Avira AntiVir Professional

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 Professional 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 Professional 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.avira.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
- Компонент ProActiv для постоянного контроля за действиями программ (только для 32-битных систем, недоступно в Windows 2000)
- MailGuard (сканер POP3, сканер IMAP и сканер SMTP) для постоянной проверки ваших писем на содержание вирусов и вредоносных программ. Включая проверку почтовых вложений
- 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 или внутренней сети
- Удобная система управления лицензиями
- 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)
- Avira FireWall — для защиты компьютера от неразрешенного доступа из Интернета или сети, а также от неразрешенного доступа к Интернету/сети неавторизованных пользователей.

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)

3.3 Лицензирование и обновление

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

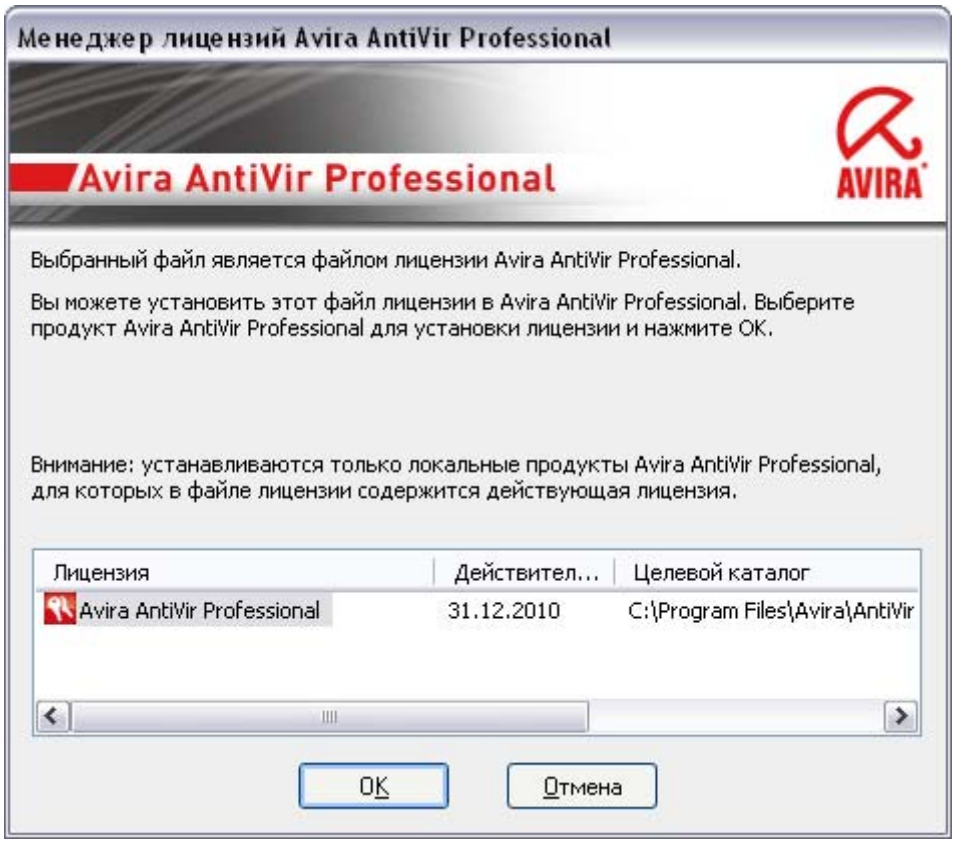
Лицензия предоставляется посредством цифрового ключа в виде файла hbedv.key. Этот цифровой лицензионный ключ является диспетчером Вашей персональной лицензии. Ключ содержит точные данные о том, какие программы и на какой срок были Вами лицензированы. Цифровой лицензионный ключ может содержать лицензии для нескольких продуктов.

Цифровой ключ лицензии высылается электронной почтой, если программа AntiVir куплена через Интернет, или находится на CD/DVD-диске с программой. Файл лицензии можно загрузить во время установки программы или после нее — через Менеджер лицензий.

3.3.1 Управление лицензиями

Менеджер лицензий Avira AntiVir Professional позволяет легко установить лицензии на использование Avira AntiVir Professional.

Менеджер лицензий Avira AntiVir Professional



Вы можете произвести установку лицензии, выбрав файл лицензии в файловом менеджере или выбрав двойным щелчком файл лицензии в письме активации и следуя далее экранным подсказкам.

Примечание
Менеджер лицензий Avira AntiVir Professional автоматически копирует соответствующую лицензию в соответствующую папку. Если лицензия уже есть, отображается информация о том, может ли файл лицензии быть заменен на новый. В этом случае новый файл лицензии будет записан поверх уже существующего.

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
- Установка и удаление в сети
- 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

- Устанавливаются не все доступные компоненты программы. Не устанавливаются следующие компоненты:

  Avira AntiVir ProActiv

  Avira FireWall

- 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)
- Обновление по завершении установки выполняется при необходимости
- Сохраните файл лицензии hbedv.key на локальном диске вашего компьютера, если вы хотите активировать программу AntiVir.

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.

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:

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

- 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 Professional*.

- 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 *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**.

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**.

→ Если для установки выбран компонент ProActiv, появится диалоговое окно *AntiVir ProActiv Community*. Вы можете подтвердить свое участие в AntiVir ProActiv Community: при активированной опции Avira AntiVir ProActiv

пересылает данные подозрительных программ, о которых сообщил компонент ProActiv, в Avira Malware Research Center. Данные используются только для расширенной онлайн-проверки и для расширения и усовершенствования технологии распознавания. Через ссылку **Дополнительная информация** вы можете запросить подробности для онлайн-проверки.

- Активируйте или деактивируйте участие в AntiVir ProActiv Community и подтвердите, нажав **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

→ Возникает окно *Установить файл лицензии*:

- Выберите папку, в которой Вы сохранили файл лицензии, обратите внимание на Примечание в диалоговом окне, нажмите **Далее**.

→ Копируется файл лицензии, устанавливаются и запускаются компоненты.

→ 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 для установки был выбран модуль Avira FireWall, появится диалоговое окно *Уровень безопасности FireWall*. Здесь можно установить, будет ли разрешать Avira FireWall внешний доступ к таким открытым ресурсам, как сетевой доступ приложений высоконадежных поставщиков.

- Активируйте необходимые опции, нажмите *Далее*.

→ 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 следующем диалоговом окне *Выбор настроек электронной почты* вы можете настроить сервер для отправки электронных писем. Программа AntiVir использует отправку электронной почты через SMTP при отправке уведомлений электронной почты.

- Сделайте необходимые настройки и 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.

4.3 Установочный модуль

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

- **AntiVir Professional**
  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 ProActiv**
  Компонент ProActiv контролирует операции приложений и сообщает о подозрительном поведении приложений. Это основанное на поведении распознавание позволяет защищаться от неизвестных вредоносных программ. Компонент ProActiv встроен в модуль AntiVir Guard.
- **AntiVir MailGuard**
  MailGuard является интерфейсом между вашим компьютером и почтовым сервером, с которого Ваша почтовая программа (почтовый клиент) загружает письма. MailGuard является так называемым прокси между почтовой программой и почтовым сервером. Все входящие письма перенаправляются через этот Proxy, проверяются на наличие вирусов и вредоносных программ, а затем пересылаются на Вашу почту. Программа автоматически обрабатывает инфицированные письма и запрашивает пользователя о необходимых действиях.
- **AntiVir WebGuard**
  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.
- **Avira FireWall**
  Avira FireWall контролирует входящий и исходящий трафик. Он разрешает или запрещает соединение, основываясь на правилах безопасности.

- *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**.

→ Появится запрос, следует ли снова активировать брандмауэр Windows (так как Avira FireWall деактивирован).

- ▶ 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.

4.5 Установка и удаление в сети

Чтобы упростить системному администратору установку программы AntiVir в сети с большим количеством клиентских машин, AntiVir предлагает специальную технологию для первоначальной установки программы и ее последующих изменений.

Автоматическую установку обеспечивает Установщик с управляющим файлом setup.inf. Установщик (presetup.exe) содержится в установочном пакете программы. Установка запускается скриптом или Batch-файлом и получает всю необходимую информацию из управляющего файла. Команды в скрипте заменяют при этом обычные действия пользователя, производимые вручную.

Примечание
Помните, что для первичной установки в сети обязательно наличие файла лицензии.

Примечание
Обратите внимание на то, что для установки по сети вам потребуется установочный пакет программы AntiVir. Установочный файл для установки через интернет не обязателен.

Легко распределить программу AntiVir по сети можно с помощью логин-скрипта сервера или через SMC.

Здесь содержится информация по установке и удалению в сети:

- см. раздел: Параметры командной строки для установщика
- см. раздел: Аргумент файла setup.inf
- см. раздел: Установка в сети
- см. раздел: Удаление продуктов из сети

Примечание
Еще одну удобную возможность установки и удаления AntiVir в сети предлагает AntiVir Security Management Center. AntiVir Security Management Center используется для удаленной установки и обслуживания программ AntiVir в сети. Дополнительную информацию вы можете найти на нашем веб-сайте:
http://www.avira.ru

4.5.1 Установка в сети

Установка может быть выполнена с помощью скрипта в Batch-режиме.

Это подходит для следующих типов установки:

- Первичная установка через сеть (необслуживаемая установка)
- Установка персональных компьютеров

▶ Установка изменений или обновление

Примечание
Мы рекомендуем протестировать автоматическую установку, прежде чем выполнять установочную процедуру в сети.

Автоматически установить программу AntiVir в сети можно следующим образом:

✓ Требуются права администратора (в т.ч. и в Batch-режиме)

- ▶ Настройте параметры файла *setup.inf* и сохраните файл.
- ▶ Запустите установку с параметром /inf или добавьте параметр в логин-скрипт сервера.
  - Примеры: `presetup.exe /inf="c:\temp\setup.inf"`

→ Установка производится автоматически.

4.5.2 Удаление продуктов из сети

Автоматически удалить из сети программу AntiVir можно следующим образом:

✓ Требуются права администратора (в т.ч. и в Batch-режиме)

- ▶ Запустите деинсталляцию с параметром `/remsilent` или `/remsilentaskreboot` или добавьте параметр в логин-скрипт сервера.

  Дополнительно можно указать аргумент для протоколирования процесса удаления.
  - Примеры: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

→ Удаление происходит автоматически.

Примечание
Не запускайте Установщик для деинсталляции на открытом сетевом диске, его следует выполнять на локальном компьютере, на котором должна быть удалена программа AntiVir.

4.5.3 Параметры командной строки для установщика

Все пути или файлы должны быть взяты в кавычки.

Возможные параметры для установки:

- `/inf`

  Программа установки запускается с указанным скриптом и получает из него все необходимые параметры.

  Пример: `presetup.exe /inf="c:\temp\setup.inf"`

Возможные параметры для удаления:

- `/remove`

  Установщик удаляет программу AntiVir.

  Пример: `presetup.exe /remove`

- `/remsilent`

  Установщик удаляет программу AntiVir, не отображая при этом диалоговых окон. После установки компьютер будет перезагружен.

  Пример: `presetup.exe /remsilent`

– /remsilentaskreboot

Установщик удаляет программу AntiVir, не показывая диалоговые окна, и после деинсталляции выдает запрос на перезагрузку компьютера.

Пример: presetup.exe /remsilentaskreboot

Для протоколирования удаления возможен следующий параметр:

– /unsetuplog

Фиксируются все действия при удалении.

Пример: presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"

4.5.4 Аргумент файла setup.inf

В управляющем файле setup.inf в разделе [DATA] вы можете установить следующие параметры для автоматической установки программы AntiVir. Последовательность параметров значения не имеет. Если не указан или неверно указан аргумент, процедура установки прекращается с сообщением об ошибке.

– DestinationPath

Папка, в которую устанавливается программа. Он должен быть указан в скрипте. Помните, что программа установки автоматически прикрепляет название компании и продукта. Могут использоваться переменные среды.

Пример: DestinationPath=%PROGRAMFILES% возвращает, например, установочный путь C:\Programme\Avira\AntiVir Desktop

– ProgramGroup

Создает в меню Пуск Windows группу программ для всех пользователей.

1: Создать группу программ

0: Не создавать группу программ

Пример: ProgramGroup=1

– DesktopIcon

Создает на рабочем столе ярлык для всех пользователей.

1: Создать ярлык на рабочем столе

0: Не создавать ярлык

Пример: DesktopIcon=1

– ShellExtension

Регистрирует в реестре расширение оболочки. Расширение оболочки позволит Вам проверять файлы и папки из контекстного меню, вызываемого правой кнопкой мыши.

1: Зарегистрировать Shell-Extension

0: Не регистрировать Shell-Extension

Пример: ShellExtension=1

– Guard

Устанавливает AntiVir Guard (антивирусный монитор).

1: Установить AntiVir Guard

0: Не устанавливать AntiVir Guard

Пример: Guard=1

– MailScanner

Устанавливает модуль AntiVir MailGuard.

1: Установить модуль AntiVir MailGuard

0: Не устанавливать AntiVir MailGuard

Пример: MailScanner=1

– KeyFile

Указывает путь к файлу лицензии, который копируется при установке. При первой установке: срочно требуется. Имя файла необходимо указывать полностью. (при установке изменений: опционально.)

Пример: KeyFile=D:\inst\license\hbedv.key

– ShowReadMe

Отображает после установки файл readme.txt

1: Показать файл

0: Не показывать файл

Пример: ShowReadMe=1

– RestartWindows

Перезапускает компьютер после установки. Эта строка имеет более высокий приоритет как ShowRestartMessage.

1: Перезагрузить компьютер

0: Не перезагружать компьютер

Пример: RestartWindows=1

– ShowRestartMessage

Отображает информацию перед автоматической перезагрузкой в процессе установки

0: Не отображать информацию

1: Отображать информацию

Пример: ShowRestartMessage=1

– SetupMode

Не требуется при первой установке. Программа установки распознает, выполнена ли установка в первый раз. Определяет вид установки. Если продукт уже установлен, необходимо выбрать режим установки: обновление, модификация или удаление.

Обновление: Выполняет обновление имеющейся установки. При этом параметры настройки, такие как Guard, пропускаются.

Модификация: Выполняет модификацию существующей установки. При этом в целевую папку не копируются файлы.
Remove: Удаляет программу AntiVir из системы.

Пример: SetupMode=Обновление

– AVWinIni (опционально)

Указывает целевую папку файла настроек, который можно скопировать при установке. Имя файла необходимо указывать полностью.

Пример: AVWinIni=d:\inst\config\avwin.ini

– Password

Эта опция передает процедуре установки пароль, требуемый для установки или удаления программы. Строка проверяется процедурой установки только после указания пароля. Если пароль был определен, но не был указан в виде параметра или был указан неверно, процедура установки будет прервана.

Пример: Password=Password123

– WebGuard

Устанавливает модуль AntiVir WebGuard.

1: Установить модуль AntiVir WebGuard

0: Не устанавливать AntiVir WebGuard

Пример: WebGuard=1

– Руткит

Устанавливает модуль AntiVir для защиты от руткит-программ Без модуля AntiVir для защиты от руткит-прогрмм сканер не сможет искать руткит-программы в системе!

1: Установить модуль AntiVir для защиты от руткит-программ

0: Не устанавливать модуль AntiVir для защиты от руткит-программ

Пример: RootKit=1

– HIPS</1

Устанавливает компонент AntiVir ProActiv. AntiVir ProActiv – это построенная на ролях технология распознавания, с помощью которой распознается еще неизвестное вредоносное ПО.

1: Установить ProActiv

0: Не устанавливать ProActiv

Пример: HIPS=1

– Брандмауэр

Устанавливает брандмауэр Avira FireWall. Avira FireWall контролирует и управляет входящим и исходящим трафиком на Вашем компьютере и защищает компьютер от большого количества угроз из интернета и прочего сетевого окружения.

1: Установить брандмауэр

0: Не устанавливать брандмауэр

Пример: Firewall=1

5 Обзор

главы содержится обзор функций и управления программы AntiVir.

