Avira Internet Security

Руководство пользователя

AVIRA

Торговые марки и авторское право

Торговые марки

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 торговые марки не отмечены в этом Руководстве соответствующим образом. Но это не означает, что их можно использовать без разрешения.

Информация об авторских правах

Для Avira Internet Security используется код другой компании. Мы благодарим обладателей авторских прав за предоставленный в наше распоряжение код.
Подробную информацию об авторском праве Вы можете найти в разделе справки Avira Internet Security в пункте "Лицензии третьих лиц".

Содержание

1. Введение

Продукт Avira защищает ваш компьютер от вирусов, червей, троянов, вредоносного и шпионского ПО и других опасностей. В настоящем руководстве дается краткая информация о вирусах, вредоносном ПО и нежелательных программах.

В руководстве описываются установка и обслуживание программы.

На нашем сайте предложены многочисленные опции и приведена дополнительная информация:

http://www.avira.ru

На сайте Avira можно:

- просмотреть информацию о других программах Avira для персональных компьютеров
- загрузить новейшие версии программ Avira для персональных компьютеров
- загрузить новейшие версии руководств по работе с продуктами в формате PDF
- загрузить бесплатные инструменты поддержки и восстановления
- воспользоваться обширной базой знаний и статьями из раздела "Часто задаваемые вопросы" для устранения проблем
- получить адреса службы поддержки в своем регионе.

Ваши сотрудники компании Avira

1.1 Символы и способы выделения

Используются следующие символы:

Символ / Обозначение	Объяснение
✓	Обозначает условие, которое необходимо для выполнения действия.
▸	Обозначает этап действия, которое вы выполняете.
↪	Обозначает результат выполненного действия.
Предупреждение	Обозначает предупреждение о возможности критической потери данных.

Примечание	Обозначает примечание, содержащее особо важную информацию, или рекомендацию по использованию продукта Avira.

Используются следующие способы выделения:

Способ выделения	Объяснение
Курсив	Имя или путь файла.
	Отображаемые элементы интерфейса (например, области окон или сообщения об ошибках).
Жирный	Элементы интерфейса, выбранные щелчком мыши, (например, пункты меню, разделы, поля опций или кнопки).

2. Информация о продукте

В этой главе содержится информация о приобретении и использовании продукта Avira:

- см. главу: Объем услуг
- см. главу: Системные требования
- см. главу: Лицензирование и обновление
- см. главу: Менеджер лицензий

Продукты Avira предоставляют широкий спектр гибких инструментов для надежной защиты вашего компьютера от вирусов, вредоносных и нежелательных программ и от других опасностей.

▸ Обратите внимание:

Предупреждение
Потеря ценных данных может иметь серьезные последствия. Даже самая лучшая антивирусная программа не может полностью защитить вас от потери данных. Регулярно создавайте резервные копии своих данных.

Указание
Программа, защищающая от вирусов, вредоносных, нежелательных программ и других опасностей, считается надежной и эффективной, только если она регулярно обновляется. Позаботьтесь об актуальности продукта Avira с помощью автоматического обновления. Настройте программу соответствующим образом.

2.1 Объем функций

Ваш продукт Avira имеет следующие функции:

- Центр управления для контроля, администрирования и управления всей программой
- Централизованная настройка в стандартном и экспертном режимах с контекстной Справкой
- System Scanner (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

- Real-Time Protection (On-Access Scan) для постоянного отслеживания попыток доступа к файлам
- Компонент ProActiv для постоянного контроля за действиями программ (только для 32-битных систем)
- Mail Protection (POP3-сканер, IMAP-сканер и SMTP-сканер) для постоянной проверки электронной почты на наличие вирусов и вредоносных программ, включая проверку вложений
- Avira SearchFree Toolbar, поисковая панель, встраиваемая в веб-браузер, обеспечит быстрый и удобный поиск в Интернете. Она также содержит виджеты для основных функций при работе в Интернете.
- Web Protection для контроля данных и файлов, передаваемых из Интернета через HTTP-протокол (контроль портов 80, 8080, 3128)
- Компонент Child Protection для основанной на ролях фильтрации нежелательных веб-сайтов и для ограничения времени Интернет-доступа
- Avira Free Android Security - это приложение для защиты от кражи и/или утери. Приложение предоставляет функции, с помощью которого можно легко найти ваше мобильное устройство, если вы потеряли его или оно было украдено. Кроме того, приложение позволяет блокировать входящие выховы и SMS. Avira Free Android Security защищает мобильные телефоны и смартфоны, работающие на операционной системе Android.
- Backup-компонент для создания резервных копий данных (зеркальные копии)
- Встроенный менеджер карантина для изоляции подозрительных файлов и работы с ними
- Rootkits Protection для поиска вредоносных программ, скрыто установленных в системе компьютера (так наз. Rootkits) (недоступно для Windows XP 64 бита)
- Прямой доступ к подробной информации об обнаруженных вирусах и вредоносном ПО через 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
- 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 (Smart Extension)
- Высокая производительность многопоточной технологии (одновременное сканирование нескольких файлов)

