@avira.ru.

13 Ссылка: Опции меню настройки

В информации о настройке содержатся все данные об опциях, доступных в Avira Premium Security Suite.

13.1 Scanner

Раздел Scanner блока Avira Premium Security Suite. Настройка отвечает за настройку параметров проверки, т.е. за работу сканера.

13.1.1 Поиск

Здесь Вы можете определить основные параметры поведения поисковых процедур в процессе проверки. Если Вы выбираете определенные папки для проверки, Scanner осуществляется в зависимости от настроек:

- с определенной производительностью поисковой системы,
- с проверкой загрузочных секторов и сканированием памяти,
- с проверкой всех или конкретных загрузочных секторов и памяти,
- с проверкой всех или указанных файлов в папках.

Файлы

Scanner может применять фильтр, чтобы проверить файлы с определенным расширением.

Все файлы

Если эта опция включена, все файлы, независимо от содержания и файловых расширений, проверяются на наличие вирусов или вредоносных программ. Фильтр не используется.

Примечание
Если определена опция Все файлы, невозможно воспользоваться кнопкой Расширения.

Базовый список расширений

Если выбран этот параметр, выбор файлов для проверки определяется автоматически программой Avira Premium Security Suite. Это означает, что Avira Premium Security Suite принимает решение о необходимости проверки файла на наличие вирусов и вредоносных программ, основываясь на его содержании. Эта процедура занимает несколько больше времени, чем проверка с использованием редактируемого списка расширений, но является значительно более надежной, так как проверка производится не только на основании расширения файлов. Эта установка определена по умолчанию и рекомендуется разработчиком.

Примечание
Если Вы выбрали Базовый список расширений, невозможно воспользоваться кнопкой Расширения.

Редактируемый список расширений

Если эта опция включена, проверяются только файлы с определенными расширениями. Предварительно определены все типы файлов, в которых могут содержаться вирусы и вредоносные программы. Кнопка Расширения позволяет редактировать список вручную.

Примечание
Если эта опция включена, а Вы удалили все расширения из списка, информация от этом отображается в виде текста "Расширения не определены", расположенного под кнопкой Расширения.

Расширения

С помощью этой кнопки вызывается окно, в котором отображаются все расширения файлов, проверяемых с использованием **редактируемого списка расширений**. В списке уже приведены некоторые расширения файлов, но Вы можете легко добавлять новые или удалять их.

Примечание
Помните, что стандартный список может меняться от версии к версии.

Дополнительные настройки

Проверить загрузочные секторы

Если эта опция включена, служба Scanner сканирует загрузочные секторы выбранных дисков. Эта настройка активна по умолчанию.

Проверить загрузочные секторы

Если опция включена, Scanner проверяет главные загрузочные секторы используемых жестких дисков.

Пропускать offline-файлы

Если опция включена, то при прямой проверке так называемые Offline-файлы не проверяются полностью. Т.е., эти файлы не проверяются на наличие вирусов и вредоносных программ Offline-файлы представляют собой файлы, которые с помощью т.н. иерархической системы управления памятью (HSMS) физически переносятся с жесткого диска на пленку. Эта настройка активна по умолчанию.

Проверка совместимости системных файлов

Если опция включена, то при каждом прямом поиске важнейшие системные файлы Windows проверяются на изменения из-за вредоносных программ. При обнаружении измененного файла появится сообщение о подозрительном объекте. Для этой функции необходимо много ресурсов. Поэтому по умолчанию эта опция отключена.

Оптимальная проверка

Если опция включена, то мощность процессора при проверке Scanner будет распределяться оптимально. Вследствие особенностей производительности протоколирование при оптимальной проверке осуществляется на уровне По умолчанию.

Примечание
Опция доступна только для многопроцессорных компьютеров. Если Premium Security Suite администрируется через SMC, то каждый раз отображается и может быть активирована опция: Если в компьютере не установлено несколько процессоров, то опция Scanner не используется.

Следовать по ссылкам

Если опция включена, Scanner при проверке следует по всем ссылкам поискового профиля или выбранной папки, чтобы проверить файлы на вирусы. Эта опция не поддерживается Windows 2000 и по умолчанию отключена.

Важно
Сюда не относятся ссылки на файлы (ярлыки), но подходят исключительно символьные ссылки, созданные с помощью mklink.exe, или Junction Points (junction.exe), которые открыто размещены в файловой системе.

Поиск руткит-программ

Если опция включена, то Scanner при каждом запуске проверки осуществляет быструю проверку системных папок Windows на руткит-программы. Эта технология проверяет Ваш компьютер не так тщательно, как специальный профиль **поиска руткит-программ**, но она работает гораздо быстрее.

Важно
Поиск руткит-программ недоступен для 64-битных систем.

Процесс сканирования

Разрешать остановку проверки

Если опция включена, "Luke Filewalker" может остановить проверку на вирусы после нажатия кнопки Стоп. Если Вы отключили эту настройку, кнопка Стоп в окне "Luke Filewalker" становится неактивной (серой). Остановка проверки до ее окончания становится невозможной! Эта настройка активна по умолчанию.

Приоритет проверки

Scanner различает при проведении проверки три уровня приоритета. Это возможно только в том случае, если на компьютере запущены одновременно несколько процессов. Выбор оказывает влияние на скорость поиска.

низкий

Scanner получает от операционной системы процессорное время только в том случае, если оно не требуется другим процессам. Т.е. до тех пор, пока Scanner работает в одиночку, скорость является максимальной. Значительно облегчается одновременная работа с другими программами: Компьютер работает быстрее, если другие программы используют процессорное время, когда Scanner продолжает работать в фоновом режиме. Эта установка определена по умолчанию и рекомендуется разработчиком.

средний

Scanner выполняется с нормальным приоритетом. Все процессы получают от операционной системы одинаковое количество процессорного времени. При определенных обстоятельствах затрудняется работа с другими приложениями.

высокий

Scanner получает наивысший приоритет. Одновременная работа с другими приложениями практически невозможна. Scanner выполняет свои поисковые задачи максимально быстро.

13.1.1.1. Действие при обнаружении

Действие при обнаружении

Вы можете определить операции, которые будут выполняться, если Scanner обнаружит вирус или вредоносную программу.

Интерактивно

Если опция включена, то об обнаружении вирусов при проверке Scanner сообщается в диалоговом окне. При поиске программ-руткитзагрузочных вирусов и при проверке активных процессов появляется диалоговое окно, в котором Вы можете выбрать действие для инфицированных объектов. При проверке файлов оповещение и выбор действия для инфицированных файлов зависит от выбранного режима уведомления. Эта настройка активна по умолчанию.

Подробная информация доступна здесь.

Режим уведомления

В режиме уведомлений Вы определяете, в какой форме Scanner должен сообщать об обнаружении вируса. В режиме уведомлений Вы устанавливаете возможность/невозможность выбора действий над инфицированными файлами.

Комбинированный

В комбинированном режиме уведомления при завершении проверки файлов Вы получите уведомление со списком обнаруженных инфицированных файлов. У Вас нет возможности выбора действий над инфицированным файлом. Вы можете выполнить стандартное действие Scanner для всех инфицированных файлов или прервать Scanner.

Комбинированный (экспертный)

В экспертном режиме уведомления при завершении проверки файлов Вы получите уведомление со списком обнаруженных инфицированных файлов. Вы можете выбрать действие над инфицированным файлом в контекстном меню. Вы можете выполнить выбранное действие для всех инфицированных файлов или завершить Scanner

Индивидуальный

В индивидуальном режиме уведомлений при проверке файлов о каждом обнаруженном вирусе сообщается отдельно. Вы можете выбрать, что делать с зараженным файлом.

Автоматически

Если опция включена, при обнаружении вируса или вредоносной программы действие происходит автоматически, не предлагая выбора. Scanner реагирует на определенные Вами в этом разделе установки.

Копировать файл в карантин перед действием

Если эта опция включена, Scanner создает резервную копию (Backup) перед осуществлением первичного (или, в случае необходимости, вторичного) действия. Резервная копия хранится в карантине, откуда можно восстановить файл, если он имеет ценность. Кроме того, Вы можете отправить разработчику (Центр исследования вредоносных программ) резервную копию для дальнейшего изучения.

Первичное действие

Первичное действие выполняется в случае, если Scanner обнаруживает вирус или вредоносную программу. Если выбрана опция **Вылечить**, но лечение инфицированного файла невозможно, выполняется операция, определенная пунктом **Вторичное действие**.

Примечание
Опция **Вторичное действие** доступна только в том случае, если для **Первичного действия** определена операция **Вылечить**.

лечить

Если эта опция включена, Scanner автоматически пытается лечить инфицированный файл. Если Scanner не может вылечить инфицированный файл, выполняется операция, предусмотренная Вторичным действием.

Примечание
Разработчик рекомендует автоматическое лечение, но это означает, что Scanner изменяет файлы на Вашем компьютере.

удалить

Если эта опция включена, файл удаляется, но может быть позже восстановлен с помощью соответствующих утилит (например, Avira UnErase). Вирусная сигнатура может быть обнаружена повторно. Эта процедура значительно быстрее, чем "переписать и удалить".

переписать и удалить

Если опция включена, Scanner заменяет файл стандартным шаблоном, а затем удаляет его. Он не может быть восстановлен.

переименовать

Если опция включена, Scanner переименовывает файл. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Файлы могут быть позже вылечены и переименованы обратно.

Пропустить

Если опция включена, доступ к файлам разрешается, а сами файлы остаются без изменений.

Предупреждение
Инфицированный файл все еще активен в Вашей системе! Это может причинить вред Вашему компьютеру!

Карантин

Если эта опция включена, Scanner помещает файлы в карантин. Эти файлы могут быть позже вылечены или, в случае необходимости, отправлены разработчику (Центр исследования вредоносных программ).

Вторичное действие

Опция **Вторичное действие** доступна только в случае, если для **Первичного действия** выбрано действие вылечить. С помощью этой опции можно выбрать операцию, которая должна быть произведена с инфицированным файлом, если его невозможно вылечить.

удалить

Если эта опция включена, файл удаляется, но может быть позже восстановлен с помощью соответствующих утилит (например, Avira UnErase). Вирусная сигнатура может быть обнаружена повторно. Эта процедура значительно быстрее, чем "переписать и удалить".

переписать и удалить

Если эта опция включена, Scanner заменяет файл шаблоном, а затем удаляет этот файл. Он не может быть восстановлен.

переименовать

Если опция включена, Scanner переименовывает файл. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Файлы могут быть позже вылечены и переименованы обратно.

Пропустить

Если опция включена, доступ к файлам разрешается, а сами файлы остаются без изменений.

Предупреждение
Инфицированный файл все еще активен в Вашей системе! Это может причинить вред Вашему компьютеру!

Карантин

Если эта опция включена, Scanner помещает файл в карантин. Эти файлы могут быть позже вылечены или, в случае необходимости, отправлены разработчику (Центр исследования вредоносных программ).

Примечание
Если в качестве первичного или вторичного действия выбрали **удалить** или **переписать и удалить**, учитывайте следующее: Если инфицированные файлы были обнаружены системой эвристического поиска, то они не удаляются, а помещаются на карантин.

При сканировании архивов Scanner применяет технологию рекурсивного поиска. Распаковываются и проверяются также архивы, находящиеся в архивах. Файлы проверяются, затем они распаковываются и вновь проверяются.

Проверять архивы

Если эта опция включена, проверяются все архивы, выделенные в списке архивов. Эта настройка активна по умолчанию.

Все типы архивов

Если эта опция включена, проверяются все типы архивов, выделенные в списке архивов.

Smart Extensions

Если эта опция включена, Scanner определяет, соответствует ли тип файла формату упакованных файлов (архив), даже если расширение файлов отличается от обычных архивных расширений, а затем проверяет этот архив. Для этого каждый файл должен быть открыт, что значительно уменьшает скорость проверки. Пример: Если *.zip архив имеет расширение *.zzz, Scanner распаковывает и этот архив, осуществляя его проверку. Эта настройка активна по умолчанию.

Примечание
Проверяются только те типы архивов, которые выделены в списке архивов.

Ограничить уровень рекурсии

Распаковка и проверка архивов с высокой степенью вложенности (рекурсии) требует много ресурсов и времени. Если эта опция включена, Вы ограничиваете глубину поиска определенным уровнем паковки (Максимальная глубина рекурсии). Так Вы экономите время и ресурсы машины.

Примечание
Для того, чтобы определить наличие в архиве вируса или вредоносной программы, Scanner производит проверку архива до того уровня рекурсии, на котором находится подозрительный объект.

Макс. глубина рекурсии

Для того, чтобы определить максимальную глубину рекурсии, используйте опцию Ограничить уровень рекурсии.
Вы можете определить желаемую глубину рекурсии вручную или с помощью клавиш со стрелками справа от поля ввода. Допустимые значения: от 1 до 99. Рекомендуемое стандартное значение - 20.

Значения по умолчанию

Кнопка восстанавливает заранее определенные значения для поиска в архивах.

Список архивов

В этом поле Вы можете установить, какие архивы должны проверяться системой Scanner. Для этого необходимо выделить соответствующие строки.

13.1.1.2. Исключения

Scanner не сканирует следующие файловые объекты

Список в этом окне содержит файлы и пути, которые необходимо проверить на наличие вирусов или вредоносных программ системой Scanner.

Вносите как можно меньше исключений, это должны быть файлы, которые по определенным причинам не должны проверяться. Старайтесь исключать из проверки только те файлы, которые по разным причинам не подвергаются обычной проверке.

Примечание
Совокупная длина строк в списке не должна превышать 6000 знаков.

Предупреждение
Эти файлы не проверяются при проверке.

Примечание
Файлы, указанные в этом списке, отмечаются в Файле отчета. Проверяйте время от времени файл отчета на наличие в нем информации об исключенных из проверки файлах. Возможно, причины исключения файлов из проверки больше не существует. Удалите имя этого файла из списка.

Поле ввода

В этом поле укажите имя файлового объекта, который не должен проверяться. По умолчанию список не содержит объектов.

Кнопка открывает окно, в котором Вы можете выбрать желаемый файл или путь.
Если Вы ввели имя файла с указанием полного пути к нему, только этот файл не будет проверяться на наличие вирусов. Если Вы ввели имя файла без указания полного пути к нему, не будут проверяться все файлы, имеющие это имя, вне зависимости от того, где они находятся в системе.

Добавить

С помощью этой кнопки можно добавлять к списку файловый объект, имя (и путь) которого Вы указали в поле ввода.

