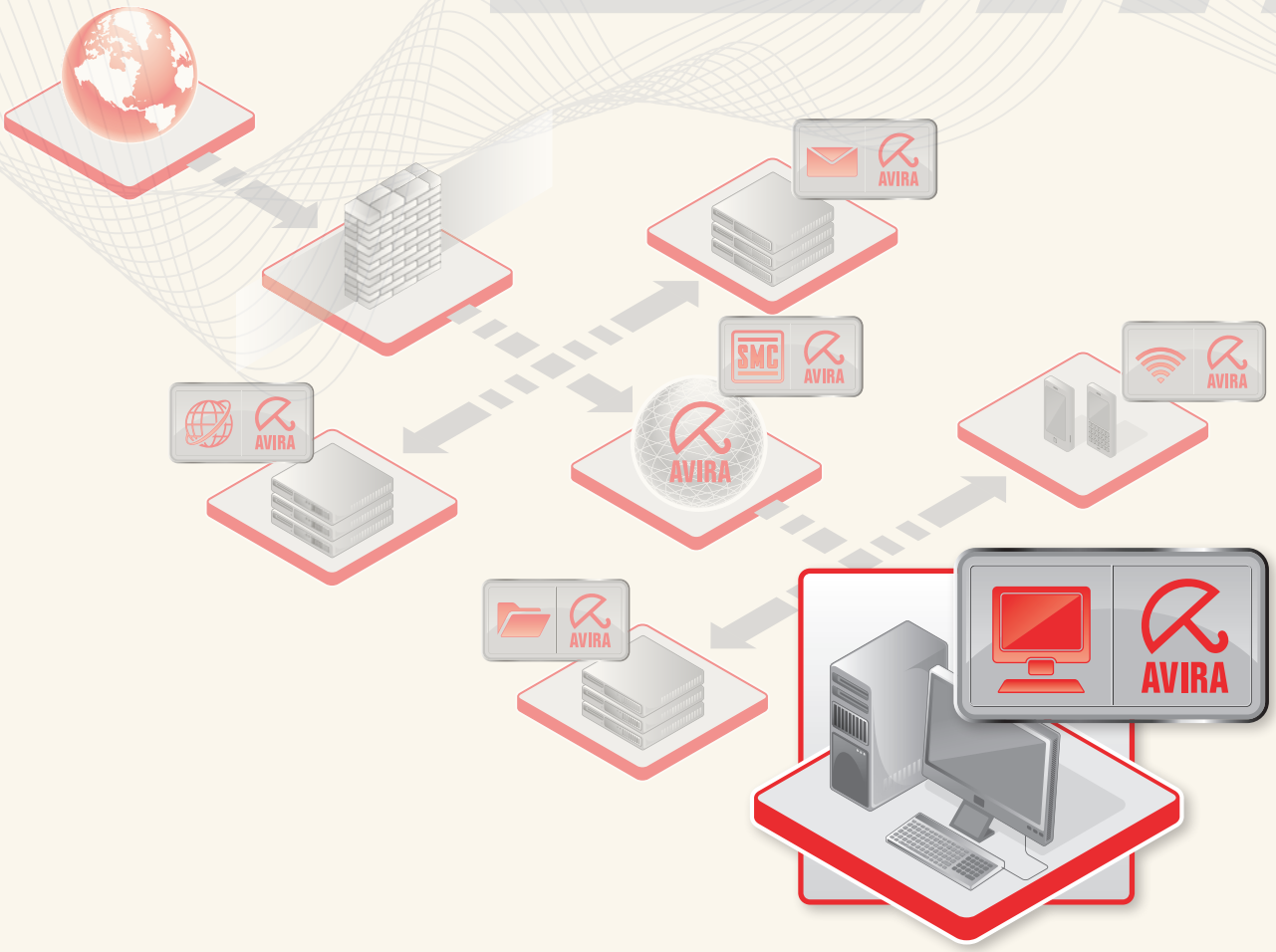
AVIRA
More Than Security

Руководство пользователя

Avira AntiVir Personal



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 AntiVir Personal 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 AntiVir Personal TPL.