- FireWall для защиты Вашего компьютера от несанкционированного доступа из сети Интернет или локальной сети, а также от несанкционированного доступа к сети Интернет/локальной сети

2.2 Системные требования

Предусмотрены следующие системные требования:

- Компьютер с процессором Pentium или выше, с тактовой частотой как минимум 1 ГГц
- Операционная система
  - Windows XP, последний SP (32 или 64 бита) или
  - Windows 7, последний SP (32 или 64 бита)

> **Указание**
> Сертифицирование Avira Internet Security для Windows 8 находится на стадии обработки.

- Не менее 150 Мб свободной памяти на жестком диске (при использовании Карантина и для временной памяти - больше)
- - Минимум 512 Мб ОЗУ для Windows XP
- - Минимум 1024 Мб ОЗУ для Windows 7
- Для установки программы: права администратора
- Для всех установок: Windows Internet Explorer 6.0 или выше
- При необходимости Интернет-соединение (см. Установка)

Avira SearchFree Toolbar

- Операционная система
  - Windows XP, последний SP (32 или 64 бита) или
  - Windows 7, последний SP (32 или 64 бита)
- Веб-браузер
  - Windows Internet Explorer 6.0 или выше
  - Mozilla Firefox 3.0 или выше
  - Google Chrome 18.0 или выше

> **Указание**
> При необходимости удалите установленные поисковые панели перед установкой Avira SearchFree Toolbar. В противном случае установка Avira SearchFree Toolbar невозможна.

Примечания для пользователей Windows Vista

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

По этой причине компания Microsoft в операционной системе Windows Vista ввела "Контроль учетных записей пользователей" (User Account Control). Он обеспечивает больше защиты для пользователей, работающих с правами администратора: в Windows Vista администратор обладает привилегиями обычного пользователя. Действия, для которых необходимы права администратора, Windows Vista четко выделяет специальным примечанием. Кроме того, пользователь должен явно подтверждать желаемое действие. Только после получения подтверждения производится повышение привилегий и операционная система выполняет задание администратора.

Продукт Avira для выполнения некоторых действий в Windows Vista требует права администратора. Эти действия обозначаются следующим символом:  . Если этот символ отображается на кнопке, для выполнения данного действия требуются права администратора. Если ваша текущая учетная запись не имеет прав администратора, то система управления учетными записями пользователей Windows Vista требует указания пароля администратора. Если у вас нет пароля администратора, вы не сможете выполнить требуемое действие.

2.3 Лицензирование и обновление

2.3.1 Лицензирование

Чтобы использовать ваш продукт Avira, вам необходима лицензия. Тем самым вы соглашаетесь с лицензионными условиями.

Лицензия выдается в форме кода активации. Код активации — это буквенно-цифровой код, который вы получили при приобретении продукта Avira. Код активации определяет точные параметры вашей лицензии — на какие программы предоставляется лицензия и каков срок ее действия.

Код активации высылается вам по электронной почте, если вы приобрели ваш продукт Avira в Интернете, или находится на упаковке продукта.

Чтобы лицензировать программу, укажите код активации в процессе активации программы. Активация продукта может быть выполнена во время установки. Однако вы также можете активировать ваш продукт Avira после его установки с помощью диспетчера лицензий в меню **Справка > Управление лицензиями**.

2.3.2 Продление лицензии

Если срок действия вашей лицензии вскоре истекает, Avira предложит продлить ее во всплывающем окне. Для этого необходимо перейти по ссылке в онлайн-магазин Avira. Однако вы также можете продлить лицензию на ваш продукт Avira с помощью диспетчера лицензий в меню **Справка > Управление лицензиями**.

