Avira AntiVir Personal – Free Antivirus

Руководство пользователя

AVIRA

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

Программа AntiVir поможет защитить ваш компьютер от вирусов, вредоносного и шпионского ПО, нежелательных программ и других угроз. В настоящем Руководстве дается краткая информация о вирусах, вредоносном и нежелательном ПО.

В руководстве описываются установка и обслуживание программы.

На нашем веб-сайте можно найти многочисленные опции и другие информационные возможности:

http://www.free-av.ru

На веб-сайте Avira вы можете...

- запросить информацию о других программах AntiVir
- загрузить самые последние версии программ AntiVir
- загрузить самые последние версии Руководств по продуктам в формате PDF
- бесплатно загрузить инструментарий поддержки и восстановления
- воспользоваться обширной базой знаний разделом FAQ при устранении проблем
- запросить адреса служб поддержки в конкретной стране.

Сотрудники Avira

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 особо важную информацию, или совет, облегчающий понимание и использование программы AntiVir.

Используются следующие выделения:

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

3 Информация о продукте

главы вы получите всю необходимую для приобретения и использования продукта AntiVir информацию:

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

Программа AntiVir — 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. Обеспечьте актуальность программы AntiVir с помощью автоматического обновления. Настройте программу соответственно.

3.1 Производительность

Программа AntiVir располагает следующими функциями:

- Центр управления для контроля, администрирования и управления всей программой
- Централизованная настройка в стандартном и экспортном режимах с чувствительной к контексту Справкой.
- Сканер (сканирование по требованию) с управляемой профилем и настраиваемой проверкой по всем известным типам вирусов и вредоносных программ
- Интегрированный в Windows Vista модуль управления учетными записями пользователей (User Account Control) для выполнения задач, требующих прав администратора.
- Guard (антивирусный монитор) для постоянного контроля за доступом к файлам
- Avira SearchFree Toolbar (powered by Ask.com) — интегрированная в веб-браузер панель инструментов поиска, позволяющая быстро и удобно просматривать интернет-сайты.
- Для пользователей Avira AntiVir Personal Edition — только в сочетании с Avira SearchFree Toolbar: WebGuard для контроля за получаемыми из интернета по протоколу HTTP данными и файлами (контроль портов 80, 8080, 3128)

- Встроенный менеджер карантина для изоляции подозрительных файлов и работы с ними
- Защита от руткит-программ позволяет обнаружить ПО, скрыто установленное в системе (Руткит)
  (недоступно в Windows XP 64 Bit)
- 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 Интернете
- Встроенный планировщик для планирования таких однократных или повторяющихся задач, как обновление или проверка
- 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

Система должна удовлетворять следующим требованиям:

- Минимум - Pentium 266 МГц
- Операционная система
- Windows XP, SP2 (32 или 64 бита) или
- Windows Vista (32 или 64 бит, SP 1)
- Windows 7 (32 или 64 бита)
- Не менее 150 Мб свободной памяти на жестком диске (при использовании Карантина и для временной памяти - больше)
- Минимум 256 МБ ОЗУ для Windows XP
- Минимум 1024 МБ ОЗУ для Windows Vista, Windows 7
- Для установки программы: Права администратора
- Для установки всех продуктов: Windows Internet Explorer 6.0 и выше
- При необходимости интернет-соединение (см. Установка)

Avira SearchFree Toolbar

- Операционная система
- Windows XP, SP2 (32 или 64 бита) или
- Windows Vista (32 или 64 бит, SP 1)
- Windows 7 (32 или 64 бита)
- Веб-браузер
- Windows Internet Explorer 6.0 и выше или
- Mozilla Firefox 3.0 или выше

Примечание
Перед установкой Avira SearchFree Toolbar при необходимости удалите уже установленные панели инструментов поиска. В противном случае установка Avira SearchFree Toolbar будет невозможна.

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.

Для выполнения некоторых действий под Windows Vista программа AntiVir требует прав 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 и обновление

Для того, чтобы воспользоваться продуктом AntiVir, необходима лицензия. Вы соглашаетесь с условиями лицензии.

Лицензия предлагается в форме кода активации. Код активации — это код, состоящий из букв и цифр, который вы получили при покупке продукта AntiVir. 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 программу AntiVir через Интернет, или размещен на упаковке продукта.

Чтобы лицензировать программу, укажите код активации в процессе активации программы. Продукт может быть активирован в процессе установки. Можно активировать программу AntiVir также после установки в Менеджере лицензий: Справка::Управление лицензиями.

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

В менеджере лицензий можно запустить обновление до программы из семейства AntiVir: Удаление старой программы вручную и установка новой программы вручную не требуются. При обновлении из менеджера лицензий в поле ввода необходимо ввести код активации программы, на которую Вы хотите перейти. После этого будет выполнена автоматическая установка новой программы.

С помощью менеджера лицензий можно автоматически выполнять следующие обновления программы:

- Обновление с Avira AntiVir Personal до Avira AntiVir Premium
- Обновление с Avira AntiVir Personal до Avira Premium Security Suite
- Обновление с Avira AntiVir Premium до Avira Premium Security Suite

4 Установка и удаление

данной главы содержится информация об установке и удалении программы AntiVir

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

4.1 Установка

Перед установкой убедитесь в том, что ваш компьютер соответствует минимальным системным требованиям. Если ваш компьютер отвечает всем требованиям, вы можете установить программу AntiVir.

Примечание
В процессе установки вы можете создать точку восстановления системы. Точка восстановления системы служит для отката операционной системы к состоянию, какое было у нее до установки программы. Если вы собираетесь использовать эту опцию, позаботьтесь о том, чтобы операционная система позволяла создавать точки восстановления:
Windows XP: Свойства системы -> Восстановление системы Деактивируйте опцию **Отключить восстановление системы**.
Windows Vista / Windows 7: Свойства системы -> Защита компьютера: В области **Настройки защиты** выделите системный диск и нажмите кнопку **Настроить**. В окне **Защита системы** активируйте опцию **Восстановить системные настройки и предыдущие версии файлов**.

Типы установки

Во время установки Вы можете выбрать тип установки:

Быстрая установка

- Программа AntiVir устанавливается полностью со всеми компонентами.
- Программные файлы устанавливаются в стандартную папку `C:\Program Files`.
- Программа AntiVir устанавливается со стандартными настройками. Вы не можете изменять предварительные настройки в помощнике настройки.

Настройки пользователя

- 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.

– В мастере конфигурации можно изменить предварительные настройки программы AntiVir и задать быструю проверку системы, которая будет автоматически выполнена после установки.

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
- Обновление по завершении установки выполняется при необходимости
- Приобретите ключ лицензии для программы AntiVir, если собираетесь ее активировать.

Примечание
Установка через интернет:
Имеется программа установки через Интернет, которая перед выполнением установки загружает актуальные программные файлы с серверов Avira GmbH. Этот способ обеспечивает установку программы AntiVir с актуальным файлом вирусных сигнатур.
Установка через пакет для инсталляции
Пакет для инсталляции содержит программу установки и необходимые программные файлы. Следует учитывать, что при установке с помощью пакета инсталляции отсутствует возможность выбора языка для программы AntiVir. Рекомендуется после завершения установки выполнить обновление, чтобы обновить файл вирусных сигнатур.

Примечание
Для регистрации программа AntiVir соединяется через порт 80 по протоколу HTTP (веб-коммуникация), а также через порт 443 по защищенному протоколу SSL 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.

Установка программы AntiVir:

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

Установка через интернет

→ Появится *окно приветствия*.

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

→ Появится диалоговое окно *Выбор языка*.

- Выберите язык для установки программы AntiVir и подтвердите выбор, нажав **Далее**.

→ Появится диалоговое окно *Загрузить*. С серверов 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 с лицензионным соглашением.

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

→ Появится диалоговое окно *Частное использование*.

- Подтвердите, что программа AntiVir будет использована вами исключительно в частных некоммерческих целях, нажмите **Далее**.

→ Появится диалоговое окно *Создание серийного номера*.

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

→ Откроется окно *Тип установки*.

- Активируйте опцию **Быстрая установка** или **Установка по выбору**. Если вы желаете создать точку восстановления системы, активируйте опцию **Создать точку восстановления системы**. Подтвердите правильность данных, нажав **Далее**.

→ Появится диалоговое окно *WebGuard с Avira SearchFree Toolbar (powered by Ask.com)*.

- Если вы хотите установить Avira SearchFree Toolbar, подтвердите, что принимаете условия лицензионного соглашения Ask.com и желаете установить WebGuard с Avira SearchFree Toolbar.

Примечание
Перед установкой Avira SearchFree Toolbar при необходимости удалите уже установленные панели инструментов поиска. В противном случае установка Avira SearchFree Toolbar будет невозможна.

- При необходимости активируйте опцию **Назначить Ask.com поисковой системой по умолчанию** и нажмите **Далее**.

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 **Далее**.

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

▶ Нажмите **Далее**.

Продолжение: Быстрая и пользовательская установка

↪ Открывается ассистент лицензий.

Ассистент лицензий дает возможность зарегистрироваться в качестве клиента и оформить подписку на рассылку новостей Avira. 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 диалоговом окне можно выбрать, будет ли открыт после завершения установки файл Readme и потребуется ли перезапуск компьютера.

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

↪ Ассистент установки будет закрыт.

Продолжение: Выборочная установка
Ассистент настроек

↪ При выборе пользовательской установки на следующем этапе откроется помощник установки. В мастере конфигурации можно задать важные предустановки для программы AntiVir.

▶ Нажмите в окне приветствия мастера конфигурации **Далее**, чтобы начать конфигурацию программы.

↪ В диалоговом окне *Настройка AHeAD*, Вы можете выбрать уровень для обнаружения для технологии AHead. Выбранная степень обнаружения сохраняется для настройки технологии AHead сканера (прямой поиск) и модуля Guard (постоянная защита) .

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

↪ В следующем диалоговом окне *Выбор дополнительных категорий угроз* можно выбрать категории угроз и настроить функции защиты программы AntiVir.

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

↪ Если при установке вы выбрали модуль AntiVir Guard, появится диалоговое окно *Режим запуска модуля Guard*. Можно установить момент

запуска модуля Guard. Модуль Guard будет запускаться при каждом запуске компьютера в указанном режиме.

Примечание
Указанный режим запуска модуля Guard сохраняется в реестре и не может быть изменен при конфигурации.

- 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.

→ При активированной опции *Быстрая проверка системы* открывается окно Luke Filewalker. Сканер выполняет быструю проверку системы.

Продолжение: Быстрая и пользовательская установка

→ Если в помощнике установки выбрана опция **Перезагрузить компьютер**, будет выполнена перезагрузка компьютера.

→ После перезагрузки компьютера показывается файл Readme, если в мастере установки была выбрана опция **Показать Readme.txt**.

После успешной установки в центре управления в *Обзор :: Статус* Проверить актуальность программы.

- При необходимости выполните обновление, чтобы актуализировать файл вирусных сигнатур.
- Выполните полную проверку системы.

4.2 Изменить

У вас есть возможность добавлять или удалять отдельные компоненты установленной в данный момент программы AntiVir (см. главу Установка и удаление::Установочные модули)

Если вы хотите добавить или удалить отдельные компоненты установленной программы, воспользуйтесь пунктом **Программы** > **Изменение или удаление** программ в **Панели управления Windows**.

Выберите в списке программу AntiVir и нажмите **Изменить**. В окне приветствия программы выберите пункт **Изменить программу**. Вы пройдете через процедуру изменения установленной программы.

Примечание
После удаления Avira SearchFree Toolbar, при необходимости, удаляется также WebGuard.

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 программы AntiVir.
- **AntiVir Guard**
  Модуль AntiVir Guard работает в фоновом режиме. Он контролирует и по возможности восстанавливает файлы при таких операциях, как открытие, закрытие и копирование в режиме реального времени (On-Access = при доступе). Если пользователь производит операцию с файлом (загрузка, выполнение, копирование), программа AntiVir автоматически проверяет файл. При переименовании файлов проверка модулем AntiVir Guard не выполняется.
- **AntiVir WebGuard** (для пользователей Avira AntiVir Personal Edition только в сочетании с Avira SearchFree Toolbar)
  При навигации в Интернете вы получаете данные с сервера через свой веб-браузер. Получаемые с веб-сервера данные (HTML-файлы, скрипты и изображения, флеш-анимация, видеопотоки, музыка и пр.) попадают обычно из кэша браузера прямо на выполнение в веб-браузер, из-за чего постоянная проверка, выполняемая, например, в AntiVir Guard, недоступна. Так вирусы и вредоносные программы попадают в Вашу систему. Модуль WebGuard является так называемым HTTP-прокси, контролирующим используемые для передачи данных порты (80, 8080, 3128) и проверяющим передаваемые данные на наличие вирусов и вредоносных программ. Программа автоматически обрабатывает инфицированные файлы и запрашивает пользователя о необходимых действиях.
- *Модуль защиты от рутким-программ AntiVir*
  Защита AntiVir Rootkit проверяет, не установлено ли уже на вашем компьютере ПО, которое после проникновения в компьютерную систему не сможет быть обнаружено обычными методами распознавания вредоносного ПО.
- **Shell Extension**
  Расширение оболочки создает в контекстном меню проводника Windows (вызов правой клавишей мыши) пункт Проверить выбранные файлы с помощью AntiVir. Эта строка позволяет проверить отдельные файлы или папки.

4.4 Удаление

Если Вы хотите удалить программу AntiVir со своего компьютера, воспользуйтесь пунктом **Программы** > **Изменение или удаление** программ в Панели управления Windows.

Программа AntiVir удаляется следующим образом (описано на примере Windows XP и Windows Vista):

▶ Откройте пункт меню Windows **Пуск**, **Панель управления**.

- Сделайте двойной щелчок на **Program Files** (Windows XP: **Установка и удаление программ**).
- Выберите в списке программу AntiVir и нажмите **Удалить**.

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

- Подтвердите кнопкой **Да**.