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

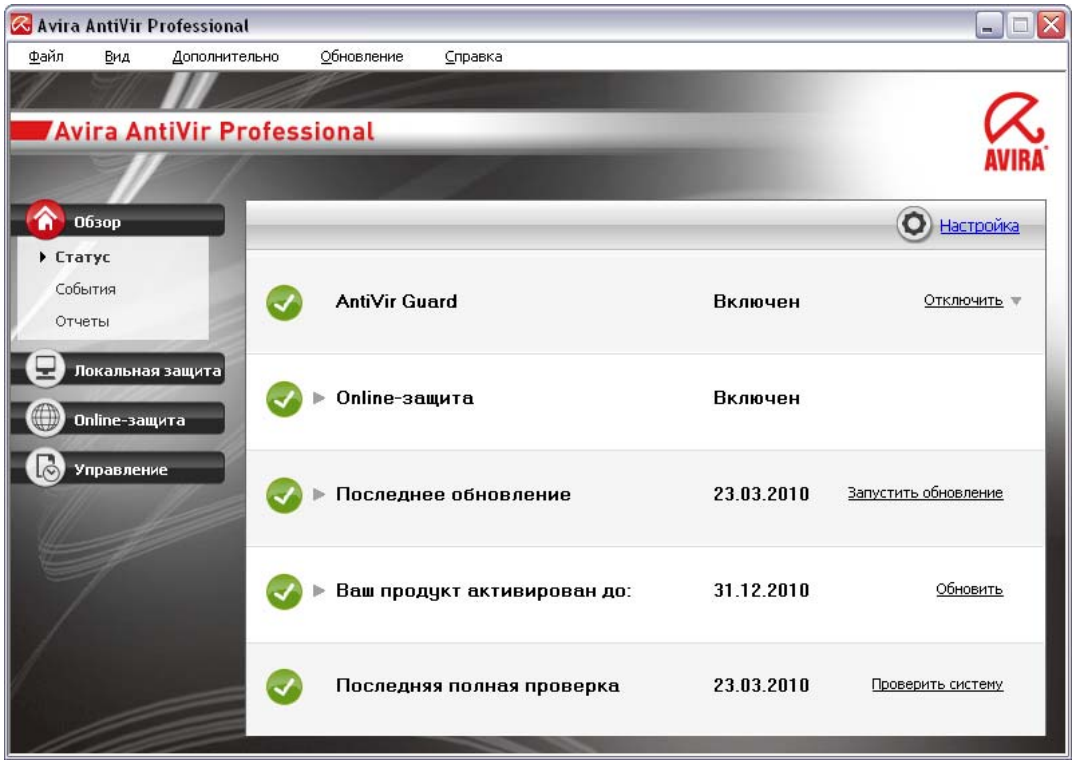
5.1 Интерфейс и работа с программой

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.

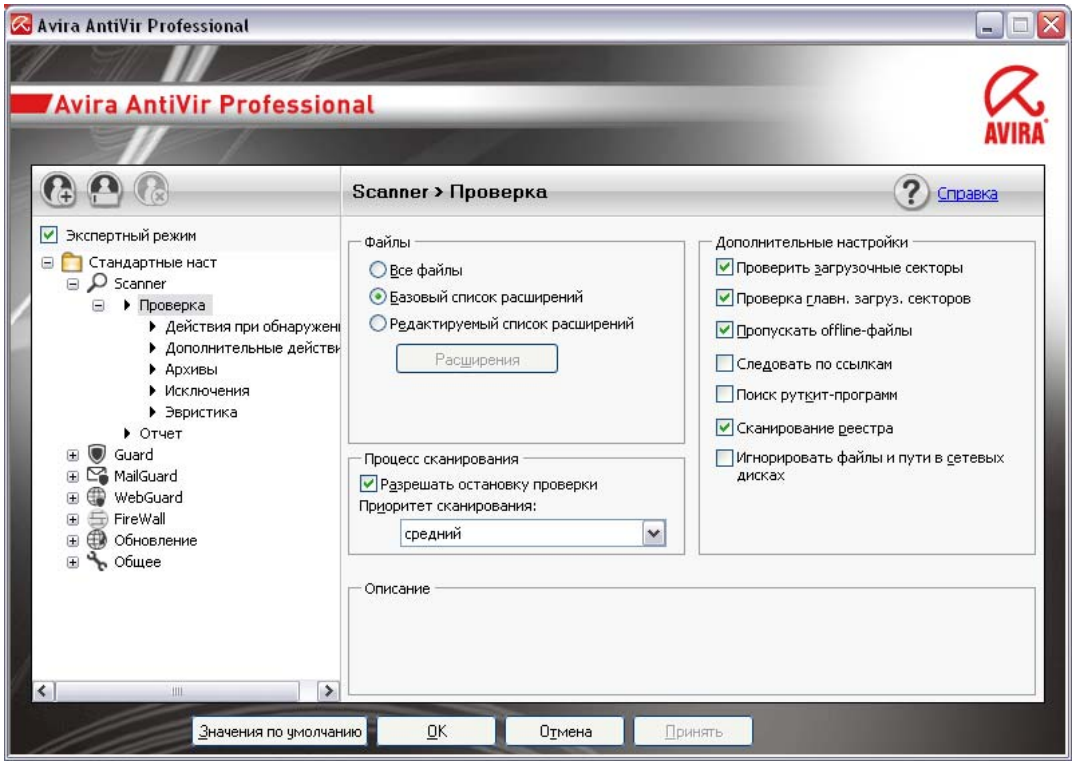
▶ Щелкните по кнопке в верхней части основного окна, чтобы обработать объект.

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) или путем создания пользовательского профиля, 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.
- Во вкладке MailGuard показываются проверенные модулем MailGuard письма, их свойства и прочие статические данные.
- 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".
- В разделе FireWall можно изменять основные настройки Avira FireWall. Отображается также скорость передачи данных и все активные приложения, использующие сетевые соединения.
- **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.

Профили настройки

Вы можете сохранить свои настройки в профиле настройки. В профиле настройки сохраняются все опции, относящиеся к одной группе. Настройки отображаются в строке меню в виде дерева каталогов. Вы можете добавить свои настройки к стандартным. Существует возможность определения правил для переключения на определенную настройку:
При таком переключении настройки могут быть сопряжены с соединением LAN или интернет-соединением (идентификация через стандартный межсетевой шлюз): Вы можете, например, установить профили настроек для различных сценариев использования ноутбука:

- Использование в сети организации: Обновление через сервер Intranet, WebGuard деактивирован
- Использование дома: Активировано обновление через стандартный веб-сервер компании Avira GmbH, WebGuard активирован

Если правила переключения не определены, переключиться на настройку можно вручную в контекстном меню Tray Icons. С помощью кнопок строки меню или при помощи команды из контекстного меню разделов настроек Вы можете добавлять, переименовывать, удалять, копировать, отменять настройки и определять правила для переключения на определенные настройки.

Примечание
В Windows 2000 автоматическое переключение настроек не поддерживается. В Windows 2000 невозможно определить правила для переключения настроек.

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

- **MailGuard**: Настройка модуля MailGuard

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

  Действия при обнаружении вредоносной программы

  Эвристика проверки модулем MailGuard

Исключения из проверки модулем MailGuard

Настройка буфера памяти, очистка буфера

Настройка строки примечания в отправленных письмах

Настройка отчетов

– **WebGuard**: Настройка модуля WebGuard

Опции проверки, активация и деактивация модуля WebGuard

Действия при обнаружении вируса

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

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

Эвристика модуля WebGuard

Настройка отчетов

– **FireWall**: Настройки FireWall

Добавление правила адаптера

Добавление индивидуальных правил адаптера

Список надежных производителей (исключения при доступе приложений к сети)

Расширенные настройки: Период для правил, блокировка хост-файла Windows, остановка брандмауэра Windows, уведомления

Настройка всплывающих окон (уведомления при доступе приложений к сети)

– **Общее**:

Настройка отправки писем через SMTP

Расширенные категории угроз для проверки и постоянной защиты

Защита паролем доступа к центру управления и настройкам

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, загрузка с веб-сервера или сервера файлов, настройка обновления программы

Уведомления: Настройка уведомлений компонентов по электронной почте:
Сканер
Guard
Программа обновлений
Настройка сетевых предупреждений компонента (компонентов) Сканер, Guard

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 и FireWall активированы
	AntiVir Guard или FireWall деактивирован

Значок в трее показывает статус служб Guard и FireWall .

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 MailGuard**: Включает или отключает AntiVir MailGuard.
- **Активация AntiVir WebGuard**: Включает или отключает AntiVir WebGuard.
- **FireWall**:
- Активация FireWall: Включает или отключает FireWall
- Блокировка всего трафика: Включено: Блокирует любые передачи данных за исключением передачи собственной компьютерной системе (Local Host / IP 127.0.0.1).
- Активация игрового режима: Включает или отключает режим: Активирован: Применяются все установленные правила адаптера и приложений. Приложениям, для которых не определены правила, разрешены сетевые взаимодействия, при этом не появляются всплывающие окна.
- **Запуск AntiVir**: Открывает Центр управления.
- **Настройка AntiVir**: Открывает Настройки.
- **Запуск обновления**: Запускает Обновление.
- **Установить настройки**: Открывает подменю с доступными профилями конфигурации. Щелкните по конфигурации, чтобы активировать ее. Команда меню деактивирована, если вы уже определили правила для автоматического переключения на конфигурацию.
- **Справка**: Открывает справочную онлайн-систему.
- **О программе AntiVir Professional:** 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 Это делается так

5.2.1 Активировать лицензию

Лицензия программы AntiVir активируется следующим образом:

Активируйте лицензию программы AntiVir с помощью файла лицензии hbedv.key. Получите файл лицензии по электронной почте. В файле лицензии содержится лицензия для всей заказанной Вами продукции.

Если вы еще не установили программу AntiVir:

- Сохраните файл лицензии в папке на локальном диске Вашего компьютера.
- Установите программу AntiVir.
- При установке укажите путь к файлу лицензии.

Если вы уже установили программу AntiVir:

- Сделайте двойной щелчок в файловом менеджере или в письме активации по файлу лицензии и следуйте указаниям в открывшемся окне управления лицензиями.

  - ИЛИ -

- В Центре управления программы AntiVir выберите пункт меню Справка / Загрузить файл лицензии....

Примечание
В ОС Windows Vista появится окно диалога Управление учетными записями пользователей. Войдите в систему как администратор. Нажмите **Продолжить**.

- Выберите файл лицензии и нажмите **Открыть**.

→ Появится сообщение.

- Подтвердите кнопкой **OK**.

→ Лицензия активирована.

- Перезапустите систему.

5.2.2 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**
  - – **Логин**

Примечание
Мы рекомендуем выполнять регулярное и частое автоматическое обновление. Рекомендованный промежуток между обновлениями: 60 .

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

    Помимо выполнения задач с установленной частотой осуществляется дополнительный запуск задач при каждом установленном интернет-соединении.
  - – **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

5.2.3 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: 60 .

Примечание
Вы можете выполнить обновление вручную через Центр безопасности Windows.

5.2.4 Проверка: Искать с помощью профиля поиска вирусы и вредоносное ПО

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

Существует несколько способов проведения проверки через профиль поиска:

- Использовать предустановленный профиль поиска

Если предустановленные профили соответствуют Вашим требованиям.

- Адаптация и использование профиля поиска (выбор вручную)

Создать индивидуальный профиль поиска.

- Создание и использование нового профиля поиска

Если Вы хотите создать собственный профиль поиска.

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

– Windows XP и 2000:

 С помощью этого символа запускается проверка через профиль поиска.

– Windows Vista:

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

- ИЛИ -

▶ Создайте новый профиль поиска.

▶ 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 и папки , которые необходимо проверить.

– Нажмите на значок **+**: Отобразится следующий уровень каталогов.

– Нажмите на значок **-**: Следующий уровень каталогов будет скрыт.

▶ Отметьте узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле необходимого уровня каталогов.

Существует несколько способов выбора папок:

– Каталог с подкаталогами (черный флажок)

– Каталог без подкаталогов (зеленый флажок)

- Только подкаталоги в каталоге (серый флажок, у подкаталогов флажок черный)
- Не выделять (галочка отсутствует)

Если Вы хотите создать новый профиль поиска.

- ▶ Нажмите пиктограмму **Создать новый профиль.**
- → Среди имеющихся профилей появится новый *Новый профиль*.
- ▶ При необходимости переименуйте профиль поиска, нажав пиктограмму .
- ▶ Отметьте узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле.

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

5.2.5 Проверка: Поиск вирусов и вредоносного ПО посредством перетаскивания

Целенаправленный поиск вирусов и вредоносного ПО с помощью перетаскивания:

- ✓ Центр управления программы AntiVir открыт.
- ▶ Выделите файл или папку, который/которую необходимо проверить.
- ▶ Перетяните левой кнопкой мышки выделенный файл или выделенный каталог на *центр управления*.
- → Появится окно *Luke Filewalker* и запустится прямой поиск.
- → По окончании проверки будут показаны результаты.

5.2.6 Проверка: Искать с помощью контекстного меню вирусы и вредоносное ПО

Искать с помощью контекстного меню вирусы и вредоносное ПО:

- ▶ Щелкните правой кнопкой мыши (например, в проводнике Windows, на рабочем столе иил в открытой папке Windows) по файлу или папке, который/которую Вы хотите проверить.
- → Появится контекстное меню проводника Windows.
- ▶ В контекстном меню выберите **Проверить выбранные файлы с помощью AntiVir**.
- → Появится окно *Luke Filewalker* и запустится прямой поиск.
- → По окончании проверки будут показаны результаты.

5.2.7 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**
  - **Логин**
- 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

5.2.8 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.

5.2.9 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 ProActiv не существует настраиваемых опций действия. Об обнаружении всегда сообщается в окне *Guard: Обнаружено подозрительное поведение приложения*.

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. При активации опции *Показывать предупреждение* при обнаружении вируса Вы будете получать предупреждение, в котором будет показано выполненное действие.

Доступные действия для Guard ::

– **Интерактивный**

В интерактивном режиме блокируется доступ к данным и показывается уведомление на рабочем столе. 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):

– **Автоматический**

В автоматическом режиме при обнаружении вируса или вредоносной программы автоматически выполняется действие, которое Вы выбрали в этой области. Если активирована опция *Показывать предупреждение*, при обнаружении вируса вы получите уведомление на рабочем столе.

Доступные действия для MailGuard, 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. При активации опции *Показывать предупреждение* при обнаружении вируса Вы будете получать предупреждение, в котором можно будет подтвердить выполняемое действие.

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 MailGuard, AntiVir WebGuard), который сообщает о найденном объекте, и от вредоносной программы.

Действия сканера и модуля Guard (без обнаружения модулем ProActiv):

- **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. Этот процесс значительно быстрее, чем *переписать и удалить*. При обнаружении установочного вируса удаляется загрузочный сектор. Записывается новый загрузочный сектор.

- **Переписать и удалить**

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

- **Переименовать**

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

- **Пропустить**

  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 Guard при обнаружении компонентом ProActiv (сообщение о подозрительных действиях приложения):

– **Высоконадежный поставщик**

Выполнение программы продолжается. Программа добавляется в список разрешенных приложений и больше не проверяется компонентом ProActiv. При добавлении в список разрешенных программ устанавливается тип контроля *Содержимое*. Это означает, что программа не будет проверяться компонентом ProActiv только при неизменном содержимом (см. Настройки::Guard::ProActiv::фильтр приложения: Разрешенные приложения).

– **Единожды блокировать программу**

Программа блокируется, т.е. выполнение приложения завершается. Компонент ProActiv продолжает контролировать действия программы.

– **Всегда блокировать эту программу**

Программа блокируется, т.е. выполнение приложения завершается. Программа добавляется в список блокируемых приложений и больше не будет выполняться (см. Настройки::Guard::ProActiv::фильтр приложения: Блокируемые приложения).

– **Пропустить**

Выполнение программы продолжается. Компонент ProActiv продолжает контролировать действия программы.

Действия модуля MailGuard: Входящие письма

– **Поместить на карантин**

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

– **Удалить**

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

– **Удалить приложение**

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

– **Поместить приложение на карантин**

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

– **Пропустить**

Инфицированное письмо доставляется адресату.

Предупреждение
Таким образом в Вашу систему могут проникнуть вирусы и вредоносные программы. Выбирайте опцию **Пропустить** в исключительных случаях. Выключите предварительный просмотр в Microsoft Outlook, не запускайте приложения двойным щелчком!

Действия модуля MailGuard: Исходящие письма

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

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

- **Блокировать почту (не отправлять)**

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

- **Пропустить**

  Инфицированное письмо будет отправлено.

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

Действия 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.

Примечание
Отправьте нам для проверки файлы, отмеченные эвристикой.
Вы можете загрузить их на наш вэб-сервер:http://www.avira.ru/file-upload
Файлы, о которых сообщает эвристический модуль, можно узнать по обозначению *HEUR/* или *HEURISTIC/*, которое ставится перед названием файла, например: *HEUR/тестовый_файл.**.