Содержание

1 Введение

Avira AntiVir Personal 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.free-av.ru Вы можете загрузить руководство Avira AntiVir Personal как PDF-файл, Avira AntiVir Personal обновлять его или получить информацию о Avira AntiVir Premium платной версии .

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 AntiVir Personal.

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 AntiVir Personal информацию:

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

Avira AntiVir Personal - 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 AntiVir Personal с помощью автоматического обновления. Настройте программу соответственно.

3.1 Производительность

Avira AntiVir Personal 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
- 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

- 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)

3.2 Системные требования

Для безупречной работы Avira AntiVir Personal 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 AntiVir Personal: 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 AntiVir Personal 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 AntiVir Personal, Вам необходима лицензия. Вы соглашаетесь с лицензионными условиями Avira AntiVir Personal.

Лицензия предлагается в форме кода активации. Код активации - это код, состоящий из букв и цифр, который Вы получили при приобретении Avira AntiVir Personal. 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 AntiVir Personal в Интернет-магазине, или размещен на упаковке продукта.

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

В Avira AntiVir Personal уже содержится действительный код активации. В этом случае не требуется активировать продукт.

4 Установка и удаление

этой главы содержится информация об установке и удалении Avira AntiVir Personal:

- 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 AntiVir Personal в том, что Ваш компьютер соответствует Минимальным системным требованиям. Если Ваш компьютер отвечает всем требованиям, Вы можете установить Avira AntiVir Personal.

Примечание
Начиная с Windows XP Avira AntiVir Personal создает точку восстановления перед установкой Avira AntiVir Personal. Это позволит Вам безопасно удалить Avira AntiVir Personal 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 AntiVir Personal точку восстановления системы вы сможете определить по строке AntiVir Personal.

Типы установки

Во время установки Вы можете выбрать тип установки:

полная

AntiVir Personal 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)
- Регистрация пользователя Avira AntiVir Personal
- Выполнение обновления AntiVir Personal по завершении установки
- Приобретите ключ лицензии AntiVir Personal, если Вы хотите активировать AntiVir Personal.

Примечание
Установка через интернет:
Для установки Avira AntiVir Personal через интернет Avira GmbH предлагает программу установки, которая перед выполнением установки загружает с сервера Avira GmbH актуальные программные файлы. Этот способ обеспечивает установку AntiVir Personal 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 AntiVir Personal. Рекомендуется после завершения установки выполнить обновление, чтобы обновить файл вирусных сигнатур.

Примечание
Для регистрации продукта Avira AntiVir Personal 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 AntiVir Personal:

- 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 AntiVir Personal 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 AntiVir Personal*.

▶ 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 AntiVir Personal и указания по расширению защитных функций AntiVir Personal.

▶ Нажмите **Далее**.

→ Возникает окно с лицензионным соглашением.

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

→ Появится окно *Частное использование*.

▶ Подтвердите, что AntiVir Personal будет использован Вами исключительно в частных некоммерческих целях, нажмите **Дальше**.

→ Появится окно *создания серийного номера*.

▶ Подтвердите, что будет сгенерирован случайный серийный номер, который будет передан при обновлении, нажмите **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**.

→ В следующем окне Вы можете установить, необходимо ли создавать

иконку на рабочем столе и/или новую группу программ в меню Пуск.

▶ Нажмите **Далее**.

Далее для полной и выборочной установки

→ Открывается ассистент лицензий.

Ассистент лицензий дает Вам возможность зарегистрироваться в качестве клиента AntiVir Personal и оформить подписку на рассылку новостей Avira GmbH. Для этого необходимо указать персональные данные.

▶ Укажите Ваши данные и подтвердите их нажатием кнопки **Далее**.

→ В процессе регистрации в следующем окне отображается результат процесса активации.

→ 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 AntiVir Personal. Если Вы прервете конфигурацию, то AntiVir Personal 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 AntiVir Personal.