Удалить

Кнопка удаляет из списка выделенную строку. Кнопка неактивна, если ни одна строка не выделена.

Примечание
Если Вы добавите к списку исключений из проверки целый раздел, из проверки исключаются только файлы, сохраненные непосредственно в этом разделе, но не файлы, находящиеся в размещенных в разделе папках: Пример: Исключенный из проверки файловый объект: `D:\` = `D:\file.txt` исключен из проверки модулем Scanner, `D:\folder\file.txt` из проверки не исключается.

13.1.1.3. Эвристика

Этот раздел настроек содержит параметры эвристического поиска Avira Premium Security Suite.

Avira Premium Security Suite содержит эвристические системы, которые сразу распознают вредоносные программы, то есть до составления специальной вирусной сигнатуры и получения обновления защиты от вирусов. Распознавание вирусов осуществляется при помощи подробного анализа инфицированного кода на предмет выполняемых функций и действий, типичных для вредоносных программ. Если исследуемый код имеет характерные признаки, он получает статус подозрительного. Это не означает, что объект в любом случае является вредоносной программой. Возможны также ложные срабатывания. Решение о том, что необходимо сделать с подозрительным объектом, принимает сам пользователь. Решение может быть основано, например, на знании о происхождении файла.

Эвристическое обнаружение макровирусов

Эвристическое обнаружение макровирусов

Avira Premium Security Suite имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, подозрительные файлы регистрируются, пользователь получает об этом уведомление. Эта настройка по умолчанию включена и является нашей рекомендацией.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Avira Premium Security Suite благодаря технологии AntiVir AHeAD содержит очень мощную эвристическую систему для определения даже неизвестных вирусов и (новых) вредоносных программ. Вы можете установить уровень "резкости" эвристики. Эта настройка активна по умолчанию.

Низкий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite обнаруживает меньше неизвестных вредоносных программ.

Средний уровень обнаружения

Эта настройка по умолчанию включена, если Вы выбрали применение этой эвристической технологии.

Высокий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite распознает значительно больше неизвестных вирусов или вредоносных программ, но возможны и ложные срабатывания.

13.1.2 Отчет

Scanner имеет функцию подробного протоколирования. С ее помощью Вы получите точную информацию о результатах проверки. Файл отчета содержит все записи системы, а также предупреждения и сообщения службы проверки.

Примечание
Для того, чтобы при обнаружении вируса или вредоносной программы, можно было бы определить, какие действия выполняет Scanner, необходимо всегда составлять файл отчета.

Протоколирование

Не требуется

Если эта опция включена, Scanner не составляет отчета о выполнении действий и результатах проверки.

По умолчанию

Если эта опция включена, Scanner записывает в лог-файлы имена инфицированных файлов с указанием пути к ним. Кроме того, параметры настройки Проверки, информации о версии и лицензии записываются в файл отчета.

Расширенный

Если опция включена, Scanner протоколирует также все предупреждения и примечания.

полная

Если эта опция включена, Scanner дополнительно включает в отчет имена всех проверенных файлов. В файл отчета включаются имена всех инфицированных файлов, все предупреждения и примечания.

Примечание
Если Вы будете отправлять нам файл отчета (например, для поиска ошибок), просим Вас высылать отчет в этом режиме.

13.2 Guard

Секция Guard в блоке Avira Premium Security Suite. Настройка создана для настройки постоянной защиты в режиме реального времени (монитор).

13.2.1 Поиск

Рекомендуется не отключать постоянную защиту. Для этого используется Guard (Антивирусный монитор). Так Вы можете все файлы, которые копируются или открываются на данном компьютере, проверять "на лету".

Режим проверки

Здесь определяется момент начала проверки файла.

Во время чтения

Если эта опция включена, Guard проверяет файлы до того, как они открываются/читаются каким-нибудь приложением или операционной системой.

Во время записи

Если эта опция включена, Guard проверяет файл в момент записи. Только после завершения этого процесса Вы можете получить доступ к файлу.

Во время чтения и записи

Если эта опция включена, Guard проверяет файлы перед открытием, чтением и выполнением, а также после записи. Эта настройка по умолчанию включена и является нашей рекомендацией.

Файлы

Guard может применять фильтр, чтобы проверять только файлы с определенным расширением.

Все файлы

Если эта опция включена, все файлы проверяются на наличие вирусов и вредоносных программ, независимо от содержания и расширения.

Примечание
Если выбран параметр Все файлы, кнопка Расширения неактивна.

Базовый список расширений

Если выбран этот параметр, выбор файлов для проверки определяется автоматически программой Avira Premium Security Suite. Это означает, что Avira Premium Security Suite принимает решение о необходимости проверки файла на наличие вирусов и вредоносных программ, основываясь на его содержании. Эта процедура несколько медленнее, чем проверка с использованием редактируемого списка расширений, но она обеспечивает более высокую степень безопасности, так как проверка производится не только с учетом расширения файла.

Примечание
Если используется базовый список расширений, кнопка Расширения остается неактивной.

Редактируемый список расширений

Если эта опция включена, проверяются только файлы с определенным типом расширения. Предварительно определены все типы файлов, в которых могут содержаться вирусы и вредоносные программы. Кнопка Расширения позволяет редактировать список вручную. Эта установка определена по умолчанию и рекомендуется разработчиком.

Примечание
Если эта опция включена, и Вы удалили все записи из списка, под кнопкой Расширения отображается текст "Расширения не определены".

Расширения

С помощью этой кнопки вызывается окно, в котором отображаются все расширения файлов, проверяемых программой в режиме **Редактируемый список расширений**. В списке уже приведены некоторые расширения файлов, но Вы можете легко добавлять новые или удалять их.

Примечание
Помните о том, что базовый список может меняться в зависимости от версии программы.

Архивы

Проверять архивы

При включенной опции проверяются архивы. Проверяются сжатые файлы, затем они распаковываются и вновь проверяются. По умолчанию опция отключена. Проверка архивов ограничивается глубиной рекурсии, количеством файлов и размером архива. Вы можете установить максимальные полказатели глубины рекурсии, количества файлов и размера архива.

Примечание
По умолчанию опция отключена, так как процесс использует слишком много ресурсов. Мы рекомендуем проверять архивы с помощью Проверки.

Макс. глубина рекурсии

При сканировании архивов Guard применяет технологию рекурсивного поиска. Распаковываются и проверяются также архивы, находящиеся в архивах. Вы можете определить глубину рекурсии. Значение глубины рекурсии по умолчанию - 1. Оно является рекомендуемым: Все архивы, находящиеся в основном архиве, распаковываются и проверяются.

Макс. число файлов

При проверке архивов Вы можете ограничить поиск определенным числом файлов в архиве. Значение для максимального количества проверяемых файлов по умолчанию - 10. Оно является рекомендуемым.

Макс. объем [KB]

При проверке архивов Вы можете определить максимальный размер распаковываемого архива. Значение по умолчанию - 1000 KB. Оно является рекомендуемым.

13.2.1.1. Действие при обнаружении

Действие при обнаружении

Вы можете определить операции, которые будут выполняться, если Guard обнаружит вирус или вредоносную программу.

Интерактивно

Если эта опция включена, система постоянной защиты отображает окно, в котором можно выбрать дальнейшие действия с инфицированным файлом. Эта опция включена по умолчанию.

Подробная информация доступна здесь.

Автоматически

Если опция включена, при обнаружении вируса или вредоносной программы действие происходит автоматически, не предлагая выбора. Guard реагирует на определенные Вами в этом разделе установки.

Копировать файл в карантин перед действием

Если эта опция включена, Guard создает резервную копию (Backup) перед осуществлением выбранных первичного и вторичного действия. Резервная копия сохраняется в Карантине. Она может быть восстановлена из Менеджера Карантина, если в этом возникнет необходимость. Кроме того Вы можете отправить резервную копию объекта (Центр исследования вредоносных программ). В зависимости от типа объекта, Менеджер Карантина располагает дополнительными возможностями выбора.

Первичное действие

Первичное действие выполняется, если Guard обнаруживается вирус или вредоносная программа. Если было выбрано действие **лечить**, но лечение соответствующего файла невозможно, выполняется операция, предусмотренная **Вторичным действием**.

Примечание
Возможность определить Вторичное действие существует только в том случае, если для Первичного действия установлена операция лечить.

лечить

Если опция включена, Guard автоматически пытается лечить инфицированные файлы. Если Guard не может вылечить инфицированный файл, это приводит к выполнению операции, предусмотренной для Вторичного действия.

Примечание
Разработчиком рекомендуется автоматическое лечение файлов, но при этом Guard модифицирует файлы.

удалить

Если эта опция включена, файл удаляется, но может быть позже восстановлен с помощью соответствующих утилит (например, Avira UnErase). Вирусная сигнатура может быть обнаружена повторно. Эта процедура значительно быстрее, чем "переписать и удалить".

переписать и удалить

Если опция включена, Guard заменяет файл стандартным шаблоном и удаляет его. Он не может быть восстановлен.

переименовать

Если опция включена, Guard переименовывает файл. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Файлы могут быть позже вылечены и переименованы обратно.

Пропустить

Если опция включена, доступ к файлам разрешается, а сами файлы остаются без изменений.

Предупреждение
Инфицированный файл все еще активен в Вашей системе! Это может причинить вред Вашему компьютеру!

запретить доступ

Если эта опция включена, Guard вносит информацию об обнаружении подозрительного объекта только в Файл отчета. Кроме того, Guard записывает соответствующую строку в Протокол, если эта опция включена.

Карантин

Если эта опция включена, Guard помещает файл в папку карантина. Файлы из этой папки могут быть позже вылечены или, в случае необходимости, отправлены разработчику (Центр исследования вредоносных программ).

Вторичное действие

Опция **Вторичное действие** может быть выбрано только в том случае, если для **Первичного действия** была определена операция **лечить**. С помощью этой опции можно выбрать операцию, которая должна быть произведена с инфицированным файлом, если его невозможно вылечить.

удалить

Если эта опция включена, файл удаляется, но может быть позже восстановлен с помощью соответствующих утилит (например, Avira UnErase). Вирусная сигнатура может быть обнаружена повторно. Эта процедура значительно быстрее, чем "переписать и удалить".

переписать и удалить

Если опция включена, Guard заменяет файл стандартным шаблоном и удаляет его. Он не может быть восстановлен.

переименовать

Если опция включена, Guard переименовывает файл. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Файлы могут быть позже вылечены и переименованы обратно.

Пропустить

Если опция включена, доступ к файлам разрешается, а сами файлы остаются без изменений.

Предупреждение
Инфицированный файл все еще активен в Вашей системе! Это может причинить вред Вашему компьютеру!

запретить доступ

Если эта опция включена, Guard вносит информацию об обнаружении подозрительного объекта только в Файл отчета. Кроме того, Guard записывает соответствующую строку в Протокол, если эта опция включена.

Карантин

Если эта опция включена, Guard помещает файл в Карантин. Файлы могут быть позже вылечены или, в случае необходимости, отправлены разработчику (Центр исследования вредоносных программ).

Примечание
Если в качестве первичного или вторичного действия выбрали **удалить** или **переписать и удалить** , учитывайте следующее: Если инфицированные файлы были обнаружены системой эвристического поиска, то они не удаляются, а помещаются на карантин.

13.2.1.2. Дополнительные действия

Уведомления

Журнал регистрации событий

Если опция включена, информация о каждом обнаружении сохраняется в журнале регистрации событий. Администратор может получать уведомления об обнаружении и соответственно реагировать. Эта настройка активна по умолчанию.

13.2.1.3. Исключения

С этой опцией Вы можете настроить параметры исключения из проверки Guard (Монитор). Указанные объекты не проверяются системой постоянной защиты. Guard может игнорировать обращения к файлам со стороны исключенных из проверки процессов. Это, например, может быть полезно при работе с базами данных или системами резервного копирования.

Процессы, исключенные из проверки службой Guard

Любой доступ к файлам со стороны процессов, указанных в этом списке, остается без внимания со стороны службы Guard.

Поле ввода

В этом поле укажите имя процесса, который не должен проверяться службой постоянной защиты. В установках по умолчанию процессы не указываются. Имя конкретного процесса проще всего узнать с помощью диспетчера задач. Вкладка "Процессы" (англ.: "Processes") содержит имена всех текущих процессов. Найдите "Ваш" процесс и внесите его имя в колонке "Имя образа" "Image Name") в список.

Примечание
Вы можете ввести до 20 процессов.

Предупреждение:
Принимаются во внимание только первые 15 знаков имени процесса (включая расширения файлов). Если имена двух процессов совпадают в первых 15 символах, оба этих процесса исключаются из проверки Guard.

Предупреждение
Помните, что все обращения к файлам со стороны процессов, обозначенных в списке, игнорируются при проверке на наличие вирусов и вредоносных программ! Windows Explorer и сама операционная система не могут быть исключены из проверки. Соответствующая строка в списке игнорируется.

Добавить

Эта кнопка позволяет Вам добавить в окно процесс, указанный в поле ввода.

Удалить

Нажмите на кнопку и удалите выделенный процесс из списка.

Guard не проверяет объекты:

Обращения к файлам объектов из этого списка игнорируются программой.

Примечание
Совокупная длина строк в списке не должна превышать 6000 знаков.

Поле ввода

Введите имя файлового объекта, который не должен быть включен в проверку системой постоянной защиты. По умолчанию список не содержит объектов.

Кнопка открывает окно, дающее Вам возможность выбрать файловый объект, который Вы хотите исключить из проверки.

Добавить

С помощью этой кнопки можно добавлять к списку файловый объект, имя (и путь) которого Вы указали в поле ввода.

Удалить

Эта кнопка удаляет выделенный файловый объект из списка.

Примите к сведению следующие пункты:

- В названии файлов разрешены заменители символов * (любое количество знаков) и ? (один знак).
- После имени папки должен обратный слэш - \ , иначе имя считается именем файла.
- Список обрабатывается сверху вниз.
- Можно исключать из проверки и отдельные расширения файлов (включая заменитель символов).
- Если исключается папка, автоматически исключаются и папки, находящиеся внутри.
- Чем длиннее список, тем больше процессорного времени требуется для обработки списка при каждой операции. Рекомендуется не добавлять в список объекты без особой необходимости.
- Для исключения объектов, обращение к которым осуществляется с помощью коротких имен файлов DOS (DOS name convention 8.3), необходимо добавить в список соответствующее короткое имя.

Примечание
К имени файла, содержащего заменитель символов, нельзя добавлять обратный слэш.