→ Удаляются все компоненты программы.

- Нажмите **Готово** для завершения деинсталляции.

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

- Подтвердите кнопкой **Да**.

→ Программа AntiVir удалена. Компьютер при необходимости перезагружается. При этом все папки, файлы и записи программы в реестре уничтожаются.

Примечание
Avira SearchFree Toolbar не удаляется вместе с программой, а должен деинсталлироваться отдельно, согласно описанной выше процедуре. Для этого Avira SearchFree Toolbar должен быть активирован в Firefox через Add-On Manager (недействительно для Internet Explorer). После деинсталляции панель инструментов поиска в браузере исчезает.

Примечание
После удаления Avira SearchFree Toolbar, при необходимости, удаляется также WebGuard.

5 Обзор

главы содержится обзор функций и управления программы AntiVir.

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

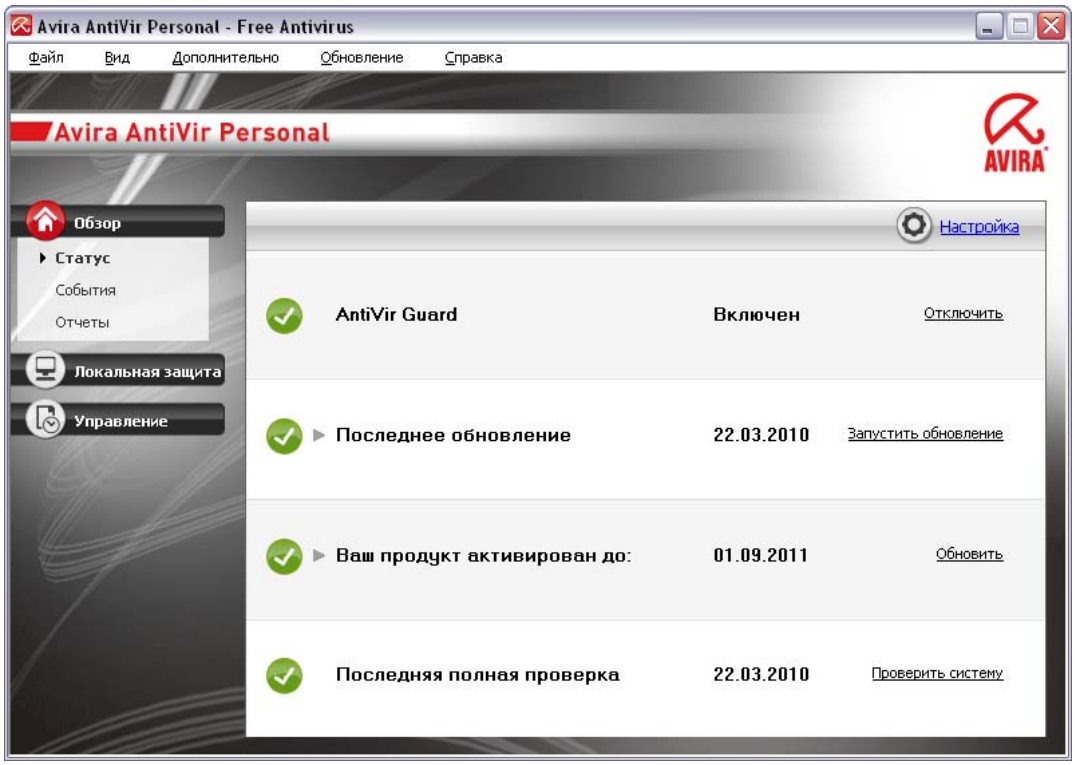
5.1 Интерфейс и работа с программой

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

- Центр управления: Управление программой AntiVir и контроль за ней
- Настройка: Конфигурация программы AntiVir
- Пиктограмма в системном трее на панели задач: Открывается центр управления и дополнительные функции

5.1.1 Центр Управления

Центр управления служит для контроля за состоянием защиты вашей системы и для управления и работы с компонентами защиты и функциями программы AntiVir.



Окно центра управления делится на три области: **Меню**, **Строка меню** и основное окно **Вид**:

- **Меню:** В меню центра управления можно вызвать общие функции программы и получить информацию о ней.

- **Навигационное поле:** В навигационном поле можно быстро переключаться между отдельными закладками центра управления. Отдельные разделы содержат информацию и функции компонентов программы, они расположены 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.

Запуск и завершение работы центра управления

Есть несколько способов запуска Центра управления:

- Двойным щелчком по ярлыку на рабочем столе
- С помощью пункта в меню Пуск | Программы.
- Через Tray Icon программы AntiVir.

Завершить работу центра управления можно с помощью команды меню **Завершить** в меню **Файл** или щелчком мышки по крестику в правом верхнем углу окна центра управления.

Работа с центром управления

Навигация в центре управления

▶ 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 открытия, закрытия и навигации в пунктах меню центра управления можно использовать сочетания 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.

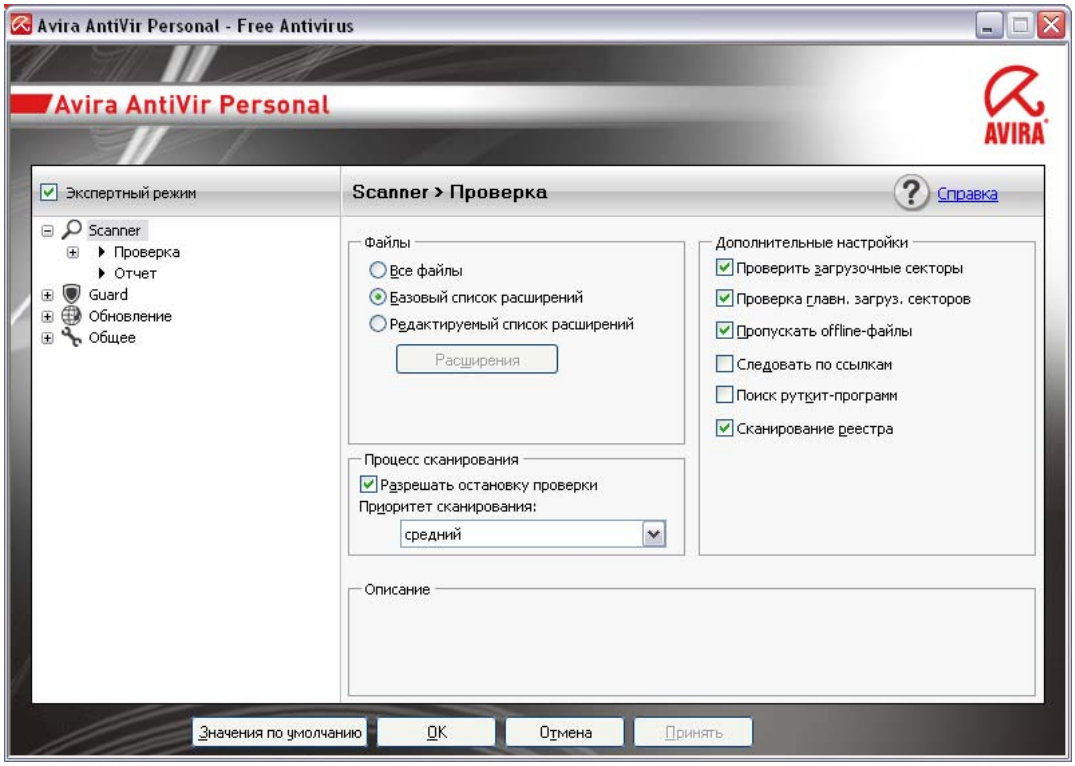
▶ Щелкните по кнопке в верхней части основного окна, чтобы обработать объект.

Обзор центра управления

- **Обзор**: В **Обзор** находятся все разделы контроля за функциями программы AntiVir.
- Раздел **Статус** позволяет легко определить, какие модули программы активны, и предоставляет информацию о последнем выполненном обновлении. Можно видеть, обладает ли пользователь действующей лицензией.
- Раздел События позволяет получить информацию о событиях, созданных модулями программы.
- Раздел Отчеты позволяет получить информацию о результатах выполненных действий.
- **Локальная защита**: **Локальная защита** содержит компоненты, с помощью которых Вы можете проверить файлы на Вашем компьютере на наличие вирусов.
- Во вкладкеПроверка можно выполнять прямой поиск, т.е. настраивать поиск по собственному желанию и запускать его. Предустановленный профиль позволит произвести проверку с оптимальными стандартными настройками. С помощью Выборочной проверки (настройка не сохраняется) Вы можете настроить параметры проверки.
- Во вкладке Guard показывается информация о проверенных файлах, а также дополнительные статические данные, которые можно сбросить в любое время, здесь также можно посмотретьфайл отчета. Подробная информация о последнем обнаруженном вирусе или вредоносной программе вызывается "одним щелчком".
- **Онлайн-защита**: В разделе **Онлайн-защита** Вы найдете компоненты, которые позволят защитить Вашу систему от вирусов, вредоносных программ и сетевых атак.
- В разделе WebGuard показывается информация о проверенных URL и обнаруженных вирусах, а также дополнительные статические данные, которые можно сбросить в любое время, здесь также можно просмотреть файл отчета. Подробная информация о последнем обнаруженном вирусе или вредоносной программе вызывается "одним щелчком".
- **Управление**: В разделе **Управление** находятся инструменты, позволяющие изолировать подозрительные или зараженные вирусами 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. Кроме этого выбранный файл можно отправить по электронной почте в центр исследований вирусов компании Avira.
- В рубрике Планировщик можно создавать выполняемые в определенное время задачи по проверке и обновлению , а также согласовывать или удалять существующие задачи.

5.1.2 Настройка

В настройках можно устанавливать параметры программы AntiVir . После установки программа AntiVir имеет стандартные настройки, позволяющие оптимально защитить ваш компьютер. Тем не менее, ваша система и компьютер могут предъявлять особые требования к программе AntiVir, из-за чего потребуется индивидуальная настройка компонентов защиты программы.



Настройки имеют структуру 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 меню настроек

Вы можете запустить блок настроек несколькими способами:

- Через Панель управления Windows.
- С помощью центра безопасности Windows - начиная с Windows XP SP 2.
- Через Tray Icon программы AntiVir.
- В Центре управления в пункте меню Дополнительно | Настройки.
- В Центре управления с помощью кнопки Настройки.

Примечание
Если Вы открываете окно настроек с помощью кнопки **Настройки** в центре управления, Вы попадете раздел настроек вкладки, которая активна в центре управления. Для выбора отдельных пунктов настройки должен быть включен режим эксперта. В этом случае отображается диалоговое окно, в котором Вы должны включить режим эксперта.

Работа с настройкой

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 активации и деактивации опций или нажатия кнопок можно 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 принять сделанные 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:

- **Сканер** Настройка прямой 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

– **WebGuard**: Настройка модуля WebGuard

Опции проверки, активация и деактивация модуля WebGuard

Действия при обнаружении вируса

Запрещенный доступ: веб-фильтры для известных нежелательных URL (вредоносные программы, фишинг и т. д.)

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

Эвристика модуля WebGuard

Настройка отчетов

– **Общее**:

Расширенные категории угроз для проверки и постоянной защиты

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

WMI: Активировать WMI-поддержку

Настройка уведомления о событиях

Настройка функций отчетов

Настройка используемых папок

Обновление: Настройка соединения с сервером загрузки, настройка обновления программы

Настройка акустических сигналов при обнаружении вируса

5.1.3 Значок в трее

После установки вы увидите значок программы AntiVir на панели задач системного трея:

Пиктограмма	Описание
	AntiVir Guard
	AntiVir Guard

Значок в трее показывает статус служб Guard .

Через контекстное меню значка в трее можно быстро вызвать основные функции программы AntiVir. Для вызова контекстного меню необходимо щелкнуть правой кнопкой мыши по значку в трее.

Пункты контекстного меню

- **Активация AntiVir Guard**: Включает или отключает AntiVir Guard.
- **Активация AntiVir WebGuard**: Включает или отключает AntiVir WebGuard.
- **Запуск AntiVir**: Открывает Центр управления.
- **Настройка AntiVir**: Открывает Настройки.
- **Запуск обновления**: Запускает Обновление.
- **Справка**: Открывает справочную онлайн-систему.
- **О программе AntiVir Personal:** Открывается диалоговое окно с информацией о программе AntiVir: информация о программе, версии, лицензии.
- **Avira в Интернете**: Открывает веб-портал Avira в Интернете. Для этого Вам необходимо иметь доступ к интернету.

5.2 Панель инструментов

5.2.1 Обзор

После успешной установки Avira SearchFree Toolbar интегрируется в веб-браузер. При первом вызове браузера открывается окно статуса, которое содержит важные сведения о функции Toolbar.

Toolbar состоит из поля поиска, логотипа Avira со ссылкой на веб-сайт Avira, двух отображений статуса и меню **Опции**.

- **Панель инструментов поиска**
  Используйте панель инструментов поиска, чтобы быстро и комфортно путешествовать по Интернету с помощью поисковой машины Ask.com.
- **Отображение статуса**
  Отображения статуса показывают статус WebGuard и текущий статус обновления Avira AntiVir. Они помогают узнать какие действия вы должны выполнить, при необходимости, для защиты вашего компьютера.
- **Опции**
  С помощью меню опций вы можете воспользоваться опциями Toolbar, удалить историю поиска, запросить информацию и справку по Toolbar и удалить Avira SearchFree Toolbar прямо через веб-браузер (только Firefox).

5.2.2 Использование

Панель инструментов поиска

С помощью панели инструментов поиска можно осуществлять поиск в Интернете одного или нескольких произвольных понятий.

Для этого введите понятие в поле поиска и нажмите кнопку Enter или щелкните **Поиск**. Поисковая машина Ask.com просматривает Интернет и о всех совпадениях сообщает в окне браузера.

Как настроить Avira SearchFree Toolbar в Internet Explorer и Firefox в соответствии с личными предпочтениями, см. в разделе **Опции.**

Отображение статуса

WebGuard

WebGuard активирован.