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

▶ 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 AntiVir Personal на Windows XP и при этом деактивировали Windows Firewall, то появится окно с предложением перезагрузить систему.

▶ Завершите установку, нажав **Готово**.

После успешной установки Центр контроля рекомендует в *Обзор :: Статус* проверить актуальность AntiVir Personal.

▶ Обновите AntiVir Personal, 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 AntiVir Personal (см. главу Установка и удаление::Установочные модули)

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

Выберите Avira AntiVir Personal и нажмите кнопку **Изменить**. В окне приветствия Avira AntiVir Personal 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 :

- **AntiVir Personal**
  Этот модуль содержит все компоненты, необходимые для успешной установки Avira AntiVir Personal.
- **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 AntiVir Personal автоматически проверяет файл. При операции Переименования AntiVir Guard не проверяет файл.

- ***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 AntiVir Personal 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.

4.4 Удаление

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

Так Вы удалите Avira AntiVir Personal (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 AntiVir Personal** и нажмите **Удалить**.

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

- ▶ 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 AntiVir Personal удален. Компьютер при необходимости требуется перезагрузить. При этом будут удалены все папки, файлы и записи реестра Avira AntiVir Personal.

5 Обзор AntiVir Personal

этой главы содержится обзор функций и особенности использования AntiVir Personal.

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

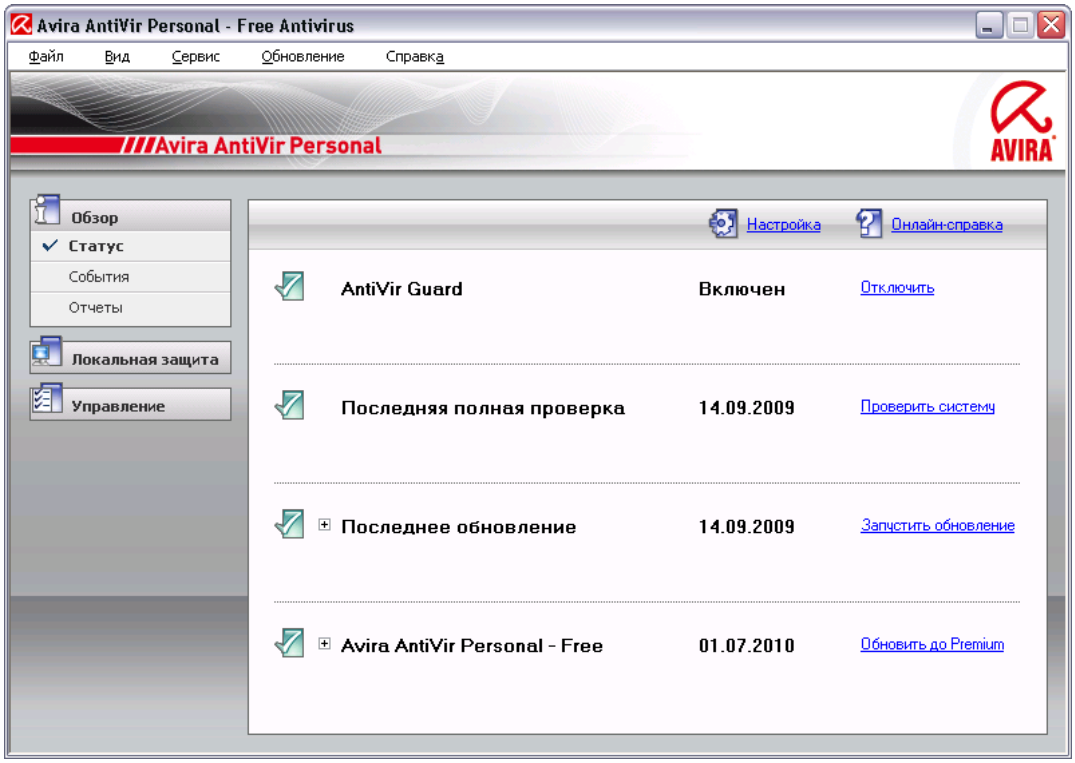
5.1 Интерфейс и работа с программой

Вы можете управлять AntiVir Personal с помощью трех элементов интерфейса программы:

- Центр контроля: Мониторинг и управление AntiVir Personal
- Avira AntiVir Premium. Настройка: Настройка AntiVir Personal
- 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 AntiVir Personal.