Например:

```
C:\Program Files\Приложения\прилож*.exe\
```

Эта запись недействительна. Программа не исключает объект из проверки!

Примечание
Для динамических дисков, которые подключены (замонтированы) как папка на другом диске, Вам необходимо применять для подключенных дисков алиасы операционной системы из списка исключений:
например, \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
Если Вы используете точку монтирования, например, C:\DynDrive динамический диск все равно будет проверен. Используемые операционной системой алиасы Вы можете получить из файла отчетов Guard:

Примечание
На основании файла отчета Guard Вы можете указать пути, которые использует Guard при поиске инфицированных файлов. Используйте в списке исключений те же пути. Действуйте следующим образом: Установите параметр протоколирования Guard в настройках: Guard :: Отчет на **Полная**. Обратитесь с помощью активированного Guard к файлам, папкам, к подключенным дискам . Вы можете прочитать используемый путь в файле отчетов Guard. Файл отчета можно вызвать в разделе Центр контроля Локальная защита :: Guard.

Примеры:

```
C:
C:\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Program Files\Приложения\приложение.exe
C:\Program Files\Приложения\прилож*.exe
C:\Program Files\Приложения\прилож*
C:\Program Files\Приложения\прилож????.e*
C:\Program Files\
C:\Program Files
C:\Program Files\Приложения\*.mdb
```

13.2.1.4. Эвристика

Этот раздел настроек содержит параметры эвристического поиска Avira Premium Security Suite.

Avira Premium Security Suite содержит эвристические системы, которые сразу распознают вредоносные программы, то есть до составления специальной вирусной сигнатуры и получения обновления защиты от вирусов. Распознавание вирусов осуществляется при помощи подробного анализа инфицированного кода на предмет выполняемых функций и действий, типичных для вредоносных программ. Если исследуемый код имеет характерные признаки, он получает статус подозрительного. Это не означает, что объект в любом случае является вредоносной программой. Возможны также ложные срабатывания. Решение о том, что необходимо сделать с подозрительным объектом, принимает сам пользователь. Решение может быть основано, например, на знании о происхождении файла.

Эвристическое обнаружение макровирусов

Эвристическое обнаружение макровирусов

Avira Premium Security Suite имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, подозрительные файлы регистрируются, пользователь получает об этом уведомление. Эта настройка по умолчанию включена и является нашей рекомендацией.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Avira Premium Security Suite благодаря технологии AntiVir AHeAD содержит очень мощную эвристическую систему для определения даже неизвестных вирусов и (новых) вредоносных программ. Вы можете установить уровень "резкости" эвристики. Эта настройка активна по умолчанию.

Низкий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite обнаруживает меньше неизвестных вредоносных программ.

Средний уровень обнаружения

Эта настройка по умолчанию включена, если Вы выбрали применение этой эвристической технологии.

Высокий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite распознает значительно больше неизвестных вирусов или вредоносных программ, но возможны и ложные срабатывания.

13.2.2 Отчет

Guard располагает мощной функцией протоколирования, что дает пользователю/администратору точные данные о типе и способе обнаружения.

Протоколирование

Здесь определяются объемные параметры файла отчета.

Не требуется

Если эта опция включена, Guard не создает протокола.
Мы рекомендуем отказываться от протоколирования только в экстренных случаях, например, если Вы производите тестирование продукта на большой базе вирусов.

По умолчанию

Если эта опция включена, Guard записывает важную информацию о вирусах и вредоносных программах, предупреждения и сообщения об ошибках в файл отчета, менее важная информация в отчете не отражается. Эта настройка активна по умолчанию.

Расширенный

Если эта опция включена, Guard отображает в отчете и менее значимую информацию.

полная

При включенной опции Guard записывает информацию (размер и тип файла, дата создания) в файл отчета.

Ограничения для файлов отчетов

Максимум n MB

Если эта опция включена, файл отчета ограничивается определенным размером (от 1 до 100 Мб). от 1 до 100 Мб. Эта настройка по умолчанию включена. Установлено ограничение в 1 Мб.

Не сокращать файл отчета

Если опция включена, создается резервная копия файла отчета перед его сокращением.

Сохранение настроек в файле отчета

Данные о настройках постоянной защиты вносятся в файл отчета.

13.3 MailGuard

Раздел MailGuard блока Avira Premium Security Suite. Настройка отвечает за настройку службы MailGuard.

13.3.1 Поиск

Вы используете MailGuard для защиты почты от вирусов и спама. MailGuard может проверять исходящие письма на вирусы. Исходящие письма, отправленные неизвестным ботом для рассылки спама с Вашего компьютера, могут быть блокированы MailGuard.

Поиск

Проверять входящие письма

Если опция включена, входящие письма проверяются на наличие вирусов и спама. MailGuard поддерживает протоколы POP3 и IMAP. Активируйте протокол входящих писем, который использует Ваш почтовый клиент, для контроля посредством MailGuard.

Контроль протокола POP3

Если опция включена, то протоколы POP3 на входящих портах проверяются.

Проверяемые порты

В это поле необходимо ввести порт, который будет использоваться для протокола входящих писем POP3. Несколько портов разделяются между собой запятыми.

По умолчанию

Кнопка возвращает заданные порты к стандартному порты для POP3.

Контроль протокола IMAP

Если опция включена, то протоколы IMAP на входящих портах проверяются.

Проверяемые порты

В это поле необходимо ввести порт, который будет использоваться для протокола IMAP. Несколько портов разделяются между собой запятыми.

По умолчанию

Кнопка возвращает заданные порты к стандартному порты для IMAP.

Проверять исходящие письма (SMTP)

Если опция включена, исходящие письма проверяются на вирусы и вредоносное ПО. Письма, рассылаемые неизвестными бот-программами, будут блокированы.

Проверяемые порты

В это поле необходимо ввести порт, который будет использоваться для протокола исходящих писем SMTP. Несколько портов разделяются между собой запятыми.

По умолчанию

Кнопка возвращает заданные порты к стандартному порты для SMTP.

Примечание
Для верификации используемых протоколов и портов откройте в Вашем почтовом клиенте свойства Вашей учетной записи. Как правило, используются стандартные порты.

13.3.1.1. Действие при обнаружении

Здесь содержатся данные о том, какие действия необходимо выполнить, если MailGuard обнаружит в письме или вложении вирус или вредоносную программу.

Примечание
Установленные здесь действия выполняются как при обнаружении вируса во входящем, так и в исходящем письме.

Действие при обнаружении

Интерактивно

Если эта опция включена, при обнаружении вируса или вредоносной программы, содержащихся в Email или во вложении, отображается окно, в котором Вы можете определить дальнейшие действия с инфицированным Email или вложением. Эта опция включена по умолчанию.

показывать прогресс выполнения

Если эта опция включена, MailGuard отображает индикатор выполнения в процессе загрузки электронной корреспонденции. Эта опция доступна, если была выбрана опция **интерактивно**.

Автоматически

Если эта опция включена, Вы не будете получать уведомлений при обнаружении вируса или вредоносной программы. MailGuard реагирует на определенные Вами в этом разделе установки.

Первичное действие

Первичное действие определяет операцию, выполняемую в случае, если MailGuard обнаруживает в письме вирус или вредоносную программу. Если установлена опция **пропустить письмо**, в меню **инфицированные вложения** можно дополнительно определить, какие действия должны выполняться в случае обнаружения подозрительных объектов в приложении.

удалить письмо

Если эта опция включена, инфицированное письмо автоматически удаляется при обнаружении вируса или вредоносной программы. Тело письма заменяется текстовым шаблоном. Такая же операция определена и для вложений. Такая же процедура определена и для всех вложений. Они также заменяются текстовым шаблоном.

поместить письмо в карантин

Если опция включена, при обнаружении вируса или вредоносной программы в карантин помещается все письмо, включая вложения. Позже, если потребуется, можно восстановить письмо. Инфицированное письмо удаляется. Тело письма заменяется текстовым шаблоном. Такая же операция определена и для вложений. Они также заменяются стандартным текстовым шаблоном.

пропустить письмо

Если эта опция включена, инфицированное письмо пропускается даже в случае обнаружения в нем вируса или вредоносной программы. Вы можете решить, какие действия необходимо выполнить с вложением:

Инфицированные вложения

Опция **Инфицированные вложения** может быть выбрана только в том случае, когда для **Первичного действия** определена операция **пропустить письмо**. Эта опция определяет, какие действия должны быть предприняты в случае обнаружения подозрительных объектов во вложении.

удалить

Если эта опция включена, инфицированное вложение удаляется при обнаружении вируса или вредоносной программы. Файл при этом заменяется другим файлом, содержащим текстовый шаблон.

поместить в карантин

Если эта опция включена, инфицированное приложение помещается в карантин, а затем удаляется (заменяется текстовым шаблоном). Инфицированное вложение может быть позже, если потребуется, восстановлено.

Пропустить

Если эта опция включена, инфицированное вложение, несмотря на обнаружение вируса или вредоносной программы, игнорируется и пропускается адресату.

Предупреждение
Если Вы выбираете эту опцию, MailGuard больше не защищает Вашу систему от вирусов и вредоносных программ. Выбирайте этот пункт только в том случае, если Вы точно знаете, что делаете. Отключите предварительный просмотр в Вашей почтовой программе и ни в коем случае ни запускайте приложения двойным щелчком!

13.3.1.2. Другие действия

Этот раздел настроек содержит дополнительные настройки, выбор действий, которые могут быть выполнены после обнаружения MailGuard вируса или вредоносного ПО в письме или вложении.

Примечание
Выбранные здесь действия происходят автоматически при обнаружении вируса во входящих письмах.

Шаблон для удаленных и перемещенных Email

Этот текст добавляется в тело письма в виде сообщения. Вы можете редактировать это сообщение. Текст не может превышать 500 знаков.

Следующая комбинация клавиш может использоваться для форматирования:

Strg + Enter добавляет разрыв строки.

По умолчанию

Кнопка позволяет добавить стандартный шаблон в текстовое поле.

Шаблон для удаленных и перемещенных вложений

Этот текст заменяет собой инфицированное вложение. Вы можете редактировать это сообщение. Текст не может превышать 500 знаков.

Следующая комбинация клавиш может использоваться для форматирования:

Strg + Enter добавляет разрыв строки.

По умолчанию

Кнопка позволяет добавить стандартный шаблон в текстовое поле.

13.3.1.3. Эвристика

Этот раздел настроек содержит параметры эвристического поиска Avira Premium Security Suite.

Avira Premium Security Suite содержит эвристические системы, которые сразу распознают вредоносные программы, то есть до составления специальной вирусной сигнатуры и получения обновления защиты от вирусов. Распознавание вирусов осуществляется при помощи подробного анализа инфицированного кода на предмет выполняемых функций и действий, типичных для вредоносных программ. Если исследуемый код имеет характерные признаки, он получает статус подозрительного. Это не означает, что объект в любом случае является вредоносной программой. Возможны также ложные срабатывания. Решение о том, что необходимо сделать с подозрительным объектом, принимает сам пользователь. Решение может быть основано, например, на знании о происхождении файла.

Эвристика (Макровирусы)

Обнаруживать макровирусы эвристическими методами

Avira Premium Security Suite имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, подозрительные файлы регистрируются, пользователь получает об этом уведомление. Эта настройка по умолчанию включена и является нашей рекомендацией.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Avira Premium Security Suite благодаря технологии AntiVir AHeAD содержит очень мощную эвристическую систему для определения даже неизвестных вирусов и (новых) вредоносных программ. Вы можете установить уровень "резкости" эвристики. Эта настройка активна по умолчанию.

Низкий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite обнаруживает меньше неизвестных вредоносных программ.

Средний уровень обнаружения

Эта настройка определена по умолчанию, если Вы используете эвристический поиск. Эта настройка по умолчанию включена и является нашей рекомендацией.

Высокий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite распознает значительно больше неизвестных вирусов или вредоносных программ, но возможны и ложные срабатывания.

13.3.1.4. AntiBot

Функция AntiBot модуля MailGuard предотвращает использование Вашего компьютера как части так называемой Бот-сети, создающейся для распространения спама. При распространении спама с помощью бот-сетей злоумышленник инфицирует чужие компьютеры ботом, который подключается к IRC-серверу на определенный канал и переходит в режим ожидания команды на рассылку нежелательной корреспонденции. Для того, чтобы отличать спам-письма неизвестного бота от писем пользователя, MailGuard проверяет, указан ли используемый SMTP-сервер и отправитель исходящего письма в списке разрешенных серверов и отправителей. Если сервера или адреса нет в списке, исходящее письмо блокируется и не будет отправлено. Отображается диалоговое окно, в котором Вы можете выбрать производимое с письмом действие.

Примечание
Функция AntiBot может быть использована, если в MailGuard включена проверка исходящих писем (см. опцию **Проверять исходящие письма** в разделе MailGuard :: Проверка).

Разрешенные серверы

Все серверы из этого списка имеют разрешение MailGuard для отправки писем: Письма, отправляемые на эти серверы, **не** блокируются MailGuard. Если в списке не указаны серверы, при отправке писем используемый SMTP-сервер не проверяется. Если в списке есть строки, MailGuard блокирует письма, отправленные на SMTP-сервер, но не содержащиеся в списке.

Поле ввода

Здесь Вы указываете host или IP-адрес SMTP-сервера, который Вы используете для отправки Ваших писем.

Примечание
Параметры SMTP-серверов, применяемых для отправки Ваших писем, Вы найдете в Вашей клиентской программе среди параметров учетных записей.

Добавить

Кнопка добавляет указанный в поле ввода сервер к списку разрешенных.

Удалить

Кнопка удаляет выделенную строку из списка разрешенных серверов. Кнопка неактивна, если ни одна строка не выделена.

Удалить все

Кнопка удаляет все строки списка разрешенных серверов.

Разрешенный отправитель

Все отправители из этого списка имеют разрешение MailGuard для отправки писем: письма, отправляемые с этого адреса, не блокируются MailGuard. Если в списке не указан ни один отправитель, разрешенные адреса для исходящих писем не проверяются. Если в списке есть строки, MailGuard блокирует письма отправителей, не содержащихся в списке.

Поле ввода

В этом поле укажите адрес отправителя.

Добавить

Кнопка добавляет указанные в поле ввода адреса отправителей к списку разрешенных отправителей.

Удалить

Кнопка удаляет выделенную строку из списка разрешенных отправителей. Кнопка неактивна, если ни одна строка не выделена.