Avira WebGuard включен, компьютер защищен.

WebGuard деактивирован.

Avira WebGuard выключен. Проверьте свое приложение и активируйте WebGuard, чтобы оно было защищено.

Статус обновления

Справа находится сообщение о статусе, которое дает справку о статусе обновления Avira. Здесь посредством значков и сообщений вы можете узнать, какие действия, при необходимости, следует предпринять для защиты вашего компьютера.

Ежедневное обновление отключено.

Наведя курсор мыши на значок, вы получите следующее сообщение: **Программа Avira имеет самую последнюю версию; ваш компьютер защищен.**

- Никакие действия не требуются.

Обновите программу Avira.

Наведя курсор мыши на значок, вы получите следующее сообщение: Версия программы**Avira устарела. Щелкните здесь, чтобы загрузить новую версию и защитить компьютер.**

- Для обновления Avira AntiVir щелкните желтый значок или текст. Это происходит согласно предварительным настройкам Avira AntiVir.

→ Во время обновления выдается сообщение **Идет обновление...**

→ Если обновление закончилось успешно, появляется зеленый значок с сообщением **Ежедневное обновление выполнено**.

Программа Avira недоступна.

Наведя курсор мыши на значок, вы получите следующее сообщение: **Программа Avira недоступна. Чтобы гарантировать защиту компьютера, убедитесь, что ваше приложение установлено и выполняется.**

- Для загрузки онлайн-справки Avira щелкните желтый значок или текст. Там вы найдете указания по дальнейшим действиям.

5.2.3 Опции

Avira SearchFree Toolbar совместим с Internet Explorer и Firefox и может быть настроен в обоих этих браузерах в соответствии с вашими личными предпочтениями:

Опции настройки Internet Explorer
Опции настройки Firefox

Internet Explorer

В веб-браузере Internet Explorer в меню **Опции** доступны следующие опции для настройки Avira SearchFree Toolbar:

Опции Toolbar

Поиск

- **Поисковая машина Ask**
  В меню **Поисковая машина Ask** можно выбрать, какую поисковую машину Ask использовать для поиска. Доступны поисковые машины США, Бразилии, Германии, Испании, Европы, Франции, Италии, Нидерландов, России и Великобритании.
- **Открыть поиск в**
  В меню опций **Открыть поиск в** можно выбрать, где будет показываться результат поиска — в **текущем окне**, в **новом окне** или на **новой вкладке**.
- **Показывать последние запросы поиска**
  Если активирована опция **Показывать последние запросы поиска** , под полем ввода текста панели инструментов поиска будут отображаться введенные перед этим запросы поиска.
- **Удалить поиск при закрытии браузера**
  Активируйте опцию **Удалить поиск при закрытии браузера**, если вы не сохраняете уже выполненные поиски и хотите их удалить.

Другие опции

- **Язык Toolbar**
  В **Язык Toolbar** вы можете выбрать язык, на котором Avira SearchFree Toolbar выводит на экран информацию. Доступны английский, немецкий, испанский, французский, итальянский и португальский языки.

Примечание
Установленный по умолчанию язык Avira SearchFree Toolbar соответствует, если это возможно, вашей программе. Если Toolbar на вашем языке недоступен, по умолчанию устанавливается английский язык.

- **Показывать подсказки для кнопок**
  Деактивируйте опцию **Показывать подсказки для кнопок**, если хотите скрыть текст рядом со значками Avira SearchFree Toolbar.

Удалить поиск

Активируйте опцию **Удалить поиск**, если необходимо не сохранять уже выполненные поиски,
а сразу удалять их.

Справка

Нажмите **Справка** для перехода на веб-сайт с часто задаваемыми вопросами (FAQ) по Toolbar.

Удаление

Можно удалить Avira SearchFree Toolbar также прямо в Internet Explorer: Удаление в веб-браузере.

Информация

Нажмите **Информация**, чтобы узнать, какая версия Toolbar у вас установлена.

Firefox

В веб-браузере Firefox в меню **Опции** доступны следующие опции для настройки Avira SearchFree Toolbar:

Опции Toolbar

Поиск

- **Поисковая машина Ask**
  В меню **Поисковая машина Ask** можно выбрать, какую поисковую машину Ask использовать для поиска. Доступны поисковые машины США, Бразилии, Германии, Испании, Европы, Франции, Италии, Нидерландов, России и Великобритании.
- **Показывать последние запросы поиска**
  Если активирована опция **Показывать последние запросы на поиск**, то нажав стрелку на панели инструментов поиска, вы можете посмотреть введенные до этого запросы поиска. Выберите один из них, если вы снова хотите посмотреть результат поиска.
- **Удалить поиск при закрытии браузера**
  Активируйте опцию **Удалить поиск при закрытии браузера**, если вы не сохраняете уже выполненные поиски и хотите их удалить.
- **Результаты поиска Ask показывают, если в адресное поле браузера введены ключевые слова или недействительные адреса URL**
  Если эта опция активирована, каждый раз, когда вы вводите в адресное поле веб-браузера ключевые слова или недействительный адрес URL, запускается поисковый запрос и отображается результат поиска.

Другие опции

- **Языки Toolbar**
  В разделе **Языки Toolbar** вы можете выбрать язык, на котором Avira SearchFree Toolbar выводит на экран информацию. Доступны английский, немецкий, испанский, французский, итальянский и португальский языки.

Примечание
Установленный по умолчанию язык Avira SearchFree Toolbar соответствует, если это возможно, вашей программе. Если Toolbar на вашем языке недоступен, по умолчанию устанавливается английский язык.

- **Показывать названия кнопок**
  Деактивируйте опцию **Показывать названия кнопок**, если хотите скрыть текст рядом со значками Avira SearchFree Toolbar.

Удалить поиск

Нажмите **Очистить историю поиска**, чтобы удалить все введенные до этого в поиске Avira SearchFree Toolbar запросы.

Справка

Нажмите **Справка** для перехода на веб-сайт с часто задаваемыми вопросами (FAQ) по Toolbar.

Удаление

Можно удалить Avira SearchFree Toolbar также прямо в Firefox: Удаление в веб-браузере.

Информация

Нажмите **Информация**, чтобы узнать, какая версия Toolbar у вас установлена.

5.2.4 Удаление

Avira SearchFree Toolbar удаляется следующим образом (описано на примере Windows XP и Windows Vista):

- Откройте пункт меню Windows **Пуск**, **Панель управления**.
- Сделайте двойной щелчок на **Program Files** (Windows XP: **Установка и удаление программ**).
- Выберите **Avira SearchFree Toolbar plus WebGuard** в списке и щелкните **Удалить**.

→ Появится запрос подтверждения, что вы действительно хотите удалить продукт.

- Подтвердите кнопкой **Да**.

→ Программа Avira SearchFree Toolbar plus WebGuard удалена. Компьютер при необходимости перезагружается. При этом все папки, файлы и записи программы в реестре уничтожаются.

Удаление с помощью веб-браузера

Можно удалить Avira SearchFree Toolbar прямо в браузере:

- На панели инструментов поиска откройте справа меню **опции**.
- Нажмите **Удалить**.

→ Если веб-браузер еще открыт, появится запрос на его закрытие.

- Закройте веб-браузер и нажмите **OK**.

→ Программа Avira SearchFree Toolbar plus WebGuard удалена. Компьютер при необходимости перезагружается. При этом все папки, файлы и записи программы в реестре уничтожаются.

Примечание
После удаления Avira SearchFree Toolbar, при необходимости, удаляется также WebGuard.

Примечание
Учтите, что для удаления Avira SearchFree Toolbar из Firefox, должен быть активирован Toolbar в менеджере дополнений.

5.3 Это делается так

5.3.1 Выполнять автоматическое обновление

С помощью Планировщика AntiVir создается задача, с помощью которой программа AntiVir обновляется автоматически:

- В центре управления выберите во вкладке **Управление :: Планировщик**.

- ▶ Нажмите пиктограмму  *Создать новый профиль с помощью ассистента*.

→ 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**
  - **Однократно**

Примечание
Мы рекомендуем выполнять регулярное и частое автоматическое обновление. Рекомендованный промежуток между обновлениями: 24 .

- ▶ В зависимости от выбора задайте время.
- ▶ При необходимости выберите дополнительные опции(в зависимости от типа задачи):
  - **Запуск задачи, даже если установленное время запуска 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**.

→ Созданная Вами новая задача появится на начальной странице вкладки **Управление:: Проверка** как активированная (галочка).

- ▶ Деактивируйте задачи, которые не должны выполняться.

Используя следующие значки, вы можете обрабатывать задачи:

 просмотреть свойства задачи

 изменить задачу

 удалить задачу

 запустить задачу

 остановить задачу

5.3.2 Запустить обновление вручную

Существует несколько способов запустить обновление вручную: При выполнении обновления вручную производится обновление файла вирусных сигнатур и поискового движка. Обновление программы выполняется лишь в том случае, если в настройках в Общее :: Обновление активирована опция **Загружать и автоматически устанавливать обновления программы**.

Запуск вручную обновления программы AntiVir производится следующим образом:

- ▶ Щелкните правой кнопкой мыши значок AntiVir в трее на панели задач.
- → Появится контекстное меню.
- ▶ Выберите **Запуск обновления**.
- → Появится диалоговое окно *Модуль обновления* .

- ИЛИ -

- ▶ В центре управления выберите во вкладке **Обзор :: Состояние**.
- ▶ В области *Последнее обновление* нажмите ссылку **Запустить обновление**.
- → Появится диалоговое окно Модуль обновления.

- ИЛИ -

- ▶ В центре управления в меню **Обновление** выберите команду меню *Запуск обновления*.
- → Появится диалоговое окно Модуль обновления.

Примечание
Мы рекомендуем выполнять регулярное автоматическое обновление. Рекомендованный промежуток между обновлениями: 24 .

Примечание
Вы можете выполнить обновление вручную через Центр безопасности Windows.

5.3.3 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 админимстратора 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

- ▶ В центре управления нажмите во вкладке **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* и запустится прямой поиск.
- → 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:

5.3.4 Проверка: Поиск вирусов и вредоносного ПО посредством перетаскивания

Целенаправленный поиск вирусов и вредоносного ПО с помощью перетаскивания:

✓ Центр управления программы AntiVir открыт.

- Выделите файл, который необходимо проверить.
- Перетяните левой кнопкой мышки выделенный файл на *центр управления*.

→ Появится окно *Luke Filewalker* и запустится прямой поиск.

→ По окончании проверки будут показаны результаты.

5.3.5 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* и запустится прямой поиск.

→ По окончании проверки будут показаны результаты.

5.3.6 Проверка: Автоматический поиск вирусов и вредоносного ПО

Примечание
После установки программы в планировщике создана задача проверки *Полная проверка системы*: Через рекомендованный промежуток времени автоматически выполняется полная проверка системы.

Вы создаете задачу, с помощью которой Вы задаете автоматический поиск вирусов и вредоносного ПО:

- В Центре управления нажмите выберите раздел **Управление :: Планировщик**.
- Нажмите пиктограмму  .

→ 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**
- **Однократно**

▶ В зависимости от выбора задайте время.

▶ При необходимости выберите дополнительную опцию из следующих (в зависимости от типа задачи):

- **Запуск задачи, даже если установленное время запуска 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

▶ Выберите опцию *Выключить компьютер*, если Вы хотите автоматически отключить компьютер, как только задача будет выполнена и завершена. Опция доступна только в минимизированном и максимизированном режиме отображения.

▶ Нажмите кнопку **Готово**.

→ Созданная Вами новая задача появится на начальной странице вкладки *Управление:: Планировщик* активирован (галочка).

▶ Деактивируйте задачи, которые не должны выполняться.

Используя следующие символы, Вы можете обработать задания:

 просмотреть свойства задачи

 изменить задачу

 удалить задачу

 запустить задачу

 остановить задачу

5.3.7 Проверка: Прямой поиск активных руткит-программ

Для поиска активных руткитов используйте предварительно определенный профиль поиска *Поиск руткитов и активного вредоносного ПО*.

Прямой поиск активных руткит-программ:

▶ Выберите в Центре управления в разделе **Локальная защита :: Проверка**.

→ Появятся предустановленные профили поиска.

- Выберите предварительно определенный профиль поиска **Поиск руткитов и активного вредоносного ПО**.
- Отметьте дополнительные узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле.
- Выберите символ (Windows XP:  или Windows Vista: ).

→ Появится окно *Luke Filewalker* и запустится прямой поиск.

→ По окончании проверки будут показаны результаты.

5.3.8 Реагировать на найденные вирусы и вредоносное ПО

Для отдельных компонентов защиты программы AntiVir в настройках в разделе *Действие при обнаружении* можно установить, как программа AntiVir будет реагировать при обнаружении вируса или вредоносного ПО.

Для компонента Guard не существует настраиваемых опций действия. При обнаружении на рабочем столе появится уведомление. В уведомлении на рабочем столе Вы можете удалить найденное вредоносное ПО или передать вредоносное ПО с помощью кнопки Подробно сканеру для дополнительной обработки вируса. Сканер сообщает об обнаружении в окне, в контекстном меню которого доступны различные опции для обработки соответствующего файла (см. Обнаружение::Сканер):

Опции действия для сканера:

– **Интерактивный**

В интерактивном режиме обнаруженные сканером объекты показываются в диалоговом окне. Эта настройка активна по умолчанию. При проверке **сканером** по завершении проверки выдается предупреждение со списком обнаруженных файлов. С помощью контекстного меню Вы можете выбрать действие для подозрительных или инфицированных файлов. Вы можете применить выбранное действие ко всем файлам или завершить работу сканера.

– **Автоматический**

В автоматическом режиме при обнаружении вируса или вредоносной программы автоматически выполняется действие, которое Вы предварительно выбрали.

Доступные действия для , WebGuard:

– **Интерактивный**

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

– **Автоматический**

В автоматическом режиме при обнаружении вируса или вредоносной программы автоматически выполняется действие, которое Вы предварительно выбрали.