5.2.10 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.
Подозрительный файл: Вы определили файл как подозрительный и поэтому поместили его на карантин, однако проверка файла на вирусы говорит об обратном.
Ложное срабатывание: Вы исходите из того, что обнаружение вируса является ложным срабатыванием: Программа AntiVir сообщает об обнаружении вируса в файле, который, однако, с высокой вероятностью не инфицирован.

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

Примечание
Вы можете одновременно отправить несколько файлов, выделив их и нажав кнопку **Отправить объект**.

Для копирования объекта из карантина в другой каталог:

▶ Выделите объект карантина и нажмите  .

→ Откроется ассистент окно обзора, где Вы можете выбрать нужную папку.

▶ Выберите папку, в которую необходимо скопировать объект карантина и подтвердите выбор.

→ Выбранный объект карантина будет сохранен в указанном каталоге.

Примечание
Объект карантина не идентичен восстановленному файлу. Объект карантина зашифрован и не может быть выполнен или считан в первоначальном формате.

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

5.2.11 Карантин: Восстановление файлов в карантине

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

– Windows XP и 2000:

 С помощью этого 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.

5.2.12 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

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

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

✓ 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 ?) .

5.2.14 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.

5.2.15 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
- MailGuard
- Сканер
- Планировщик
- FireWall
- WebGuard
- Временная служба
- ProActiv

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.

5.2.16 MailGuard: Исключить адреса из проверки

Настройка исключения адресов электронной почты (отправители) из проверки модулем MailGuard (так называемый "белый список"):

- В центре управления нажмите во вкладке **Онлайн-защита :: MailGuard**.

→ В списке Вы увидите входящие письма.

- Отметьте письма, которые Вы хотите исключить из проверки модулем MailGuard.
- Нажмите на нужную пиктограмму для того, чтобы исключить адрес из проверки модулем MailGuard.

 Выделенный адрес электронной почты в дальнейшем не будет проверяться на наличие вирусов и вредоносных программ.

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

Предупреждение
Рекомендуется исключать из проверки модулем MailGuard только абсолютно надежных отправителей.

Примечание
В настройках в MailGuard :: Общее :: Исключения Можно добавлять адреса в список исключений или удалять из него.

5.2.17 FireWall: Выбор уровня безопасности в FireWall

Можно выбрать разные уровни безопасности. В зависимости от этого у Вас появятся различные возможности конфигурации для правил адаптера.

Доступны следующие уровни безопасности:

- **Низкий**
- Распознается сканирование портов и флудинг.
- **Средний**
- Запрещаются подозрительные TCP- и UDP-пакеты.
- Предотвращается сканирование портов и флудинг.
- **Высокий**
- Компьютер невидим в сети.
- Блокируются соединения из вне.

- Предотвращается сканирование портов и флудинг.
- **Пользователь**
- Правила, установленные пользователем: Программа автоматически переключается на этот режим, если Вы изменили правила адаптера.

Примечание
Стандартная настройка уровня безопасности для всех предустановленных правил Avira FireWall - **Высокий**.

Уровень безопасности FireWall выбирается следующим образом:

- ▶ В центре управления нажмите во вкладке **Онлайн-защита :: FireWall**.
- ▶ Установите ползунковый регулятор на необходимый уровень безопасности.

→ Уровень безопасности становится активным.

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: 60 . 60 . 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

Обновления Вы получаете из интернета по веб-серверу изготовителя или по веб-серверу или серверу файлов в сети Intranet, который загружает файлы обновления из интернета и предоставляет их другим компьютерам в сети. Это имеет смысл, если Вы хотите обновить программу AntiVir на нескольких компьютерах в сети. Благодаря наличию сервера загрузки в сети Intranet обеспечивается актуальность программы AntiVTIFY_ONLY ir на защищаемых компьютерах при небольшом потреблении ресурсов. Для создания работоспособного сервера загрузки в сети Intranet необходим сервер, обеспечивающий структуру обновления программы AntiVir .

Примечание
В качестве веб-сервера или сервера файлов в сети Intranet можно использовать AntiVir Internet Update Manager (сервер файлов или веб-сервер в ОС Windows). AntiVir Internet Update Manager отражает сервер загрузки продуктов Avira AntiVir и может быть приобретен через Интернет на веб-сайте Avira.
http://www.avira.ru

При использовании Веб-сервера применяется HTTP-протокол. При использовании сервера файлов доступ к файлам обновления осуществляется по сети. Параметры соединения с веб-сервером или сервером данных можно изменить в настройках Общее :: Обновление. В стандартной конфигурации используется существующее интернет-соединение с веб-серверами Avira GmbH.

8 Avira FireWall :: Обзор

Avira FireWall контролирует и управляет входящим и исходящим трафиком на Вашем компьютере и защищает от большого количества атак и интернет-угроз: На основании правил безопасности разрешается или запрещается входящий и исходящий обмен данными или прослушивание порта. На рабочем столе появляется уведомление, когда Avira FireWall отклоняет сетевую активность и блокирует таким образом сетевые соединения. Существует несколько вариантов настройки Avira FireWall:

- с помощью настройки уровня безопасности в центре управления

  В Центре управления можно настраивать уровень безопасности. Каждый уровень безопасности — *Низкий*, *Средний* и *Высокий* — содержит несколько дополняющих друг друга правил безопасности, основанных на фильтрах пакетов. Эти правила безопасности являются предустановленными правилами адаптера в настройках в FireWall::Правила адаптера.

- сохранением действий в окне Сетевое событие

  Если приложение будет устанавливать сетевое или Интернет-соединение, то появится всплывающее окно *Сетевое событие*. В окне *Сетевое событие* пользователь может выбрать, разрешить сетевую активность приложению или запретить. Если активирована опция **Сохранить действие для этого приложения**, в качестве правила приложения создается действие и сохраняется в конфигурации в FireWall::Правила приложений. При сохранении действий в окне Сетевое событие у Вас появится набор правил для сетевой активности приложений.

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

- путем создания правил адаптера и приложений в настройках

  В меню настроек можно изменять или создавать новые правила адаптера. При добавлении или изменении правил адаптера уровень безопасности FireWall автоматически устанавливается на значение *Пользователь*.
  С помощью правил приложения Вы можете определить правила мониторинга, рассчитанные для приложений:
  С помощью простых правил приложений можно установить, запретить или разрешить сетевую активность приложения или управлять ею интерактивно из всплывающего окна *Сетевое событие*.
  В расширенной конфигурации раздела *Правила приложения* Вы можете определить различные фильтры пакетов для приложения, которые определены специально для правил приложения.

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

9 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

9.1 Помощь в случае возникновения проблем

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

- Появляется уведомление об ошибке *открытия файла лицензии*.
- AntiVir MailGuard не работает.
- В виртуальных машинах сетевое соединение недоступно, если Avira FireWall установлен в главной операционной системе и уровень безопасности Avira FireWall установлен на средний или высокий.
- Блокируется соединение Virtual Private Network (VPN), если уровень безопасности Avira FireWall установлен на средний или высокий.
- Письмо, отправленное по соединению TSL, было заблокировано модулем MailGuard.
- Не работает чат: не отображаются сообщения пользователей чата

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

Причина: файл зашифрован.

▶ Для активации лицензии не следует открывать файл. Достаточно сохранить его в папке программы. См. также Менеджер лицензий.

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. Тоже самое касается AntiVir MailGuard.

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 и AntiVir MailGuard осуществляется по протоколу интернета TCP/IP. Брандмауэр отслеживает все соединения, производящиеся по этому протоколу.

▶ Установите полное разрешение для AntiVir Guard и AntiVir MailGuard. Модуль AntiVir Guard работает исключительно с адресом 127.0.0.1 (localhost). Не устанавливается соединение с интернетом. Тоже самое касается AntiVir MailGuard.

AntiVir MailGuard не работает.

Проверьте работоспособность AntiVir MailGuard с помощью следующих контрольных таблиц, если при использовании AntiVir MailGuard возникают проблемы.

Контрольная таблица

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

▶ Проверьте, регистрируется ли Ваш почтовый клиент через SSL (также часто называется TSL - Transport Layer Security) на сервере. AntiVir MailGuard не поддерживает SSL и поэтому завершает работу зашифрованных соединений SSL. Если Вы хотите использовать зашифрованные соединения SSL без защиты MailGuard, Вам следует использовать другой порт для соединения, но не контролируемые модулем MailGuard порты. Контролируемые модулем MailGuard порты можно изменить в настройкахMailGuard::Поиск.

▶ Активна ли служба AntiVir MailGuard (сервис)? 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 MailGuard*. Должен быть определен тип запуска "Авто" и состояние "Работает" Запустите службу вручную. Выбрав соответствующую строку, нажмите кнопку "Пуск" При возникновении уведомления об ошибке проверьте его. Если возникает сообщение об ошибке, проверьте то, что предложено системой. Если не удалось исправить положение, необходимо полностью удалить программу AntiVir ("Пуск | Панель управления | Установка и удаление программ"), перезагрузить компьютер и вновь установить программу AntiVir.

Общее

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

▶ Аутентификация на почтовом сервере возможна только с помощью "пароля". "Kerberos" и "RPA" в настоящее время не поддерживаются.

▶ Программа AntiVir не проверяет отправляемые письма на наличие в них вирусов и вредоносного ПО.

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

В виртуальных машинах сетевое соединение недоступно, если Avira FireWall установлен в главной операционной системе и уровень безопасности Avira FireWall установлен на средний или высокий.

Если Avira FireWall установлен на компьютере, на котором дополнительно используется виртуальная машина (например, VMWare, Virtual PC и пр.), FireWall будет блокировать все сетевые соединения виртуальной машины, если уровень безопасности Avira FireWall установлен на средний или высокий. При уровне безопасности низкий FireWall будет реагировать согласно ожиданиям.

Причина: Виртуальная машина эмулирует программными средствами сетевую карту. С помощью такой эмуляции пакеты данных гостевой системы собираются в специальный UDP-пакет и переправляются через внешний шлюз обратно к хост-системе. Начиная с уровня безопасности средний, в Avira FireWall они блокируются поступающими извне пакетами.

Чтобы этого избежать, проделайте следующее:

- В центре управления нажмите во вкладке **Онлайн-защита :: FireWall**.
- Воспользуйтесь ссылкой **Настройка**.
- Появится диалоговое окно *Настройки*. Вы находитесь в разделе настройки *правил приложений*.
- Включите **Режим эксперта**.
- Выберите раздел настроек **Правила адаптера**.
- Нажмите кнопку **Добавить**.
- Выберите во *Входящих правилах* **UDP**.
- Укажите имя правила в поле **Имя**.
- Нажмите кнопку **OK**.
- Проверьте, расположено ли данное правило над правилом **Запрещать все IP-пакеты**.

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

Блокируется соединение Virtual Private Network (VPN), если уровень безопасности Avira FireWall установлен на средний или высокий.

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

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

Письмо, отправленное по соединению TSL, было заблокировано модулем MailGuard.

Причина: Transport Layer Security (TLS: протокол шифрования для передачи данных в интернете в настоящее время не поддерживается модулем MailGuard. У Вас есть несколько возможностей отправить письмо:

▶ Используйте другой порт, но не используемый SMTP порт 25. Это позволит Вам обойти модуль MailGuard

▶ Откажитесь от защищенного TSL-соединения и отключите поддержку TSL в Вашем почтовом клиенте.

▶ Отключите (временно) контроль исходящих писем модулем MailGuard в настройках в MailGuard::Поиск.

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).

9.2 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.

9.2.1 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.

9.2.2 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.

9.2.3 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
F2	Переименование выбранного профиля
F3	Запуск проверки с выбранным профилем
F4	Создание ярлыка на рабочем столе для выбранного профиля
Ins	Добавление нового профиля
Del	Удаление выбранного профиля

Раздел FireWall

Горячие клавиши	Описание
Enter	Свойства

Раздел Карантин

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

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 событие(я)
Enter	Показать событие
Del	Удалить событие(я)

9.3 Центр безопасности Windows

- начиная с Windows XP SP 2 -

9.3.1 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.

9.3.2 Центр обеспечения безопасности Windows и программа AntiVir

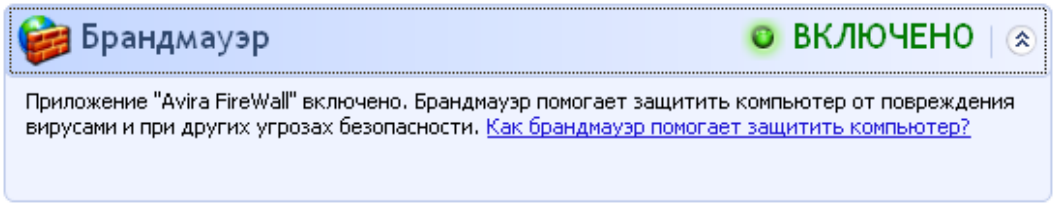
Брандмауэр

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

- Брандмауэр АКТИВИРОВАН / Брандмауэр включен
- Брандмауэр ДЕАКТИВИРОВАН / Брандмауэр выключен

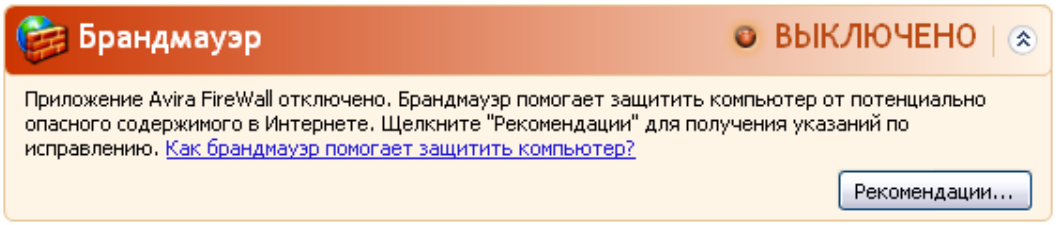
Брандмауэр АКТИВИРОВАН / Брандмауэр выключен

После установки программы AntiVir и отключения брандмауэра Windows вы получите следующее уведомление:



Брандмауэр ДЕАКТИВИРОВАН / Брандмауэр выключен

При деактивации Avira FireWall выдается следующее сообщение:



Примечание
Активация и деактивация Avira FireWall выполняется во вкладке Статус в Центре управления.

Предупреждение
При отключении Avira FireWall ваш компьютер больше не будет защищен от несанкционированного доступа по сети или через Интернет.

Антивирусное ПО / Защита от вредоносных программ

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

Антивирусных программ НЕ ОБНАРУЖЕНО

Антивирусные базы УСТАРЕЛИ

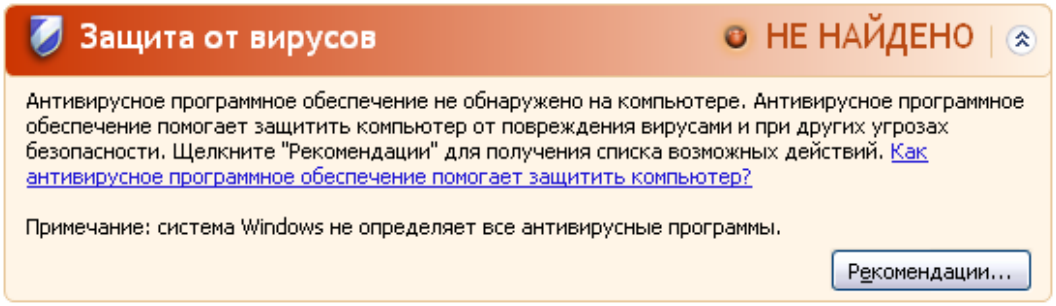
Защита от вирусов ВКЛЮЧЕНА

Защита от вирусов ВЫКЛЮЧЕНА

Защита от вирусов НЕ КОНТРОЛИРУЕТСЯ

Защита от вирусов НЕ ОБНАРУЖЕНА

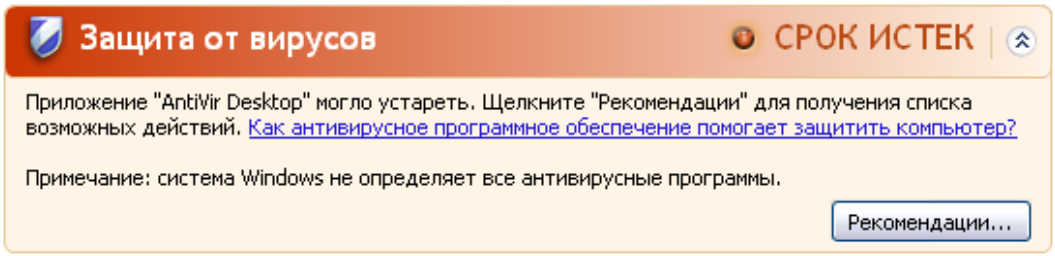
Это сообщение отправляется Центром обеспечения безопасности Windows, если на компьютере не было обнаружено антивирусных программ.