Если вы зарегистрированы на портале лицензий Avira, вы также можете продлить лицензию в разделе **Обзор лицензий** или же выбрать автоматическое продление.

2.3.3 Обновление

В диспетчере лицензий также есть возможность обновления вашего продукта с его заменой на продукт из серии Avira Desktop: удаление старой версии и установка новой программы вручную не требуются. При обновлении из диспетчера лицензий в поле ввода необходимо ввести код активации программы, на которую вы хотите перейти. После этого будет выполнена автоматическая установка новой программы.

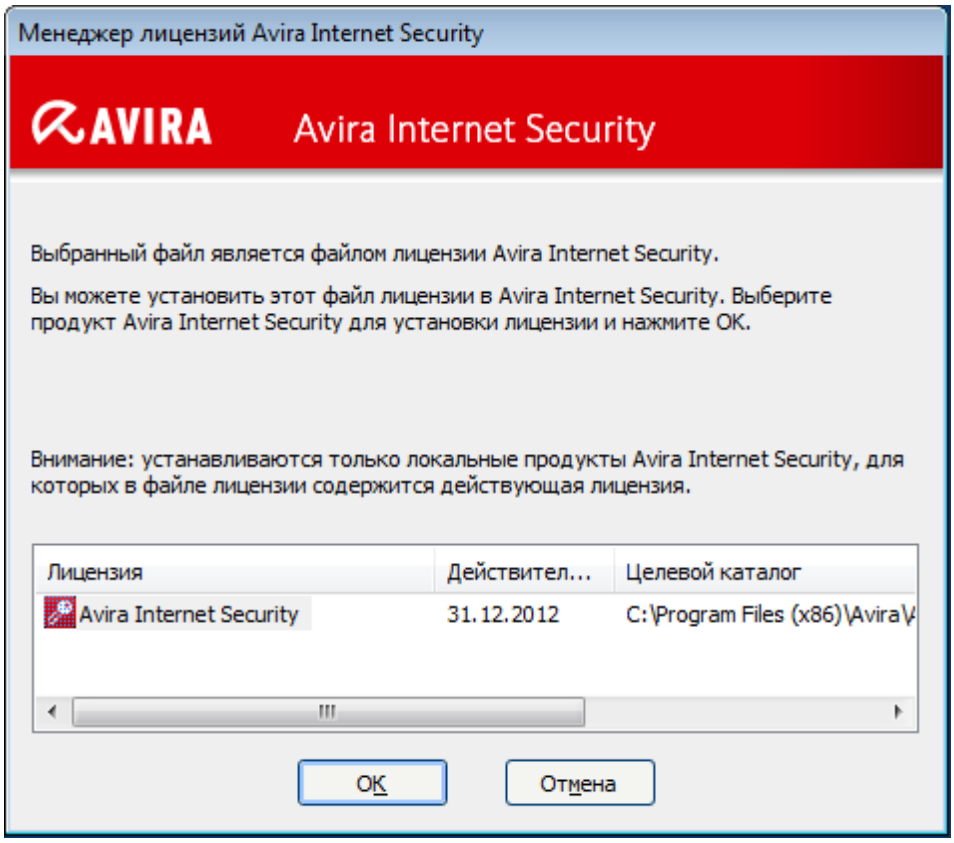
Чтобы гарантировать высокий уровень надежности и безопасности для вашего компьютера, Avira напомнит вам о предстоящем обновлении до новой версии. Нажмите кнопку **Обновить** во всплывающем окне, чтобы перейти на страницу обновления для вашего продукта. Вы можете выполнить обновление вашего продукта или приобрести продукт Avira с расширенными свойствами. Страница обзора продуктов Avira покажет, какую версию вы используете в настоящее время, и предоставит вам возможность сравнить ее с другими программами Avira. Для получения дополнительной информации нажмите символ информации справа от названия продукта. Если вы не хотите устанавливать новый продукт, нажмите кнопку **Обновить**, чтобы немедленно установить самую актуальную версию вашего прежнего продукта с улучшенными функциями. Если вы хотите приобрести продукт с расширенными свойствами, нажмите кнопку **Купить** под столбцом для соответствующего продукта. Вы перейдете в онлайн-магазин Avira, где ваш заказ будет выполнен.