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
Выбор доступных действий зависит от операционной системы, от компонента защиты (AntiVir Guard, AntiVir Scanner, AntiVir WebGuard), который сообщает о найденном объекте, и от вредоносной программы.

Действия сканера и модуля 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 позднее вылечены или, в случае необходимости, отправлены компании Avira GmbH.

- **Удалить**

  Файл удаляется. 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**

  Другие действия не выполняются. Инфицированный файл все еще активен в Вашей системе!

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

- **Всегда игнорировать**

  Возможные действия при обнаружении модулем Guard: Guard не выполняет дальнейших действий. Доступ к файлу разрешен. Все следующие доступы к этому файлу разрешены и до перезапуска компьютера или обновления файла вирусных сигнатур сообщения больше не поступают.

- **Копировать в карантин**

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

- **Восстановление загрузочного сектора | Загрузка программы восстановления**

  Доступные действия при обнаружении инфицированных загрузочных секторов: Для инфицированных дискет доступны опции восстановления. Если восстановление с помощью программы AntiVir невозможно, можно загрузить специальную программу для обнаружения и удаления вирусов в загрузочном секторе.

Примечание
Используемые действия не могут быть применены к работающим процессам.

Действия модуля WebGuard:

– **Запретить доступ**

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

– **Поместить на карантин**

Запрошенная веб-сервером страница или переданные данные и файлы будут помещены на карантин. Файл может быть восстановлен из менеджера карантина, если в этом возникнет необходимость, или его можно отправить разработчику - в центр исследования вирусов компании Avira.

– **Пропустить**

Запрошенная веб-сервером страница или переданные данные и файлы не будут перенаправлены Вашему браузеру модулем WebGuard.

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

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

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

Обращение с файлами, помещенными на карантин:

- В центре управления выберите во вкладке **Управление :: Карантин**.
- Проверьте тип файлов, чтобы Вы могли обратно загрузить на Ваш компьютер их оригиналы.

Если Вам необходима более подробная информация:

- Выделите 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 программы AntiVir был обновлен и существует подозрение о ложном срабатывании. При повторной проверке Вы можете подтвердить ложное срабатывание и восстановить файл.

- Выделите 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:

▶ Выделите файл и нажмите  .

Для загрузки файла на анализ на веб-сервер в центр исследований вирусов компании Avira:

▶ 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.**.

→ Файл загружается в заархивированном виде на веб-сервер в центр исследований вирусов компании Avira.

Примечание
В следующих случаях рекомендуется выполнить анализ с помощью центра исследования вирусов компании Avira:
Эвристика (подозрительный файл): При проверке программа AntiVir распознала файл как подозрительный и отправила его в Карантин: В диалоговом окне, появившемся в связи с обнаружением вируса, или в файле отчета проверки было рекомендовано выполнить анализ файла с помощью центра исследования вирусов компанией Avira.

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

Примечание
Вы можете отправить только один файл.

Экспорт свойств объекта карантина в текстовый файл:

▶ Выделите объект карантина и нажмите  .

→ Откроется текстовый файл с данными о выбранном объекте карантина.

▶ Сохраните текстовый файл.

Файлы, помещенные на карантин, могут быть восстановлены:

– см. раздел: Карантин: Восстановление файлов в карантине

5.3.10 Карантин: Восстановление файлов в карантине

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

– Windows XP и 2000:

 С помощью этого значка файлы восстанавливаются в исходную папку.

 С помощью этого значка файлы восстанавливаются в выбранную вами 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 админимстратора выдаются профилем поиска при каждом запуске.

 С помощью этого значка файлы восстанавливаются в выбранную вами папку.

 С помощью этого значка файлы восстанавливаются в исходную 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* только в исключительных случаях. Восстанавливайте только те файлы, которые могут быть вылечены при повторной проверке.

✓ Повторно проверить и вылечить файл.

▶ В центре управления выберите во вкладке **Управление :: Карантин**.

Примечание
Электронные письма и приложения к ним можно восстановить только при включенной 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
Электронные письма и приложения к ним можно восстановить только при включенной 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:

▶ Выделите 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.

5.3.11 Карантин: Поместить подозрительный файл на карантин

Вы можете поместить подозрительный файл на карантин вручную:

- ▶ В центре управления выберите во вкладке **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, можно проверить сканером AntiVir:

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

5.3.12 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):

✓ В Центре управления нажмите в разделе **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 файлов* со списком всех типов файлов, которые будут проверяться 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 файлов в поле ввода.

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

5.3.13 Профиль поиска: Создание ярлыка для профиля поиска

С помощью ярлыка прямого поиска можно запускать его непосредственно с рабочего стола, не открывая Центр управления программы AntiVir.

Создать ярлык к выбранному профилю на рабочем столе:

✓ В Центре управления нажмите в разделе **Локальная защита :: *Проверка***.

- ▶ Выберите профиль поиска, для которого Вы хотите создать ярлык.
- ▶ Нажмите пиктограмму  .

→ Появится ярлык на рабочем столе.

5.3.14 События: Фильтровать события

В центре управления в **Обзор :: События** Показываются события, вызванные компонентами программы AntiVir (аналогично уведомлениям о событиях операционной системы Windows). В компоненты программы входят:

- Программа обновлений
- Guard
- Сканер
- Планировщик
- WebGuard
- Временная служба

Отображаются следующие типы событий:

- Информация
- Предупреждение
- Ошибка
- Обнаружение

Фильтрация отображаемых событий:

- ▶ В центре управления выберите во вкладке **Обзор :: выберите 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 Сканер

С помощью сканера можно выполнять целенаправленный поиск вирусов и вредоносных программ (прямой поиск). Существует несколько способов проведения проверки на вирусы:

- **Проверка через контекстное меню**
  Прямой поиск с помощью контекстного меню (правая клавиша мышки - пункт **Проверить выбранные файлы с помощью AntiVir**) рекомендуется в том случае, когда требуется проверить отдельные файлы и папки в проводнике Windows. Еще одно преимущество заключается в том, что для прямого поиска с помощью контекстного меню даже не требуется запуск Центра управления.
- **Проверка с помощью Drag & Drop**
  При перетаскивании файла или папки в окно программы Центр управления сканер проверяет файл или каталог, а также все имеющиеся подкаталоги. 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.
- **Прямой поиск с помощью планировщика**
  Планировщик позволяет запускать проверки в заданное время.

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

- Поиск руткитов с помощью профиля поиска *Поиск активного вредоносного ПО*
- 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 модуль обновления встроен в AntiVir . Модуль обновления отвечает за то, чтобы программа AntiVir всегда находилась на самом актуальном уровне и могла обнаруживать ежедневно появляющиеся новые вирусы. Этот модуль обновляет следующие компоненты:

- VDF-файл:

  VDF-файл содержит образцы вредоносных кодов, используемых программой AntiVir при поиске вирусов и лечении файлов.

- Ядро:

  Поисковый движок содержит методы, с помощью которых программа AntiVir обнаруживает вирусы.

- 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 модуль обновления дополнительно может выполнять обновление программы или сообщает о доступных обновлениях. После обновления программы может потребоваться перезапуск компьютера. Если обновляется только файл VDF и поисковый движок, перезагрузка не требуется.

Примечание
Для обеспечения безопасности модуль обновления проверяет, не был ли изменен hosts-файл Windows в вашем компьютере, не изменили ли вредоносные программы URL обновления и не перенаправили ли они модуль обновления на нежелательные сайты загрузки. Если осуществлялись манипуляции с hosts-файлом Windows, это будет видно в файле отчета модуля обновления.

Обновление автоматически выполняется через следующие интервалы: 24 . 24 . Автоматическую настройку можно изменить или отключить в (Настройки::Обновление).

В центре управления в планировщике можно создавать дополнительные задачи обновления, которые будут выполняться модулем обновления в заданные промежутки времени. У Вас есть возможность вручную запустить обновление:

- В центре управления: В меню Обновление и разделе Состояние
- С помощью контекстного меню значка в трее

Вы закачиваете обновления из интернет с веб-сервера разработчика. По умолчанию используется существующее сетевое соединение с серверами загрузки Avira GmbH. Изменить это значение по умолчанию можно в настройках Общее :: Обновление.

8 Устранение проблем, советы

в этой главе вы найдете важные указания по решению проблем и советы по работе с программой AntiVir.

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.

- Не работает чат: не отображаются сообщения пользователей чата

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

Причина: Ваше интернет-соединение неактивно. Поэтому не удалось установить соединение с веб-сервером.

▶ 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 параметры в настройках (режим эксперта) в Общее :: Обновление.

Вирусы и вредоносные программы невозможно удалить или переместить.

Причина: Файл загружается Windows и находится в активном состоянии.

▶ Обновите свой продукт AntiVir.

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

▶ Запустите компьютер в безопасном режиме.

▶ Запустите программу AntiVir и настройку (режим эксперта).

▶ Выберите Сканер :: Поиск :: Файлы :: Все файлы и подтвердите нажатием **OK**.

▶ 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: Служба AntiVir Guard остановлена.

- В центре управления нажмите во вкладке Обзор:: Статус в области AntiVir Guard ссылку **Активировать**.

Причина: AntiVir Guard блокируется брандмауэром.

- В настройках своего брандмауэра установите полное разрешение для AntiVir Guard. Модуль AntiVir Guard работает исключительно с адресом 127.0.0.1 (localhost). Не устанавливается соединение с интернетом.

Иначе:

- Перепроверьте вид 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 запись *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 во время создания резервной копии проверяет все файлы, с которыми работает резервное копирование данных.

- В настройках выберите (режим эксперта) Guard :: Поиск :: Исключения и введите название процесса программы резервного копирования.

Мой брандмауэр сообщает об AntiVir Guard и AntiVir MailGuard, как только я их включаю.

Причина: Связь между AntiVir Guard осуществляется по протоколу интернета TCP/IP. Брандмауэр отслеживает все соединения, производящиеся по этому протоколу.

- Установите полное разрешение для AntiVir Guard. Модуль AntiVir Guard работает исключительно с адресом 127.0.0.1 (localhost). Не устанавливается соединение с интернетом.

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

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

Эта ситуация может возникать в чатах, работающих по HTTP-протоколу с параметром 'transfer-encoding= chunked’.

Причина: WebGuard сначала полностью проверяет отправленные данные на наличие вирусов и вредоносного ПО, только потом данные грузятся в веб-браузер. При передаче данных с помощью ’r;r;transfer-encoding= chunked’ модуль WebGuard не может определить длину сообщения или количество данных.

▶ В настройках введите URL веб-чата в качестве исключения (см. настройки: WebGuard::Исключения).

8.2 Горячие клавиши

Команды клавиатуры (горячие клавиши) дают возможность использовать альтернативную навигацию по программе, вызывать отдельные модули и запускать действия.

Ниже представлен обзор доступных команд клавиатуры. 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	Навигация в центре управления Перейти к следующему разделу.
Ctrl + Shift + Tab Ctrl + Page up	Навигация в центре управления Перейти к предыдущему разделу.
← ↑ → ↓	Навигация по вкладкам настроек Сначала установите курсор мышки на вкладку настроек.
Tab	Переход к следующей опции / группе опций.
Shift + Tab	Переход к предыдущей опции / группе опций.
← ↑ → ↓	Переключение между опциями в выделенном ниспадающем 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	Открыть выбранный раскрывающийся список.
Esc	Закрывает раскрывающийся список. Отмена команды и закрытие окна.
Enter	Выполнение команды активной оции 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.
Page up Page down	Перемещение внутри темы.

8.2.3 В центре управления

Общее

Горячие клавиши	Описание
F1	Вызов Справки
Alt + F4	Закрыть центр управления
F5	Обновить вид
F8	Открыть меню настройки
F9	Запустить обновление

Раздел 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

Раздел 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)

Раздел События

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

8.3 Центр безопасности Windows

- начиная с 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 обеспечения безопасности Windows и программа AntiVir

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

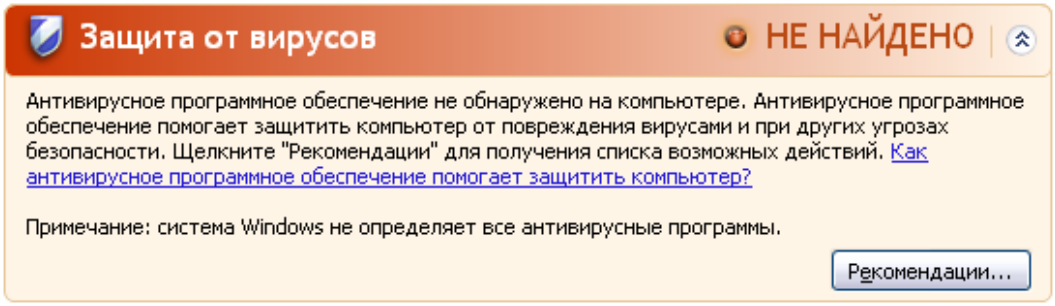
Защита от вирусов ВКЛЮЧЕНА

Защита от вирусов ВЫКЛЮЧЕНА

Защита от вирусов НЕ КОНТРОЛИРУЕТСЯ

Защита от вирусов НЕ ОБНАРУЖЕНА

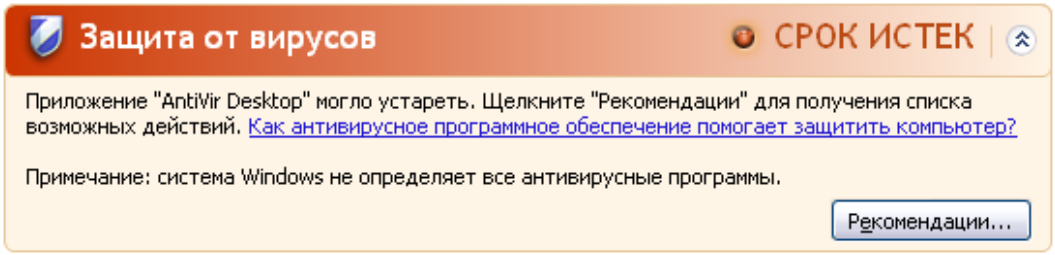
Это сообщение отправляется Центром обеспечения безопасности Windows, если на компьютере не было обнаружено антивирусных программ.