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 AntiVir Personal.

- **Навигационное поле:** В разделе навигации Вы можете выбирать между различными вкладками Центр контроля. Отдельные вкладки содержат информацию и доступ к функциям программных компонентов AntiVir Personal, 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 AntiVir Personal в меню Пуск | Программы.
- Через Avira AntiVir Personal 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.

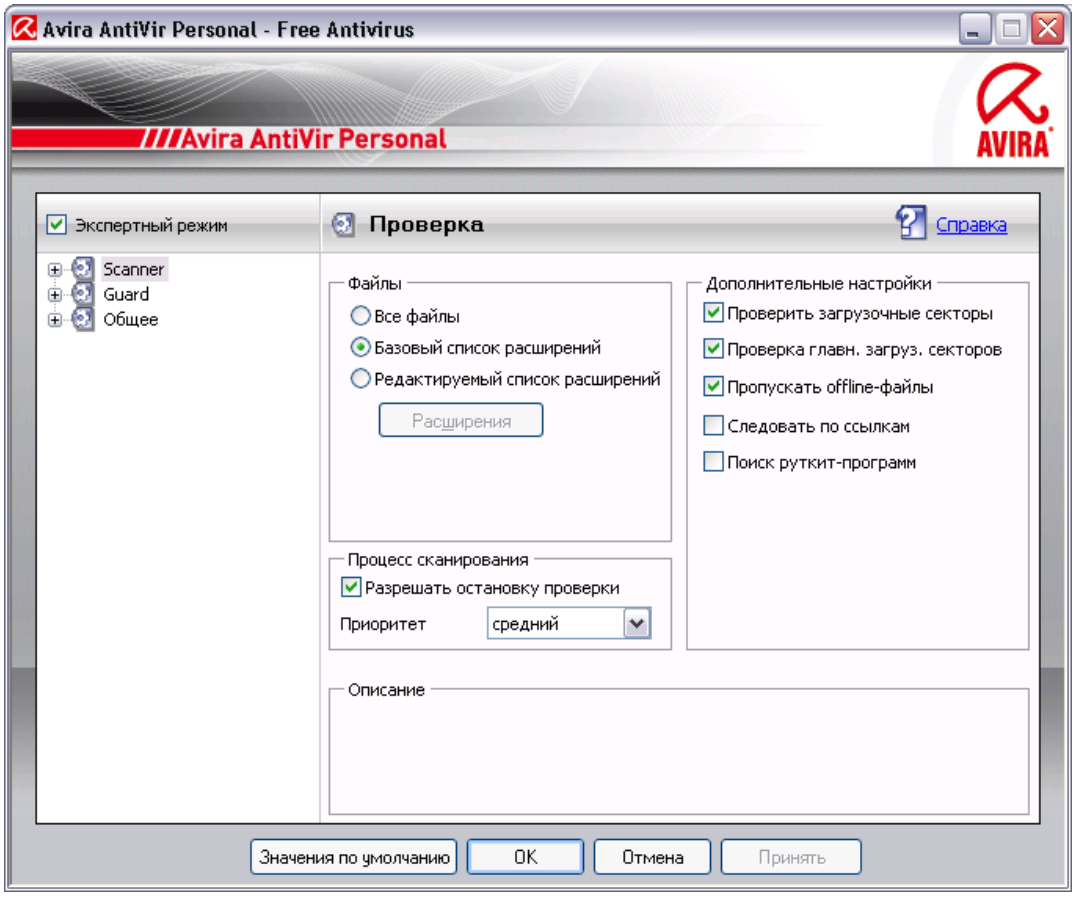
▶ Щелкните по кнопке в верхней части основного окна, чтобы обработать объект.