Указание
В зависимости от вашего продукта и операционной системы, для выполнения обновления вам могут потребоваться права администратора. Перед выполнением обновления войдите в систему как администратор.

2.3.4 Управление лицензиями

Менеджер лицензий Avira Internet Security позволяет легко установить лицензию на использование Avira Internet Security.

Менеджер лицензий Avira Internet Security



Вы можете произвести установку лицензии, выбрав файл лицензии в файловом менеджере или щелкнув в письме по ссылке активации лицензии.

Указание
Менеджер лицензий Avira Internet Security автоматически копирует соответствующую лицензию в соответствующую папку. Если лицензия уже есть, отображается информация о том, может ли файл лицензии быть заменен на новый. Уже существующий файл в этом случае заменяется новым файлом лицензии.

3. Установка и удаление

В этой главе содержится информация об установке и удалении программы Avira:

- см. главу: Перед установкой: Условия, подготовка компьютера к установке
- см. раздел: Экспресс-установка: Установка по умолчанию в соответствии с предварительными настройками
- см. главу: Выборочная установка: Конфигурируемая установка
- см. главу: Установка тестового продукта
- см. главу: Ассистент настроек
- см. главу: Установка изменений
- см. главу: Установочные модули
- см. главу: Удаление: Выполнить удаление

3.1 Типы установки

Во время установки вы можете выбрать тип установки:

Экспресс-установка

- Будут установлены стандартные компоненты.
- Программные файлы устанавливаются в стандартную папку *C:\Program Files*.
- Программа Avira устанавливается со значениями по умолчанию. Вы не можете изменять предварительные настройки в помощнике настройки.

Определяемая клиентом

- У вас есть возможность установить отдельные компоненты программы (см. главу Установка и удаление > Установочные модули).
- Можно выбрать папку, в которую будет произведена установка.
- В следующем окне вы можете установить, необходимо ли создавать значок на рабочем столе и/или новую группу программ в меню Пуск.
- С помощью ассистента настроек вы можете выполнить пользовательские настройки для программы Avira и запустить быструю проверку системы сразу после установки.

3.2 Перед установкой

Указание
Перед установкой проверьте, соблюдены ли системные требования. Если ваш компьютер отвечает всем требованиям, то вы можете установить программу Avira.

Инициализация перед установкой

✓ 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.

↳ Программа Avira выполнит поиск на возможные несовместимые программы.

↳ При нахождении несовместимых программ будет сгенерирован соответствующий список этих программ.

↳ Рекомендуется удалить программы, угрожающие безопасности вашего компьютера.

▸ Выберите из списка те программы, которые должны быть автоматически удалены с вашего компьютера и нажмите **Далее**.

▸ Некоторые программы можно удалить с компьютера только вручную. Выберите программы и нажмите **Далее**.

↳ Удаление одной или нескольких программ требует перезагрузки компьютера. После перезагрузки установка продолжится.

Предупреждение
Ваш компьютер будет без защиты, пока не завершится установка программы Avira.

Установка

Программа установки работает в диалоговом режиме. При большом количестве этапов установки достаточно одного щелчка мыши, чтобы продолжить.

Важнейшие кнопки выполняют следующие функции:

- **OK**: Подтвердить действие.
- **Отмена**: Отменить действие.
- **Далее**: Перейти к следующему этапу.
- **Назад**: Вернуться к предыдущему этапу.

- Установите Интернет-соединение. Интернет-соединение необходимо для выполнения следующих этапов установки:
  - Загрузка актуальных программных файлов и поискового ядра, а также файл вирусных сигнатур через программу установки (при установке через Интернет)
  - Активация программы
  - При необходимости выполнение обновления по завершении установки
- Подготовьте код активации или файл лицензии для программы Avira, если вы хотите активировать ее.

Указание
Установка через Интернет:
Для установки программы через Интернет доступна программа установки, которая перед выполнением установки загружает с сервера Avira программные файлы последней версии. Этот способ обеспечивает установку программы Avira с новым файлом вирусных сигнатур.

Установка с пакетом для инсталляции:
Пакет для инсталляции содержит программу установки и необходимые программные файлы. При установке через пакет для инсталляции у вас нет возможности выбора языка для программы Avira. Рекомендуется после завершения установки выполнить обновление, чтобы обновить файл вирусных сигнатур.