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

Антивирусные базы УСТАРЕЛИ

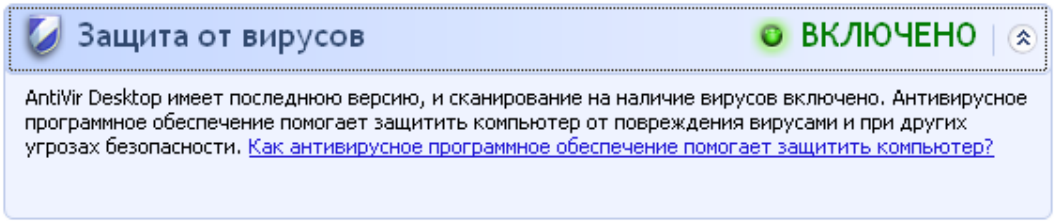
Если вы уже установили Windows XP Service Pack 2 или Windows Vista, а теперь устанавливаете программу AntiVir или устанавливаете Windows XP Service Pack 2 или Windows Vista на систему, в которой уже была установлена программа AntiVir, будет выдано следующее сообщение:



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

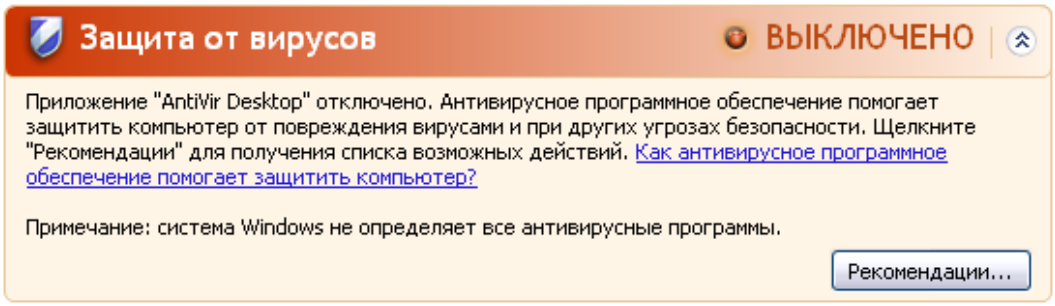
После установки и последующего обновления программы AntiVir вы получите следующее сообщение:



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.

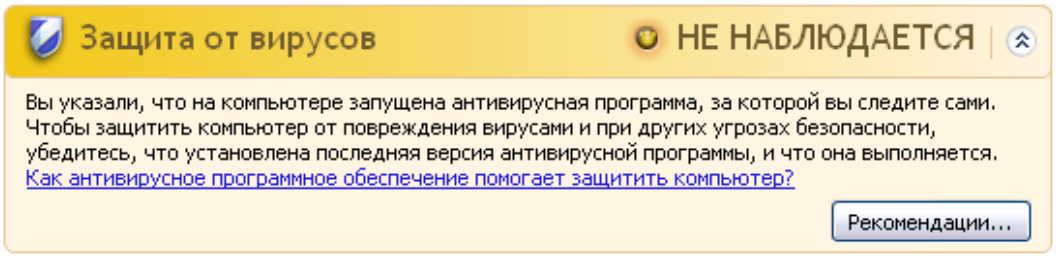


Примечание
Активировать и деактивировать модуль AntiVir Guard можно во вкладке Обзор :: Активировать или деактивировать статус Центра управления. Если AntiVir Guard включен, на панели задач появляется открытый красный зонтик.

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.

10 Вирусы и другое

10.1 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.

10.2 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.

11 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

См. главу Обратная связь

11.1 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 Professional.

11.2 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/onlineshop

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

- **Информация о лицензии**. Эта информация отображается в меню программы в пункте Справка :: О программе Avira AntiVir Professional. Информация о лицензии.
- **Информация о версии**. Эта информация отображается в меню программы в пункте Справка :: О программе Avira AntiVir Professional. 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.

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

У вас есть также возможность отправить нам подозрительный файл через наш сайт: http://www.avira.ru/file-upload

11.4 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@avira.ru

Т.к. некоторые почтовые шлюзы работают с антивирусным ПО, защитите файл(ы) паролем и не забудьте сообщить его нам.

11.5 Обратная связь для вашей безопасности

Для компании Avira безопасность ее клиентов стоит на первом месте. Для этого каждое отдельное решение Avira GmbH и каждое отдельное обновление до выпуска на рынок тщательно проверяются нашими экспертами на предмет качества и безопасности. Само собой разумеющимся является для нас серьезное отношение к возможным уязвимостям системы, быстрая и открытая реакция на них.

Если вы обнаружили уязвимость в одном из наших программных продуктов, отправьте, пожалуйста, нам сообщение об этом на следующий адрес:

vulnerabilities@avira.ru

12 Ссылка: Опции меню настройки

В ссылке содержится информация о всех доступных настроечных опциях.

12.1 Сканер

Раздел блока Сканер отвечает за настройку параметров проверки, т.е. за работу сканера.

12.1.1 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. Если Вы администрируете программу AntiVir через SMC, то эта опция недоступна.

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. Если программа AntiVir администрируется через SMC, то каждый раз отображается и может быть активирована опция: Если в компьютере не установлено несколько процессоров, то опция 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.

Не проверять файлы и пути на сетевых дисках

Если опция включена, из проверки исключаются сетевые диски, подключенные к компьютеру. Эта опция рекомендуется, если сервер или другие рабочие станции сами защищены от вирусов с помощью антивирусного ПО. Эта опция по умолчанию отключена.

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.

12.1.1.1. 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
В диалоге сканера по умолчанию отображается действие 'Поместить на карантин'.

Разрешенные действия

В этом окне Вы можете выбирать действия, которые при обнаружении вируса будут выполняться в индивидуальном режиме уведомлений или в режиме эксперта. Для этого должны быть активированы соответствующие опции.

лечить

Сканер вылечит инфицированный файл, если это будет возможно.

Переименовать

Сканер переименовывает файл. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Позже файл может быть вылечен и переименован обратно.

Карантин

Сканер помещает файлы на карантин. Файл может быть восстановлен из менеджера карантина, если он имеет информационное значение, или, при необходимости, его можно отправить в Avira Malware Research Center. В зависимости от типа файла у Вас есть возможность выбора действий.

удалить

Файл удаляется. Эта процедура значительно быстрее, чем "переписать и удалить".

пропустить

Файл пропускается.

Переписать и удалить

Сканер переписывает файл, заменяя его стандартным шаблоном, а затем удаляет файл. Он не может быть восстановлен.

По умолчанию

С помощью этой кнопки вы можете определить стандартное действие сканера для лечения инфицированных файлов. Выделите действие и нажмите кнопку **"По умолчанию"**. В комбинированном режиме уведомлений для инфицированных файлов может выполняться только выбранное действие по умолчанию. В индивидуальном и экспертном режиме уведомлений выбранное действие по умолчанию для инфицированных файлов может быть выбрано предварительно.

Примечание
Действие **вылечить** не может быть выбрано в качестве действия по умолчанию.

Примечание
Если в качестве действия по умолчанию выбрали *удалить* или *переписать и удалить* и хотите установить комбинированный режим уведомлений, то учитывайте следующее: Если инфицированные файлы были обнаружены системой эвристического поиска, то они не удаляются, а помещаются на карантин.

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.

Показывать предупреждения

Если опция включена, при обнаружении вируса или вредоносной программы отображается предупреждение с предложением выбора действий.

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. Эта процедура значительно быстрее, чем "переписать и удалить".

Переписать и удалить

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

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. Эта процедура значительно быстрее, чем "переписать и удалить".

Переписать и удалить

Если опция включена, сканер заменяет файл стандартным шаблоном, а затем удаляет его (очистить). Он не может быть восстановлен.

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 **переписать и удалить** , учитывайте следующее: Если инфицированные файлы были обнаружены системой эвристического поиска, то они не удаляются, а помещаются на карантин.

12.1.1.2. Дополнительные действия

Запуск программы после обнаружения

После проверки Сканер может открыть любой файл по Вашему выбору, если был обнаружен хотя бы один вирус, например, почтовый клиент, чтобы уведомить других пользователей и/или администратора о факте обнаружения объекта.

Примечание
По соображениям безопасности, есть возможность запустить программу только в том случае, если пользователь находится в системе. Файл запускается с правами, действующими для активного пользователя. Если пользователь не находится в системе, эта функция не используется.

Имя программы

В этом поле Вы можете указать имя файла, который запускает Сканер после обнаружения опасного объекта с указанием пути к нему.

...

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

Аргументы

В этом поле Вы можете указать параметры командной строки для запуска требуемых программ.

Протокол событий

Журнал регистрации событий

Если опция включена, то при завершении проверки Сканер в журнал регистрации событий Windows будет передано сообщение о событии. События можно просмотреть в списке событий Windows. Эта опция по умолчанию отключена.

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.

12.1.1.3. 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.

Примечание
Если программа AntiVir администрируется в SMC, при указании пути для исключаемых файлов можно использовать переменные. Список переменных, которые можно использовать, вы найдете здесь: Переменные: Исключения Guard и Scanner.

12.1.1.4. 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.

12.1.2 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.

12.2 Guard

Раздел Guard в настройке отвечает за настройку постоянной защиты.

12.2.1 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.

Дисководы

Сетевые диски

Если эта опция включена, то проверяться будут только файлы сетевых дисков, например, Server-Volumes, пиринговые диски и т.д.

Примечание
Чтобы не загружать слишком сильно Ваш компьютер, опцию **Сетевые диски** следует активировать только в исключительных случаях.

Предупреждение
Если эта функция отключена, сетевые диски **не** будут контролироваться. Они больше не защищены от вирусов или нежелательных программ!

Примечание
Если файлы выполняются на сетевых дисках, они проверяются Guard независимо от настройки опции *Сетевые диски*. В некоторых случаях файлы проверяются на сетевых дисках при открытии, хотя опция *Сетевые диски* отключена. Причина: К этим файлам обращаются с полномочием 'Выполнить файл'. Если Вы хотите исключить эти файлы или выполняемые на сетевых дисках файлы из проверки Guard, внесите их в список пропускаемых объектов данных (см.: Guard::Поиск::Исключения).

Активировать кэшинг

Если эта опция активирована, то проверяемые файлы на сетевых дисках будут доступны в кэше Guard. Проверка сетевых дисков без функции кэшинга отличается большей безопасностью, однако меньшей производительностью по сравнению с проверкой сетевых дисков с функцией кэшинга.

12.2.1.1. Действие при обнаружении

Действие при обнаружении

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

Интерактивный

Если эта опция активирована, то при обнаружении вируса Guard выведет сообщение на рабочий стол. Вы можете удалить обнаруженную вредоносную программу или выбрать дополнительные действия для обработки вирусов нажатием кнопки 'Подробно'. Действия отображаются в диалоговом окне. Эта опция включена по умолчанию.

Разрешенные действия

В этом разделе Вы можете выбрать действия, которые должны отображаться в диалоговом окне в качестве дополнительных действий для обработки вирусов. Для этого должны быть активированы соответствующие опции.

Вылечить

Guard вылечит инфицированный файл, если это будет возможно.

Переименовать

Guard переименовывает файл. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Позже файл может быть вылечен и переименован обратно.

Карантин

Guard помещает файл на карантин. Файл может быть восстановлен из менеджера карантина, если в этом возникнет необходимость, или его можно отправить разработчику - центр исследования вирусов компании Avira. В зависимости от типа файла менеджер карантина может предложить на выбор дополнительные функции.

удалить

Файл удаляется. Эта процедура значительно быстрее, чем "переписать и удалить".

пропустить

Доступ к файлу разрешается, никаких действий с ним не выполняется.

Переписать и удалить

Guard переписывает файл, заменяя его шаблоном, а затем удаляет. Он не может быть восстановлен.

По умолчанию

Кнопка позволяет выбрать действие, которое активно по умолчанию в случае обнаружения вируса. Выделите действие, которое должно быть по умолчанию активно, и нажмите на кнопку "**По умолчанию"**.

Примечание
В качестве действия по умолчанию нельзя выбрать **Лечить**.

Подробная информация доступна здесь.

Автоматический

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

файл перед действием копировать в карантин

Если эта опция включена, Guard создает резервную копию (Backup) перед осуществлением первичного (или, в случае необходимости, вторичного) действия. Резервная копия сохраняется в Карантине. Она может быть восстановлена из Менеджера Карантина, если в этом возникнет необходимость. Кроме того, Вы можете отправить резервную копию в Avira Malware Research Center для дальнейшего изучения. В зависимости от типа объекта, Менеджер Карантина располагает дополнительными возможностями выбора.

Показывать предупреждения

Если опция включена, при обнаружении вируса или вредоносной программы отображается предупреждение.

Первичное действие

Первичное действие выполняется, если Guard 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, Guard автоматически пытается лечить инфицированный файл. Если Guard не может вылечить инфицированный файл, выполняется операция, предусмотренная Вторичным действием.

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

удалить

Если опция включена, файл удаляется. Эта процедура значительно быстрее, чем "переписать и удалить".

Переписать и удалить

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

Переименовать

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

пропустить

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

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

Запретить доступ

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

Карантин

Если эта опция включена, Guard помещает файл в папку карантина. Файлы из этой папки могут быть позже вылечены или, в случае необходимости, отправлены разработчику (Avira Malware Research Center).

Вторичное действие

Опция "**Вторичное действие"** может быть выбрана только в том случае, если для "**Первичного действия"** была выбрана опция **" 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. Эта процедура значительно быстрее, чем "переписать и удалить".

Переписать и удалить

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

Переименовать

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

пропустить

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

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

Запретить доступ

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

Карантин

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

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

12.2.1.2. Дополнительные действия

Уведомления

Протокол событий

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.

12.2.1.3. 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.
Полное указание пути требуется для процессов, исполняемые файлы которых находятся на внешних, например, сетевых дисках. При этом руководствуйтесь общими указаниями к записи Исключения на внешних сетевых дисках.
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
\Компьютер1\C\Папка1

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
Для исключений на связанных сетевых дисках следует помнить следующее: При использовании букв-названий дисков для связанных сетевых дисков, указанные файлы и папки НЕ будут исключаться из поиска Guard. Если UNC-путь в списке исключений отличается от UNC-пути, используемого для соединения с сетевым диском, (указание IP-адреса в списке исключений - указание имени компьютера для соединения с сетевым диском), указанные папки и файлы НЕ будут исключаться из поиска Guard. Определите используемый UNC-путь с помощью файла отчета Guard:
\\<Имя компьютера>\<Доступ>\ - ИЛИ- \\<IP-адрес>\<Доступ>\

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 или к сетевым дискам . Вы можете прочитать используемый путь в файле отчетов Guard . Файл отчета можно вызвать в Control Center в разделе Локальная защита :: Guard начиная с

Примечание
Если программа AntiVir администрируется с помощью SMC, при указании пути для исключаемых процессов и файлов можно использовать переменные. Список переменных, которые можно использовать, вы найдете здесь: Переменные: Исключения Guard и Scanner.

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.

- \\Имя компьютера1\Общая папка1\

  Все файлы, к которым имеется доступ через соединение '\\Имя компьютера1\Общая папка1\', исключаются из поиска Guard. В большинстве случаев это внешний сетевой диск, доступ к которому осуществляется через имя компьютера 'Имя компьютера1' и название общей папки 'Общая папка1' на другом компьютере с общей папкой.

- \\1.0.0.0\Общая папка1*.mdb

  Все файлы с расширением 'mdb', доступ к которым осуществляется через соединение '\\1.0.0.0\Общая папка1', исключаются из поиска Guard. В большинстве случаев это внешний сетевой диск, доступ к которому осуществляется через IP-адрес '1.0.0.0' и название общей папки 'Общая папка1' на другом компьютере с общей папкой.

-

12.2.1.4. 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.