Обзор Центр контроля

- **Обзор**: В **Обзор** Вы найдете все вкладки, которые служат для наблюдения за функциями Avira AntiVir Personal.
- Раздел **Статус** показывает, какие модули Avira AntiVir Personal 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 AntiVir Personal.
- Раздел Отчеты позволяет Вам получить информацию о результатах действий, выполненных Avira AntiVir Personal.
- **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).
- 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".
- **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, запускаемые в указанное время, а также задачи резервирования.

5.1.2 Настройка

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



Avira AntiVir Premium. 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 AntiVir Premium. Настройка

Вы можете запустить блок настроек несколькими способами:

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

– **Общее** :

Настройка отправки писем через SMTP

Дополнительные категории угроз для проверки и постоянной защиты

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 AntiVir Personal на панели задач системного трея:

Пиктограмма	Описание
	AntiVir Guard включен
	AntiVir Guard отключен

Значок в трее отображает статус службы AntiVir Guard.

Через контекстное меню значка в трее доступны основные функции Avira AntiVir Personal. 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.
– **Запустить AntiVir**: Открывает Avira AntiVir Personal Центр контроля.
– **Настройка AntiVir**: Открывает Avira AntiVir Premium. Настройка.
– **Запустить обновление**: Запускает Обновление.
– **Справка**: Открывает справочную онлайн-систему.
– **Avira в Internet**: Открывает веб-портал производителя AntiVir Personal. Для этого Вам необходимо иметь доступ к Интернет.

5.2 Это делается так

5.2.1 Avira AntiVir Personal обновить автоматически

Примечание
По умолчанию устанавливается задача обновления, при которой Avira AntiVir Personal обновляется при установленном интернет-соединении 24 часа и при создании интернет-соединения.

С помощью AntiVir Планировщик Вы определяете задачу автоматического обновления Avira AntiVir Personal:

- ▶ 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**

Примечание
Рекомендуется регулярно обновлять Avira AntiVir Personal, например, с интервалом все 24 часа.

- ▶ В зависимости от выбора задайте время.
- ▶ При необходимости выберите дополнительные опции(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 :: 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

5.2.2 Запустить обновление вручную

Существует несколько способов запустить обновление Avira AntiVir Personal 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 AntiVir Personal вручную:

▶ Щелкните правой кнопкой мыши по значку Avira AntiVir Personal 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 AntiVir Personal, например, все 24 часа.

Примечание
Вы можете выполнить обновление вручную через Центр безопасности Windows.

5.2.3 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.

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*.
- ▶ 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 , которые необходимо проверить:

- Отметьте узлы, которые необходимо проверить, поставив флажок в поле:

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

Поиск вирусов и вредоносного ПО с помощью Drag&Drop:

✓ Центр контроля от Avira AntiVir Personal открыт.

- Выделите файл, который необходимо проверить.
- Удерживая нажатой левую кнопку мыши, перетащите отмеченный файл в *Центр контроля*.

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

→ По окончании проверки будут показаны результаты.

5.2.5 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, который 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.

5.2.6 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**

▶ 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

5.2.7 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.

5.2.8 Реагировать на найденные вирусы и вредоносное ПО

Для отдельных компонентов защиты AntiVir Personal в разделе *Действия при обнаружении* Вы можете определить действия AntiVir Personal 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:

– **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), 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. При обнаружении установочного вируса удаляется загрузочный сектор. Записывается новый загрузочный сектор.

– **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 AntiVir Personal 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.

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

5.2.9 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 AntiVir Personal 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 AntiVir Personal 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 .

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

5.2.10 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.

5.2.11 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

5.2.12 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):

✓ 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 `?`) .

5.2.13 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 AntiVir Personal.

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.

5.2.14 События: Фильтровать события

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

- Программа обновлений
- Guard
- Scanner
- Планировщик

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.

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 AntiVir Personal Центр контроля.
- **Проверка с помощью Drag & Drop**
  Перетащите файл или папку в программное окно Avira AntiVir Personal 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 рутkит-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 AntiVir Personal встроен компонент Программа обновлений. Программа обновлений обеспечивает, чтобы Avira AntiVir Personal 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 AntiVir Personal при проверке на вирусы или лечении файлов.