Указание
Для активации продукта программа Avira соединяется через HTTP-протокол и порт 80 (веб-коммуникация), а также через зашифрованный протокол SSL и порт 443 с серверами Avira. Если вы используете брандмауэр, убедитесь в том, что входящий/исходящий трафик не блокируется им.

3.3 Быстрая установка

Установка программы Avira:

Запустите установщик двойным щелчком по установочному файлу, который вы загрузили из Интернета, или находящемуся на CD.

Установка через Интернет

↪ На экране появится диалоговое окно **Добро пожаловать**.

- Чтобы продолжить установку, нажмите **Далее**.

↪ Появится диалоговое окно **Выбор языка**.

- Выберите язык для установки программы Avira и подтвердите выбор, нажав **Далее**.
  - ↪ Появится диалоговое окно **Загрузка**. С сервера Avira будут загружены все файлы, необходимые для установки. По завершении загрузки окно **Загрузка** будет закрыто.

Установка через пакет для инсталляции

- ↪ На экране появится окно **Подготовка к установке**.
- ↪ Выполнится распаковка установочного файла. Запустится процедура установки.
- ↪ Откроется диалоговое окно **Выбрать тип установки**.

Примечание
По умолчанию выбрана Экспресс-установка, при которой стандартные компоненты устанавливаются без возможности настройки. Если вы хотите выполнить выборочную установку, прочитайте: Установка и удаление > Выборочная установка.

- По умолчанию опция **Я хочу улучшить защиту с помощью Avira ProActiv и Cloud Protection** (Настройка > Общее > Расширенная защита) активирована. Если вы не хотите участвовать в сообществе Avira Community, снимите этот флажок.
  - ↪ Если вы подтвердите свое согласие на участие в Avira Community, Avira будет отправлять данные о подозрительных программах в центр Avira Malware Research Center. Эти данные используются только для расширенной онлайн-проверки и для улучшения технологии распознавания. По ссылкам **ProActiv** и **Protection Cloud** можно получить подробную информацию о расширенной онлайн- и облачной проверке.
- Подтвердите, что вы принимаете **Лицензионное соглашение с конечным пользователем**. Чтобы прочитать **Лицензионное соглашение с конечным пользователем**, нажмите на соответствующую ссылку.
  - ↪ Откроется **Мастер лицензий**, который поможет вам при активации программы.
  - ↪ Здесь вы получите возможность задать настройки прокси-сервера.
- При необходимости нажмите на **Настройки прокси**, чтобы настроить прокси-сервер, а затем нажмите **OK**.
- Если вы уже получили активационный код, выберите **Активировать продукт** и введите активационный код.

  -ИЛИ-
- Если у вас нет активационного кода, нажмите на ссылку **Получить активационный код**.

↪ Вы будете перенаправлены на веб-сайт Avira.

Или щелкните по ссылке **У меня уже есть действующий файл лицензии**.

↪ Появится **диалоговое окно Открыть файл**.

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

  ↪ Активационный код будет скопирован в Мастер лицензий.

- Если вы хотите протестировать продукт, прочитайте информацию в разделе Установка тестового продукта.

- Нажмите **Далее**.

  ↪ Ход установки будет отображаться в виде зеленой строки.

- Нажмите **Далее**.

  ↪ Откроется диалоговое окно **Присоединяйтесь к миллионам пользователей Avira, которые уже установили Avira SearchFree**.

- Если вы не хотите устанавливать Avira SearchFree Toolbar, снимите флажок с компонента **Лицензионное соглашение** Avira SearchFree Toolbar и Avira SearchFree Updater и деактивируйте установку **Avira SearchFree (search.avira.com)** в качестве стартовой страницы.

Примечание
Если в вашей системе установлены другие панели инструментов поиска, удалите их перед установкой Avira SearchFree Toolbar. В противном случае установка Avira SearchFree Toolbar будет невозможна.

- Нажмите **Далее**.

  ↪ Ход установки Avira SearchFree Toolbar будет отображаться в виде зеленой строки.

  ↪ На панели задач появится значок Avira.

  ↪ Модуль **Updater** запустит поиск обновлений для оптимальной защиты вашего компьютера.

  ↪ При первом запуске проверки откроется окно **Luke Filewalker**, в котором будет отображаться информация о состоянии и результат проверки.