Удалить все

Кнопка удаляет все строки списка разрешенных отправителей.

13.3.2 Общее

13.3.2.1. Исключения

Адреса, не подвергающиеся проверке

Эта таблица показывает список адресов, исключенных из проверки модулем AntiVir MailGuard (белый список).

Примечание
Список исключений применяется только для входящих писем MailGuard.

Статус

Пиктограмма	Описание
	Этот адрес больше не проверяется на предмет спама.
	Этот адрес не проверяется на наличие вредоносных программ.
	Этот адрес не проверяется на наличие вредоносного ПО и спама.

Email

Адреса, которые больше не подвергаются проверке.

Вредоносное ПО

Если опция включена, адрес больше не проверяется на наличие вредоносного ПО.

Спам

Если опция включена, адрес больше не проверяется на наличие спама.

вверх

Кнопка перемещает выделенный адрес на одну позицию вверх. Кнопка неактивна, если не выделена ни одна строка или курсор стоит вверху списка.

вниз

Кнопка перемещает выделенные выделенный адрес на одну позицию вниз. Кнопка неактивна, если не выделена ни одна строка или курсор находится на нижней строке.

Поле ввода

В этом поле укажите адрес, который хотите добавить к списку адресов, не подвергающихся проверке. В дальнейшем в зависимости от Ваших настроек Email-адрес более не проверяется модулем MailGuard.

Примечание
При вводе Email-адресов Вы можете применять заменители символов: ***** - для последовательности знаков, **?** для замены одного символа. Заменители могут использоваться только в адресах, которые не проверяются модулем AntiSpam. Вы получите сообщение об ошибке, если попытаетесь добавить адрес с заменителем символов в список исключений, активирую в списке исключений Checkbox **Вредоносное ПО**. При вводе адресов с заменителями символов следите за соблюдением структуры адреса электронной почты(*@*.*)

Предупреждение
При использовании заменителей символов помните о приведенных примерах. Применяйте заменители символов осторожно и всегда проверяйте, какие адреса Email вы добавляете таким образом в "белый" список.

Примеры: Использование заменителей в адресах Email ("белый" список)

- `virus@avira.* /` = охватывает все письма с этим адресом и любым доменом первого уровня: virus@avira.de, virus@avira.com, virus@avira.net,...
- `*@avira.com` = охватывает все письма, отправленные из домена **avira.com:** info@avira.com, virus@avira.com, marketing@avira.com
- `info@*.com` = охватывает все адреса Email с доменов первого уровня **com** и с адресом **info**: домен второго уровня может быть любым: info@name1.com, info@name2.com,...

Добавить

Вы можете добавить к списку не подвергающихся проверке адресов, адрес, указанный в поле ввода.

Удалить

Кнопка удаляет выделенный адрес из списка

Импортировать адресную книгу Outlook

С помощью этой кнопки Вы можете импортировать адреса Email из адресной книги MS Outlook в список исключений. Импортированные адреса Email не проверяются на наличие спама.

Импортировать адресную книгу Outlook Express

С помощью этой кнопки Вы можете импортировать адреса Email из адресной книги MS Outlook Express список исключений. Импортированные адреса Email не проверяются на наличие спама.

13.3.2.2. Буферная память

Буферная память

Буферная память MailGuard содержит данные о проверенных письмах, которые отображаются в статистике в Центр контроля / MailGuard. Копии входящих писем сохраняются в буферной памяти. Письма используются для целей обучения модуля AntiSpam (Снять отметку спам &endash;(режим обучения), Отметить письмо как спам &endash;(режим обучения)).

Примечание
Для сохранения входящих писем в буферной памяти необходимо активировать модуль антиспам.

Максимальное число писем для хранения в буферной памяти

В этом поле указывается максимальное число писем, которые могут храниться в буферной памяти модуля MailGuard. При переполнении буфера сначала удаляются старые письма.

Максимальная продолжительность хранения писем в днях:

В этом поле указывается максимальная продолжительность хранения писем в днях. По истечении этого времени письма удаляются из буфера.

Очистить буфер

Для очищения буфера от писем, хранящихся в нем, нажмите эту кнопку.

13.3.2.3. MailGuard

Антиспам

AntiVir MailGuard проверяет письма на вирусы и вредоносные программы. Система имеет функции защиты от нежелательной корреспонденции (спама).

Антиспам

Включить Антиспам

Если опция включена, функция АнтиСпам в модуле MailGuard активна.

Выделить тему письма

Если эта опция включена, при обнаружении объекта к теме письма добавляется примечание.

Просто

К строке "касательно" спам- или фишинг-письма добавляется примечание [СПАМ] или [Фишинг]. Эта опция включена по умолчанию.

Подробно

К теме спам- или фишинг-письма добавляется расширенное примечание о вероятности того, что вы имеете дело со спамом.

Протоколировать

Если опция включена, MailGuard создает специальный AntiSpam-отчет.

Использовать черный список

Если эта опция включена, в режиме реального времени опрашивается т.н. "черный список", помогающий классифицировать письма неизвестного происхождения как спам.

Период: n сек

Если через n секунд данные из черного списка все еще недоступны, попытка запроса черного списка прерывается.

Удалить учебную базу данных

Кнопка удаляет учебную базу данных.

Автоматически добавлять получателя исходящего письма в "белый" список

Если опция включена, все адреса получателей автоматически добавляются в белый спам-список (список писем, не проверяемых на наличие спама **MailGuard ::Общее :: Исключения**). Входящие письма, отправленные с адресов, находящихся в белом списке, не проверяются модулем AntiSpam. Проверка на вирусы и вредоносное ПО не прекращается. Эта опция по умолчанию отключена.

Примечание
Эта опция может быть выбрана, если MailGuard проверяет исходящие письма (см. опцию **Проверять исходящие письма** в MailGuard :: Проверка).

13.3.3 Отчет

MailGuard располагает мощной функцией протоколирования, что дает пользователю/администратору точные данные о типе и способе обнаружения.

Протоколирование

Здесь определяются объемные параметры файла отчета.

Не требуется

Если опция включена, MailGuard не создает файл отчета.
Мы рекомендуем отказываться от протоколирования только в экстренных случаях, например, если Вы производите тестирование продукта на большой базе вирусов.

По умолчанию

Если опция включена, MailGuard сохраняет важную информацию (об обнаружениях, предупреждениях и ошибках) в файле отчета, менее важная информация в отчет не вносится. Эта настройка активна по умолчанию.

Расширенный

Если опция включена, MailGuard записывает в файл отчета и менее важную информацию.

полная

При включенной опции MailGuard записывает информацию (размер и тип файла, дата создания) в файл отчета.

Ограничения для файлов отчетов

Максимум n Мб

Если опция включена, файл отчета может быть ограничен до определенного размера; диапазон: от 1 до 100 Мб. Эта настройка по умолчанию включена. Установлено ограничение в 1 Мб. Чтобы избежать высокой загрузки системы, устанавливается ограничение в 50 Кб сверх нормы. Если размера файла отчета превышает установленный лимит на 50 Кб, старые записи автоматически удаляются до тех пор, пока размер не приводится в соответствие.

Не сокращать файл отчета

Если опция включена, создается резервная копия файла отчета перед его сокращением.

Сохранение настроек в файле отчета

Если опция включена, применяемые настройки MailGuard записываются в файл отчета.

13.4 Firewall

Рубрика Firewall в Avira Premium Security Suite. Настройка отвечает за настройку Avira Firewall.

13.4.1 Правила адаптера

Под адаптером в Avira Firewall понимается эмулируемая программными средствами аппаратура (напр., miniport, bridge connection и т.д.) или аппаратные средства (напр., сетевая карта).

Avira Firewall показывает правила адаптера для всех адаптеров Вашего компьютера, имеющих установленный драйвер.

Предустановленное правило адаптера зависит от уровня безопасности. Вы можете изменять уровень безопасности в разделе Online-защита :: Firewall des Avira Premium Security Suite Центр контроля или привести правила адаптера в соответствие с Вашими потребностями. Если Вы настроили правила адаптера под Ваши потребности, в разделе Firewall Avira Premium Security Suite Центр контроля ползунок будет перемещен в положение Выбор.

Примечание
Стандартная настройка Уровня безопасности для всех предопределенных правил Avira Firewall - **Высокий**.

ICMP-Protokoll

Internet Control Message Protocol (ICMP) служит для сетевого обмена информационными сообщениями и сообщениями об ошибках. Протокол применяется также для статусных сообщений Ping или Tracert.
Эти правила позволят Вам назначить типы входящих и исходящих ICMP, которые необходимо блокировать, установить параметры для флудинга и определить поведение в отношении фрагментированных ICMP-пакетов. Это правило служит для предотвращения т.н. ICPM флуд-атак, которые могут привести к загрузке или перегрузке процессора атакуемого компьютера в связи с необходимостью обработки каждого запроса.

Предустановленные правила для ICMP-протокола

Установка: низкий	Установка: средний	Установка: высокий
Блокирует входящие типы: **ни один тип**. Блокирует исходящие типы: **ни один тип**. Подозрение на флудинг, если задержка между пакетами составляет менее **50** миллисекунд. Фрагментированные ICMP-пакеты **отклонять**.	Правило аналогичное опции Низкий.	Блокирует входящие типы: **различные типы**. Блокирует исходящие типы: **различные типы**. Подозрение на флудинг, если задержка между пакетами составляет менее **50** миллисекунд. Фрагментированные ICMP-пакеты **отклонять**.

Заблокированные входящие типы: ни один тип/различные типы

Щелчком по ссылке можно открыть список типов пакетов ICMP. Из этого списка Вы можете выбрать те входящие типы сообщений ICMP, которые необходимо блокировать.

Заблокированные исходящие типы: ни один тип/различные типы

Щелчком по ссылке можно открыть список типов пакетов ICMP. Из этого списка Вы можете выбрать те исходящие типы сообщений ICMP, которые необходимо блокировать.

Флудинг

Здесь Вы можете ввести максимальное значение для разрешенной ICMP-задержки.

Фрагментированные ICMP-пакеты

Здесь Вы можете установить правила, по которым принимаются или отклоняются фрагментированные ICMP пакеты.

TCP Port-Scan

Здесь Вы можете установить правила, по которым Firewall принимает решение о TCP Port-Scan и определить, как он должен действовать в этом случае. Правило для предотвращения т.н. TCP Port-Scan атак, с помощью которых можно определить открытые FTP порты Вашего компьютера. Атаки такого рода предназначены для того, чтобы максимально использовать слабые места Вашего компьютера, через которые можно проводить более опасные атаки.

Предустановленные правила для TCP Port-Scan

Установка: низкий	Установка: средний	Установка: высокий
Подозрение на TCP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в**файл отчета** и для блокирования атаки установить правило**не добавлять**.	Подозрение на TCP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в **файл отчета** и для блокирования атаки установить правило **добавлять**.	Правило аналогичное опции Средний.

Порты

Здесь Вы можете выбрать число сканируемых портов, при достижении которого принимается решение об обнаружении TCP Port-Scan.

Временные параметры Port-Scan

Здесь Вы можете определить период времени для сканирования установленного числа портов, достаточный для принятия решения об обнаружении TCP Port-Scan.

Файл отчета

Здесь Вы можете определить необходимость сохранения в файле отчета IP-адрес злоумышленника.

Правило

Здесь Вы можете определить правила, по которым принимается решение о необходимости блокирования атаки TCP Port-Scan.

UDP Port-Scan

Здесь Вы можете определить, когда Firewall принимает решение об обнаружении UDP Port-Scan, а также указать необходимые действия. Правило для предотвращения т.н. UDP Port-Scan атак, с помощью которых можно определить открытые UDP порты Вашего компьютера. Атаки такого рода предназначены для того, чтобы максимально использовать слабые места Вашего компьютера, через которые можно проводить более опасные атаки.

Предустановленные правила для UDP Port-Scan

Установка: низкий	Установка: средний	Установка: высокий
Подозрение на UDP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении UDP Port-Scan, IP-адрес злоумышленника сохранять в **файл отчета** и для	Подозрение на UDP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в **файл отчета** и для блокирования	Правило аналогичное опции Средний.

предотвращения атаки **не добавлять** правила.	атаки установить правило **добавлять**.	

Порты

Здесь Вы можете выбрать число сканируемых портов, при достижении которого принимается решение об обнаружении UDP Port-Scan.

Временные параметры Port-Scan

Здесь Вы можете определить период времени для сканирования установленного числа портов, достаточный для принятия решения об обнаружении UDP Port-Scan.

Файл отчета

Здесь Вы можете определить необходимость сохранения в файле отчета IP-адрес злоумышленника.

Правило

Здесь Вы можете определить правила, по которым принимается решение о необходимости блокирования атаки UDP Port-Scan.

13.4.1.1. Входящие правила

Посредством входящих правил Avira Firewall контролирует входящий трафик.

Примечание
Так как при фильтрации пакетов определенные правила применяются друг за другом, их последовательность имеет важнейшее значение. Старайтесь изменять последовательность только когда Вы полностью уверены в том, какие последствия это вызовет.

Предустановленные правила мониторинга TCP-трафика

Установка: низкий	Установка: средний	Установка: высокий
Avira Firewall не блокирует входящий трафик.	– Разрешить установленное через порт 135 TCP-соединение Разрешить TCP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если номер локального порта **{135}** и номер удаленного порта **{0-65535}**. Применять для **Пакетов существующих соединений**.	– Отслеживать разрешенный TCP-трафик Разрешать TCP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт **{0-65535}** и удаленный порт **{0-65535}**. Применять для **Пакетов существующих соединений**. **Не сохранять в файл отчета**, если пакет соответствует

	Не сохранять в файл отчета, если пакет соответствует правилу. Расширенн.: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**. – Запрещать TCP пакеты для порта 135 Запрещать TCP-пакеты , с адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в**{135}** а удаленный порт находится в **{0-65535}**. Применять ко **всем пакетам**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенн.: Отклонять пакеты объемом **<пустые>** с маской **<пустые>** оффсет **0**. – Отслеживать конформный TCP трафик Разрешать TCP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт **{0-65535}** и	правилу. Расширенн.: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.

	удаленный порт **{0-65535}**. Применять **началу установления соединения и к пакетам существующего соединения. Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенн.: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**. – Запрещать все TCP-пакеты Запрещать TCP-пакеты , с адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в **{0-65535}** а удаленный порт находится в **{0-65535}**. Применять ко **всем пакетам**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенн.: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.	