Примечание
Установите программу AntiVir на ваш компьютер для того, чтобы защитить его от вирусов и иных вредоносных программ!

Антивирусные базы УСТАРЕЛИ

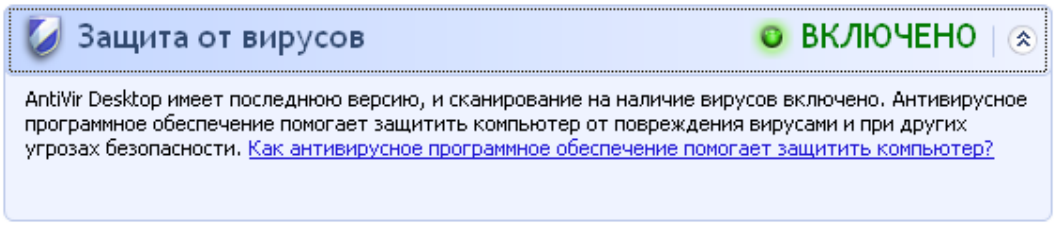
Если вы уже установили Windows XP Service Pack 2 или Windows Vista, а теперь устанавливаете программу AntiVir или устанавливаете Windows XP Service Pack 2 или Windows Vista на систему, в которой уже была установлена программа AntiVir, будет выдано следующее сообщение:



Примечание
Чтобы Центр обеспечения безопасности Windows посчитал программу AntiVir актуальной, после установке программы обязательно необходимо произвести обновление. Вы можете актуализировать свою систему, произведя Обновление.

Защита от вирусов ВКЛЮЧЕНА

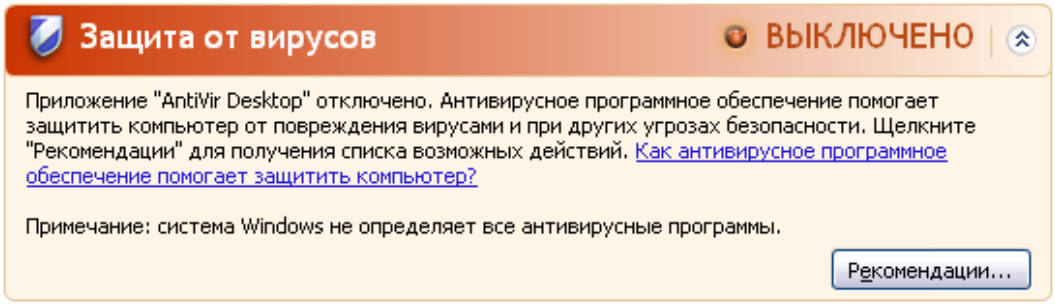
После установки и последующего обновления программы AntiVir вы получите следующее сообщение:



Теперь ваша программа AntiVir имеет самую последнюю версию и AntiVir Guard активен.

Защита от вирусов ОТКЛЮЧЕНА

Следующее сообщение появляется при деактивации модуля AntiVir Guard или остановке службы Guard.

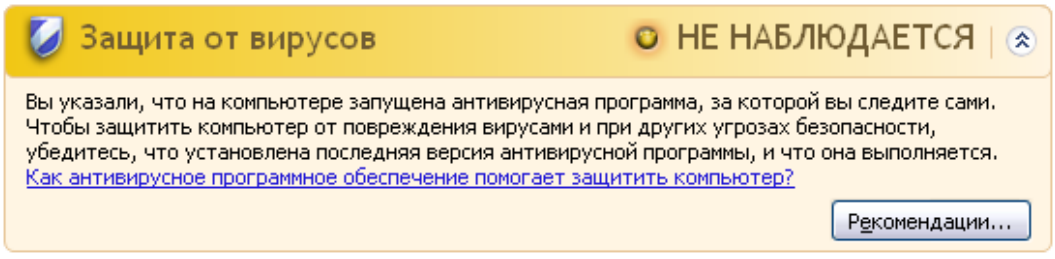


Примечание
Активировать и деактивировать модуль AntiVir Guard можно во вкладке Обзор :: Активировать или деактивировать статус Центра управления. Если AntiVir Guard включен, на панели задач появляется открытый красный зонтик.

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 программой AntiVir. Вы можете включить эту опцию в любое время с помощью кнопки "Рекомендации...".

Примечание
Даже если вы установили на своей системе Windows XP Service Pack 2 или Windows Vista, вам все равно требуется антивирусное решение. Хотя Windows XP SP 2 контролирует Ваше антивирусное ПО, Центр обеспечения безопасности Windows не имеет функций антивирусной защиты. Без дополнительных специальных средств защиты Ваша система не защищена от вирусов и вредоносного ПО.

9 Вирусы и другое

9.1 Категории угроз

Программы дозвона на платные номера (DIALER)

Определенные услуги, предлагаемые в интернете, 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 онлайн-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 программа AntiVir 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.

Программа AntiVir способна распознавать компьютерные игры. Если в настройках в разделе Дополнительные категории угроз включена опция **Игры (GAMES)**, вы получите соответствующее уведомление при обнаружении подобных объектов. 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.

AntiVir 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.

Программа AntiVir распознает программы категории "Security Privacy Risk". Если в настройках в разделе Дополнительные категории угроз включена опция **Security Privacy Risk (SPR)**, вы получите соответствующее уведомление при обнаружении подобных объектов.

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.

AntiVir способна распознавать программы категории "Backdoor Steuersoftware". Если в настройках в разделе Дополнительные категории угроз включена опция **Backdoor Steuersoftware (BDC)**, вы получите соответствующее уведомление при обнаружении подобных объектов.

Рекламные и шпионские программы (ADSPY)

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

AntiVir способна распознавать программы категории "Adware/Spyware". Если в настройках в разделе Дополнительные категории угроз включена опция Adware/Spyware (ADSPY), вы получите соответствующее уведомление при обнаружении подобных объектов.

Необычные средства сжатия данных (PCK)

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

AntiVir способна распознавать программы категории "Необычные паковщики". Если в настройках в разделе Дополнительные категории угроз включена опция **Необычные паковщики (PCK)**, пользователь получает предупреждение в случае, если обнаружит подобные объекты.

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

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

Программа AntiVir 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 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.

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

Приложение (APPL)

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

Программа AntiVir способна распознавать "Приложение (APPL)". Если в настройках в группе Дополнительные категории угроз включена опция **Приложение (APPL)**, пользователь получает уведомление при обнаружении таких объектов.

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 интернете), состоящая из отдельных персональных компьютеров, связывающихся 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.

Hoaxes (англ.: hoax - обман, ложь, мистификация, шутка)

Уже несколько лет пользователи интернета 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 интернета, а основываясь на этих данных, демонстрируют рекламные банеры 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

главы содержатся 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 Контакты

Мы с удовольствием поможем вам, если у вас есть вопросы и пожелания по линейке продукции AntiVir. Наши контактные данные указаны в центре управления в Справка :: О программе Avira AntiVir Personal.

10.2 Техническая поддержка

Служба технической поддержки компании Avira всегда готова помочь вам; мы ответим на ваши вопросы и решим технические проблемы.

На нашем сайте вы можете получить всю необходимую информацию, касающуюся техподдержки:

http://www.avira.ru/classic-support

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

- **Информация о версии**. Эта информация отображается в меню программы в пункте Справка :: О программе Avira 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 файл в менеджере карантина центра управления и с помощью контекстного меню или соответствующей кнопки выберите пункт Отправить файл.

- Отправьте требуемый файл в заархивированном виде (WinZIP, PKZip, Arj и т.д.), как приложение 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 программа AntiVir пометила заведомо чистый, по вашему мнению, файл, как инфицированный, отправьте этот файл в заархивированном (WinZIP, PKZIP, Arj и пр.) виде по следующему адресу:

- 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 ссылке содержится информация о всех доступных настроечных опциях.

11.1 Сканер

Раздел блока Сканер 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, сканер осуществляет проверку в зависимости от настроек:

- с определенной производительностью поисковой системы (приоритет),
- 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

Сканер может использовать фильтр, чтобы проверять только файлы с определенным окончанием (тип).

Все файлы

Если эта функция включена, все файлы, независимо от их содержания и расширения, будут проверяться на вирусы или нежелательные программы. Фильтр не используется.

Примечание
Если включена опция Все файлы, кнопка **Расширения файлов** будет недоступна.

Интеллектуальный отбор файлов

Если эта опция включена, то программа выбирает файлы для проверки полностью автоматически. Это означает, что программа AntiVir принимает решение о необходимости проверки файла на наличие вирусов и вредоносных программ, исходя из его содержания. Эта процедура длиться немного дольше, чем Использовать список расширений файлов, но она значительно надежнее, поскольку проверка выполняется не только на основании расширений файлов. Эта опция включена по умолчанию и рекомендована.

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

Использовать список расширений файлов

Если эта функция включена, то в поиск будут включаться только файлы с указанным расширением. По умолчанию указаны все типы файлов, которые могут содержать вирусы и нежелательные программы. Кнопка "**Расширение файла"** позволяет редактировать список вручную.

Примечание
Если эта опция включена, а вы удалили все записи из списка расширений, информация об этом отображается в виде текста "Расширения не определены", расположенного под кнопкой **Расширения файлов**.

Расширения файлов

С помощью этой кнопки вызывается диалоговое окно со всеми расширениями файлов, которые проверяются при поиске в режиме "**Использовать список расширений файлов"**. 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 сканер сканирует загрузочные секторы выбранных дисков. Эта настройка активна по умолчанию.

Проверка главн. загруз. секторов

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

Пропускать оффлайн-файлы

Если опция включена, то при прямой проверке так называемые оффлайн-файлы не проверяются полностью. Т.е., эти файлы не проверяются на наличие вирусов и вредоносных программ. Оффлайн-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 целостности 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.

Важно
Эта функция доступна только начиная с Windows Vista.

Примечание
Если используются программы третьих поставщиков, изменяющие системные файлы и, например, экраны загрузки, не используйте эту опцию! Примеры таких программ: Skinpacks, TuneUp Utilities или Vista Customization.

Оптимизированный поиск

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

Примечание
Опция доступна только для многопроцессорных компьютеров. не используется Сканером.

Следовать по ссылкам

Если опция включена, то Сканер 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 Сканер при каждом запуске проверки осуществляет быструю проверку системных папок Windows на руткит-программы. Этим способом компьютер проверяется на активный руткит не так тщательно, как через профиль поиска "**Поиск руткит-программ"**, но гораздо быстрее.

Важно
Поиск руткитов в Windows XP 64 Bit недоступен!

Сканирование реестра

Если эта опция включена, то при проверке реестр сканируется на наличие вредоносных программ.

Процесс сканирования

Разрешать остановку проверки

Если эта опция включена, то в любое время можно остановить процесс поиска вирусов и вредоносных программ нажатием кнопки "**Стоп"** в окне "Luke Filewalker". Если вы отключили эту настройку, то кнопка **Стоп** в окне "Luke Filewalker" будет неактивна. Остановка проверки до ее окончания станет невозможной! Эта настройка активна по умолчанию.

Приоритет сканирования

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

Низкий

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

Средний

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

Высокий

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

11.1.1.1. Действие при обнаружении

Действие при обнаружении

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

Интерактивный

Если опция включена, то об обнаружении вирусов при проверке Сканером сообщается в диалоговом окне. При проверке сканером по завершении проверки выдается предупреждение со списком обнаруженных файлов. С помощью контекстного меню Вы можете выбрать действие для подозрительных или инфицированных файлов. Вы можете применить выбранное действие ко всем файлам или завершить работу сканера.

Примечание
По умолчанию в диалоговом окне по обработке вирусов стоит 'Переместить в карантин'. С помощью контекстного меню можно выбирать дополнительные действия.

Подробная информация доступна здесь.

Автоматический

Если опция включена, при обнаружении вируса или вредоносной программы действие происходит автоматически, не предлагая выбора. Сканер работает автоматически в соответствии с выбранными Вами настройками.

файл перед действием копировать в карантин

Если эта опция включена, Сканер 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 резервную копию в Avira Malware Research Center для дальнейшего изучения.

Первичное действие

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

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

лечить

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

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

удалить

Если опция включена, файл удаляется.

Переименовать

Если опция включена, сканер 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

При включенной опции сканер перемещает файл на карантин. Файлы могут быть позже вылечены или, в случае необходимости, отправлены разработчику (Avira Malware Research Center).

Вторичное действие

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

удалить

Если опция включена, файл удаляется.

Переименовать

Если опция включена, сканер 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

При включенной опции сканер перемещает файл на карантин. Файлы могут быть позже вылечены или, в случае необходимости, отправлены разработчику (Avira Malware Research Center).

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 проверке архивов Сканер применяет технологию рекурсивного поиска. Содержащиеся в архивах архивы также распаковываются и проверяются на наличие вирусов и нежелательных программ. Файлы проверяются, затем они распаковываются и вновь проверяются.

Просмотреть архив

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.

Базовый список расширений

Если эта опция включена, то Сканнер 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 *. xyz, то Сканер 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, Сканер производит проверку архива до того уровня рекурсии, на котором находится подозрительный объект.

Максимальная 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.

Архивы

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

11.1.1.2. Исключения

Файловые объекты, исключенные из проверки

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

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
Содержащиеся в этом списке файлы фиксируются 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.

Нажатием на кнопку открывается 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 запись. Кнопка неактивна, если ни одна запись 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 Сканером, `D:\folder\file.txt` из проверки не исключается.

11.1.1.3. Эвристика

Этот раздел настроек содержит параметры эвристического поиска.