- Если после системной проверки потребуется перезапуск компьютера, щелкните **Да** и выполните его, чтобы ваша система была полностью защищена.

После успешной установки рекомендуется проверить актуальность программы защиты в меню **Статус** Центра управления.

- Если программа Avira показывает, что ваш компьютер защищен не полностью, нажмите **Устранить проблему**.

  ↪ Откроется диалоговое окно **Восстановить защиту**.

- Увеличьте степень защиты системы, активировав заданные опции.
- При необходимости снова запустите полную проверку системы.

3.4 Выборочная установка

Установка программы Avira:

Запустите установщик двойным щелчком по установочному файлу, который вы загрузили из Интернета, или находящемуся на CD.

Установка через Интернет

→ На экране появится диалоговое окно **Добро пожаловать**.

- Чтобы продолжить установку, нажмите **Далее**.

→ Появится диалоговое окно **Выбор языка**.

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

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

Установка через пакет для инсталляции

→ На экране появится окно **Подготовка к установке**.

→ Выполнится распаковка установочного файла. Запустится процедура установки.

→ Откроется диалоговое окно **Выбрать тип установки**.

Указание
По умолчанию включена Экспресс-установка, при которой стандартные компоненты устанавливаются без возможности настройки. Если вы хотите выполнить быструю установку, прочитайте: Установка и удаление > Быстрая установка.

- Выберите **Определенную пользователем** в качестве предпочтительного вида установки.
- Опция **Я хочу улучшить защиту с помощью Avira ProActiv и Cloud Protection** установлена по умолчанию. Если вы не хотите участвовать в сообществе Avira Community, снимите этот флажок.

→ Если вы подтвердите свое согласие на участие в Avira Community, Avira будет отправлять данные о подозрительных программах в центр Avira Malware Research Center. Эти данные используются только для расширенной онлайн-проверки и для улучшения технологии распознавания.

По ссылкам **ProActiv** и **Protection Cloud** можно получить подробную информацию о расширенной онлайн- и облачной проверке.

- Подтвердите, что вы принимаете **Лицензионное соглашение с конечным пользователем**. Чтобы прочитать **Лицензионное соглашение с конечным пользователем**, нажмите на соответствующую ссылку.
- Нажмите **Далее**.
  - ↪ Откроется окно **Выбрать папку установки**.
  - ↪ По умолчанию установлена папка *C:\Program Files\Avira\AntiVir Desktop*
- Нажмите **Далее**, чтобы продолжить установку.

  -ИЛИ-

  Выберите другую папку нажатием кнопки **Поиск**, а затем подтвердите кнопкой **Далее**.
  - ↪ Откроется диалоговое окно **Компоненты**.
- Включите или отключите желаемые компоненты, а затем подтвердите кнопкой **Далее**.
- Если вы выбрали компонент **Cloud Protection** и хотите каждый раз вручную подтверждать, какие файлы необходимо загружать для Cloud-анализа, активируйте опцию **Подтвердить вручную отсылку подозрительный файлов в центр Avira**.
- Нажмите **Далее**.
- В следующем окне вы можете установить, необходимо ли создавать иконку на рабочем столе и/или новую группу программ в меню Пуск.
- Нажмите **Далее**.
  - ↪ Открывается **Мастер лицензий**.

Вы имеете на выбор следующие опции активации программы:

- Ввод кода активации.
  - ↪ Ввод кода активирует вашу программу Avira с лицензией.
- Если у вас нет активационного кода, нажмите на ссылку **Получить активационный код**.
  - ↪ Вы будете перенаправлены на веб-сайт Avira.
- Выбор опции **Тестировать продукт**
  - ↪ Выберите **Тестировать продукт**, во время процесса активации сгенерируется тестовая лицензия, которая активируется программой. Вы можете протестировать программу Avira со всеми ее функциями в течение определенного времени (см. Установка тестового продукта).

Указание
С помощью опции **У меня уже есть действующий файл лицензии** вы можете прочитать файл лицензии. Файл лицензии создается в процессе активации программы с действующим кодом активации и сохраняется в программной папке Avira. Используйте эту опцию, если вы уже выполнили активацию продукта и хотите заново установить программу Avira.