TCP-пакеты разрешать / запрещать

Здесь Вы можете установить разрешения или запреты для определенных TCP-пакетов.

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Локальные порты

Здесь Вы можете указать желаемые локальные порты или целые диапазоны портов.

Удаленные порты

Здесь Вы можете указать желаемые удаленные порты или целые диапазоны портов.

Метод применения

Здесь Вы можете определить необходимость применения правила к пакетам существующих соединений или ко всем соединениям.

Файл отчета

Здесь Вы можете определить необходимость сохранения информации в файле отчета, если пакет соответствует правилу.

Опция **Расширенный** позволяет фильтровать на основании содержимого. Вы можете, например, отклонять пакеты, содержащие специальные данные, которые имеют определенный оффсет. Если Вы не желаете использовать эту опцию, не выбирайте вообще или выберите пустой файл.

Фильтр содержимого: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтр содержимого: маска

Здесь Вы можете указать специальную маску.

Фильтр содержимого: оффсет

Здесь Вы можете указать оффсет для фильтра содержимого. Оффсет рассчитывается с конца заголовка TCP.

Предустановленные правила мониторинга UDP-трафика

Установка: низкий	Установка: средний	Установка: высокий
-	– Отслеживание конформного UDP трафика Разрешать UDP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт **{0-65535}** и удаленный порт **{0-65535}**.	Отслеживать разрешенный UDP-трафик Разрешать UDP-Pakete , с адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в **{0-65535}** а удаленный

	Применять правило к **открытым портам**. **Расширенн.: Отклонять пакеты следующего объема <пустые> с маской <пустые> на оффсет 0.** – **Запрещать все UDP-пакеты** **Запрещать UDP-пакеты , с адреса 0.0.0.0 с маской 0.0.0.0, если локальный порт находится в {0-65535} а удаленный порт находится в {0-65535}. Применять ко всем портам. Не сохранять в файл отчета, если пакет соответствует правилу. Расширенн.: Отклонять пакеты следующего объема <пустые> с маской <пустые> на оффсет 0.**	порт находится в**{53, 67, 68, 123}**. Применять правило к **открытым портам**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенн.: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** на оффсет **0**.

Разрешать / запрещать UDP-пакеты

Здесь Вы можете установить разрешения или запреты для определенных UDP-пакетов.

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Локальные порты

Здесь Вы можете указать желаемые локальные порты или целые диапазоны портов.

Удаленные порты

Здесь Вы можете указать желаемые удаленные порты или целые диапазоны портов.

Метод применения

Здесь Вы можете определить необходимость применения правила ко всем портам или только ко всем открытым портам.

Файл отчета

Здесь Вы можете определить необходимость сохранения информации в файле отчета, если пакет соответствует правилу.

Опция **Расширенный** позволяет фильтровать на основании содержимого. Вы можете, например, отклонять пакеты, содержащие специальные данные с определенным оффсет. Если Вы не желаете использовать эту опцию, не выбирайте вообще или выберите пустой файл.

Фильтр содержимого: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтр содержимого: маска

Здесь Вы можете указать специальную маску.

Фильтр содержимого: оффсет

Здесь Вы можете указать оффсет для фильтра содержимого. Оффсет рассчитывается с конца заголовка UDP.

Предустановленные правила мониторинга ICMP-трафика

Установка: низкий	Установка: средний	Установка: высокий
-	– Не отклонять ICMP-пакеты на основании IP-адреса РазрешатьICMP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенн.: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** на оффсет **0**.	Правило аналогичное опции Средний.

Разрешать / запрещать ICMP-пакеты

Здесь Вы можете установить разрешения или запреты для определенных ICMP-пакетов.

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Файл отчета

Здесь Вы можете определить необходимость сохранения информации в файле отчета, если пакет соответствует правилу.

Опция **Расширенный** позволяет фильтровать на основании содержимого. Вы можете, например, отклонять пакеты, содержащие специальные данные с определенным оффсет. Если Вы не желаете использовать эту опцию, не выбирайте вообще или выберите пустой файл.

Фильтр содержимого: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтр содержимого: маска

Здесь Вы можете указать специальную маску.

Фильтр содержимого: оффсет

Здесь Вы можете указать оффсет для фильтра содержимого. Оффсет рассчитывается с конца заголовка ICMP.

Предустановленное правило для IP-пакетов

Установка: низкий	Установка: средний	Установка: высокий
-	-	Запрещать все IP-пакеты Запретить IP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**. **Не сохранять в файл отчета**, если пакет соответствует правилу.

Разрешать / запрещать IP-пакеты

Здесь Вы можете определить необходимость разрешения или запрета определенных IP-пакетов.

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Файл отчета

Здесь Вы можете определить необходимость сохранения информации в файле отчета, если пакет соответствует правилу.

Возможные правила мониторинга IP-пакетов на основании IP-протоколов

IP-пакеты

Здесь Вы можете определить необходимость разрешения или запрета определенных IP-пакетов.

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Протокол

Здесь Вы можете выбрать желаемый IP-протокол.

Файл отчета

Здесь Вы можете определить необходимость сохранения информации в файле отчета, если пакет соответствует правилу.

13.4.1.2. Исходящие правила

Avira Firewall контролирует исходящий трафик с помощью исходящих правил. Вы можете различать правила для протоколов: IP, ICMP, UDP и TCP.

Примечание
Так как при фильтрации пакетов определенные правила применяются друг за другом, их последовательность имеет важнейшее значение. Старайтесь изменять последовательность только когда Вы полностью уверены в том, какие последствия это вызовет.

Кнопки

Кнопка	Описание
Добавить	Позволяет создать новое правило. Щелкните по этой кнопке для отображения окна "Добавить правило". В этом диалоговом окне Вы можете выбрать новые входящие и исходящие правила.
Удалить	Удалить правило.
Вниз	Переместить выбранное правило на одну позицию вниз, благодаря чему снизиться приоритет данного правила.
Вверх	Переместить выбранное правило на одну позицию вверх.
Переименовать	Переименовать правило.

Примечание
Вы можете добавлять новые правила для отдельных адаптеров или для всех адаптеров компьютера. Чтобы добавить правило для всех адаптеров, выберите **Компьютер** в представленной структуре адаптеров и нажмите кнопку **Добавить**.

Примечание
Чтобы изменить позицию правила, вы можете перенести его в нужную позицию с помощью мыши.

13.4.2 Правила применения

Правила применения для пользователя

Этот список содержит имена всех пользователей системы. Если Вы зарегистрированы с правами администратора, Вы можете выбрать пользователя, для которого желаете создать правила. Если Вы не являетесь пользователем с привилегированными правами, Вы увидите в списке только имя текущего пользователя.

Список приложений

Здесь отображается список приложений, для которых определены правила. Список содержит настройки для каждого приложения, которые было запущено после того, как был установлен Avira Firewall, а также, если для приложения было создано правило.

Стандартный вид

	Описание
Приложение	Имя приложения.
Режим	Показывает установленный режим правила приложения : Отфильтрованные в режиме проверяются и выполняются правила адаптера в соответствии с выполнением правила приложения. Привилегированные в режиме правила адаптера игнорируются. Здесь с помощью щелчка мыши Вы можете сменить режим.
Действие	Отображает действие, которое Avira Firewall выполняет автоматически, если приложение каким-либо образом использует сеть. Здесь с помощью щелчка мыши Вы можете сменить тип выполняемого действия. Типы действий **Спрашивать**, **Разрешать** или **Запрещать**. Стандартная установка **Спрашивать**.

Расширенная настройка

Если Вы хотите индивидуально регулировать сетевые доступы приложения, то Вы можете создавать определенные правила приложения, сравнимые с правилами адаптера, основанные на фильтрах пакетов. Для выбора расширенной настройки правил приложения сначала должен быть включен режим эксперта. Измените в разделе Firewall:: Настройки следующие настройки правил приложения: Активируйте опцию **Расширенные настройки** и сохраните настройки с помощью команды **Применить** или **OK**. В списке правил приложения Вы можете дополнительно выбрать вид действия *Расширенный* с помощью ссылки *Настроить*:

	Описание
Приложение	Имя приложения.
Режим	Показывает установленный режим правила приложения :

	Отфильтрованные в режиме проверяются и выполняются правила адаптера в соответствии с выполнением правила приложения. Привилегированные в режиме правила адаптера игнорируются. Здесь с помощью щелчка мыши Вы можете сменить режим.
Действие	Отображает действие, которое Avira Firewall выполняет автоматически, если приложение каким-либо образом использует сеть. Здесь Вы можете сменить тип выполняемого действия. Типы действий **Спрашивать**, **Разрешать, Запрещать** или *Расширенный*.
Расширенный	Показывает при выборе типа действий *Расширенный* ссылку *Настроить*. С помощью настройки Вы можете перейти к расширенной настройке правил приложения.

Определенные правила приложения в расширенной настройке.

С помощью определенных правил приложения вы можете разрешить или запретить определенный трафик приложения, а также разрешить или запретить пассивное прослушивание отдельных портов. Вы располагаете следующими опциями настройки:

- Разрешить или запретить кодовую инъекцию

  Кодовая инъекция - это способ запуска кода на исполнение в адресном пространстве другого процесса, при котором этот процесс вынужден загружать Dynamic Link Library (DLL). Кодовых инъекций используется разработчиками вредоносных программ для выполнения кода под прикрытием другой программы. Так можно, например, обмануть Firewall, скрыв от него сетевую атаку. По умолчанию кодовые инъекции разрешены для всех подписанных приложений.

- Разрешить или запретить пассивное прослушивание приложения портов
- Разрешить или запретить трафик:

  Разрешить или запретить входящие и/или исходящие IP-пакеты

  Разрешить или запретить входящие и/или исходящие TCP-пакеты

  Разрешить или запретить входящие и/или исходящие UDP-пакеты

Для каждого приложения Вы можете создать любое количество правил приложения. Правила приложения выполняются в отображенной последовательности .

Примечание
Если Вы измените действие *Расширенное* для правила приложения, то заданные ранее правила приложения в расширенной настройке будут не окончательно удалены, а только отключены. Если Вы снова перейдете к типу действия *Расширенный*, то заданные ранее правила приложения будут снова включены и отображены в окне расширенной настройки для правил приложения.

Информация о приложении

Здесь отображается детальная информация о приложении, выбранном Вами в списке приложений.

	Описание

Имя	Имя приложения.
Путь	Полный путь к исполняемому файлу.

Кнопки

Кнопка	Описание
Добавить приложение.	Вы можете создать новое правило приложения. После щелчка по этой кнопке отображается окно. Вы можете выбрать приложение, для которого необходимо создать правило.
Удалить правило	Удалить выбранное правило приложения.
Обновить	Обновление списка приложений с одновременной отменой всех изменений, сделанных в правилах приложения.

13.4.3 Надежные разработчики

В разделе *Надежные разработчики* показывается список надежных производителей программного обеспечения. Вы можете добавить или удалить разработчика из списка, используя опцию *Всегда доверять этому разработчику* в окне Popup *сетевого события*. Вы можете разрешить по умолчанию сетевой доступ приложений, которые подписаны разработчиками из списка, активировав опцию **Автоматически разрешать приложения от надежных разработчиков**.

Надежные разработчики для пользователей

Этот список содержит имена всех пользователей системы. Если Вы зарегистрированы с правами администратора, Вы можете выбрать пользователя, список надежных разработчиков которого Вы хотите просмотреть или редактировать. Если Вы не являетесь пользователем с привилегированными правами, Вы увидите в списке только имя текущего пользователя.

Автоматически разрешать приложения от надежных производителей

При включенной опции приложения, подписанные известными и надежными производителями, получают доступ к сети. Эта опция включена по умолчанию.

Производители

Список показывает всех производителей, которые классифицируются как надежные.

Кнопки

Кнопка	Описание

Удалить	Отмеченная запись удаляется из списка надежных разработчиков. Чтобы окончательно удалить производителя из списка, нажмите **Применить** или **OK** в окне настройки.
Обновить	Изменения отменяются. Последний сохраненный список загружается.

Примечание
Если Вы удалите разработчика из списка, а затем нажмете кнопку **Применить**, разработчики окончательно удаляются из списка. Изменение не может быть отменено командой *Обновить*. Однако у Вас есть возможность с помощью опции *Всегда доверять этому производителю* во всплывающем окне *Сетевое событие* снова добавить в список надежного производителя.

Примечание
Firewall дает приоритет правилам приложения перед записями, внесенными в список надежных разработчиков: Если Вы создали правило приложения и разработчик находится в списке надежных поставщиков, то правило приложения выполняется.

13.4.4 Установки

Временной интервал

Всегда блокировать

Если опция включена, правило, созданное автоматически при сканировании портов, сохраняется.

Удалять правило через n сек.

Если эта опция включена, правила, созданные автоматически при сканировании портов, удаляются по истечении указанного Вами времени. Эта опция включена по умолчанию.

Расширенные настройки

Windows Host-файл НЕ ЗАБЛОКИРОВАН/ЗАБЛОКИРОВАН

Если эта опция установлена как ЗАБЛОКИРОВАНО, Windows Host-файл защищен от записи. Любые манипуляции с файлами больше невозможны. Вредоносное ПО, например, больше не в состоянии перенаправлять Ваши запросы на нежелательные страницы. По умолчанию эта опция установлена на НЕ ЗАБЛОКИРОВАН.

Отключать при загрузке Windows Firewall

Если опция включена, при загрузке системы отключается Windows Firewall. Эта опция включена по умолчанию.

Уведомления

Определите среди уведомлений, при каких событиях Вы хотите получать уведомление в виде всплывающего окна Firewall.

Port-Scan

При включенной опции Вы получаете уведомление в виде всплывающего окна, если Firewall был распознан Port Scan.

Блокируются соединения.

При включенной опции Вы получаете уведомление в виде всплывающего окна, если Firewall запретил, т.е. блокировал сетевую активность приложения.

Флудинг

При включенной опции Вы получаете уведомление в виде всплывающего окна, если Firewall был распознана флуд-атака.

IP блокирован

При включенной опции Вы получаете уведомление в виде всплывающего окна, если Firewall запретил трафик данных с IP-адреса.

Правила приложения

С помощью опций в области правил приложения Вы устанавливаете возможности настройки правил приложения в разделе Firewall::Правила приложения.

Расширенные настройки

При включенной опции у Вас есть возможность индивидуальной регулировки различных сетевых доступов приложения.

Основные установки

При включенной опции может быть установлено единственное действие для различных сетевых доступов приложения.