Продукт AntiVir 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

Продукт AntiVir 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 опция включена по умолчанию и рекомендована.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Благодаря технологии AntiVir AHeAD программа AntiVir содержит очень мощную эвристическую систему для определения даже неизвестных вирусов и (новых) вредоносных программ. При активированной опции здесь можно установить уровень "резкости" эвристики. Эта настройка активна по умолчанию.

Низкий уровень распознавания

Если опция активирована, обнаруживается меньше неизвестных вредоносных программ, зато ниже вероятность ошибочного обнаружения.

Средний уровень распознавания

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

Высокий уровень распознавания

Если опция активирована, распознается значительно больше вредоносных программ, но возможны и ложные срабатывания.

11.1.2 Отчет

Сканер 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 Сканер, необходимо всегда составлять файл отчета.

Протоколирование

Не требуется

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

По умолчанию

при установленной опции сканер протоколирует имя соответствующих файлов с указанием пути. Кроме того, параметры настройки Проверки, информации о версии и лицензии записываются в файл отчета.

Расширение

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

Полная

При установленной опции сканер дополнительно протоколирует все проверенные файлы. 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

Раздел Guard в настройке отвечает за настройку постоянной защиты.

11.2.1 Поиск

Рекомендуется не отключать постоянную защиту. Для этого используется Guard (поиск в реальном времени = On-Access-Scanner). Это позволяет "на лету" проверить все файлы, скопированные или открытые на компьютере, на наличие вирусов или нежелательных программ.

Режим поиска

Здесь задается время проверки файла.

Проверить при считывании

Если эта опция включена, Guard проверяет файлы, перед тем, как они будут считаны или выполнены приложением или операционной системой.

Проверить при записи

Если эта функция включена,Guard проверяет файл при записи. К файлу можно обратиться только после завершения этой операции.

Проверить при записи и считывании

Если эта функция включена,Guard проверяет файлы перед открытием, считыванием и выполнением, а также после записи. Эта опция включена по умолчанию и рекомендована.

Файлы

Guard может использовать фильтр, чтобы проверять только файлы с определенным окончанием (тип).

Все файлы

Если эта функция включена, все файлы, независимо от их содержания и расширения, будут проверяться на вирусы или нежелательные программы.

Примечание
Ist Все файлы, кнопка **Расширения файлов** будет недоступна.

Интеллектуальный отбор файлов

Если эта опция включена, то программа выбирает файлы для проверки полностью автоматически. Это означает, что программа решает на основании содержания файла, нужно ли проверять его на наличие вирусов и нежелательных программ. Эта процедура длиться немного дольше, чем Использовать список расширений файлов, но она значительно надежнее, поскольку проверка выполняется не только на основании расширений файлов.

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

Использовать список расширений файлов

Если эта функция включена, то в поиск будут включаться только файлы с указанным расширением. По умолчанию указаны все типы файлов, которые могут содержать вирусы и нежелательные программы. С помощью кнопки "**Расширение файла"** список можно редактировать вручную. Эта опция включена по умолчанию и рекомендована.

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 файлов

С помощью этой кнопки вызывается диалоговое окно со всеми расширениями файлов, которые проверяются при поиске в режиме "**Использовать список расширений файлов"**. В списке уже приведены некоторые расширения файлов, но Вы можете легко добавлять новые или удалять их.

Примечание
Помните, что список расширений файлов может изменяться в зависимости от версии

Архивы

Просмотреть архив

При включении этой опция будет осуществляться проверка архивов. Проверяются сжатые файлы, затем они распаковываются и вновь проверяются. По умолчанию опция отключена. Поиск в архиве ограничивается глубиной рекурсии, количеством проверяемых файлов и размером архива. Вы можете задать максимальную глубину рекурсии, количество проверяемых файлов и максимальный размер архива.

Примечание
По умолчанию эта опция отключена, поскольку данный процесс требует много ресурсов. Рекомендуется проверять архив путем прямого поиска.

Максимальная глубина рекурсии

При поиске в архивах Guard применяет рекурсивный поиск: Содержащиеся в архивах архивы также распаковываются и проверяются на наличие вирусов и нежелательных программ. Можно задать глубину рекурсии. Стандартное рекомендуемое значение для глубины рекурсии составляет 1 день: Все архивы, расположенные непосредственно в главном архиве, проверяются.

Максимальное количество файлов

При поиске в архивах поиск ограничивается максимальным количеством файлов в архиве. Стандартное рекомендуемое значение для максимального количества проверяемых файлов составляет 10 дней.

Максимальный размер (КБ)

При поиске в архивах поиск ограничивается максимальным размером распаковываемого файла архива. Значение по умолчанию – 1000 Кб. Оно является рекомендуемым.

11.2.1.1. Действие при обнаружении

Уведомления

Журнал регистрации событий

Если опция включена, при каждом обнаружении в Журнал событий Windows добавляется соответствующая запись. События можно просмотреть в списке событий Windows. Эта настройка активна по умолчанию.

Автозапуск

Блокировать функцию автозапуска

Если эта опция активирована, то выполнение функции автозапуска Windows на всех подключаемых дисках, например, USB-накопители, CD и DVD-диски, сетевые диски, блокируется. Благодаря функции автозапуска Windows информация на носителях или сетевых дисках при подключении сразу считывается, файлы сразу запускаются. Однако эта функция небезопасна, так как существует вероятность автоматического запуска и установки вредоносных программ. Особенно опасна функция автозапуска для USB-накопителей, т.к. данные на них могут постоянно меняться.

Исключить CD и DVD диски

Если эта опция включена, то функция автозапуска допускается для CD и DVD дисков.

Предупреждение
Деактивируйте функцию автозапуска для CD и DVD дисков только тогда, когда Вы уверенны, что используете надежные носители информации.

11.2.1.2. Исключения

С помощью этих опций можно конфигурировать объекты-исключения для Guard (поиск в режиме реального времени). В этом случае данные объекты не будут учитываться при поиске в режиме реального времени. Guard может игнорировать обращения к файлам в соответствии со списком исключенных процессов. Это, в частности, целесообразно для баз данных или решений для резервного копирования.
При указании исключаемых процессов и файловых объектов учитывайте следующее: Список обрабатывается сверху вниз. Чем длиннее список, тем больше времени процессора требует обработка списка для каждого доступа. Поэтому списки должны быть как можно короче.

Процессы, исключенные из постоянной проверки

Все обращения процессов к файлам из этого списка будут исключены из контроля Guard.

Поле ввода

В этом поле можно указать имя процесса, который не нужно включать в поиск в режиме реального времени. По умолчанию не указано ни одного процесса.

Примечание
Вы можете ввести до 128 процессов.

Примечание
При указании процессов используются знаки Юникода. Поэтому вы можете указывать имя процесса или папки, содержащее специальные символы.

Примечание
У вас есть возможность исключать процессы без полного указания пути проверки Guard:
anwendung.exe
Однако, это действительно только для процессов, исполняемые файлы которых находятся на жестком диске.
Не указывайте исключения для процессов, исполняемые файлы которых находятся на динамических дисках. Динамические дисководы используются для сменных носителей, таких как CD, DVD или USB-накопитель.

Примечание
Дисководы должны указываться следующим образом: [буквенное обозначение дисковода]:\
Знак двоеточия (:) можно использовать только для указания дисководов.

Примечание
При указании процессов можно использовать символы-заполнители * (произвольное количество знаков) и ? (один знак):
C:\Program Files\Приложения\приложение.exe
C:\Programme\приложение\anwendun?.exe
C:\Program Files\Приложение\прилож*.exe
C:\Programme\приложение*.exe
Во избежание глобального исключения процессов из проверки Guard недействительным является указание только при помощи следующих знаков: * (звездочка), ? (вопросительный знак), / (слэш), \ (обратный слэш), . (точка), : (двоеточие).

Примечание
Заданный путь и имя файла процесса не должны превышать 255 символов. Совокупная длина строк в списке не должна превышать 6000 знаков.

Предупреждение
Помните, что все обращения процессов, отмеченных в этом списке к файлам, будут исключены из поиска вирусов или нежелательных программ. Windows Explorer и сама операционная система не могут быть исключены из проверки. Соответствующая запись списке будет проигнорирована.

Нажатием на кнопку открывается окно, в котором можно выбрать выполняемый файл.

Процессы

Нажатие кнопки "**Процессы"** открывает окно "*Выбор процессов"*, в котором отображаются текущие процессы.

Добавить

С помощью этой кнопки можно перенести указанный в поле ввода процесс в окно просмотра.

Удалить

С помощью этой кнопки можно удалить отмеченный процесс из окна просмотра.

Файловые объекты, исключенные из постоянной проверки

Все обращения процессов к объектам из этого списка будут исключены из контроля Guard.

Поле ввода

В этом поле можно указать имя файлового объекта, который не нужно включать в проверку в режиме реального времени. По умолчанию список не содержит объектов.

Примечание
При указании исключаемых файловых объектов можно использовать символы-заполнители * (произвольное количество знаков) и ? (один знак). Можно исключать из проверки и отдельные расширения файлов (включая символы-заполнители):
C:\папка*.mdb
*.mdb
*.md?
.xls
C:\папка*.log

Примечание
Имя папки должно заканчиваться на обратный слеш \, в противном случае оно будет рассматриваться как имя файла.

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

Примечание
Если исключается папка, автоматически исключаются и папки, находящиеся внутри.

Примечание
На один диск можно задать не более 20 исключений с полным путем (начиная с буквенного обозначения диска).
Пример: C:\Programme\приложение\Name.log

Максимальное количество исключений без полного пути составляет 64.
Пример: *.log

Примечание
В динамических дисках, подключенных в качестве папки к другому диску, в списке исключений нужно использовать псевдоним операционной системы для подключенного диска:
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:

Нажатием на кнопку открывается окно, в котором можно выбрать исключаемый файловый объект.

Добавить

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

Удалить

С помощью этой кнопки можно удалить отмеченный файловый процесс из окна просмотра.

При указании исключений учитывайте следующее:

Примечание
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 файла.

Примечание
К имени файла, содержащего символы-заполнители, нельзя добавлять в конце обратный слэш.

Например:

```
C:\Program Files\Anwendung\anwend*.exe\
```

Эта запись недействительна. Программа не исключает объект из проверки!

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 Control Center в разделе Локальная защита :: Guard начиная с

Примеры исключаемых процессов:

- anwendung.exe

Процесс anwendung.exe исключается из поиска Guard, независимо от того, на каком из жестких дисков и в каком каталоге находится anwendung.exe.

– C:\Programme1\anwendung.exe

Процесс файла anwendung.exe, который находится в папке C:\Programme1, исключается из поиска Guard.

– C:\Programme1*.exe

Все процессы исполняемых файлов anwendung.exe, которые находятся в папке C:\Programme1, исключаются из поиска Guard.

Примеры для исключаемых файлов:

– *.mdb

Все файлы с расширением 'mdb' исключаются из поиска Guard.

– *.xls*

Все файлы, расширение которых начинается с 'xls', исключаются из поиска Guard, например, файлы с расширениями .xls и xlsx.

– C:\папка*.log

Все Log-файлы с расширением 'log', которые находятся в папке C:\папка, исключаются из поиска Guard.

-

11.2.1.3. Эвристика

Этот раздел настроек содержит параметры эвристического поиска.

Продукт AntiVir 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

Продукт AntiVir 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 опция включена по умолчанию и рекомендована.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Благодаря технологии AntiVir AHeAD программа AntiVir содержит очень мощную эвристическую систему для определения даже неизвестных вирусов и (новых) вредоносных программ. При активированной опции здесь можно установить уровень "резкости" эвристики. Эта настройка активна по умолчанию.

Низкий уровень распознавания

Если опция активирована, обнаруживается меньше неизвестных вредоносных программ, зато ниже вероятность ошибочного обнаружения.

Средний уровень распознавания

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

Высокий уровень распознавания

Если опция активирована, распознается значительно больше вредоносных программ, но возможны и ложные срабатывания.

11.2.2 Отчет

Guard обладает обширными функциями протоколирования, которые могут предоставить пользователю или администратору точные сведения о виде и характере найденного объекта.

Протоколирование

Здесь определяются объемные параметры файла отчета.

Не требуется

Если опция включена, то Guard не составляет протокол.
Отказываться от протоколирования следует только в исключительных случаях, например, только при выполнении тестовых прогонов с большим количеством вирусов или нежелательных программ.

По умолчанию

Если эта опция активирована, компонент Guard записывает в файле отчета важную информацию (о найденном объекте, предупреждениях и ошибках), менее важная информация не включаются из соображений лучшей наглядности. Эта настройка активна по умолчанию.

Расширение

Если эта опция активна, Guard также записывает в файл отчета менее важную информацию.

Полная

Если опция включена, Guard включает данные (тип, размер и дату файла) в файл отчета.

Ограничения для файлов отчетов

Ограничить размер n МБ

Если эта функция включена, то можно ограничить размер файла отчета, возможные значения: от 1 до 100 МБ. Чтобы избежать высокой загрузки системы, при ограничении файла отчета устанавливается ограничение в 50 Кб сверх нормы. Если размера файла отчета превышает установленный лимит на менее 50 Кб, старые записи автоматически удаляются до тех пор, пока размер не приводится в соответствие.

Защитить файл отчета от сокращения

Включив эту опцию, можно защитить файл отчета от сокращения.

Записать конфигурацию в файл отчета

Если эта опция активна, используемая конфигурация поиска в режиме реального времени записывается в файл отчета.

Примечание
Если Вы не указали ограничение для файла отчета, новый файл отчета автоматически создается, когда файл отчета достигает размера 100 МБ. Предусматривается сохранение старого файла отчета. Сохраняются до трех старых файлов отчета. При переполнении буфера сначала удаляются самые старые сохраненные файлы.

11.3 WebGuard

Раздел WebGuard в настройке отвечает за настройку защиты WebGuard.

11.3.1 Поиск

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

Поиск

Запустить WebGuard

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

Защита Drive-By

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

Блокировать подозрительные I-фреймы

Если эта опция включена, то I-Frames на заданных страницах будут проверяться по определенным критериям. Если на веб-странице будут обнаружены подозрительные I-Frames, то они блокируются. В окне I-Frames отобразится сообщение об ошибке.