12.2.2 ProActiv

Используя Avira AntiVir ProActiv, вы защищаете себя от новых и неизвестных угроз, для которых еще нет описания вирусов и эвристических методов. Технология ProActiv интегрирована в компонент Guard; она наблюдает и анализирует выполняемые программами действия. Поведение программ исследуется на наличие активности, типичной для вредоносного ПО: Тип активности и последовательность действий. Если программа демонстрирует поведение, типичное для вредоносного ПО, считается, что обнаружен вирус, и отправляется соответствующее сообщение : У Вас есть возможность блокировать выполнение программы или игнорировать сообщение и продолжить выполнение программы. Вы можете классифицировать программу как надежную и добавить ее в список разрешенных программ фильтра приложений. У Вас также есть возможность при помощи команды *Всегда блокировать* добавить программу в список блокируемых программ фильтра приложений.

Для определения подозрительного поведения компонент ProActiv использует наборы правил, разработанные центром исследований вирусов компании Avira. Наборы правил загружаются банками данных Avira GmbH. Для сбора информации в базах данных компании Avira программа Avira AntiVir ProActiv пересылает информацию о найденных подозрительных объектах. Вы можете отключить передачу данных в базы данных компании Avira.

Примечание
Технология ProActiv недоступна для 64-битных систем! Windows 2000 не поддерживает компонент ProActiv.

Общее

Активация Avira AntiVir ProActiv

Если опция включена, программы на вашем компьютере контролируются и проверяются на подозрительную активность. При возникновении типичного для вредоносного ПО поведения Вы получаете сообщение. Вы можете блокировать программу или, выбрав "*Игнорировать"*, продолжить выполнение программы. Из контроля исключены: Программы, классифицированные как надежные, надежные и подписанные программы, которые по умолчанию содержатся в списке разрешенных приложений фильтра приложений, все программы, добавленные Вами к списку разрешенных программ фильтра приложений.

Увеличьте безопасность вашего компьютера, приняв участие в AntiVir ProActiv Community.

При активированной опции Avira AntiVir ProActiv пересылает данные подозрительных программ, а в некоторых случаях и подозрительные программные файлы (исполняемые файлы), в Avira Malware Research Center для расширенной проверки. Данные после их анализа включаются в наборы правил анализа поведения ProActiv. Таким образом Вы участвуете в сообществе Avira ProActiv и вносите свой вклад в непрерывное усовершенствование и повышение качества технологии безопасности ProActiv. Если эта опция выключена, данные не отправляются. Это никак не сказывается на работоспособности ProActiv.

Нажмите сюда, чтобы получить дополнительную информацию

По этой ссылке вы попадете на веб-страницу, содержащую подробную информацию о расширенной онлайн-проверке. Данные, передаваемые при расширенной онлайн-проверке, полностью указываются на интернет-сайте.

12.2.2.1. Фильтр приложений: Блокируемые приложения

В разделе *Фильтр приложений: Блокируемые приложения*: вы можете добавить приложения, которые вы классифицируете, как вредоносные, и которые по умолчанию должны блокироваться Avira AntiVir ProActiv. Добавленные приложения не смогут выполняться Вашей системой. Вы можете добавлять программы к фильтру приложений для блокируемых приложений также при помощи сообщений Guard о подозрительном поведении программ, используя опцию *Всегда блокировать эту программу*, (см. .

Блокируемые приложения

Приложения

В списке приведены все приложения, которые Вы классифицировали как вредоносные и добавили с помощью Настройки или сообщений компонента ProActiv. Приложения из списка блокируются Avira AntiVir ProActiv и не смогут выполняться на вашем компьютере. При запуске блокируемой программы появляется сообщение операционной системы. Avira AntiVir ProActiv идентифицирует блокируемые приложения на основании указанного пути и имени файла и блокирует их независимо от их содержания.

Поле ввода

В этом поле Вы указываете приложение, которое должно быть заблокировано. Для идентификации приложения необходимо указать полный путь и имя файла с расширением. Указание пути должно либо содержать обозначение диска, на котором размещено приложение, либо начинаться с переменных окружения.

Нажатие кнопки откроет окно, в котором можно выбрать приложение, которое необходимо заблокировать.

Добавить

С помощью кнопки "**Добавить"** Вы можете добавить заданное в поле ввода приложение в список приложений, которые необходимо заблокировать.

Примечание
Приложения, необходимые для работы операционной системы, не могут быть добавлены.

Удалить

С помощью кнопки "**Удалить"** Вы можете удалить выбранное приложения из списка приложений, которые необходимо заблокировать.

12.2.2.2. Фильтр приложений: Разрешенные приложения

В разделе *Фильтр приложений: Разрешенные приложения* перечислены приложения, исключенные из проверки компонента ProActiv: Подписанные программы, которые классифицируются как надежные и по умолчанию находятся в списке, все приложения, которые Вы классифицировали как надежные и внесли в фильтр приложений: В настройке Вы можете добавить приложения в список разрешенных приложений. Вы также можете с помощью сообщений Guard о подозрительных программах добавить приложения, используя в сообщении Guard опцию **Программа с высокой надежностью**.

Исключаемые приложения

Приложения

Список содержит приложения, исключенные из проверки компонента ProActiv. В настройках по умолчанию после установки список содержит подписанные приложения надежных производителей. Вы можете классифицировать приложение как надежное с помощью настройки или сообщения Guard. ProActiv идентифицирует приложения на основании пути, имени файла и его содержания. Проверка содержания необходима, так как с помощью изменений, например, обновлений, к программе можно добавить вредоносный код. На основании заданного типа Вы можете определить необходимость проверки содержания: При типе "*Содержание"* заданные с путем и именем файла приложения проверяются на изменения содержания файлов, прежде чем они будут исключены из проверки компонента ProActiv. При измененном содержании файлов приложение снова будет проверяться компонентом ProActiv. Тип "*Путь"* : проверка содержания не осуществляется до тех пор, пока приложение не будет исключено из проверки элементом Guard. Чтобы изменить список исключений, щелкните по отображаемому типу.

Предупреждение
Используйте тип *Путь* только в исключительных случаях. Путем обновления к приложению можно добавить вредоносный код. Изначально безопасное приложение становится вредоносной программой.

Примечание
Некоторые надежные приложения, например, все компоненты программы AntiVir, по умолчанию исключены из проверки компонента ProActiv, однако они не включены в список.

Поле ввода

В этом поле укажите приложение, которое необходимо исключить из проверки компонента ProActiv. Для идентификации приложения необходимо указать полный путь и имя файла с расширением. Указание пути должно либо содержать обозначение диска, на котором размещено приложение, либо начинаться с переменных окружения.

Нажатие кнопки откроет окно, в котором можно выбрать приложение, которое необходимо исключить.

Добавить

С помощью кнопки "**Добавить"** Вы можете добавить заданное в поле ввода приложение в список приложений, которые необходимо исключить.

Удалить

С помощью кнопки "**Удалить"** вы можете удалить выбранное приложения из списка приложений, которые необходимо исключить.

12.2.3 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. Место сохранения см. Настройка :: Общее :: Папки :: Папка для отчетов.

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.

12.3 MailGuard

Раздел MailGuard в настройке отвечает за настройку защиты MailGuard.

12.3.1 Поиск

Вы используете MailGuard для защиты почты от вирусов . MailGuard может проверять исходящие письма на вирусы и вредоносные программы.

Поиск

Включение MailGuard

Если опция включена, MailGuard контролирует почтовый трафик. MailGuard — это прокси-сервер, который проверяет трафик между почтовым сервером, который вы используете, и клиентской почтовой программой на вашем компьютере: При настройках по умолчанию входящие письма проверяются на наличие вредоносного ПО. Если опция выключена, то служба MailGuard будет работать, однако контроль программой MailGuard будет деактивирован.

Проверять входящую почту

Если эта опция активирована, то входящие письма проверяются на вирусы и вредоносные программы, . MailGuard поддерживает протоколы POP3 и IMAP. Активируйте протокол входящих писем, который использует Ваш почтовый клиент, для контроля посредством MailGuard.

Контролировать аккаунты POP3

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

Контролируемые порты

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

По умолчанию

Кнопка возвращает заданные порты к стандартному порту для POP3.

Контролировать аккаунты IMAP

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

Контролируемые порты

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

По умолчанию

Кнопка возвращает заданные порты к стандартному порту для IMAP.

Проверять исходящую почту (SMTP)

Если опция включена, исходящие письма проверяются на вирусы и вредоносное ПО.

Контролируемые порты

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

По умолчанию

Кнопка возвращает заданные порты к стандартному порту для SMTP.

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

12.3.1.1. Действие при обнаружении

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

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

Действие при обнаружении

Интерактивный

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

Разрешенные действия

В этом окне Вы имеете возможность выбрать действия, которые могут быть выполнены при обнаружении вируса или вредоносной программы. Для этого должны быть активированы соответствующие опции.

Поместить на карантин

Если опция включена, Email с вложениями помещается в Карантин. Оно может быть позже доставлено через Менеджер карантина. Инфицированное письмо удаляется. Тело письма и при необходимости вложения письма будут заменены стандартным текстом.

Удалить

Если опция включена, инфицированное письмо при обнаружении вируса / вредоносной программы удаляется. Тело письма и возможные приложения заменяются стандартным текстовым шаблоном.

Удалить приложение

Если опция включена, инфицированное приложение заменяется стандартным текстовым шаблоном. В случае, если инфицировано тело письма, оно удаляется и также заменяется стандартным текстовым шаблоном. Письмо доставляется адресату.

Поместить приложение на карантин

При включенной опции инфицированное вложение помещается в Карантин , а затем удаляется (заменяется текстовым шаблоном). Текст письма доставляется адресату. Инфицированное приложение может быть позже доставлено адресату из Менеджера карантина.

Пропустить

Если опция включена, инфицированное письмо доставляется адресату, несмотря на обнаружение в нем вируса или вредоносной программы.

По умолчанию

Кнопка позволяет выбрать действие, которое активно по умолчанию в случае обнаружения вируса. Выделите действие, которое должно быть по умолчанию активно, и нажмите на кнопку **По умолчанию**.

показывать прогресс выполнения

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

Автоматический

Если эта опция включена, Вы не будете получать уведомлений при обнаружении вируса или вредоносной программы. MailGuard работает автоматически в соответствии с выбранными Вами настройками.

Первичное действие

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

удалить письмо

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

поместить письмо в карантин

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

пропустить письмо

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

Инфицированные вложения

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

удалить

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

поместить на карантин

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

пропустить

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

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

12.3.1.2. Другие действия

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

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

Шаблон для удаленных и перемещенных писем

Этот текст добавляется в тело письма в виде сообщения. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующая комбинация клавиш может использоваться для форматирования:

Strg + Enter вставляет разрыв строки.

По умолчанию

Кнопка позволяет добавить стандартный шаблон в текстовое поле.

Шаблон для удаленных и перемещенных вложений

Этот текст заменяет собой инфицированное вложение. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующая комбинация клавиш может использоваться для форматирования:

Strg + Enter вставляет разрыв строки.

По умолчанию

Кнопка позволяет добавить стандартный шаблон в текстовое поле.

12.3.1.3. 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

Обнаруживать макровирусы эвристическими методами

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 определена по умолчанию, если Вы используете эвристический поиск. Эта опция включена по умолчанию и рекомендована.

Высокий уровень распознавания

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

12.3.2 Общее

12.3.2.1. Исключения

Адреса, не подвергающиеся проверке

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

Примечание
Список исключений применяется MailGuard только для входящих писем.

Статус

Пиктограмма	Описание
	Этот адрес не проверяется на наличие вредоносных программ.

адресу эл. почты

Адреса, которые больше не подвергаются проверке.

Вредоносное ПО

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

наверх

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

вниз

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

Поле ввода

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

Добавить

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

Удалить

Кнопка удаляет выделенный адрес из списка

12.3.2.2. Буферная память

Буферная память

Буферная память MailGuard содержит данные о проверенных письмах, которые отображаются в статистике в центре управления в разделе MailGuard.

Максимальное число писем для хранения в буферной памяти

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

Максимальная продолжительность хранения писем в днях:

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

Очистить буфер

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

12.3.2.3. Нижний колонтитул

В разделе *Нижний колонтитул* Вы можете настроить нижний колонтитул письма, который будет отображаться в отправляемых Вами письмах. Эта функция может быть использована при активации проверки MailGuard для исходящих писем (см. опцию *Сканировать исходящую почту (SMTP)* в разделе Настройка::MailGuard::Поиск) . Вы можете использовать заданный нижний колонтитул AntiVir MailGuard, которым Вы подтверждаете, что отправленное письмо было проверено антивирусной программой. Вы также можете ввести собственный текст в качестве нижнего колонтитула. Если Вы используете обе опции для нижнего колонтитула, то приоритет будет отдаваться пользовательскому тексту нижнего колонтитула AntiVir MailGuard.

Нижний колонтитул в отправляемых письмах

AntiVir MailGuard, присоединить нижний колонтитул

Если эта опция активирована, то в тексте отправляемого письма будет отображаться нижний колонтитул AntiVir MailGuard. Нижним колонтитулом AntiVir MailGuard Fußzeile Вы подтверждаете, отправленное письмо было проверено на вирусы и вредоносные программы антивирусом AntiVir MailGuard . Нижний колонтитул AntiVir MailGuard содержит следующий текст: "Проверено антивирусной программой AntiVir MailGuard [версия продукта] [сокращенное название и номер версии поискового движка] [сокращенное название и номер версии файла вирусных сигнатур]".

Присоединить этот нижний колонтитул

Если эта опция активирована, то текст, который задается в строку ввода, будет отображаться в отправленных письмах как нижний колонтитул.

Поле ввода

Здесь задается текст, который будет отображаться в отправленных письмах как нижний колонтитул.

12.3.3 Отчет

MailGuard 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 MailGuard 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 MailGuard 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, MailGuard также записывает в файл отчета менее важную информацию.

Полная

Если эта опция активна, MailGuard записывает в файл отчета всю информацию.

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. Место сохранения см. Настройка :: Общее :: Папки :: Папка для отчетов.

Записать конфигурацию в файл отчета

Если опция включена, применяемые настройки MailGuard записываются 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.

12.4 Брандмауэр

Раздел FireWall блока Настройка отвечает за настройку компонента Avira FireWall.

12.4.1 Правила адаптера

Под адаптером в Avira FireWall понимаются моделируемая программными средствами аппаратура (напр., miniport, bridge connection и т.д.) или аппаратные средства (напр., сетевая карта).

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

Предустановленное правило адаптера зависит от уровня безопасности. В разделе Онлайн-защита :: FireWall в Control Center можно изменить уровень безопасности или привести правила адаптера в соответствие с вашими потребностями. Если Вы настроили правила адаптера под свои потребности, в разделе FireWall в Control Center регулятор в поле Уровень безопасности переместится в положение Пользователь.

Примечание
Стандартно установленный уровень безопасности для всех предопределенных правил Avira FireWall — **Средний**.

ICMP-Protokoll

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

Предустановленные правила для ICMP-протокола

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

Заблокированные входящие типы: ни один тип/различные типы

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

Заблокированные исходящие типы: ни один тип/различные типы

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

Флудинг

Щелчком мыши по ссылке можно открыть диалоговое окно, в которое ввести максимальное значение для разрешенной ICMP-задержки.

Фрагментированные ICMP-пакеты

Щелчком мыши по ссылке можно выбрать, принимаются или отклоняются фрагментированные ICMP пакеты.

TCP Port-Scan

При помощи этого правила Вы можете определить, когда FireWall должен предполагать наличие TCP Port-Scan и как он должен действовать в этом случае. Это правило служит для предотвращения т. н. атак TCP Port-Scan, с помощью которых можно определить открытые порты на Вашем компьютере. Атаки такого рода большей частью предназначены для того, чтобы использовать слабые места Вашего компьютера, через которые можно проводить более опасные атаки.

Предустановленные правила для TCP Port-Scan

Установка: Низкий	Установка: Средний	Установка: Высокий
Подозрение на TCP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в **файл отчета** и для блокирования атаки **не добавлять** к правилам.	Подозрение на TCP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в **файл отчета** и для блокирования атаки **добавлять** к правилам.	Правило, аналогичное установке "Средний".

Порты

Щелчком мыши можно открыть диалоговое окно, в котором Вы можете ввести число сканируемых портов, при достижении которого принимается решение об обнаружении TCP Port-Scan.

Временные параметры Port-Scan

Щелчком по ссылке можно открыть диалоговое окно, в которое Вы можете ввести период времени для сканирования установленного числа портов, достаточный для принятия решения об обнаружении TCP Port-Scan.

Файл отчета

Щелчком мыши по этой ссылке Вы можете определить необходимость сохранения в файле отчета IP-адреса злоумышленника.