13.4.5 Настройки всплывающего окна

Настройки всплывающего окна

Проверить стартовый блок процесса

Если опция включена, происходит точная проверка списка процессов. Firewall исходит из того, что каждый подозрительный процесс из списка, порождает дочерний процесс, через который можно получить доступ к сети. Поэтому в таких случаях для каждого подозрительного процесса из списка открывается отдельное всплывающее окно. Эта опция по умолчанию отключена.

Показывать несколько диалоговых окон для процесса

Если опция включена, каждый раз при попытке приложения установить сетевое соединение открывается Popup-окно. Альтернативно это может происходить только после первой попытки. Эта опция по умолчанию отключена.

Автоматически подавлять всплывающее уведомление в игровом режиме

При активированной опции происходит автоматическое переключение Avira Firewall в игровой режим, если приложение на Вашем компьютере выполняется в полноэкранном режиме. В игровом режиме применяются все установленные правила адаптера и приложений. Приложения, для которых не определено таких правил с действиями, как *Разрешить* или *Запретить*, сетевой доступ разрешается временно, так что окно Popup с запросами по сетевым событиям не открывается.

Сохранять действие для приложения

Всегда вкл.

Если опция включена, по умолчанию активна опция "Сохранять действие для приложения" диалогового окна "Сетевое событие". Эта опция включена по умолчанию.

Всегда откл.

Если опция включена, неактивна опция "Сохранять действие для приложения" диалогового окна "Сетевые события".

Разрешать подписанные приложения

Если опция включена, при получении подписанным приложением определенного разработчика доступа к сети автоматически активна опция "Сохранять действие для приложения" диалогового окна "Сетевое событие" Производители: Производители: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Сохранять состояние

При включенной опции активация опции "Сохранить действие для этого приложения" диалогового окна "Сетевое событие" используется как при последнем сетевом событии. Если при последнем сетевом событии была активна опция "Сохранять действие для приложения", она также будет активна при следующем. Если при последнем сетевом событии опция "Сохранять действие для приложения" отключена, опция отключена также при следующем.

Показывать подробности

В этой группе опций настройки Вы можете настроить отображение в окне **сетевых событий** подробной информации.

Подробности - по запросу

Если опция включена, в окне *сетевых событий* информация отображается только по запросу, т.е. отображение подробной информации осуществляется после нажатия кнопки **Подробности** в окне *Сетевые события*.

Всегда показывать подробности

Если опция включена, подробности всегда отображаются в окне *сетевых событий*.

Сохранять состояние

Если опция включена, статус отображения подробностей сохраняется на будущее. Если при последнем сетевом событии подробности отображались или вызывались, они также будут отображаться при наступлении следующего события. Если при последнем сетевом событии подробности не отображались или были отключены, подробности при последующих событиях отображаться не будут.

Разрешать привилегированные

В этой группе опций настройки Вы можете настроить статус опции *Разрешать привилегированные* в окне **Сетевое событие**.

Всегда вкл.

Если опция включена, по умолчанию активна опция *Разрешать привилигерованные* в окне *Сетевое событие*.

Всегда откл.

Если опция выключена, по умолчанию активна опция *Разрешать привилигерованные* в окне *Сетевое событие*.

Сохранять состояние

При включенной опции статус опции *Разрешать привилегированные* в окне *Сетевое событие* используется как при предыдущем сетевом событии. Если при выполнении последнего сетевого события опция *Разрешать привилегированные* включена, опция включена также при следующем событии. Если при выполнении последнего сетевого события опция *Разрешать привилегированные* отключена, опция по умолчанию отключена также при следующем событии.

13.5 WebGuard

Рубрика WebGuard в блоке Avira Premium Security Suite. Настройка отвечает за настройку модуля WebGuard.

13.5.1 Поиск

WebGuard помогает защитить Ваш компьютер от вирусов и вредоносных программ, которые загружаются из Интернет через браузер. В разделе *Поиск* Вы можете настроить действия WebGuard.

Поиск

Активировать Webguard

Если опция включена, то сайты, которые загружаются на Ваш компьютер, проверяются на вирусы и вредоносные программы. WebGuard контролирует данные, передаваемые через Интернет посредством протокола HTTP на порты 80, 8080 и 3128. Загрузка инфицированных веб-сайтов будет блокироваться. Если опция выключена, то служба WebGuard будет работать, однако поиск вирусов и вредоносных программ будет деактивирован.

Примечание
Функция защиты детей не зависит от активации/деактивации WebGuard.

Защита Drive-By

Защита Drive-By предлагает Вам возможность настроить блокировку кадров I-Frames. I-Frames - это элементы HTML, т.е. элементы Интернет-страниц, которые отграничивают участок веб-страницы. При помощи I-Frames другие URLs - с другим содержанием - загружаются и отображаются как отдельные документы в отдельном окне браузера. Чаще всего I-Frames используются для баннерной рекламы. Иногда I-Frames используются для распространения вредоносных программ. В таком случае область I-Frame в браузере практически или вовсе не видна. С помощью опции *Блокировать подозрительные I-Frames* Вы можете контролировать и блокировать загрузку I-Frames.

Блокировать подозрительные I-Frames

Если эта опция включена, то I-Frames на заданных страницах будут проверяться по определенным критериям. Если на веб-странице будут обнаружены подозрительные I-Frames, то они блокируются. В окне кадра I-Frames отобразится сообщение об ошибке (код состояния HTTP 403).

По умолчанию

Если опция включена, то все I-Frames с подозрительным содержанием блокируются.

Расширенный

Если опция включена, то все I-Frames с подозрительным содержанием и I-Frames, используемые подозрительным образом, будут блокироваться. Подозрительное использование кадров I-Frames означает, что I-Frame слишком мал или его не видно в браузере или если I-Frame расположен на необычном месте на веб-странице.

13.5.1.1. Действие при обнаружении

Действие при обнаружении

Вы можете определить операции, которые будут выполняться, если WebGuard обнаружит вирус или вредоносную программу.

Интерактивно

Если опция включена, при обнаружении вируса или вредоносной программы отображается окно, предлагающее выбор действий, которые можно выполнить с инфицированным файлом. Эта настройка активна по умолчанию.

Более подробная информация - здесь.

Показывать прогресс выполнения

Если опция включена, возникает уведомление с отображением прогресса выполнения, если время ожидания загрузки с сайта превышает 20 сек. Это уведомление служит для контроля при загрузке файлов больших объемов с веб-страниц: при открытии Интернет-страниц WebGuard содержание этой страницы загружается постепенно, так как производится проверка на вирусы и вредоносные программы в процессе загрузки. Эта опция по умолчанию отключена.

Автоматически

Если опция включена, при обнаружении вируса или вредоносной программы действие происходит автоматически, не предлагая выбора. WebGuard работает автоматически в соответствии с выбранными Вами настройками.

Первичное действие

Первичное действие - это действие, выполняемое в случае, когда WebGuard обнаруживает вирус или вредоносную программу.

запретить доступ

Запрошенная веб-сервером страница или переданные данные и файлы не будут перенаправлены Вашему браузеру. В окне веб-браузера отображается информация об отказе в доступе. WebGuard вносит обнаружение в файл отчета, если опция протоколирования включена. Если опция включена, WebGuard вносит запись о событии в протокол.

поместить на карантин

Запрошенная с веб-сервера страница или переданные файлы и данные в случае обнаружения вируса или вредоносной программы помещаются на карантин. Инфицированный файл может быть восстановлен из менеджера карантина, если в нем возникнет необходимость. Файлом также может заняться Центр исследования вредоносных программ.

Пропустить

Запрошенная веб-сервером страница или переданные данные и файлы отправляются модулем WebGuard Вашему веб-браузеру. Доступ к файлу разрешается, никаких действий с ним не выполняется.

Предупреждение
Инфицированный файл все еще активен в Вашей системе! Это может причинить вред Вашему компьютеру!

13.5.1.2. Запрет доступа

В пункте **Запрет доступа** Вы можете указывать типы файлов и MIME (типы содержимого передаваемых данных), которые будет блокироваться WebGuard. С помощью веб-фильтра Вы можете заблокировать известные, нежелательные URL, например, URL фишинг-программ или вредоносных программ. WebGuard препятствует передаче данных из Интернет на Ваш компьютер.

Блокируемые WebGuard типы данных / MIME (по выбору)

WebGuard блокирует все приведенные в списке типы данных и MIME (типы содержимого переданных файлов).

Поле ввода

Здесь укажите типы MIME и файлов, которые должен блокировать WebGuard. Для типов файлов указывайте расширения, например, **htm**. Укажите тип и подтип MIME. Оба типа отделяются друг от друга обычной косой чертой, например, **video/mpeg** или **audio/x-wav**.

Примечание
Файлы, которые уже сохранены на Вашем компьютере как временные Интернет-файлы, хотя и блокируются WebGuard, но могут быть загружены локально из Интернет-браузера. Временные Интернет-файлы - это файлы, которые сохраняются Интернет-браузером для более быстрой загрузки веб-страниц.

Примечание
Список блокируемых типов файлов / MIME игнорируется, если имеются строки в списке исключений из проверки типов файлов и MIME в WebGuard::Проверка::Исключения.

Примечание
При указании типов данных и типов MIME Вы не можете применять заменители символов (* для любого числа символов и ? для замены одного конкретного символа).

MIME-типы: Примеры медиа-типов:

- `text`= для текстовых файлов
- `image` = для графических данных
- `video` = для видео файлов
- `audio` = для аудио файлов
- `application` = для файлов, связанных с определенной программой

Примеры: Непроверяемые типы файлов и MIME

- `application/octet-stream` = файлы MIME-типа application/octet-stream (исполняемые файлы *.bin, *.exe, *.com, *dll, *.class) блокируются WebGuard.
- `application/olescript` = файлы MIME-типа application/olescript (ActiveX Skript-Dateien *.axs) блокируются WebGuard.
- `.exe` = все файлы с расширением .exe (исполняемые файлы) блокируются WebGuard.
- `.msi` = все файлы с расширением .msi (файлы Windows Installer) блокируются WebGuard.

Добавить

С помощью этой кнопки Вы можете добавить к списку исключений введенный MIME-тип или тип файла.

Удалить

Кнопка удаляет из списка выделенную строку. Кнопка неактивна, если ни одна строка не выделена.

Веб-фильтр

Веб-фильтр имеет собственную пополняемую базу данных, в которой ссылки URL расположены в соответствии с содержанием.

Активировать веб-фильтр

Если функция включена, то все адреса URL, которые относятся к выбранным категориям в списке веб-фильтра, блокируются.

Список веб-фильтра

В списке веб-фильтра Вы можете выбрать категории содержания, адреса URL которых должны блокироваться WebGuard.

Примечание
Веб-фильтр игнорируется, если в списке исключенных из проверки ссылок WebGuard::Проверка::Исключения содержатся строки.

Примечание
К группе Спам-URL относятся адреса, через которые распространяются спам-письма. Категория Обман и Дезинформация включает в себя Интернет-страницы с 'абонементами-ловушками' и различными услугами, размер оплаты которых скрывается.

13.5.1.3. Исключения

Вы можете исключить и проверки WebGuard MIME-типы (типы содержимого передаваемых файлов) и типы файлов для URL (Интернет-адреса). Указанные MIME-типы и URL не будут проверяться WebGuard на наличие вирусов или вредоносных систем при пересылке в Вашу компьютерную систему.

WebGuard не проверяет MIME-типы

В этом поле Вы можете выбрать MIME-типы (тип содержимого переданных данных), которые WebGuard проверять не будет.

Не проверяемые WebGuard типы файлов / MIME (определено пользователем)

Типы файлов и MIME-типы (тип содержимого переданных данных), указанные в списке, WebGuard исключает из проверки.

Поле ввода

В этом поле укажите имя MIME-типа и типа файла, которые WebGuard исключает из проверки. Для типов файлов укажите расширение, например, **htm**. Укажите тип и подтип MIME. Оба типа данных отделяются друг от друга обычной косой чертой, например, **video/mpeg** или **audio/x-wav**.

Примечание
При указании типов данных и типов MIME Вы не можете применять заменители символов (* для любого числа символов и ? для замены одного конкретного символа).

Предупреждение
Все типы файлов и типы содержимого файлов, находящиеся в списке исключений, могут быть без дальнейшей проверки запрета доступа (список блокируемых типов файлов и MIME в WebGuard::Проверка::Запрет доступа) или WebGuard загружены в Интернет-браузер: При наличии позиций в списке исключений игнорируется список блокируемых типов файлов и MIME. Поиск на наличие вирусов и вредоносного ПО не производится.

MIME-типы: Примеры типов:

- `text`= для текстовых файлов
- `image` = для графических данных
- `video` = для видео файлов
- `audio` = для аудио файлов
- `application` = для файлов, связанных с определенной программой

Примеры: Исключенные типы файлов и MIME-типы

- `audio/`= все файлы типа Audio исключаются из проверки WebGuard
- `video/quicktime` = все видео файлы подтипа Quicktime (*.qt, *.mov) исключаются из проверки WebGuard
- `.pdf` = все файлы Adobe-PDF исключаются из проверки WebGuard.

Добавить

С помощью этой кнопки Вы можете добавить к списку исключений введенный MIME-тип или тип файла.

Удалить

Кнопка удаляет из списка выделенную строку. Кнопка неактивна, если ни одна строка не выделена.

URL, разрешенные WebGuard

Все адреса из этого списка исключаются из проверки модулем WebGuard.

Поле ввода

Здесь укажите Интернет адреса, которые необходимо исключить из проверки WebGuard, например, **www.domainname.com/**. Вы можете задать части URL, в конце и в начале укажите уровень домена: .domainname.de для всех страниц и всех поддоменов домена. Веб-страница с любым доменом верхнего уровня (.com или .net) заканчивается точкой: **domainname.**. Если Вы записываете набор символов без точки в начали или в конце, такая последовательность интерпретируется как домен высшего уровня, например, **net** для всех доменов зоны NET (www.domain.net)

Примечание
При вводе адреса URL Вы можете использовать специальный символ * для любого количества знаков. Используйте в сочетании со специальными символами точки для обозначения уровня домена:
.domainname.*
*.domainname.com
.*name*.com (действительно, но не рекомендуется)
Данные без точки, как например, *name* интерпретируются как части первого уровня домена и нецелесообразны.

Предупреждение
Все веб-страницы в списке непроверяемых адресов загружаются в браузер без проверки веб-фильтром или WebGuard: все записи из списка игнорируются веб-фильтром (см. WebGuard::Поиск::Запрет доступа. Поиск на наличие вирусов и вредоносного ПО не производится. Поэтому исключайте из проверки WebGuard только надежные адреса.