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

Указание
Для активации программы создается соединение с серверами Avira. В настройках **Настройки прокси** вы можете настроить Интернет-соединение через прокси-сервер.

- Выберите тип процедуры активации и подтвердите нажатием кнопки **Далее**.
- Если у вас уже есть действующий файл лицензии, перейдите к разделу "Выбор опции *У меня уже есть действующий файл лицензии*".

Активация продукта

↪ Открывается диалоговое окно, в котором вы можете указать свои персональные данные.

- Введите ваши данные и нажмите **Далее**.

↪ Ваши данные будут переданы на серверы Avira и проверены. Avira будет активирована с вашей лицензией.

↪ В следующем диалоговом окне отображаются данные вашей лицензии.

- Нажмите **Далее**.
- Перейдите к следующему разделу "Выбор опции *У меня уже есть действующий файл лицензии*".

Выбор опции "У меня уже есть действующий файл лицензии"

↪ Открывается диалог чтения файла лицензии.

- Выберите файл лицензии (в форме файла *.KEY*) с вашими данными о лицензии программы и нажмите **Открыть**.

↪ В следующем диалоговом окне отображаются данные вашей лицензии.

- Нажмите **Далее**.

После завершения активации или загрузки файла лицензии нажмите «Далее»

  ↪ Откроется диалоговое окно **Присоединяйтесь к миллионам пользователей Avira, которые уже установили Avira SearchFree**.

- Если вы не хотите устанавливать инструмент Avira SearchFree Toolbar, уберите галочку с Avira SearchFree Toolbar и Avira SearchFree Updater **Лицензионное соглашение** и деактивируйте установку **Avira SearchFree (search.avira.com)** в качестве стартовой страницы.

> **Примечание** Если в вашей системе установлены другие панели инструментов поиска, удалите их перед установкой Avira SearchFree Toolbar. В противном случае установка Avira SearchFree Toolbar будет невозможна.

- Нажмите **Далее**.

  ↪ Ход установки Avira SearchFree Toolbar будет отображаться в виде зеленой строки.

  ↪ **Ассистент установки** закроется, откроется **ассистент настройки**.

3.5 Установка тестового продукта

Установка программы Avira:

Запустите установщик двойным щелчком по установочному файлу, который вы загрузили из Интернета, или находящемуся на CD.

Установка через Интернет

  ↪ На экране появится диалоговое окно **Добро пожаловать**.

- Чтобы продолжить установку, нажмите **Далее**.

  ↪ Появится диалоговое окно **Выбор языка**.

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

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

Установка через пакет для инсталляции

  ↪ На экране появится окно **Подготовка к установке**.

↪ Выполнится распаковка установочного файла. Запустится процедура установки.

↪ Откроется диалоговое окно **Выбрать тип установки**.

Указание
По умолчанию включена **Экспресс-установка**, при которой стандартные компоненты устанавливаются без возможности настройки. Если вы хотите выполнить выборочную установку, прочитайте: Установка и удаление > Выборочная установка.

- По умолчанию опция **Я хочу улучшить защиту с помощью Avira ProActiv и Cloud Protection** (Настройка > Общее > Расширенная защита) активирована. Если вы не хотите участвовать в сообществе Avira Community, снимите этот флажок.

  ↪ Если вы подтвердите свое согласие на участие в Avira Community, Avira будет отправлять данные о подозрительных программах в центр Avira Malware Research Center. Эти данные используются только для расширенной онлайн-проверки и для улучшения технологии распознавания. По ссылкам **ProActiv** и **Protection Cloud** можно получить подробную информацию о расширенной онлайн- и облачной проверке.

- Подтвердите, что вы принимаете **Лицензионное соглашение с конечным пользователем**. Чтобы прочитать **Лицензионное соглашение с конечным пользователем**, нажмите на соответствующую ссылку.
- Нажмите **Далее**.

  ↪ Откроется **Мастер лицензий**, который поможет вам при активации программы.

  ↪ Ассистент предоставит вам возможность определения прокси-сервера.

- Нажмите на **Настройки прокси**, чтобы выбрать необходимую конфигурацию, нажмите **OK**.
- Выберите в ассистенте лицензий **Тестировать продукт** и нажмите**Далее**.
- Введите соответствующие данные в необходимые поля регистрации. Определите, хотите ли вы подписаться на рассылку новостей **Avira Newsletter** и нажмите **Далее**.