- Поисковый движок:

  Поисковый движок AntiVir Personal 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 AntiVir Personal необходима перезагрузка.

Примечание
Из соображения безопасности Программа обновлений проверяет, был ли изменен хост-файл Windows так, что ссылка для обновления Avira AntiVir Personal 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 AntiVir Personal 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 AntiVir Premium. Настройка: Общее :: Обновление

8 FAQ, советы

Здесь Вы найдете часто задаваемые вопросы об Avira AntiVir Personal, справку по проблемам, советы и рекомендации по работе с Avira AntiVir Personal.

См. главу Помощь в сложных случаях

См. главу Горячие клавиши

См. главу Центр безопасности Windows

8.1 Помощь в случае возникновения проблем

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

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

Причина: Ваше Интернет-соединение неактивно. Поэтому Avira AntiVir Personal 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 AntiVir Premium. 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 AntiVir Personal.
- Если Вы используете операционную систему Windows XP, отключите восстановление системы.
- Запустите компьютер в безопасном режиме.
- Запустите Avira AntiVir Personal и Avira AntiVir Premium. 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.

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

Мой брандмауэр сообщает об AntiVir Guard, как только они становятся активными.

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

- Установите разрешение для AntiVir Guard. AntiVir Guard функционирует только с адресом 127.0.0.1 (local host). Не устанавливается соединение с Интернет.

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

8.2 Горячие клавиши

Горячие клавиши дают возможность использовать альтернативную навигацию по Avira AntiVir Personal, вызывать отдельные модули и запускать действия.

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

8.2.1 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.

8.2.2 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 Page down	Перемещение внутри темы.

8.2.3 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
F3	Запуск проверки с выбранным профилем
F4	Создание ярлыка на рабочем столе для выбранного профиля

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)

8.3 Центр безопасности Windows XP

- от Windows XP SP 2 -

8.3.1 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.

8.3.2 Центр безопасности Windows и Avira AntiVir Personal

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

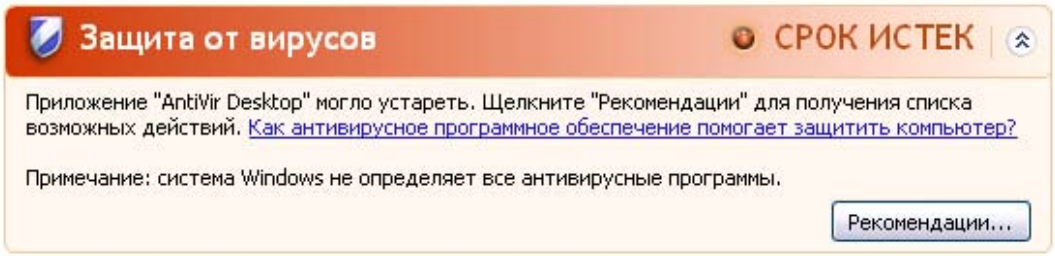
Защита от вирусов НЕ ОБНАРУЖЕНА

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

Примечание
Установите Avira AntiVir Personal на Ваш компьютер для того, чтобы защитить его от вирусов и иных вредоносных программ.

Антивирусные базы УСТАРЕЛИ

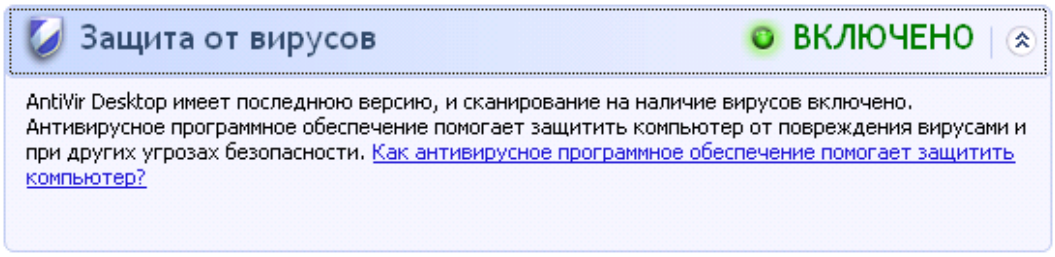
Если Вы уже установили Windows XP Service Pack 2 или Windows Vista, а теперь устанавливаете Avira AntiVir Personal, в процессе установки Вы получите следующее сообщение:



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

Защита от вирусов ВКЛЮЧЕНА

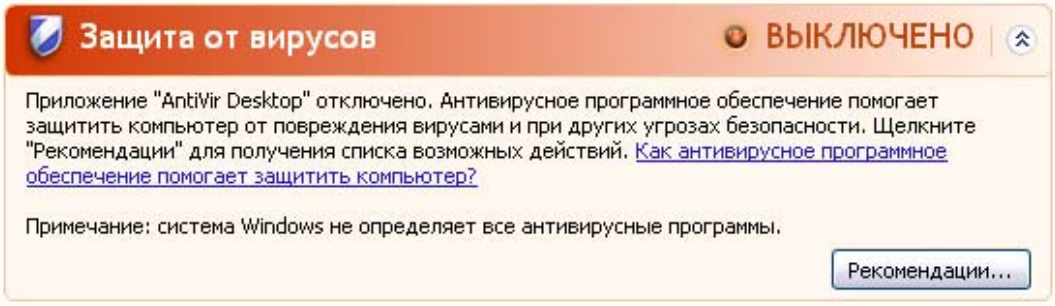
После установки Avira AntiVir Personal и последующего за ней обновления программы Вы получаете следующую информацию:



Avira AntiVir Personal 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.

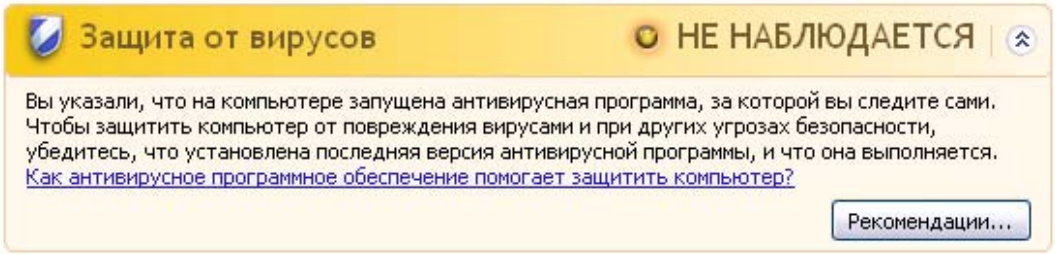


Примечание
Вы можете включить или отключить AntiVir Guard в разделе Обзор :: Статус Avira AntiVir Personal Центр контроля. Если AntiVir Guard включен, на панели задач появится открытый красный зонтик.

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 AntiVir Personal. 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 AntiVir Personal. 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.

9 Вирусы и другое

9.1 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 AntiVir Personal 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 AntiVir Personal обнаруживает компьютерные игры. Если в настройках в разделе Дополнительные категории угроз включена опция **Игры (GAMES)**, Вы получите соответствующее уведомление, если Avira AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal, 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 AntiVir Personal распознает "backdoor-утилиты удаленного администрирования". Если в настройках в разделе Дополнительные категории угроз включена опция **Backdoor-клиент (BDC)**, Вы получите уведомление, если Avira AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal рекламных и шпионских программ.

Необычные средства сжатия данных (PCK)

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

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

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

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

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

Приложение (APPL)

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

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

9.2 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.

10 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

10.1 Контактный адрес

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

10.2 Техническая поддержка

Служба техподдержки Avira AntiVir Personal всегда готова помочь, если у Вас есть вопросы или технические проблемы.

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

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

- **Информация о версии**. Вы найдете ее в Avira AntiVir Personal Центр контроля в пункте меню Справка :: О AntiVir Personal :: 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.