Добавить

С помощью этой кнопки Вы можете добавить в список адрес, содержащийся в поле ввода.

Удалить

Кнопка удаляет из списка выделенную строку. Кнопка неактивна, если ни одна строка не выделена.

Примеры: Разрешенные URL

- `www.avira.com` -ИЛИ- `www.avira.com/*`

  = Все URL с доменом 'www.avira.com' исключаются из проверки WebGuard: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,..
  URL с доменом www.avira.de не исключаются из проверки WebGuard.

- `avira.com` -ИЛИ- `*.avira.com`

  = Все URL с доменом второго и первого уровня 'avira.com' исключаются из проверки WebGuard. Данные включают все существующие поддомены к '.avira.com': www.avira.com, forum.avira.com,...

- `avira.` -ИЛИ- `*.avira.*`

  = Все URLс доменом второго уровня 'avira' исключаются из проверки WebGuard. Данные включают все существующие домены первого уровня и поддомены к '.avira.': www.avira.com, www.avira.de, forum.avira.com,...

- `.*domain*.*`

  = Все URL, содержащие домен второго уровня со строкой символов 'domain' исключаются из проверки WebGuard. www.domain.com, www.new-domain.de, www.sample-domain1.de, ...

- `net` -ИЛИ- `*.net`

  = Все URLс доменом первого уровня 'net' исключаются из проверки WebGuard. www.name1.net, www.name2.net,...

Предупреждение
Вводите адреса URL, которые Вы хотите исключить из проверки WebGuard, so как можно более точно. Не задавайте домены первого уровня и части доменов второго уровня, так как существует опасность, что из проверки WebGuard будут исключены Интернет-страницы, распространяющие вирусы и вредоносные программы. Рекомендуется задавать полный домен второго уровня и домен первого уровня: domainname.com

13.5.1.4. Эвристика

Этот раздел настроек содержит параметры эвристического поиска Avira Premium Security Suite.

Avira Premium Security Suite содержит эвристические системы, которые сразу распознают вредоносные программы, то есть до составления специальной вирусной сигнатуры и получения обновления защиты от вирусов. Распознавание вирусов осуществляется при помощи подробного анализа инфицированного кода на предмет выполняемых функций и действий, типичных для вредоносных программ. Если исследуемый код имеет характерные признаки, он получает статус подозрительного. Это не означает, что объект в любом случае является вредоносной программой. Возможны также ложные срабатывания. Решение о том, что необходимо сделать с подозрительным объектом, принимает сам пользователь. Решение может быть основано, например, на знании о происхождении файла.

Эвристическое обнаружение макровирусов

Эвристическое обнаружение макровирусов

Avira Premium Security Suite имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, подозрительные файлы регистрируются, пользователь получает об этом уведомление. Эта настройка по умолчанию включена и является нашей рекомендацией.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Avira Premium Security Suite благодаря технологии AntiVir AHeAD содержит очень мощную эвристическую систему для определения даже неизвестных вирусов и (новых) вредоносных программ. Вы можете установить уровень "резкости" эвристики. Эта настройка активна по умолчанию.

Низкий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite обнаруживает меньше неизвестных вредоносных программ.

Средний уровень обнаружения

Эта настройка по умолчанию включена, если Вы выбрали применение этой эвристической технологии.

Высокий уровень обнаружения

Если эта опция включена, Avira Premium Security Suite распознает значительно больше неизвестных вирусов или вредоносных программ, но возможны и ложные срабатывания.

13.5.2 Защита детей

Premium Security Suite оснащен функцией защиты детей для фильтрации нежелательных или нелегальных Интернет-услуг. Пользователю может быть присвоена роль. Роль пользователя может быть сконфигурирована, она может включать в себя разрешенные и запрещенные URL (адреса Интернет), а также запрещенные категории содержания. При блокировке содержания по определенным категориям используются мощные списки фильтров URL, в которых ссылки в Интернет разбиты на категории. Списки фильтров URL обновляются каждый день, поддерживают европейские языки (немецкий, английский, французский, итальянский, русский,...). Роли Ребенок, Подросток, Взрослый соответственно сконфигурированы. Для настройки защиты детей необходимо активировать соответствующую опцию.

Если Защита детей активирована, то при навигации в Интернет все открываемые в браузере страницы будут проверяться в соответствии с ролью пользователя. При запрещенных страницах адрес будет блокироваться, в браузере появится сообщение.

Предупреждение
Защитите настройку Premium Security Suite паролем, если Вы активируете защиту детей. Если настройка не защищена паролем, то все пользователи компьютера смогут изменять или отключать защиту детей. Пароль можно активировать здесь: Общее::Пароль.

Активация защиты детей:

Если Защита детей активирована, то при навигации в Интернет все открываемые в браузере страницы будут проверяться в соответствии с ролью пользователя. Будут блокироваться те страницы, которые в пределах данной роли считаются запрещенными.

Примечание
Пользователи, которым в рамках защиты детей не была присвоена роль, при активированной функции будут *по умолчанию* определяться как *Ребенок*. Вы можете изменить роль пользователя по умолчанию.

Выбор пользователя

Список ролей пользователей

В списке отображаются все добавленные пользователи с их ролями. При добавлении пользователя программа по умолчанию приписывает ему роль *Ребенок*. Щелкнув мышью по роли, Вы можете изменить ее.

Пользователь

Этот список содержит имена всех пользователей системы.

Добавить

С помощью этой кнопки Вы можете добавить выбранного пользователя к списку защищаемых пользователей.

Удалить

Кнопка удаляет из списка выделенную строку.

Примечание
Пользователя по умолчанию удалить невозможно.

Роли

Список

Список отображает все созданные роли. Дважды щелкнув мышью по роли, Вы откроете диалог для изменения роли.

Поле ввода

В это поле вводится имя роли, которую Вы хотите добавить к ролям пользователей.

Изменить

Нажав кнопку *Изменить*, Вы можете настроить выбранные роли. Появится диалоговое окно, в котором Вы можете определить запрещенные и разрешенные URL, а также выбрать запрещенное содержание в зависимости от категории.

Добавить

С помощью этой кнопки Вы можете добавить в поле ввода новую роль к списку ролей.

Удалить

Кнопка удаляет из списка выделенную роль.

Примечание
Роли, присвоенные пользователям, не могут быть удалены.

Свойства роли

Нажав кнопку *Изменить*, Вы увидите диалог *Свойства роли*, где Вы можете определить роль пользователя, указав разрешенные и запрещенные URL, а также определив запрещенное содержание веб-страниц. Вы располагаете следующими опциями настройки:

- Запретить доступ к URL
- Разрешить доступ к URL
- Блокировать содержание веб-страниц: Вы можете выбрать категории для содержания веб-страниц, которые необходимо заблокировать.

13.5.3 Отчет

WebGuard оснащена функциями протоколирования, обеспечивающими пользователя или администратора точной информацией о типе и виде обнаруженного объекта.

Протоколирование

Здесь определяются объемные параметры файла отчета.

Не требуется

Если опция включена, то WebGuard не составляет протокол.
Мы рекомендуем отказываться от протоколирования только в экстренных случаях, например, если Вы производите тестирование продукта на большой базе вирусов.

По умолчанию

WebGuard записывает важную информацию (обнаружения, предупреждения и ошибки) в файл отчета, а менее значимая информация для удобства работы с отчетом в него не включается. Эта настройка активна по умолчанию.

Расширенный

Если эта опция включена, то WebGuard вносит в отчет и менее значимую информацию.

полная

Если опция включена, WebGuard включает данные (тип, размер и дату файла) в файл отчета.

Ограничения для файлов отчетов

Максимум n MB

Если функция включена, то размер файла отчета можно ограничить. Возможные параметры: от 1 до 100 Мб. Эта настройка по умолчанию включена. Установлено ограничение в 1 Мб. Чтобы избежать высокой загрузки системы, устанавливается ограничение в 50 Кб сверх нормы. Если размера файла отчета превышает установленный лимит на 50 Кб, старые записи автоматически удаляются до тех пор, пока размер не приводится в соответствие.

Сохранение настроек в файле отчета

Если эта опция включена, то данные о настройках постоянной защиты вносятся в файл отчета.

13.6 Резервирование

Раздел Резервирование блока Avira Premium Security Suite. Настройка отвечает за настройку компонента Резервирование Avira.

13.6.1 Установки

Здесь Вы можете настроить **параметры** компонента Резервирование.

Установки

Резервировать только измененные файлы

Если опция включена, создается инкрементная резервная копия: добавляются только те файлы, которые были изменены со времени последнего резервирования. Если опция отключена, при каждом резервировании создается полная резервная копия: сохраняются все файлы. Эта опция по умолчанию активирована и рекомендуется, так как инкрементные копии создаются быстрее полных, на так сильно загружая систему.

Проверять на вирусы перед резервированием

Если опция включена, файлы перед резервированием проверяются на вирусы. Инфицированные файлы не сохраняются. Эта опция по умолчанию включена и рекомендуется.

13.6.2 Исключения

В Исключениях Вы можете определить, какие файловые объекты и типы файлов подлежат резервированию, а какие нет.

Нерезервируемые файловые объекты

Список содержит файлы, которые не подлежат резервированию, и пути к ним.

Примечание
Совокупная длина строк в списке не должна превышать 6000 знаков.

Примечание
Содержащиеся в этом списке файлы фиксируются в файле отчета.

Поле ввода

В этом поле укажите имена файловых объектов, которые не надо резервировать. По умолчанию указан путь ко временной папке для локальных настроек активного пользователя.

Кнопка открывает окно, в котором Вы можете выбрать желаемый файл или путь.
Если Вы указали имя файла и полный путь к нему, именно этот файл не подлежит резервированию. Если Вы указали имя файла, но не указали путь к нему, ни один из файлов с этим именем не будет добавлен к резервной копии.

Добавить

С помощью этой кнопки можно добавлять к списку файловый объект, имя (и путь) которого Вы указали в поле ввода.

Удалить

Кнопка удаляет из списка выделенную строку. Кнопка неактивна, если ни одна строка не выделена.

Очистить список

Эта кнопка восстанавливает настройки по умолчанию.

Примите к сведению следующие пункты:

- В названии файлов разрешены заменители символов * (любое количество знаков) и ? (один знак).
- Список обрабатывается сверху вниз.
- Если исключается папка, автоматически исключаются и папки, находящиеся внутри.
- Можно исключать из проверки и отдельные расширения файлов (включая заменитель символов).
- Для исключения объектов, обращение к которым осуществляется с помощью коротких имен файлов DOS (DOS name convention 8.3), необходимо добавить в список соответствующее короткое имя.

Примечание
К имени файла, содержащего заменитель символов, нельзя добавлять обратный слэш.

Например:

```
C:\Программы\Приложения\прилож*.exe\
```

Эта запись недействительна. Программа не исключает объект из проверки!

Примеры:

```
приложение.exe
\Программы\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Program Files\Приложения\приложение.exe
C:\Program Files\Приложения\прилож*.exe
C:\Program Files\Приложения\прилож*
C:\Program Files\Приложения\прилож????.e*
C:\Program Files\
C:\Program Files
C:\Program Files\Приложения\*.mdb
```

Списки расширений файлов

Включать все расширения файлов

Если опция включена, все файлы будут зарезервированы.

Активировать список исключаемых расширений

Если опция включена, все файлы резервируются в профиле, за исключением файлов, чьи расширения были внесены в список расширений файлов, исключаемых из проверки.

Расширения

Кнопка вызывает диалоговое окно, отображающее расширения файлов, которые не резервируются при активной опции "Непроверяемые расширения файлов". В списке уже приведены некоторые расширения файлов, но Вы можете легко добавлять новые или удалять их.

Активировать список нерезервируемых расширений

Если опция включена, резервируются файлы, расширения которых внесено в список нерезервируемых расширений.

Расширения

С помощью этой кнопки Вы получаете доступ к списку расширений файлов, резервируемых, если опция "Базовый список расширений" активна. В списке уже приведены некоторые расширения файлов, но Вы можете легко добавлять новые или удалять их.

13.6.3 Отчет

Компонент Резервирование имеет мощную функцию протоколирования.

Протоколирование

Здесь определяются объемные параметры файла отчета.

Не требуется

Если опция включена, компонент Резервирование не создает отчет. Только в исключительных случаях отказывайтесь от протоколирования.

По умолчанию

Компонент Резервирование добавляет к отчету важную информацию (резервирование, поиск вирусов, предупреждения и ошибки), более важная информация для удобства работы с отчетом игнорируется. Эта настройка активна по умолчанию.

Расширенный

Если опция включена, компонент Резервирование добавляет в файл отчета и менее важную информацию.

полная

Если опция включена, компонент Резервирование добавляет к отчету информацию о протекании резервирования и поиске вирусов.

13.7 Общее

13.7.1 Настройка :: Общее

13.7.1.1. Дополнительные категории угроз

Выбор дополнительных категорий угроз

Avira Premium Security Suite защищает Вас от компьютерных вирусов.

Кроме того, У Вас есть возможность дифференцированного поиска следующих дополнительных категорий угроз.

- Backdoor-программы (BDC)
- Программы дозвона на платные номера (DIALER)
- Игры (GAMES)
- Программы-шутки (JOKES)
- Риск вторжения в приватную сферу (SPR)
- Рекламные и шпионские программы (ADSPY)
- Необычный паковщик (PCK)
- Файлы с различными расширениями (HEUR-DBLEXT)
- Фишинг
- Приложение (APPL)

Щелчком по соответствующему полю можно активировать выбранный тип программы или деактивировать его.

Выбрать все

Если эта опция включена, производится поиск всех типов программ.

Значения по умолчанию

Эта кнопка восстанавливает настройки по умолчанию.

Примечание
Если какой-нибудь тип программ не был выбран, файлы этого типа, обнаруженные при проверке, больше не будут считаться подозрительными. Не вносится также информация об этом в файл отчета.

13.7.2 Настройка :: Общее

13.7.2.1. Пароль

Вы можете Avira Premium Security Suite в различных областях установить защиту паролем. Если для какого-либо раздела был определен пароль, Вы каждый раз при обращении к такому защищенному разделу должны будете ввести этот пароль.

Пароль

Введите пароль

Введите Ваш пароль. В целях безопасности вводимые Вами символы пароля заменяются звёздочками (*). Максимальная число символов - 20. Если пароль уже был введен хотя бы один раз, программа запрещает доступ при вводе неправильного пароля. Пустое поле означает "Без пароля".