По умолчанию

Если опция включена, то все I-Frames с подозрительным содержанием блокируются.

Расширение

Если опция включена, то все I-Frames с подозрительным содержанием и I-Frames, используемые подозрительным образом, будут блокироваться. Подозрительное использование кадров I-Frames означает, что I-Frame слишком мал или его не видно в браузере или если I-Frame расположен на необычном месте на веб-странице.

11.3.1.1. Действие при обнаружении

Действие при обнаружении

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

Интерактивный

Если опция включена, при обнаружении вируса или вредоносной программы отображается окно, предлагающее выбор действий, которые можно выполнить с инфицированным файлом. Эта настройка активна по умолчанию.

Подробная информация доступна здесь.

Показать процесс выполнения

Если опция включена, возникает уведомление с отображением прогресса выполнения, если время ожидания загрузки с сайта превышает 20 сек. Это уведомление служит для контроля при загрузке файлов больших объемов с веб-страниц: При открытии Интернет-страниц WebGuard содержание этой страницы загружается постепенно, так как производится проверка на вирусы и вредоносные программы в процессе загрузки. Эта опция по умолчанию отключена.

Автоматический

Если опция включена, при обнаружении вируса или вредоносной программы действие происходит автоматически, не предлагая выбора. WebGuard работает автоматически в соответствии с выбранными Вами настройками.

Первичное действие

Первичное действие - это действие, выполняемое в случае, когда WebGuard обнаруживает вирус или вредоносную программу.

Запретить доступ

Запрошенная веб-сервером страница или переданные данные и файлы не будут перенаправлены Вашему браузеру. В окне веб-браузера отображается информация об отказе в доступе. WebGuard добавляет данные об обнаружении в файл отчета, если Функция отчетов активна.

поместить на карантин

Запрошенная с веб-сервера страница или переданные файлы и данные в случае обнаружения вируса или вредоносной программы помещаются на карантин. Файл может быть восстановлен из менеджера карантина, если в этом возникнет необходимость, или его можно отправить разработчику - в центр исследования вирусов компании Avira.

пропустить

Запрошенная веб-сервером страница или переданные данные и файлы не будут перенаправлены Вашему браузеру модулем WebGuard. Доступ к файлу разрешается, никаких действий с ним не выполняется.

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

11.3.1.2. Запрет доступа

С помощью веб-фильтра можно заблокировать известные нежелательные URL, например, URL фишинг-программ или вредоносных программ. WebGuard препятствует передаче данных из Интернет на Ваш компьютер.

Web-фильтр

Веб-фильтр имеет собственную пополняемую базу данных, в которой ссылки URL расположены в соответствии с содержанием.

Активировать Web-фильтр

Если опция включена, то все адреса URL, которые относятся к выбранным категориям в списке веб-фильтра, блокируются.

Список веб-фильтра

В списке веб-фильтра можно выбрать категории содержания, адреса URL которых должны блокироваться WebGuard.

Примечание
Веб-фильтр игнорируется, если в списке исключенных из проверки ссылок WebGuard::Проверка::Исключения содержатся строки.

Примечание
К группе Спам-URL относятся адреса, через которые распространяются спам-письма. Категория Обман и Дезинформация включает в себя Интернет-страницы с 'абонементами-ловушками' и различными услугами, размер оплаты которых скрывается.

11.3.1.3. Исключения

Вы можете исключить и проверки WebGuard MIME-типы (типы содержимого передаваемых файлов) и типы файлов для URL (Интернет-адреса). Указанные MIME-типы и URL не будут проверяться WebGuard на наличие вирусов или вредоносных систем при пересылке в Вашу компьютерную систему.

Пропускаемые WebGuard MIME-объекты

В этом поле Вы можете выбрать MIME-типы (тип содержимого переданных данных), которые WebGuard проверять не будет.

Пропускаемые WebGuard типы файлов / тип MIME (пользовательск.)

Типы файлов и MIME-типы (тип содержимого переданных данных), указанные в списке, WebGuard исключает из проверки.

Поле ввода

В этом поле укажите имя MIME-типа и типа файла, которые WebGuard исключает из проверки. Для типов файлов указывайте расширения, например, **htm**. Укажите тип и подтип MIME. Тип и подтип отделяются друг от друга обычной косой чертой, например, **video/mpeg** или **audio/x-wav**.

Примечание
При указании типов данных и типов MIME Вы не можете применять заменители символов (* для любого числа символов и ? для замены одного конкретного символа).

Предупреждение
Все типы файлов и типы содержимого файлов, находящиеся в списке исключений, могут быть без дальнейшей проверки WebGuard загружены в Интернет-браузер: Поиск на наличие вирусов и вредоносного ПО не производится.

MIME-типы: Примеры медиа-типов:

- `text=` для текстовых файлов
- `image` = для графических данных
- `video` = для видео файлов
- `audio` = для аудио файлов
- `application` = для файлов, связанных с определенной программой

Примеры: Непроверяемые типы файлов и MIME

- `audio/=` все файлы типа Audio исключаются из проверки WebGuard
- `video/quicktime` = все видео файлы подтипа Quicktime (*.qt, *.mov) исключаются из проверки WebGuard
- `.pdf` = все файлы Adobe-PDF исключаются из проверки WebGuard.

Добавить

С помощью этой кнопки Вы можете добавить к списку исключений введенный MIME-тип или тип файла.

Удалить

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

Пропускаемые WebGuard URL

Все адреса из этого списка исключаются из проверки модулем WebGuard.

Поле ввода

Здесь укажите Интернет адреса, которые необходимо исключить из проверки WebGuard, например, **www.domainname.com/**. Вы можете задать части URL, в конце и в начале укажите уровень домена: .domainname.de для всех страниц и всех поддоменов домена. Веб-страница с любым доменом верхнего уровня (.com или .net) заканчивается точкой: **domainname.**. Если Вы записываете набор символов без точки в начали или в конце, такая последовательность интерпретируется как домен высшего уровня, например, **net** для всех доменов зоны NET (www.domain.net)

Примечание
При вводе адреса URL вы можете использовать специальный символ *, заменяющий произвольное количество знаков. Используйте в сочетании со специальными символами точки для обозначения уровня домена:
.domainname.*
*.domainname.com
.*name*.com (действительно, но не рекомендуется)
Данные без точки, как например, *name* интерпретируются как части первого уровня домена и нецелесообразны.

Предупреждение
Все веб-страницы в списке непроверяемых адресов загружаются в браузер без проверки веб-фильтром или WebGuard: все записи из списка игнорируются веб-фильтром (см. WebGuard::Поиск::Запрет доступа. Поиск на наличие вирусов и вредоносного ПО не производится. Поэтому исключайте из проверки WebGuard только надежные адреса.

Добавить

С помощью этой кнопки можно перенести в окно просмотра URL (Интернет-адрес), содержащийся в поле ввода.

Удалить

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

Примеры: Разрешенные URL

- `www.avira.com` -ИЛИ- `www.avira.com/*`

  = Все URL с доменом 'www.avira.com' исключаются из проверки WebGuard: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,..
  URL с доменом www.avira.de не исключаются из проверки WebGuard.

- `avira.com` -ИЛИ- `*.avira.com`

  = Все URL с доменом второго и первого уровня 'avira.com' исключаются из проверки WebGuard. Данные включают все существующие поддомены к '.avira.com': www.avira.com, forum.avira.com,...

- `avira.` -ИЛИ- `*.avira.*`

= Все URLc доменом второго уровня 'avira' исключаются из проверки WebGuard. Данные включают все существующие домены первого уровня и поддомены к '.avira.': www.avira.com, www.avira.de, forum.avira.com,...

– `.*domain*.*`

= Все URL, содержащие домен второго уровня со строкой символов 'domain' исключаются из проверки WebGuard. www.domain.com, www.new-domain.de, www.sample-domain1.de, ...

– `net` -ИЛИ- `*.net`

= Все URLc доменом первого уровня 'net' исключаются из проверки WebGuard. www.name1.net, www.name2.net,...

Предупреждение
Вводите адреса URL, которые Вы хотите исключить из проверки WebGuard, как можно более точно. Не задавайте домены первого уровня и части доменов второго уровня, так как существует опасность, что из проверки WebGuard будут исключены Интернет-страницы, распространяющие вирусы и вредоносные программы. Рекомендуется задавать полный домен второго уровня и домен первого уровня: domainname.com

11.3.1.4. Эвристика

Этот раздел настроек содержит параметры эвристического поиска.

Продукт AntiVir 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

Продукт AntiVir 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 опция включена по умолчанию и рекомендована.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Благодаря технологии AntiVir AHeAD программа AntiVir содержит очень мощную эвристическую систему для определения даже неизвестных вирусов и (новых) вредоносных программ. При активированной опции здесь можно установить уровень "резкости" эвристики. Эта настройка активна по умолчанию.

Низкий уровень распознавания

Если опция активирована, обнаруживается меньше неизвестных вредоносных программ, зато ниже вероятность ошибочного обнаружения.

Средний уровень распознавания

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

Высокий уровень распознавания

Если опция активирована, распознается значительно больше вредоносных программ, но возможны и ложные срабатывания.

11.3.2 Отчет

WebGuard обладает обширными функциями протоколирования, которые могут предоставить пользователю или администратору точные сведения о виде и характере найденного объекта.

Протоколирование

Здесь определяются объемные параметры файла отчета.

Не требуется

Если опция включена, то WebGuard не составляет протокол. Отказываться от протоколирования следует только в исключительных случаях, например, только при выполнении тестовых прогонов с большим количеством вирусов или нежелательных программ.

По умолчанию

Если эта опция активирована, компонент WebGuard записывает в файле отчета важную информацию (о найденном объекте, предупреждениях и ошибках), менее важная информация не включаются из соображений лучшей наглядности. Эта настройка активна по умолчанию.

Расширение

Если эта опция активна, WebGuard также записывает в файл отчета менее важную информацию.

Полная

Если опция включена, WebGuard включает данные (тип, размер и дату файла) в файл отчета.

Ограничения для файлов отчетов

Ограничить размер n МБ

Если эта функция включена, то можно ограничить размер файла отчета, возможные значения: от 1 до 100 МБ. Чтобы избежать высокой загрузки системы, при ограничении файла отчета устанавливается ограничение в 50 Кб сверх нормы. Если размера файла отчета превысит указанный размер на 50 Кб, старые записи автоматически удаляются до тех пор, пока размер не станет меньше указанного на 20 % .

Защитить файл отчета от сокращения

Включив эту опцию, можно защитить файл отчета от сокращения.

Записать конфигурацию в файл отчета

Если эта опция активна, используемая конфигурация поиска в режиме реального времени записывается в файл отчета.

Примечание
Если Вы не указали ограничение для файла отчета, самые старые записи автоматически удаляются, когда файл отчета достигает размера 100 МБ. Удаляется столько записей, чтобы размер файла отчета уменьшился до 80 МБ.

11.4 Обновление

В разделе *Обновление* Вы можете настроить автоматическое выполнение обновления. У Вас есть возможность настроить различные интервалы между обновлениями, а также включить или выключить автоматическое обновление.

Автоматическое обновление

Включить

Если опция включена, выполняется автоматическое обновление с заданными временными интервалами и при наступлении выбранных событий.

Автоматическое обновление каждые n дней / часов / минут

В этом поле можно указать интервал, с которым должно выполняться автоматическое обновление. Чтобы изменить интервал обновлений, выберите одну из временных характеристик в этом поле и измените ее при помощи кнопок со стрелками, расположенными справа от поля ввода.

Запуск задачи, даже если установленное время запуска прошло:

Если эта опция включена, выполняется задача обновления, срок выполнения которой уже прошел, но которая не могла быть запущена в назначенное время, например, если компьютер был выключен.

11.4.1 Обновление продукта

В разделе **Обновление продукта** Вы можете настроить выполнение обновления продукта или уведомление о наличии обновлений продукта.

Обновление продукта

Загрузить и автоматически установить обновления продукта

Если эта функция включена, обновления продукта будут загружаться и автоматически устанавливаться компонентом Обновления по мере доступности. Обновление файла определений вирусов и поискового движка всегда осуществляется независимо от этой настройки. Условия для работы этой функции: Полная конфигурация обновлений и действующее соединение с загрузочным сервером.

Загрузить обновления продукта. Если необходима перезагрузка, то установить обновление после следующей перезагрузки системы, если нет, то немедленно.

Если эта функция включена, то при наличии обновлений будет загружаться обновление продукта. Если перезагрузка не требуется, то обновление будет автоматически установлено после загрузки файлов обновления. Если речь идет об обновлении продукта, для которого требуется перезагрузка компьютера, обновление продукта выполняется не сразу после загрузки файлов обновления, а лишь после следующей перезагрузке системы по инициативе пользователя. Преимущество заключается в том, что перезагрузка не производится в тот момент, когда пользователь работает за компьютером. Обновление файла определений вирусов и поискового движка всегда осуществляется независимо от этой настройки. Условия для работы этой функции: Полная конфигурация обновлений и действующее соединение с загрузочным сервером.

Сообщать, когда доступны новые обновления программы

Если эта функция включена, то при наличии обновлений будет только высылаться оповещение. Обновление файла определений вирусов и поискового движка всегда осуществляется независимо от этой настройки. Условия для работы этой функции: Полная конфигурация обновлений и действующее соединение с загрузочным сервером. Оповещение осуществляется в форме всплывающего окна и с помощью предупреждающего сообщения Программы обновлений в Центре контроля в обзоре ::События.

Повторное уведомление через n дней

В этом поле укажите, через сколько дней необходимо отправить повторное уведомление о наличии обновлений продукта, если после первого оповещения обновление продукта не было выполнено.

Не загружать обновления продукта

Если эта функция включена, то обновления продукта не будут загружаться автоматически, и Программа обновлений не будет выдавать сообщения об имеющихся обновлениях продукта. Обновление файла определений вирусов и поисковой машины всегда осуществляются независимо от этой настройки.