10.3 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-classic@avira.ru. Т.к. некоторые почтовые шлюзы работают с антивирусным ПО, защитите файл(ы) паролем и не забудьте сообщить его нам.

10.4 Сообщить о ложном срабатывании

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

11 Ссылка: Опции меню настройки

В информации о настройке содержатся все данные об опциях, доступных в Avira AntiVir Personal.

11.1 Scanner

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

11.1.1 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 AntiVir Personal. Это означает, что Avira AntiVir Personal 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 AntiVir Personal 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.

11.1.1.1. 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.

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.

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 , 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.

11.1.1.2. 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.

11.1.1.3. Эвристика

Этот раздел настроек содержит параметры эвристического поиска Avira AntiVir Personal.

Avira AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal распознает значительно больше неизвестных вирусов или вредоносных программ, но возможны и ложные срабатывания.

11.1.2 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.

11.2 Guard

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

11.2.1 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 AntiVir Personal. Это означает, что Avira AntiVir Personal 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.

11.2.1.1. Действие при обнаружении

Уведомления

Журнал регистрации событий

Если опция включена, при каждом обнаружении в файл отчета добавляется соответствующая запись. Администратор может получать уведомления об обнаружении и соответственно реагировать. Эта настройка активна по умолчанию.

Акустический сигнал

Если эта опция включена, Guard при обнаружении подозрительных объектов воспроизводит звуковой сигнал. Эта настройка определена по умолчанию.

11.2.1.2. 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
```

11.2.1.3. Эвристика

Этот раздел настроек содержит параметры эвристического поиска Avira AntiVir Personal.

Avira AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal 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 AntiVir Personal распознает значительно больше неизвестных вирусов или вредоносных программ, но возможны и ложные срабатывания.

11.2.2 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.

11.3 Общее

11.3.1 Настройка :: Общее

11.3.1.1. Дополнительные категории угроз

Выбор дополнительных категорий угроз

Avira AntiVir Personal 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.

11.3.2 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 AntiVir Personal. 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 AntiVir Personal, 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.

11.3.3 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. AntiVir Personal 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 AntiVir Personal .

Активировать поддержку WMI

Если опция включена, то Вы сможете через WMI запрашивать данные о AntiVir Personal.

11.3.4 Папки

Временная папка

В этом поле укажите путь к временной папке, с которой работает Avira AntiVir Personal.

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.

11.3.5 Обновление

Вкладка **Обновление** блока Avira AntiVir Premium. 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).

11.3.5.1. 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 AntiVir Personal 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

11.3.6 Предупреждения

11.3.6.1. Акустические сигналы

Акустический сигнал

При обнаружении вируса или вредоносного ПО с помощью Scanner 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.

Нет предупреждения

При включенной опции не подается акустического сигнала при обнаружении вируса с помощью Scanner .

Воспроизводить через громкоговоритель компьютера (только при интерактивном режиме)

При включенной опции подается акустический сигнал со стандартным звуковым предупреждением при обнаружении вируса с помощью Scanner . 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 . 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 AntiVir Personal внесен по умолчанию.

Кнопка открывает окно, в котором Вы можете выбрать требуемый файл.

Тест

Эта кнопка предназначена для тестового запуска выбранного Wave-файла.

11.3.7 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.

11.3.8 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.

11.3.9 Акустические сигналы

Акустический сигнал

При обнаружении вируса или вредоносного ПО с помощью Scanner 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.

Нет предупреждения

При включенной опции не подается акустического сигнала при обнаружении вируса с помощью Scanner .

Воспроизводить через громкоговоритель компьютера (только при интерактивном режиме)

При включенной опции подается акустический сигнал со стандартным звуковым предупреждением при обнаружении вируса с помощью Scanner . 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 . 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 AntiVir Personal внесен по умолчанию.

Кнопка открывает окно, в котором Вы можете выбрать требуемый файл.

Тест

Эта кнопка предназначена для тестового запуска выбранного Wave-файла.

Avira AntiVir Personal – Free Antivirus

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 4-2009