Правило

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

UDP Port-Scan

При помощи этого правила можно определить, когда FireWall принимает решение об обнаружении UDP Port-Scan, а также указать необходимые действия в этом случае. Это правило используется для предотвращения так называемых атак сканера порта UDP, с помощью которых можно обнаружить открытые порты Вашего компьютера. Атаки такого рода большей частью предназначены для того, чтобы использовать слабые места Вашего компьютера, через которые можно проводить более опасные атаки.

Предустановленные правила для UDP Port-Scan

Установка: Низкий	Установка: Средний	Установка: Высокий
Подозрение на UDP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении UDP Port-Scan, IP-адрес злоумышленника сохранять в **файл отчета** и для предотвращения атаки **не добавлять** к правилам.	Подозрение на UDP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в **файл отчета** и для блокирования атаки **добавлять** к правилам.	Правило, аналогичное установке "Средний".

Порты

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

Временные параметры Port-Scan

Щелчком по ссылке можно открыть диалоговое окно, в которое Вы можете ввести период времени для сканирования установленного числа портов, достаточный для принятия решения об обнаружении UDP Port-Scan.

Файл отчета

Щелчком мыши по этой ссылке Вы можете определить необходимость сохранения в файле отчета IP-адреса злоумышленника.

Правило

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

12.4.1.1. Входящие правила

Посредством входящих правил Avira FireWall контролирует входящий трафик.

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

Предустановленные правила мониторинга TCP-трафика

Установка: Низкий	Установка: Средний	Установка: Высокий
Avira FireWall не блокирует входящий трафик.	– Разрешить установленное через порт 135 TCP-соединение Разрешить **TCP-пакеты** от адреса **0.0.0.0** с маской **0.0.0.0**,	– Отслеживать разрешенный TCP-трафик Разрешать TCP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный

	если номер локального порта **{135}** и номер удаленного порта **{0-65535}**. Применять для **Пакетов существующих соединений**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**. – Запрещать TCP пакеты для порта 135 Запрещать TCP-пакеты , с адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в **{135}** , а удаленный порт находится в **{0-65535}** . Применять ко **всем пакетам**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты объемом **<пустые>** с маской **<пустые>** оффсет **0**.	порт **{0-65535}** и удаленный порт **{0-65535}**. Применять для **Пакетов существующих соединений**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.

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

	Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.	

TCP-пакеты разрешать / запрещать

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Локальные порты

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

Удаленные порты

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

Метод применения

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

Файл отчета

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

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

Фильтрация по содержимому: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Здесь Вы можете указать специальную маску.

Фильтрация по содержимому: оффсет

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

Предустановленные правила мониторинга UDP-трафика

Установка: Низкий	Установка: Средний	Установка: Высокий
-	– Отслеживание конформного UDP трафика	Отслеживать разрешенный UDP-

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

	маской **<пустые>** оффсет **0**.	

Разрешать / запрещать UDP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Локальные порты

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

Удаленные порты

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

Метод применения

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

Файл отчета

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

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

Фильтрация по содержимому: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Здесь Вы можете указать специальную маску.

Фильтрация по содержимому: оффсет

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

Предустановленные правила мониторинга ICMP-трафика

Установка: Низкий	Установка: Средний	Установка: Высокий
-	– Не отклонять ICMP-пакеты на основании IP-адреса Разрешать ICMP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**. **Не сохранять в**	Правило, аналогичное установке "Средний".

	файл отчета, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.	

Разрешать / запрещать ICMP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Файл отчета

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

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

Фильтрация по содержимому: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Здесь Вы можете указать специальную маску.

Фильтрация по содержимому: оффсет

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

Предустановленное правило для IP-пакетов

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

Разрешать / запрещать IP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Файл отчета

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

Возможные правила мониторинга IP-пакетов на основании IP-протоколов

IP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Протокол

Здесь Вы можете выбрать желаемый IP-протокол.

Файл отчета

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

12.4.1.2. Исходящие правила

Посредством исходящих правил Avira FireWall контролирует исходящий трафик. Вы можете различать исходящие правила для следующих протоколов: IP, ICMP, UDP и TCP.

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

Кнопки

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

Вверх	Переместить выбранное правило на одну позицию вверх.
Переименовать	Переименовать правило.

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

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

12.4.2 Правила приложения

Правила применения для пользователя

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

Список приложений

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

Стандартный вид

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

Расширенная настройка

Если Вы хотите индивидуально регулировать сетевые доступы приложения, то Вы можете создавать определенные правила приложения, сравнимые с правилами адаптера, основанные на фильтрах пакетов. Для выбора расширенной настройки правил приложения сначала должен быть включен режим эксперта. Настройку правил приложения меняйте только в разделе FireWall:: Настройки: Активируйте опцию **Расширенные настройки** и сохраните настройки с помощью команды **Применить** или **OK**. Перейдите в конфигурации FireWall к разделу**FireWall::Правила приложения**: В списке правил приложений отобразится еще один столбец *Фильтр* с записью *Простой*. Теперь у Вас появится дополнительная опция **Фильтр:** *Действие* для *Продвинутый: Правила*, при помощи которых Вы можете перейти к расширенной настройке.

	Описание
Приложение	Имя приложения.
Режим	Показывает установленный режим правила приложения : Отфильтрованные в режиме проверяются и выполняются правила адаптера в соответствии с выполнением правила приложения. Привилегированные в режиме правила адаптера игнорируются. Здесь с помощью щелчка мыши Вы можете сменить режим.
Действие	Отображает действие, которое Avira FireWall выполнит автоматически, если приложение каким-либо образом использует сеть. При установке *Фильтр - простой* Вы можете щелчком мыши по ссылке сменить тип выполняемого действия. На выбор предлагаются типы действий **Спрашивать**, **Разрешать, Запрещать** или *Расширенный*. При установке *Фильтр - продвинутый* отображается тип выполняемого действия *Правила*. Ссылка **Правила** открывает окно **Правила приложений**, в котором Вы можете сохранить отредактированные правила для приложения.
Фильтрация	Отображает тип фильтра. Здесь Вы можете сменить тип фильтра. *Простой*: При простой фильтрации указанное действие выполняется для всей типов сетевой активности приложения программы. *Продвинутый*: При фильтрации выполняются правила, сохраненные в расширенной настройке.

Если Вы хотите создавать правила приложения, определенные для приложения, в разделе *Фильтр* выберите запись **Продвинутый**. В столбце **Действие** отобразится запись *Правила*. Щелкните мышью **Правила**, чтобы попасть в окно для создания определенных правил приложения.

Определенные правила приложения в расширенной настройке.

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

- Разрешить или запретить кодовую инъекцию

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

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

Разрешить или запретить входящие и/или исходящие IP-пакеты

Разрешить или запретить входящие и/или исходящие TCP-пакеты

Разрешить или запретить входящие и/или исходящие UDP-пакеты

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

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

Информация о приложении

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

	Описание
Имя	Имя приложения.
Путь	Полный путь к исполняемому файлу.

Кнопки

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

12.4.3 Надежные разработчики

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

Надежные разработчики для пользователей

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

Автоматически разрешать приложения от надежных производителей

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

Производители

Список показывает всех производителей, которые классифицируются как надежные.

Кнопки

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

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

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

12.4.4 Установки

Расширенные настройки

Включить FireWall

При включенной опции Avira FireWall активен и защищает Ваш компьютер от различных угроз, исходящих со стороны Интернета и других сетей.

Отключать Windows Firewall при запуске ОС

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

hosts-файл Windows НЕ ЗАБЛОКИРОВАН/ЗАБЛОКИРОВАН

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

Превышено время ожидания для правила

Всегда блокировать

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

Удалять правило через n сек.

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

Уведомления

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

Port-Scan

При включенной опции вы получаете уведомление в виде всплывающего окна, если FireWall распознал Port Scan.

Флудинг

При включенной опции вы получаете уведомление в виде всплывающего окна, если FireWall распознал флуд-атаку.

Приложения были блокированы

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

IP блокирован

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

Правила приложения

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

Расширенные настройки

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

Основные установки

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

12.4.5 Настройки всплывающего окна

Настройки всплывающего окна

Проверить стартовый блок процесса

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

Показывать несколько диалоговых окон для процесса

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

Автоматически подавлять всплывающее уведомление в игровом режиме

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

Сохранять действие для приложения

Всегда вкл.

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

Всегда откл.

Если опция включена, неактивна опция "**Сохранять действие для приложения**" диалогового окна "**Сетевое событие**".

Разрешать подписанные приложения

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

Запомнить последнее состояние

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

Отображать подробности

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

Отображать подробности по запросу

Если опция включена, в окне "*Сетевое событие",* информация отображается только по запросу, т. е. отображение подробной информации осуществляется после нажатия кнопки "**Подробности"** в окне "*Сетевое событие"*.

Всегда отображать подробности

Если опция включена, подробности всегда отображаются в окне "*Сетевое событие"*.

Запомнить последнее состояние

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

Разрешать привилегированные

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

Всегда вкл.

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

Всегда откл.

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

Запомнить последнее состояние

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

12.5 FireWall в SMC

Настройка FireWall рассчитана на специальные требования администрирования через Avira Security Management Center. Имеются расширенные опции и ограничения для отдельных опций настройки:

- Установки FireWall действительны для всех пользователей компьютеров-клиентов
- Правила адаптера: Для отдельных адаптеров с помощью контекстного меню можно настраивать уровни безопасности
- Правила приложения: Сетевой доступ для приложений может разрешаться или блокироваться. Нет возможности создавать специальные правила приложения.

Если администрирование программы AntiVir осуществляется через Avira Security Management Center, отключены следующие возможности настройки FireWall в Control Center на компьютерах-клиентах:

- Настройка уровней безопасности FireWall
- Настройка правил адаптера и приложений

12.5.1 Основные настройки

Расширенные настройки

Блокировать hosts-файл Windows

Если эта опция включена, hosts-файл Windows защищен от записи. Любые манипуляции с файлом больше невозможны. Вредоносное ПО, например, больше не в состоянии перенаправлять Ваши запросы на нежелательные страницы.

Игровой режим включен

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

Отключать Windows Firewall при запуске ОС

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

Включить FireWall

При включенной опции Avira FireWall активен и защищает Ваш компьютер от различных угроз, исходящих со стороны Интернета и других сетей.

Превышено время ожидания для правила

Всегда блокировать

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

Удалять правило через n сек.

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

12.5.2 Общие правила адаптера

Адаптерами называются установленные сетевые соединения. Можно создать правила адаптера для следующих сетевых соединений клиентов:

- Адаптер по умолчанию: LAN или высокоскоростной Интернет
- Беспроводной
- Модемное соединение

Для каждого доступного адаптера Вы можете при помощи контекстного меню к адаптеру настроить предустановленные правила адаптера:

- Высокий уровень безопасности
- Средний уровень безопасности
- Низкий уровень безопасности

У Вас также есть возможность настраивать отдельные правила адаптера индивидуально и в соответствии со своими потребностями.

Примечание
Стандартно установленный уровень безопасности для всех предопределенных правил Avira FireWall — **Средний**.

ICMP-Protokoll

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

Предустановленные правила для ICMP-протокола

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

Заблокированные входящие типы: ни один тип/различные типы

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

Заблокированные исходящие типы: ни один тип/различные типы

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

Флудинг

Щелчком мыши по ссылке можно открыть диалоговое окно, в которое ввести максимальное значение для разрешенной ICMP-задержки.

Фрагментированные ICMP-пакеты

Щелчком мыши по ссылке можно выбрать, принимаются или отклоняются фрагментированные ICMP пакеты.

TCP Port-Scan

При помощи этого правила Вы можете определить, когда FireWall должен предполагать наличие TCP Port-Scan и как он должен действовать в этом случае. Это правило служит для предотвращения т. н. атак TCP Port-Scan, с помощью которых можно определить открытые порты на Вашем компьютере. Атаки такого рода большей частью предназначены для того, чтобы использовать слабые места Вашего компьютера, через которые можно проводить более опасные атаки.

Предустановленные правила для TCP Port-Scan

Установка: Низкий	Установка: Средний	Установка: Высокий
Подозрение на TCP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в**файл отчета** и для блокирования	Подозрение на TCP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в **файл отчета** и для блокирования	Правило, аналогичное установке "Средний".

атаки**не добавлять** к правилам.	атаки **добавлять** к правилам.	

Порты

Щелчком мыши можно открыть диалоговое окно, в котором Вы можете ввести число сканируемых портов, при достижении которого принимается решение об обнаружении TCP Port-Scan.

Временные параметры Port-Scan

Щелчком по ссылке можно открыть диалоговое окно, в которое Вы можете ввести период времени для сканирования установленного числа портов, достаточный для принятия решения об обнаружении TCP Port-Scan.

Файл отчета

Щелчком мыши по этой ссылке Вы можете определить необходимость сохранения в файле отчета IP-адреса злоумышленника.

Правило

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

UDP Port-Scan

При помощи этого правила можно определить, когда FireWall принимает решение об обнаружении UDP Port-Scan, а также указать необходимые действия в этом случае. Это правило используется для предотвращения так называемых атак сканера порта UDP, с помощью которых можно обнаружить открытые порты Вашего компьютера. Атаки такого рода большей частью предназначены для того, чтобы использовать слабые места Вашего компьютера, через которые можно проводить более опасные атаки.

Предустановленные правила для UDP Port-Scan

Установка: Низкий	**Установка: Средний**	**Установка: Высокий**
Подозрение на UDP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении UDP Port-Scan, IP-адрес злоумышленника сохранять в **файл отчета** и для предотвращения атаки **не добавлять** к правилам.	Подозрение на UDP Port-Scan, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении TCP Port-Scan, сохранять IP-адрес злоумышленника в **файл отчета** и для блокирования атаки **добавлять** к правилам.	Правило, аналогичное установке "Средний".

Порты

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

Временные параметры Port-Scan

Щелчком по ссылке можно открыть диалоговое окно, в которое Вы можете ввести период времени для сканирования установленного числа портов, достаточный для принятия решения об обнаружении UDP Port-Scan.

Файл отчета

Щелчком мыши по этой ссылке Вы можете определить необходимость сохранения в файле отчета IP-адреса злоумышленника.

Правило

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

12.5.2.1. Входящие правила

Посредством входящих правил Avira FireWall контролирует входящий трафик.

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

Предустановленные правила мониторинга TCP-трафика

Установка: Низкий	Установка: Средний	Установка: Высокий
Avira FireWall не блокирует входящий трафик.	– Разрешить установленное через порт 135 TCP-соединение Разрешить **TCP-пакеты** от адреса **0.0.0.0** с маской **0.0.0.0**, если номер локального порта **{135}** и номер удаленного порта **{0-65535}**. Применять для **Пакетов существующих соединений**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.	– Отслеживать разрешенный TCP-трафик Разрешать TCP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт **{0-65535}** и удаленный порт **{0-65535}**. Применять для **Пакетов существующих соединений**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.

	– Запрещать TCP пакеты для порта 135 Запрещать TCP-пакеты , с адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в **{135}** , а удаленный порт находится в **{0-65535}** . Применять ко **всем пакетам**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты объемом **<пустые>** с маской **<пустые>** оффсет **0**. – Отслеживание конформного TCP трафика Разрешать TCP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт **{0-65535}** и удаленный порт **{0-65535}**. Применять к **началу установления соединения и к пакетам существующих соединений. Не сохранять в файл отчета**, если пакет соответствует правилу.	

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

TCP-пакеты разрешать / запрещать

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Локальные порты

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

Удаленные порты

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

Метод применения

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

Файл отчета

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

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

Фильтрация по содержимому: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Здесь Вы можете указать специальную маску.

Фильтрация по содержимому: оффсет

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

Предустановленные правила мониторинга UDP-трафика

Установка: Низкий	Установка: Средний	Установка: Высокий
-	– Отслеживание конформного UDP трафика Разрешать UDP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт **{0-65535}** и удаленный порт **{0-65535}**. Применять правило к **открытым портам**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской	Отслеживать разрешенный UDP-трафик Разрешать UDP-пакеты , с адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в **{0-65535}** а удаленный порт находится в**{53, 67, 68, 123}**. Применять правило к **открытым портам**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.

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

Разрешать / запрещать UDP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Локальные порты

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

Удаленные порты

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

Метод применения

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

Файл отчета

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

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

Фильтрация по содержимому: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Здесь Вы можете указать специальную маску.