Подтвердите пароль

Введите здесь повторно указанный выше пароль для его подтверждения. В целях безопасности символы пароля отображаются в поле ввода звездочками (*).

Примечание
Различается написание прописными и строчными буквами!

Разделы, защищенные паролем

Avira Premium Security Suite может защищать отдельные разделы с помощью паролей. Щелчком мыши по соответствующему полю может быть включен или отключен запрос пароля для отдельных модулей.

Защищенный паролем модуль	Функция
Центр контроля	Если опция включена, требуется пароль для запуска Центр контроля.
Guard Включить / Отключить	Если опция включена, требуется пароль для включения / отключения AntiVir Guard.
MailGuard включить / отключить	Если опция включена, требуется пароль для включения/отключения MailGuard.

Firewall включить / отключить	Есть опция включена, требуется пароль для включения / отключения Firewall.
WebGuard включить/ отключить	Если опция включена, требуется пароль для включения / отключения WebGuard.
Добавить и изменить задачи	Если опция включена, требуется пароль для добавления и изменения задач в модуле Планировщик.
Запустить обновление продукта	Если опция включена, при запуске обновления продукта требуется ввести пароль в меню Обновление.
Карантин	Если опция включена, активируются все разделы менеджера карантина, которые могут быть защищены паролем. Щелчком в определенном поле можно активировать или деактивировать запрос пароля.
восстановить инфицированный объект	Если опция включена, требуется пароль для восстановления объектов.
лечить инфицированный объект	Если опция включена, требуется пароль для лечения объекта.
свойства инфицированных объектов	Если опция включена, требуется пароль для отображения свойств объекта.
удалить инфицированный объект	Если опция включена, требуется пароль для удаления объекта.
Отправить AntiVir письмо	Если опция включена, требуется пароль для отправки Центр исследования вредоносных программобъекта на проверку.
Настройка	Если опция включена, настройка Avira Premium Security Suite возможна только после ввода пароля.
Режим эксперта	Если опция включена, для перехода в режим эксперта требуется пароль.
Установка / Удаление	Если опция включена, требуется пароль для установки или удаления Avira Premium Security Suite.

13.7.3 Безопасность

Обновление

Сообщать, если последнее обновление старее n дней

В этом поле Вы можете указать количество дней, которое может пройти с момента последнего обновления Avira Premium Security Suite. При превышении этого времени, Планировщик выдает предупреждение.

Отобразить уведомление, если VDF-файл устарел

При включенной опции Вы получаете предупреждение, если VDF-файл устарел. С помощью опции Предупреждения Вы можете настроить временной интервал для отображения сообщения, если последнее обновление было произведено ранее n дней назад.

Полная проверка системы

В этой области Вы можете настроить отображение статуса полной проверки системы Центр контроля в Обзор:: Статус.

Статус 'желтый', если прошло более n дней

Введите в это поле интервал времени в днях, по истечении которого после последней полной проверки системы статус должен поменяться на желтый. Указанный интервал времени должен быть меньше интервала, который соответствует красному цвету статуса. Значение по умолчанию составляет 7 дней и является рекомендуемым.

Статус 'красный', если прошло более n дней

Введите в это поле интервал времени в днях, по истечении которого после последней полной проверки системы статус должен поменяться на красный. Указанный интервал времени должен быть больше интервала, который соответствует желтому цвету статуса. Значение по умолчанию составляет 30 дней и является рекомендуемым.

Примечание
Если Вы оба временных интервала задали как равные нулю, то контроль статуса полной проверки системы отключается. Все время будет отображаться зеленый символ. Такая настройка должна быть установлена только в исключительных случаях. Если Вы установите равным 0 только один интервал, то введенные данные признаются недействительными.

Защита продукта

Защита процессов от нежелательного завершения

Если опция включена, все процессы AntiVir защищены от нежелательного завершения вредоносными программами, а также от неконтролируемого завершения пользователем, например, через диспетчер задач. Эта опция включена по умолчанию.

Важно
Защита процессов 64-битных систем пока невозможна.

Предупреждение
При включенной защите процесса могут возникнуть проблемы при взаимодействии с другими продуктами программного обеспечения. В этих случаях отключайте защиту процессов.

Защитить файлы и записи реестра от манипуляций

При включенной опции все записи реестра Premium Security Suite, а также все файлы программы (двоичные файлы и файлы настройки) защищены от манипуляций. Защита от манипуляций включает в себя защиту от доступа к записям реестра или программным файлам с целью записи, удаления и частично чтения пользователем или программами.

Примечание
При включенной опции изменения в настройке, а также изменение заданий по проверке и обновлениям могут осуществляться только через интерфейс пользователя.

Важно
Защита файлов и записей в реестр для 64-битных систем пока невозможна.

13.7.4 WMI

Поддержка для интерфейса WMI (Windows Management Instrumentation)

Windows Management Instrumentation - это технология управления Windows, которая позволяет посредством языков скриптов и программирования изменять настройки компьютера Windows локально и удаленно. Premium Security Suite поддерживает WMI и предоставляет данные (информацию о состоянии, статистику, отчеты, запланированные задачи и т.д.), события для интерфейса. Благодаря WMI Вы можете вызывать данные о Premium Security Suite .

Активировать поддержку WMI

Если опция включена, то Вы сможете через WMI запрашивать данные о Premium Security Suite.

13.7.5 Папки

Временная папка

В этом поле укажите путь к временной папке, с которой работает Avira Premium Security Suite.

Настройки по умолчанию

Если эта опция включена, для обработки временных файлов системы применяются настройки системы.

Примечание
Ваша система сохраняет временные файлы (на примере Windows XP) в: Пуск | Настройка | Панель управления | Система | Вкладка "Расширенный" | Кнопка "Переменные среды". Временные переменные (TEMP, TMP) для зарегистрированного пользователя, а также системные переменные (TEMP, TMP) имеют соответствующие значения.

Использовать следующую папку

Если эта опция включена, используется путь, указанный в поле для ввода.

Кнопка открывает окно, в котором Вы можете самостоятельно указать временную папку.

По умолчанию

Нажмите на кнопку для выбора стандартного пути к временной папке.

13.7.6 Обновление

Вкладка **Обновление** блока Avira Premium Security Suite. Настройка отвечает за настройку Службы обновлений .

Обновление продукта

Загрузить и автоматически установить обновление продукта

Если опция включена, загружаются и устанавливаются обновления продукта, как только Программа обновлений получает к ним доступ. Обновления файла вирусных сигнатур и ядра производятся всегда и независимо от этой настройки. Предпосылки для этой опции: полная настройка обновления и установленное соединение с сервером обновлений.

Уведомление в случае обнаружения обновления продукта

Если опция включена, Вы будете уведомлены только в случае появления нового обновления продукта. Обновления файла вирусных сигнатур и ядра производятся всегда и независимо от этой настройки. Предпосылки для этой опции: Полная настройка обновления и установленное соединение с сервером обновлений. Уведомление производится в виде всплывающего окна и через сообщение модуля Программа обновлений в Центр контроля Обзор ::События.

Не загружать обновления продукта

Если опция включена, автоматические обновления продукта не производятся. Программа обновлений не уведомляет также о выходе новых обновлений. Обновления файла вирусных сигнатур и поискового движка осуществляются всегда и независимо от этой установки.

Важно
Обновление файла вирусных сигнатур и поискового ядра осуществляется при каждом выполненном обновлении. Это не зависит от настроек обновления (см. Раздел Обновление).

13.7.6.1. Веб-сервер

Обновление может быть произведено непосредственно через веб-сервер в Интернет .

Соединение с веб-сервером

Использовать существующее соединение (сеть)

Эта настройка отображается, если Вы используете сетевое соединение.

Использовать следующее соединение:

Эта настройка отображается, если Вы самостоятельно выбрали параметры соединения.

Программа обновлений определяет автоматически, какие опции обновления доступны. Недоступные опции настройки соединения выделены серым цветом и не могут быть активированы. Модемное соединение может быть создано вручную, например, с помощью телефонной книги Windows.

- **Пользователь:** Введите имя пользователя выбранной учетной записи.
- **Пароль:** Укажите пароль для этой учетной записи. В целях безопасности символы пароля отображаются в поле ввода звездочками (*).

Примечание
Если Вы забыли имя Вашей учетной записи для входа в Интернет или пароль, обратитесь к Вашему Интернет-провайдеру.

Примечание
Автоматическое подключение к системе обновлений через специальные dial-up программы (например, SmartSurfer, Oleco) в настоящее время в Avira Premium Security Suite еще невозможно.

Разорвать dial-up соединение, созданное для обновления

Если опция включена, открытое для обновления соединение автоматически разрывается после завершения загрузки.

Примечание
Эта опция недоступна для Vista. В Vista модемное соединение, открытое для обновления, завершается после проведения загрузки .

Прокси

Прокси-сервер

Не использовать прокси-сервер

Если эта опция включена, устанавливается соединение с веб-сервером не через прокси сервер.

Применять системные настройки Windows

Если эта опция включена, для соединения с веб-сервером через прокси-сервер применяются текущие системные настройки Windows.

Использовать прокси-сервер

Если эта опция включена, производится подключение к веб-серверу через прокси-сервер с применением указанных Вами настроек.

Адрес

Введите URL или IP-адрес прокси-сервера, который Вы хотите использовать для соединения с веб-сервером.

Порт

Укажите номер порта прокси-сервера, который Вы хотите использовать для соединения с веб-сервером.

Логин

Укажите Ваш логин для регистрации на прокси-сервере.

Пароль

Введите соответствующий пароль для регистрации на прокси-сервере. В целях безопасности символы пароля отображаются в поле ввода звездочками (*).

Примеры:

Адрес:	proyx.domain.de	Порт:	8080
Адрес:	192.168.1.100	Порт:	3128

13.7.7 Предупреждения

13.7.7.1. Акустические сигналы

Акустический сигнал

При обнаружении вируса или вредоносного ПО с помощью Scanner или Guard в интерактивном режиме действия подается предупреждающий сигнал. У Вас есть возможность отключить или включить предупреждающий сигнал, а также выбрать в качестве предупреждающего сигнала другой WAVE-файл.

Примечание
Режим Scanner устанавливается в настройках Scanner::Поиск:: Действия при обнаружении. Режим Guard устанавливается в настройках Guard::Поиск:: Действия при обнаружении.

Нет предупреждения

При включенной опции не подается акустического сигнала при обнаружении вируса с помощью Scanner или Guard.

Воспроизводить через громкоговоритель компьютера (только при интерактивном режиме)

При включенной опции подается акустический сигнал со стандартным звуковым предупреждением при обнаружении вируса с помощью Scanner или Guard. Предупреждающий сигнал воспроизводится внутренним громкоговорителем компьютера.

Использовать следующие WAV-файлы (только при интерактивном режиме)

При включенной опции подается акустический сигнал с помощью выбранного WAVE-файла при обнаружении вируса Scanner или Guard. Выбранный WAVE-файл воспроизводится через подключенный внешний громкоговоритель.

Wave-файл

Здесь Вы можете указать имя аудио-файла для воспроизведения и путь к нему. Стандартный предупреждающий сигнал Premium Security Suite внесен по умолчанию.

Кнопка открывает окно, в котором Вы можете выбрать требуемый файл.

Тест

Эта кнопка предназначена для тестового запуска выбранного Wave-файла.

13.7.8 События

Ограничить размер базы данных событий

Установить максимальный размер не более n записей

Если опция включена, максимальное число записей в базе данных событий ограничено определенным размером; допустимые значения находятся в интервале: между 100 и 10 000 записей. Если количество введенных записей превышено, более старые записи удаляются.

Удалять все события старее n дня(ей)

Если эта опция включена, после определенного количества дней удаляется вся база данных; допустимые значения: Разрешенный диапазон - между 1 и 90 дн. Эта опция определена по умолчанию со значением в 30 дней.

Не ограничивать размер базы данных (Удалять события вручную)

При включенной опции размер базы данных событий не ограничен. В Центр контроля в разделе События могут отображаться не более 20 000 записей.

13.7.9 Ограничения отчетов

Ограничивать количество до

Ограничивать количество до n шт.

Если опция включена, максимальное число отчетов ограничено определенным размером; допустимые значения находятся в интервале: от 1 до 300. Если заданное количество введенных записей превышено, более старые отчеты удаляются.

Удалять отчеты старше n дней

Если опция включена, отчеты, созданные определенное число дней назад, автоматически удаляются. Разрешенный диапазон - между 1 и 90 дн. По умолчанию для этой опции определены 30 дней.

Не ограничивать количество отчетов (удалять вручную)

Количество отчетов не ограничивается.

13.7.10 Акустические сигналы

Акустический сигнал

При обнаружении вируса или вредоносного ПО с помощью Scanner или Guard в интерактивном режиме действия подается предупреждающий сигнал. У Вас есть возможность отключить или включить предупреждающий сигнал, а также выбрать в качестве предупреждающего сигнала другой WAVE-файл.

Примечание
Режим Scanner устанавливается в настройках Scanner::Поиск:: Действия при обнаружении. Режим Guard устанавливается в настройках Guard::Поиск:: Действия при обнаружении.

Нет предупреждения

При включенной опции не подается акустического сигнала при обнаружении вируса с помощью Scanner или Guard.

Воспроизводить через громкоговоритель компьютера (только при интерактивном режиме)

При включенной опции подается акустический сигнал со стандартным звуковым предупреждением при обнаружении вируса с помощью Scanner или Guard. Предупреждающий сигнал воспроизводится внутренним громкоговорителем компьютера.

Использовать следующие WAV-файлы (только при интерактивном режиме)

При включенной опции подается акустический сигнал с помощью выбранного WAVE-файла при обнаружении вируса Scanner или Guard. Выбранный WAVE-файл воспроизводится через подключенный внешний громкоговоритель.

Wave-файл

Здесь Вы можете указать имя аудио-файла для воспроизведения и путь к нему. Стандартный предупреждающий сигнал Premium Security Suite внесен по умолчанию.

Кнопка открывает окно, в котором Вы можете выбрать требуемый файл.

Тест

Эта кнопка предназначена для тестового запуска выбранного Wave-файла.

Avira Premium Security Suite

Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Телефон: +49 (0) 7542-500 0
Факс: +49 (0) 7542-525 10
Интернет: http://www.avira.ru

Возможны ошибки и технические изменения

Выпуск: Квартал 1-2009