Важно
Обновление файла определений вирусов и поискового движка выполняется при каждом обновлении, независимо от настроек обновления продукта (см. гл.Обновление).

Примечание
Если Вы включили функцию автоматического обновления продукта, в разделе Установки для перезагрузки Вы можете настроить другие опции для появления сообщений и для возможностей отмены перезагрузки.

11.4.2 Настройки перезагрузки

Если выполняется обновление продукта AntiVir, может потребоваться перезапуск компьютера. Если Вы настроили автоматическое обновление продукта в разделе Общее::Обновление::Обновление продукта, Вы можете в разделе **Настройки перезапуска** выбрать различные опции для появления сообщений о перезагрузке и для возможностей отмены перезагрузки.

Примечание
В отношении установок для перезагрузки учтите, что при настройке в разделе Общее::Обновление::Обновление продукта Вы можете выбирать между двумя опциями для выполнения обновления продукта с необходимой перезагрузкой компьютера:

Автоматическое выполнение обновления продукта с необходимой перезагрузкой компьютера при наличии обновления: Обновление и перезагрузка производятся, в то время как пользователь работает за компьютером. Если Вы включили эту опцию, целесообразно выбрать программы перезагрузки с возможностью отмены или с функцией напоминания.

Выполнение обновления продукта с необходимой перезагрузкой компьютера после следующего запуска системы: Обновление и перезагрузка производятся, после того как пользователь запустил компьютер и вошел в систему. Для этой опции рекомендованы программы автоматической перезагрузки.

Настройки перезагрузки

Перезагрузка компьютера через n секунд

Если эта опция включена, **автоматически** производится перезагрузка, которая может потребоваться после выполнения обновления продукта через заданный промежуток времени. Появляется обратный счетчик без возможности отменить перезагрузку компьютера.

Напоминание о перезагрузке каждые n секунд

Если эта опция включена, перезагрузка, которая может потребоваться после выполнения обновления продукта через заданный промежуток времени **автоматически не** производится. Через заданные промежутки времени Вы получаете сообщения без возможности отмены перезагрузки. В окне сообщения Вы можете подтвердить перезагрузку компьютера или выбрать опцию "**Напомнить позже"**.

Запрос, требуется ли перезагрузка компьютера

Если эта опция включена, перезагрузка, которая может потребоваться после выполнения обновления продукта через заданный промежуток времени **автоматически не** производится. Вы получаете однократное сообщение, в окне которого Вы можете подтвердить перезагрузку или завершить программу перезагрузки.

Перезагрузка компьютера без запроса

Если эта опция включена, **автоматически** производится перезагрузка, которая может потребоваться после выполнения обновления продукта. Вы не получаете сообщение.

Обновление можно выполнить непосредственно через веб-сервер в Интернете .

Соединение с веб-сервером

Использовать имеющееся соединение (сеть)

Эта настройка отображается, если используется соединение через сеть.

Использовать следующее соединение:

Эта настройка отображается, если Вы настраиваете соединение индивидуально.

Программа обновлений автоматически определяет, какие опции соединения имеются. Несуществующие опции соединения отображаются на сером фоне, их нельзя активировать. Например, модемное соединение можно настроить вручную, внеся соответствующую запись в телефонную книгу Windows.

- **Пользователь:** Укажите здесь имя пользователя для выбранного счета.
- **Пароль:** Введите пароль для этого счета. В целях безопасности символы пароля отображаются в поле ввода звездочками (*).

Примечание
Если Вы забыли имя пользователя или пароль существующего счета, обратитесь к провайдеру.

Примечание
Автоматический вызов обновления с помощью так называемого Dial-Up Tools (например, SmartSurfer, Oleco, ...) пока не предусмотрен.

Разорвать dial-up соединение, созданное для обновления

Если эта функция включена, то открытое для обновления dial-up соединение будет автоматически прервано сразу же после успешного завершения загрузки.

Примечание
Эта опция недоступна для Vista. В Vista открытое для обновления dial-up соединение всегда автоматически разрывается сразу же после успешного завершения загрузки .

11.5 Общее

11.5.1 Категории угроз

Выбор категорий угроз

Продукт AntiVir защищает Вас от компьютерных вирусов.

Кроме того, у вас есть возможность дифференцированного поиска следующих категорий угроз.

- программы Backdoor (BDC)
- наносящие финансовый ущерб программы дозвона (DIALER)
- игры (GAMES)
- программы-шутки (JOKES)
- Риск вторжения в приватную сферу (SPR)
- Adware/Spyware (ADSPY)
- Необычные паковщики (PCK)
- Файлы со скрытым расширением (HEUR-DBLEXT)
- Фишинг
- приложение (APPL)

Щелчком по соответствующему флажку можно по желанию включить (галочка установлена) или выключить (галочка снята) выбранный тип.

Включить все

Если эта опция включена, все типы активируются.

Значения по умолчанию

Эта кнопка восстанавливает настройки по умолчанию.

Примечание
Если один из типов деактивирован, то о файлах, распознанных как соответствующий тип программы, больше не сообщается. Запись в файл отчета не выполняется.

11.5.2 Безопасность

Обновление

Предупреждать, если последнее обновление было более n дней назад

В этом поле можно указать максимальное количество дней, которое может пройти с момента последнего обновления. Если этот срок превышен, в Control Center в разделе Статус отображается красный значок для статуса обновлений.

Показывать предупреждение, если устарел файл определения вирусов

Если эта функция включена, вы получите предупреждающее сообщение, файл определений вирусов устареет. С помощью функции предупреждения можно сконфигурировать временной интервал между предупреждающими сообщениями, о том, что последнее обновление выполнялось более n дней назад.

Защита продукта

Примечание
Опция защиты продукта недоступна, если Guard не был установлен при инсталляции на выбор пользователя.

Защита процессов от нежелательного завершения

Если эта опция включена, все процессы программы будут защищены от нежелательного завершения вирусными или вредоносными программами или 'неконтролируемого' завершения пользователем, например, с помощью Диспетчера задач. Эта опция включена по умолчанию.

Расширенная защита процессов

Если эта опция включена. все процессы программы будут защищены от нежелательного завершения посредством расширенных методов. Для расширенной защиты процессов требуется значительно больше ресурсов компьютера, чем для обычной защиты процессов. Эта опция включена по умолчанию. Для деактивирования опции потребуется перезапустить компьютер.

Важно
Защита процессов недоступна в Windows XP 64 Bit !

Предупреждение
При включенной защите процессов могут возникнуть проблемы взаимодействия с другими программными продуктами. В этих случаях отключайте защиту процессов.

Защита файлов и записей реестра от обработки

При включенной опции все записи программы в реестре, а также все файлы программы (двоичные файлы и файлы настройки) защищены от обработки. Защита от обработки предполагает защиту от записи, удаления и, частично, от считывания записей в реестре или программных файлов пользователем или внешними программами. Для активирования опции потребуется перезапустить компьютер.

Предупреждение
Обратите внимание на то, что при деактивированной опции восстановление компьютеров, которые инфицированы определенными видами вредоносного ПО, может не удастся.

Примечание
Если эта опция включена, то изменения в конфигурации, а также в заданиях на проверку и обновление возможны только через интерфейс пользователя.

Важно
Защита файлов и записей реестра недоступна в Windows XP 64 Bit !

11.5.3 WMI

Поддержка для инструментария управления Windows

Инструментарий управления Windows является основополагающей технологией управления Windows, которая позволяет с помощью языков скриптов и программирования путем чтения и записи воздействовать локально и удаленно на настройки Windows. поддерживает WMI и предоставляет в интерфейсе различные данные (информация о статусе, статистические данные, отчеты, запланированные задания и т. д.), события и методы (запуск и остановка процессов). Программа AntiVir поддерживает WMI и предоставляет в распоряжение на интерфейсе данные (информацию о статусе, данные статистики, отчеты, запланированные задачи и т. д.), а также события . С помощью WMI можно вызывать оперативные данные программы.

Активировать WMI-поддержку

Если эта функция включена, вы можете вызвать оперативные данные программы через WMI.

11.5.4 Папки

Временный путь

В этом поле ввода укажите путь к папке, в которой программа держит свои временные файлы.

Настройки по умолчанию

Если эта опция включена, для обработки временных файлов системы применяются настройки системы.

Примечание
Узнать, где система сохраняет временные файлы можно (на примере Windows XP) в: Пуск | Настройка | Панель управления | Система | Вкладка "Расширенный" | Кнопка "Переменные среды". Здесь приведены соответствующие значения для временных переменных (TEMP, TMP) для зарегистрированного в данный момент пользователя, а также для системных переменных (TEMP, TMP).

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.

11.5.5 Прокси

Прокси-сервер

Не использовать прокси-сервер

Если эта опция включена, соединение с веб-сервером устанавливается не через прокси-сервер.

Использовать системные настройки Windows

Если эта опция включена, то для соединения с веб-сервером через прокси-сервер будут использоваться текущие системные настройки Windows. Вы можете сконфигурировать системные настройки Windows для использования прокси-сервера в **Панель управления:: Опции Интернета:: Соединения :: Настройки LAN**. Получить доступ к опциям Интернета можно также в Internet Explorer в меню "Дополнительно".

Предупреждение
Если вы используете прокси-сервер, который требует аутентификации, полностью укажите данные в опции *Соединение через этот прокси*. Использовать опцию *Системные настройки Windows* можно только для прокси-сервера без аутентификации.

Соединение через этот прокси-сервер

Если эта функция включена, то соединение с веб-сервером осуществляется через прокси-сервер, при этом будут использоваться указанные Вами настройки.

Адрес

Укажите имя компьютера или IP-адрес прокси-сервера, который Вы хотите использовать для подключения к веб-серверу.

Порт

Укажите номер порта прокси-сервера, который Вы хотели бы использовать для подключения к веб-серверу.

Имя пользователя

Введите имя пользователя для входа на прокси-сервер.

Логин Пароль

Введите пароль для входа на прокси-сервер. Для безопасности вводимые в это поле знаки заменяются звездочками (*).

Примеры:

Адрес:	proyx.domain.de	Порт:	8080
Адрес:	192.168.1.100	Порт:	3128

11.5.6 События

Ограничить размер банка событий

Установить максимальный размер не более n записей

Если эта функция включена, можно ограничить максимальное количество записей в банке событий, допустимы следующие значения: 100 - 10 000 записей. Если количество записей превысит указанное, самые старые записи будут удалены.

Удалять все записи через n дней

Если эта функция включена, события будут удаляться из банка событий через определенное количество дней; допустимы следующие значения: 1-90 дней. По умолчанию эта опция включена со значением 30 дней.

Не ограничивать размер банка данных (Удалять события вручную)

При включенной опции размер базы данных событий не ограничен. Однако в интерфейсе программ в разделе События отображаются не более 20 000 записей.

11.5.7 Ограничения отчетов

Ограничить количество отчетов

Ограничить количество до n шт.

Если опция включена, максимальное число отчетов ограничено определенным размером; допустимые значения находятся в интервале: от 1 до 300. Если количество отчетов превысит указанное, самые старые отчеты будут удалены.

Удалять отчеты через n дней

Если опция включена, отчеты, созданные определенное число дней назад, автоматически удаляются. 1-90 дней. По умолчанию эта опция включена со значением 30 дней.

Количество отчетов не ограничено (отчеты удаляются вручную)

Если эта опция включена, количество отчетов не ограничено.

11.5.8 Акустические сигналы

Акустический сигнал предупреждения

При обнаружении вируса или вредоносного ПО с помощью Scanner или Guard в интерактивном режиме действия раздается 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 в разделе Scanner::Поиск::Действия при обнаружении.

Нет предупреждения

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

Воспроизводить через громкоговоритель компьютера (только при интерактивном режиме)

При включенной опции подается акустический сигнал со стандартным звуковым предупреждением при обнаружении вируса с помощью Scanner или Guard. Предупреждающий сигнал воспроизводится внутренним громкоговорителем компьютера.

Использовать следующие Wave-файлы (только при интерактивном режиме)

При включенной опции при обнаружении вируса Scanner или Guard подается акустический сигнал с помощью выбранного Wave-файла. 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 звуковой сигнал задан по умолчанию.

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

Тест

Эта кнопка предназначена для тестового запуска выбранного Wave-файла.

11.5.9 Предупреждения

При наступлении определенных событий программа AntiVir создает уведомления в виде всплывающего окна, так называемые выскальзывающие окошки, чтобы проинформировать вас об угрозе, а также об успешно выполненных или не удавшихся процессах, например, о выполнении обновления. В разделе *Предупреждения* Вы можете включить или отключить уведомление при наступлении определенных событий.

Для уведомлений в виде всплывающего окна есть возможность отключить уведомление непосредственно в выскальзывающем окошке. Вы можете отменить отключение уведомлений в разделе *Предупреждения*.

Предупреждения

через используемые Dial-up соединения

Если эта функция активирована, уведомления в виде всплывающего окна будут предупреждать Вас, когда программа дозвона на Вашем компьютере устанавливает селекторную связь по телефонной сети или сети ISDN. Существует опасность того, что программа дозвона представляет собой неизвестный и нежелательный диалер, который устанавливает платное соединение. (см. Вирусы и другое::Дополнительные категории угроз: Диалеры).

через успешно обновленные файлы

Если эта опция включена, Вы получаете уведомление в виде всплывающего окна в случае успешного завершения обновления и обновления файлов.

через неудачное обновление

При включенной опции Вы получаете уведомление в виде всплывающего окна, если обновление не удалось: Не удалось установить связь с сервером загрузки или не удалось установить файлы обновлений.

что обновление не требуется

Если эта опция включена, Вы получаете уведомление в виде всплывающего окна, когда обновление было запущено, однако установка файлов не потребовалась, так как Ваша программа имеет самую современную версию.

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Телефон: +49 7542-500 0
Факс: +49 7542-500 3000
Интернет: http://www.avira.ru