Фильтрация по содержимому: оффсет

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

Предустановленные правила мониторинга ICMP-трафика

Установка: Низкий	Установка: Средний	Установка: Высокий
-	– Не отклонять ICMP-пакеты на основании IP-адреса Разрешать ICMP-пакеты от адреса **0.0.0.0** с маской **0.0.0.0**. **Не сохранять в файл отчета**, если пакет соответствует правилу. Расширенный: Отклонять пакеты следующего объема **<пустые>** с маской **<пустые>** оффсет **0**.	Правило, аналогичное установке "Средний".

Разрешать / запрещать ICMP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Файл отчета

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

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

Фильтрация по содержимому: данные

Здесь Вы можете выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Здесь Вы можете указать специальную маску.

Фильтрация по содержимому: оффсет

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

Предустановленное правило для IP-пакетов

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

Разрешать / запрещать IP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Файл отчета

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

Возможные правила мониторинга IP-пакетов на основании IP-протоколов

IP-пакеты

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

IP-адрес

Здесь Вы можете указать желаемый IP-адрес.

IP-маска

Здесь Вы можете указать желаемую IP-маску.

Протокол

Здесь Вы можете выбрать желаемый IP-протокол.

Файл отчета

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

12.5.2.2. Исходящие правила

Посредством исходящих правил Avira FireWall контролирует исходящий трафик. Вы можете различать исходящие правила для следующих протоколов: IP, ICMP, UDP и TCP.

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

Кнопки

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

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

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

12.5.3 Список приложений

В окне "Список приложений" Вы можете создать правила сетевого доступа для приложений. Вы можете добавлять приложения к списку и с помощью контекстного меню устанавливать правила *Разрешить* и **Заблокировать** для выбранного приложения:

- Сетевой доступ для приложений с правилом *Разрешить* допускается.

– Сетевой доступ для приложений с правилом *Заблокировать* запрещается.

При добавлении приложений устанавливается правило *Разрешить*.

Список приложений

Здесь отображается список приложений, для которых определены правила. Символы показывают, разрешается или блокируется сетевой доступ для приложений. Вы можете изменять правила для приложений с помощью контекстного меню.

Кнопки

Кнопка	Описание
Добавление с проверкой пути	При помощи кнопки открывается диалоговое окно, в котором Вы можете выбрать приложения. Приложение добавляется к списку приложений с правилом "**Разрешить сетевой доступ**". Если активирована опция "**Добавление с проверкой пути"** добавляемое приложение идентифицируется компонентом FireWall по пути и по имени файла. Правила для приложения остаются действительными и применяются компонентом FireWall, даже если содержимое внесенного исполняемого файла изменилось, например, при обновлении.
Добавление с проверкой md5	При помощи кнопки открывается диалоговое окно, в котором Вы можете выбрать приложения. Приложение добавляется к списку приложений с правилом "**Разрешить сетевой доступ**". Если активирована опция "**Добавление с проверкой md5",** все добавляемые приложения однозначно идентифицируются по контрольной сумме MD5. Это позволяет FireWall выявлять изменения содержимого файлов. Если приложение изменяется, например, в связи с обновлением, то приложение с установленным правилом автоматически удаляется из списка. После изменения приложение вновь необходимо добавлять к списку и заново устанавливать необходимое правило.
Добавить группу	При помощи кнопки открывается диалоговое окно, в котором Вы можете выбрать каталог. Все приложения для выбранного пути добавляются к списку приложений с правилом "**Разрешить сетевой доступ**".
Удалить	Удаление выбранного правила приложения.
Удалить все	Удаление всех правил приложения.

12.5.4 Надежные разработчики

В разделе *Надежные разработчики* показывается список надежных производителей программного обеспечения. Сетевой доступ для приложений от включенных в список разработчиков программного обеспечения допускается. Вы можете удалять производителей из списка и включать их в список.

Производители

Список показывает всех производителей, которые классифицируются как надежные.

Кнопки

Кнопка	Описание
Добавить	При помощи кнопки открывается диалоговое окно, в котором Вы можете выбрать приложения. Производитель приложения устанавливается и добавляется к списку надежных разработчиков.
Добавить группу	При помощи кнопки открывается диалоговое окно, в котором Вы можете выбрать каталог. Производители всех приложений для выбранного пути устанавливаются и добавляются к списку надежных разработчиков.
Удалить	Отмеченная запись удаляется из списка надежных разработчиков. Чтобы окончательно удалить выбранного разработчика из списка, нажмите "**Применить**" или "**OK**" в окне настройки.
Удалить все	Все записи удаляются из списка надежных разработчиков.
Обновить	Изменения отменяются. Последний сохраненный список загружается.

Примечание
Если Вы удалите разработчика из списка, а затем нажмете кнопку **Применить**, разработчики окончательно удаляются из списка. Изменение не может быть отменено командой *Обновить*.

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

12.5.5 Дополнительные настройки

Уведомления

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

Port-Scan

При включенной опции вы получаете уведомление в виде всплывающего окна, если FireWall распознал Port Scan.

Флудинг

При включенной опции вы получаете уведомление в виде всплывающего окна, если FireWall распознал флуд-атаку.

Приложения были блокированы

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

IP блокирован

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

Настройки всплывающего окна

Проверить стартовый блок процесса

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

Показывать несколько диалоговых окон для процесса

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

Автоматически подавлять всплывающее уведомление в игровом режиме

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

12.5.6 Настройки отображения

Сохранять действие для приложения

Всегда вкл.

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

Всегда откл.

Если опция включена, неактивна опция "**Сохранять действие для приложения**" диалогового окна "**Сетевое событие**".

Разрешать подписанные приложения

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

Запомнить последнее состояние

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

Отображать подробности

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

Отображать подробности по запросу

Если опция включена, в окне "*Сетевое событие",* информация отображается только по запросу, т. е. отображение подробной информации осуществляется после нажатия кнопки "**Подробности"** в окне "*Сетевое событие"*.

Всегда отображать подробности

Если опция включена, подробности всегда отображаются в окне "*Сетевое событие"*.

Запомнить последнее состояние

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

Разрешать привилегированные

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

Всегда вкл.

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

Всегда откл.

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

Запомнить последнее состояние

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

12.6 WebGuard

Раздел WebGuard в настройке отвечает за настройку защиты WebGuard.

12.6.1 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.

12.6.1.1. 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.

Разрешенные действия

В этом окне Вы имеете возможность выбрать действия, которые могут быть выполнены при обнаружении вируса или вредоносной программы. Для этого должны быть активированы соответствующие опции.

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.

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.

По умолчанию

Кнопка позволяет выбрать действие, которое активно по умолчанию в случае обнаружения вируса. Выделите действие, которое должно быть по умолчанию активно, и нажмите кнопку "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.

Показывать предупреждения

Если опция включена, при обнаружении вируса или вредоносной программы отображается предупреждение с предложением выбора действий.

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!

12.6.1.2. Запрет доступа

В пункте **Запрет доступа** Вы можете указывать типы файлов и MIME (типы содержимого передаваемых данных), которые будет блокироваться WebGuard. С помощью веб-фильтра можно заблокировать известные нежелательные URL, например, URL фишинг-программ или вредоносных программ. WebGuard препятствует передаче данных из Интернет на Ваш компьютер.

Блокируемые WebGuard типы данных / MIME (по выбору)

WebGuard блокирует все приведенные в списке типы данных и MIME (типы содержимого переданных файлов).

Поле ввода

Здесь укажите типы MIME и файлов, которые должен блокировать WebGuard. Для типов файлов указывайте расширения, например, **htm**. Укажите тип и подтип MIME. Тип и подтип отделяются друг от друга обычной косой чертой, например, **video/mpeg** или **audio/x-wav**.

Примечание
Файлы, которые уже сохранены на Вашем компьютере как временные Интернет-файлы, хотя и блокируются WebGuard, но могут быть загружены локально из Интернет-браузера. Временные Интернет-файлы - это файлы, которые сохраняются Интернет-браузером для более быстрой загрузки веб-страниц.

Примечание
Список блокируемых типов файлов / MIME игнорируется, если имеются строки в списке исключений из проверки типов файлов и MIME в WebGuard::Проверка::Исключения.

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

MIME-типы: Примеры медиа-типов:

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

Примеры: Непроверяемые типы файлов и MIME

- `application/octet-stream` = файлы MIME-типа application/octet-stream (исполняемые файлы *.bin, *.exe, *.com, *dll, *.class) блокируются WebGuard.
- `application/olescript` = файлы MIME-типа application/olescript (скрипт-файлы ActiveX Skript*.axs) блокируются WebGuard.
- `.exe` = все файлы с расширением .exe (исполняемые файлы) блокируются WebGuard.
- `.msi` = все файлы с расширением .msi (файлы Windows Installer) блокируются WebGuard.

Добавить

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

Удалить

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

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.

12.6.1.3. 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 запрета доступа (список блокируемых типов файлов и MIME в WebGuard::Проверка::Запрет доступа) или WebGuard загружены в Интернет-браузер: При наличии позиций в списке исключений игнорируется список блокируемых типов файлов и MIME. Поиск на наличие вирусов и вредоносного ПО не производится.

MIME-типы: Примеры 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 URLс доменом второго уровня 'avira' исключаются из проверки WebGuard. Данные включают все существующие домены первого уровня и поддомены к '.avira.': www.avira.com, www.avira.de, forum.avira.com,...

- `.*domain*.*`

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

- `net` -ИЛИ- `*.net`

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

Предупреждение
Вводите адреса URL, которые Вы хотите исключить из проверки WebGuard, 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

12.6.1.4. 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.

12.6.2 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. Место сохранения см. Настройка :: Общее :: Папки :: Папка для отчетов.

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.

12.7 Обновление

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

Примечание
Если вы настраиваете программу в AntiVir Security Management Center, настройка автоматического обновления недоступна.

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.

Дополнительно запускать задачу при подключении к Интернету (через модем)

Если эта опция включена, в дополнение к установленному интервалу для обновлений выполняется обновление при каждом установленном интернет-соединении.

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.

Загрузить

С веб-сервера

Обновление осуществляется с веб-сервера через HTTP-соединение. Вы можете использовать веб-сервер производителя в Интернете или веб-сервер в Интранете, который загружает файлы обновлений с сервера загрузки производителя в Интернете.

Примечание
Другие установки для обновления с использованием веб-сервера Вы найдете в разделе: Настройка :: Общее :: Обновление:: Веб-сервер .

Через файловый сервер / общие папки

Обновление осуществляется через файловый сервер в Интранете, который загружает файлы обновлений с сервера загрузки производителя в Интернете.

Примечание
Другие установки для обновления с использованием файлового сервера Вы найдете в разделе: Настройка :: Общее :: Обновление:: Файловый сервер .

12.7.1 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.

12.7.2 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.

12.7.3 Файловый сервер

Если несколько компьютеров объединены в сеть, программа AntiVir может загружать обновление с файлового сервера в Интранете, который, в свою очередь, загружает файлы обновления с сервера загрузки производителя в Интернете. Это позволяет поддерживать на всех компьютерах самый современный уровень программы AntiVir, экономя ресурсы.

Примечание
Раздел настройки активен только тогда, когда в Настройка:: Обновление:: Обновление продукта выбрана опция **Через файловый сервер / Общие папки**.

Загрузка

Укажите файловый сервер, на котором находятся файлы обновления программы AntiVir, а также необходимые папки '/release/update/'. Следующие сведения обязательны: file://<IP-адрес файлового сервера>/release/update/. Каталог 'release' должен быть папкой, доступной для всех пользователей.

...

Нажатием на кнопку открывается окно, в котором можно выбрать нужную папку для загрузки.

Сервер Логин

Имя пользователя

Введите имя пользователя для входа на сервер. Используйте учетную запись с правами доступа к используемой общей папке на сервере.

Логин Пароль

Укажите пароль для выбранной учетной записи. Вводимые символы скрываются при помощи *.

Примечание
Если в поле Сервер Логин не будут введены данные, то при доступе к файловому серверу аутентификация на файловом сервере выполняться не будет. В этом случае у Вас должны быть достаточные права пользователя для работы на файловом сервере.

12.7.4 Веб-сервер

Обновление можно выполнить непосредственно через веб-сервер в Интернете или во внутренней сети.

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 .

Загрузка

Стандартный сервер

Укажите адреса (URL) веб-серверов, с которых необходимо загрузить обновления, а также необходимые папки обновлений 'update'. Действительны следующие данные веб-сервера. http://<адрес веб-сервера>[:Port]/update. Если Вы не укажете порт, будет использоваться порт 80. По умолчанию для обновления указаны доступные веб-серверы Avira GmbH. Однако Вы можете также использовать собственные веб-серверы, например, в Интранете. При указании нескольких северов, серверы разделяются запятыми.

По умолчанию

Эта кнопка позволяет восстановить предустановленные адреса.

Приоритетный сервер

Укажите в этом поле адрес (URL) веб-сервера, который должен запрашиваться при получении обновлений в первую очередь, а также необходимую папку обновлений. Если этот сервер недоступен, будут запрошены указанные стандартные серверы. Действительны следующие данные веб-сервера: http://<адрес веб-сервера>[:Port]/update. Если Вы не укажете порт, будет использоваться порт 80.

12.7.4.1. 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

12.8 Общее

12.8.1 Email

При наступлении определенных событий программа AntiVir может отправлять по электронной почте предупреждения и сообщения одному или нескольким получателям. Для этого используется Simple Message Transfer Protocol (SMTP).

Сообщения могут быть инициированы разными событиями. Следующие компоненты поддерживают отправку электронных писем:

- Guard: Отправка уведомлений
- Scanner: Отправка уведомлений
- Программа обновлений: Отправка уведомлений

Примечание
Помните о том, что ESMTP не поддерживается. Кроме того, закодированная передача по TLS (Transport Layer Security) или SSL (Secure Sockets Layer) в настоящее время невозможна.

Сообщения электронной почты

SMTP-сервер

Укажите здесь имя или IP-адрес, или прямое имя хоста для используемого хоста.
Максимально возможная длина имени хоста составляет 127 знаков.

Например:

192.168.1.100 или mail.firma.ru.

Адрес отправителя

Укажите в этом поле адрес электронной почты отправителя. Адрес отправителя не должен превышать 127 знаков.

Аутентификация

Некоторые почтовые серверы ожидают, что программа перед отправкой электронного письма пройдет аутентификацию (регистрацию) на сервере. Предупреждения по электронной почте могут передаваться одновременно с аутентификацией на SMTP-сервере.

Использовать аутентификацию

Если эта функция включена, то для аутентификации (регистрации) в соответствующем поле можно указать имя пользователя и пароль.

- **Имя пользователя**: Укажите здесь Ваше имя пользователя.
- **Пароль**: Укажите здесь соответствующий пароль. Пароль сохраняется в закодированном виде. Для безопасности вводимые в это поле знаки заменяются звездочками (*).

Отправить тестовое письмо

После нажатия на эту кнопку программа пытается отправить на адрес отправителя тестовое письмо для проверки введенных данных.

12.8.2 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.

12.8.3 Пароль

Вы можете защитить паролем разные разделы программы AntiVir. В этом случае пароль будет запрашиваться каждый раз при попытке открыть защищенную область.

Пароль

Введите пароль

Введите Ваш пароль. Для безопасности вводимые в это поле знаки заменяются звездочками (*). Вы можете ввести не более 20 символов. После первого ввода пароля программа блокирует доступ при указании неправильного пароля. Пустое поле означает "Без пароля".

Подтвердите пароль

Введите здесь повторно указанный выше пароль для его подтверждения. Для безопасности вводимые в это поле знаки заменяются звездочками (*).

Примечание
Большие и маленькие буквы различаются!

Разделы, защищенные паролем

Можно защитить паролем отдельные разделы программы AntiVir. Щелчком по соответствующему флажку можно по желанию включить или выключить запрос пароля.

Защищенный паролем модуль	Функция
Центр контроля	Если опция включена, для запуска Control Center

	требуется установленный пароль.
Включить / отключить Guard	Если опция включена, для включения и отключения AntiVir Guard требуется пароль.
Включить / отключить MailGuard	Если опция включена, для включения и отключения MailGuard требуется пароль.
Включить / отключить Firewall	Есть опция включена, для включения и отключения FireWall требуется пароль.
Включить / отключить WebGuard	Если опция включена, для включения и отключения WebGuard требуется пароль.
Загрузить Rescue-CD из Интернет	Если опция включена, для запуска загрузки Avira Rescue-CD требуется пароль.
Карантин	Если опция включена, активируются все разделы менеджера карантина, которые могут быть защищены паролем. Щелчком в определенном поле можно активировать или деактивировать запрос пароля.
Восстановление инфицированных объектов	Если опция включена, для восстановления объектов требуется пароль.
Повторная проверка затронутых объектов	Если опция включена, для новой проверки объектов требуется пароль.
Свойства поврежденных объектов	Если эта опция включена, то для просмотра свойств объекта необходим пароль.
Удаление поврежденных объектов	Если эта опция включена, то для удаления объекта необходим пароль.
Отправить электронное письмо в компанию Avira	Если эта опция включена, то для отправки объекта для проверки в Avira Malware Research Center требуется пароль.
Копирование поврежденных объектов	Если опция включена, то для копирования поврежденных объектов требуется пароль.
Добавление и изменение заданий	Если опция включена, то для добавления и изменения задач в Планировщике требуется пароль.
Запустить обновление продукта	Если опция включена, то при запуске обновления продукта требуется ввести пароль в меню Обновление.
Настройка	Если опция включена, то настройка программы возможна только после ввода пароля.

Ручное переключение настроек	Если опция включена, то для ручного переключения профиля настроек требуется пароль.
Режим эксперта	Если опция включена, то для активации режима эксперта требуется пароль.
Установка / Удаление	Если опция включена, то для установки, включения и отключения программы требуется пароль.

12.8.4 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 !

12.8.5 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 и методы (запуск и останов процессов) . С помощью WMI можно вызывать оперативные данные программы и управлять программой . Полную информацию об интерфейсе WMI можно запросить у изготовителя. После подписания соглашения о конфиденциальности Вы получите справку в формате PDF.

Активировать WMI-поддержку

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

Разрешить включение / выключение служб

Если эта опция включена, вы можете включить и выключить через WMI службы программы .

12.8.6 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.

Папка для отчетов

В этом поле ввода указан путь к папке отчета.

Нажатием на кнопку открывается окно, в котором можно выбрать нужную папку.

По умолчанию

Нажатием на эту кнопку восстанавливается предустановленный путь к папке отчета.

Папка карантина

Это поле содержит путь к папке карантина.

Нажатием на кнопку открывается окно, в котором можно выбрать нужную папку.

По умолчанию

Нажатием на эту кнопку восстанавливается предустановленный путь для папки карантина.

12.8.7 Предупреждения

12.8.7.1. Сеть

Вы можете отправить любые сконфигурированные Вами сообщения от Scanner или от Guard на любой компьютер Вашей сети.

Примечание
Проверьте, запущена ли "Служба уведомлений". Эту службу Вы найдете (на примере Windows XP) здесь: "Пуск | Настройка | Панель управления | Администрирование | Службы".

Примечание
Предупреждение всегда отправляется на компьютер, а НЕ определенному пользователю.

Предупреждение
Функция больше не поддерживается следующими операционными системами:
Windows Server 2008 и выше
Windows Vista и выше

Сообщение отправлять

Список в данном окне содержит имена компьютеров, получающих уведомления при обнаружении подозрительных объектов.

Примечание
Компьютер можно внести в список только один раз.

Добавить

С помощью этой кнопки Вы можете добавлять компьютеры. Открывается окно, в которое можно добавлять имена новых компьютеров. Длина имени компьютера не может превышать 15 знаков.

Эта кнопка открывает окно, в котором Вы можете выбрать компьютер непосредственно из Вашего сетевого окружения.

Удалить

С помощью этой кнопки Вы можете удалить из списка выделенную строку.

Guard

Сетевые предупреждения

Если эта опция включена, отправляются сетевые уведомления. По умолчанию эта опция отключена.

Примечание
Для активации этой опции в Общее :: Предупреждения :: Сеть должен быть зарегистрирован хотя бы один получатель.

Отправляемое сообщение

Окно показывает сообщение, отправляемое при обнаружении вируса или вредоносной программы. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующие комбинации клавиш используются для форматирования сообщения:

Strg + Tab	вставляет табулятор. Эта строка сдвигается на несколько символов вправо.
Strg + Enter	вставляет разрыв строки.

Сообщение может также содержать символы-заполнители для полученной во время проверки информации. Эти символы-заполнители заменяются при отправке текстом.

Применяются следующие символы-заполнители:

%VIRUS%	содержит имя обнаруженного вируса или нежелательной программы
%FILE%	содержит путь и имя инфицированного файла
%COMPUTER%	содержит имя компьютера, на котором запущен Guard
%NAME%	содержит имя пользователя, обращавшегося к инфицированному файлу
%ACTION%	содержит действие, выполненное после обнаружения вируса
%MACADDR%	содержит MAC-адрес компьютера, на котором запущен Guard

По умолчанию

Кнопка восстанавливает предустановленный стандартный текст для предупреждающего сообщения.

Сканер

Включить сетевые предупреждения

Если эта опция включена, отправляются сетевые уведомления. По умолчанию эта опция отключена.

Примечание
Для активации этой опции в Общее :: Предупреждения :: Сеть должен быть зарегистрирован хотя бы один получатель.

Отправляемое сообщение

Окно показывает сообщение, отправляемое при обнаружении вируса или вредоносной программы. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующие комбинации клавиш используются для форматирования сообщения:

Strg + Tab	вставляет табулятор. Эта строка сдвигается на несколько символов вправо.
Strg + Enter	вставляет разрыв строки.

Сообщение может также содержать символы-заполнители для полученной во время проверки информации. Эти символы-заполнители заменяются при отправке текстом.

Применяются следующие символы-заполнители:

%VIRUS%	содержит имя обнаруженного вируса или нежелательной программы
%NAME%	содержит имя зарегистрированного пользователя, запустившего Scanner

По умолчанию

Кнопка восстанавливает предустановленный стандартный текст для предупреждающего сообщения.

12.8.7.2. Email

Email

При наступлении определенных событий программа AntiVir может отправлять по электронной почте предупреждения и сообщения одному или нескольким получателям. Для этого используется Simple Message Transfer Protocol (SMTP).

Сообщения могут быть инициированы разными событиями. Следующие компоненты поддерживают отправку электронных писем:

- Guard: Отправка уведомлений
- Scanner: Отправка уведомлений
- Программа обновлений: Отправка уведомлений

Примечание
Помните о том, что ESMTP не поддерживается. Кроме того, закодированная передача по TLS (Transport Layer Security) или SSL (Secure Sockets Layer) в настоящее время невозможна.

Сообщения электронной почты

SMTP-сервер

Укажите здесь имя или IP-адрес, или прямое имя хоста для используемого хоста.
Максимально возможная длина имени хоста составляет 127 знаков.

Например:

192.168.1.100 или mail.firma.ru.

Адрес отправителя

Укажите в этом поле адрес электронной почты отправителя. Адрес отправителя не должен превышать 127 знаков.

Аутентификация

Некоторые почтовые серверы ожидают, что программа перед отправкой электронного письма пройдет аутентификацию (регистрацию) на сервере. Предупреждения по электронной почте могут передаваться одновременно с аутентификацией на SMTP-сервере.

Использовать аутентификацию

Если эта функция включена, то для аутентификации (регистрации) в соответствующем поле можно указать имя пользователя и пароль.

- **Имя пользователя**: Укажите здесь Ваше имя пользователя.
- **Пароль**: Укажите здесь соответствующий пароль. Пароль сохраняется в закодированном виде. Для безопасности вводимые в это поле знаки заменяются звездочками (*).

Отправить тестовое письмо

После нажатия на эту кнопку программа пытается отправить на адрес отправителя тестовое письмо для проверки введенных данных.

Guard

AntiVir Guard может при наступлении определенных событий высылать по электронной почте уведомление одному или нескольким пользователям.

Guard

Уведомления по электронной почте

Если эта опция включена, AntiVir Guard при наступлении определенных событий отправляет сообщения электронной почты с основными данными о них. По умолчанию эта опция отключена.

Уведомление по электронной почте при наступлении следующих событий

При проверке системы сканером обнаружен вирус или вредоносная программа.

Если эта опция активна, Вы получаете по электронной почте сообщение с именем вируса или вредоносной программы, а также с именем инфицированного файла в случае обнаружения службой Постоянной защиты таких объектов.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором Вы можете редактировать сообщение для события "Обнаружение вируса службой постоянной защиты". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Электронная почта::Уведомления::Шаблон письма).

Возникновение критической ошибки Guard.

Если эта опция включена, вы получаете по электронной почте уведомление о возникновении критической ошибки.

Примечание
В этом случае свяжитесь с нашей службой Технической поддержки и отправьте ей данные, содержащиеся в Email-уведомлении. Указанный файл также необходимо выслать для проверки.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором Вы можете редактировать сообщение для события "Критическая ошибка в Guard". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Уведомления::Электронная почта::Шаблон письма).

Получатель

В этом поле укажите адрес(а) электронной почты получателя(ей). Адреса разделяются между собой запятыми. Максимальная совокупная длина всех адресов не может превышать 260 знаков.

Сканер

Осуществляя прямую проверку, то есть поиск по требованию, программа может отправлять по электронной почте предупреждения одному или нескольким получателям при наступлении определенных событий.

Сканер

Включить предупреждения по электронной почте

Если эта опция включена, программа при наступлении определенных событий отправляет сообщения электронной почты с основными данными о них. По умолчанию эта опция отключена.

Уведомление по электронной почте при наступлении следующих событий
В результате проверки бы обнаружен вирус или вредоносная программа.

Если эта опция включена, вы получите электронное письмо с названием вируса или вредоносной программы и инфицированного файла в случае, если в результате проверки были обнаружены такие объекты.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором Вы можете редактировать сообщение для события "Обнаружение вируса при поиске". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Уведомления::Электронная почта::Шаблон письма).

Окончание плановой проверки.

При включенной опции отправляется электронное письмо, уведомляющее о выполнении задачи проверки. Электронное письмо содержит данные о времени и продолжительности проверки, именах папок и файлов, а также об обнаруженных вирусах и предупреждениях.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором вы можете редактировать сообщение для события "Завершение проверки". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Уведомления::Электронная почта::Шаблон письма).

Прикрепить файл отчета как приложение

Если эта опция включена, при отправке уведомлений Scanner текущий файл отчета компонента Scanner прикрепляется к электронному письму в качестве приложения.

Адрес(а) получателя(ей)

В этом поле укажите адрес(а) электронной почты получателя(ей). Адреса разделяются между собой запятыми. Максимальная совокупная длина всех адресов не может превышать 260 знаков.

Программа обновлений

Компонент Программа обновлений может при наступлении определенных событий направлять сообщения по электронной почте одному или нескольким получателям.

Программа обновлений

Уведомления по электронной почте

Если опция включена, компонент Программа обновлений при наступлении определенных событий отправляет по электронной почте сообщения с важнейшими данными. Опция отключена по умолчанию.

Уведомления по электронной почте при наступлении следующих событий

Обновление не требуется. Ваша программа имеет самую последнюю версию.

Если опция включена, отправляется письмо при успешном создании программой обновлений соединения с сервером, но в случае отсутствия на нем новых файлов для загрузки. Это означает, что программа AntiVir имеет самую последнюю версию.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором вы можете редактировать сообщение для события "Обновление не требуется". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Уведомления::Электронная почта::Шаблон письма).

Обновление успешно завершено. Установлены новые файлы.

Если опция включена, при каждом обновлении отправляется письмо: Это касается обновлений продукта, обновлений файлов определения вирусов или поисковой машины.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором Вы можете редактировать сообщение для события "Обновление успешно завершено - Установка новых файлов". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Уведомления::Электронная почта::Шаблон письма).

Обновление успешно завершено. Имеется обновление продукта.

Если опция включена, письмо отправляется только в том случае, если обновление поискового движка или файла определения вирусов было выполнено без обновления продукта, при этом, однако, имеется обновление продукта.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором вы можете редактировать сообщение для события "Обновление успешно завершено - Имеется обновление продукта". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Уведомления::Электронная почта::Шаблон письма).

Не удалось выполнить обновление.

Если эта опция активирована, отправляется электронное сообщение, с информацией о том, что обновление не состоялось в связи с ошибкой.

Редактировать

При помощи кнопки "*Редактировать"* открывается окно "*Шаблон письма"*, в котором вы можете редактировать сообщение для события "Не удалось выполнить обновление". Вы можете ввести тексты для темы и содержания электронного письма. При этом Вы можете использовать переменные (см. Настройка::Общее::Уведомления::Электронная почта::Шаблон письма).

Прикрепить файл отчета как приложение

Если эта опция включена, при отправке уведомлений программы обновлений текущий файл отчета компонента Программа обновлений прикрепляется к электронному письму в качестве приложения.

Получатель

В этом поле укажите адрес(а) электронной почты получателя(ей). Адреса разделяются между собой запятыми. Максимальная совокупная длина всех адресов не может превышать 260 знаков.

Примечание
При наступлении следующих событий всегда рассылаются предупреждения по электронной почте, если SMTP-сервер и адрес получателя настроены для уведомлений программы обновлений.
Для дальнейших обновлений программы требуется обновить продукт.
Не удалось обновить поисковый движок или файл определения вирусов, так как требуется обновление продукта.

Отправление этих предупреждений производится независимо от Ваших настроек предупреждений по электронной почте компонента Программа обновлений.

Шаблон письма

В окне *Шаблон письма* сконфигурируйте уведомления по электронной почте от отдельных компонентов в связи с активированными событиями. Длина текста в строке темы не должна превышать 128 символов, а длина текста в поле сообщения должна составлять не более 1024 символов.

В теме электронного письма и в тексте сообщения электронной почты могут содержаться следующие переменные:

Общепринятые переменные

Переменные	Значение

Переменные окружения Windows	Компонент уведомлений по электронной почте поддерживает все переменные окружения Windows.
%SYSTEM_IP%	IP-адрес компьютера
%FQDN%	Полное имя домена (fully qualified domain name)
%TIMESTAMP%	Время события: Форматы даты и времени соответствуют языковым настройкам операционной системы
%COMPUTERNAME%	Имя компьютера NetBIOS
%USERNAME%	Имя пользователя, имеющего доступ к компоненту
%PRODUCTVER%	Версия продукта
%PRODUCTNAME%	Название продукта
%MODULENAME%	Название компонента, отправляющего сообщение электронной почты
%MODULEVER%	Версия компонента, отправляющего сообщение электронной почты

Специфические переменные компонентов

Переменные	Значение	Электронные сообщения компонентов
%ENGINEVER%	Версия используемого поискового движка	Guard Scanner
%VDFVER%	Версия используемого файла определения вирусов	Guard Scanner
%SOURCE%	Полное имя файла	Guard
%VIRUSNAME%	Имя вируса или вредоносной программы	Guard
%ACTION%	Действие, выполняемое после обнаружения вируса	Guard
%MACADDR%	MAC-адрес зарегистрированной сетевой карты	Guard
%UPDFILESLIST%	Список обновленных файлов	Программа обновлений

%UPDATETYPE%	Тип обновления: Обновление поискового движка и файла определения вирусов или обновление продукта с обновлением поискового движка и файла определения вирусов	Программа обновлений
%UPDATEURL%	URL сервера, использованного для обновления	Программа обновлений
%UPDATE_ERROR%	Ошибка обновления в словах	Программа обновлений
%DIRCOUNT%	Проверено папок	Сканер
%FILECOUNT%	Проверено файлов	Сканер
%MALWARECOUNT%	Обнаружено вирусов или вредоносных программ	Сканер
%REPAIREDCOUNT%	Вылечено инфицированных файлов	Сканер
%RENAMEDCOUNT%	Переименовано инфицированных файлов	Сканер
%DELETEDCOUNT%	Удалено инфицированных файлов	Сканер
%WIPECOUNT%	Количество инфицированных файлов, которые были перезаписаны и удалены	Сканер
%MOVEDCOUNT%	Количество инфицированных файлов, помещенных в карантин	Сканер
%WARNINGCOUNT%	Число предупреждений	Сканер
%ENDTYPE%	Статус завершения проверки: Прервана | Успешно завершена	Сканер

%START_TIME%	Время начала проверки Время начала обновления	Scanner Программа обновлений
%END_TIME%	Окончание проверки Окончание обновления	Scanner Программа обновлений
%TIME_TAKEN%	Время выполнения проверки в минутах Время выполнения обновления в минутах	Scanner Программа обновлений
%LOGFILEPATH%	Путь и имя файла отчета	Scanner Программа обновлений

12.8.7.3. 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. Режим Guard устанавливается в настройках в разделе Guard::Поиск::Действия при обнаружении.

Нет предупреждения

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

Воспроизводить через громкоговоритель компьютера (только при интерактивном режиме)

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

Использовать следующие 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.

12.8.7.4. 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.

12.8.8 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.

12.8.9 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.

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