  ↪ Ход установки будет отображаться в виде зеленой строки.

  ↪ Откроется диалоговое окно **Присоединяйтесь к миллионам пользователей Avira, которые уже установили Avira SearchFree**.

- Если вы не хотите устанавливать инструмент Avira SearchFree Toolbar, уберите галочку с Avira SearchFree Toolbar и Avira SearchFree Updater **Лицензионное соглашение** и деактивируйте установку **Avira SearchFree (search.avira.com)** в качестве стартовой страницы.

Указание
При необходимости удалите установленные поисковые панели перед установкой Avira SearchFree Toolbar. В противном случае установка Avira SearchFree Toolbar будет невозможна.

- Нажмите **Далее**.
  - ↪ Ход установки Avira SearchFree Toolbar будет отображаться в виде зеленой строки.
- Вам необходимо будет выполнить перезагрузку компьютера, чтобы активировать программу Avira. Нажмите **Да**, чтобы выполнить перезагрузку немедленно.
  - ↪ На панели задач появится значок Avira.
  - ↪ Тестовая лицензия действительна в течение 31 дня.

3.6 Ассистент настроек

При выборе пользовательской установки в заключение откроется ассистент настроек. В ассистенте настроек можно устанавливать параметры для программы Avira.

- Нажмите в окне приветствия ассистенте настроек **Далее** для начала работы с настройками программы.
  - ↪ В диалоговом окне **Настройка AHeAD** вы можете выбрать уровень для обнаружения для технологии AHead. Выбранный уровень обнаружения будет использован для установки технологии AHead модуля System Scanner (прямая проверка) и модуля Real-Time Protection (проверка в реальном времени).
- Выберите уровень обнаружения и нажмите **Далее**.
  - ↪ В диалоговом окне **Дополнительные категории угроз** вы можете выбрать категории угроз и настроить функции защиты программы Avira.
- При необходимости активируйте категории угроз, нажмите **Далее**.
  - ↪ Если при установке вы выбрали модуль Avira FireWall , появится диалоговое окно **Стандартные правила для доступа к сети и использования сетевых ресурсов**. Здесь можно установить, будет ли разрешать брандмауэр 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 Avira Real-Time Protection, появится диалоговое окно **Режим запуска Real-Time Protection**. Можно установить момент запуска модуля Real-Time Protection. Модуль Real-Time Protection будет запускаться при каждом запуске компьютера в указанном режиме.

Указание
Заданный режим запуска модуля Real-Time Protection сохраняется в реестре и не может изменяться в меню настроек.

Указание
Выбор стартового режима по умолчанию для модуля Real-Time Protection (нормальный запуск) и быстрого входа в учетную запись пользователя при запуске системы ведет к тому, что программы, которые запускаются автоматически при запуске системы, не проверяются, так как они были запущены до полной загрузки модуля Real-Time Protection.

- Активируйте необходимые опции, нажмите **Далее**.
  - ↪ Если при установке вы выбрали модуль Avira Web Protection, появится диалоговое окно **АктивироватьSafe Browsing**. Вы можете присвоить пользователям компьютера различные роли для доступа к Интернету (дети, молодежь, взрослые). Вы можете деактивировать опцию Safe Browsing.
- Установите нужные настройки для Safe Browsing и продолжите работу с настройками нажатием кнопки **Далее**.
  - ↪ В следующем диалоговом окне **Задать пароль** вы можете защитить доступ к настройкам с помощью пароля. Особенно это рекомендуется при активированном модуле Safe Browsing.
  - ↪ 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 **Завершить** для завершения конфигурации.
  - ↪ Заданные и выбранные настройки будут сохранены.
  - ↪ При активированной опции **Быстрая проверка системы** открывается окно **Luke Filewalker**. System Scanner выполняет быструю проверку системы.
  - ↪ Если после системной проверки требуется перезапуск системы, выполните его, чтобы ваша система была полностью защищена.

После успешной установки рекомендуется проверить актуальность программы защиты в меню **Статус** Центра управления.

- Если ваша программа Avira показывает, что ваш компьютер защищен не полностью, нажмите **Удалить проблему**.
  - ↪ Откроется диалоговое окно **Восстановить защиту**.
- Увеличьте защиту своей системы, активировав заданные опции.

- При необходимости выполните полную проверку системы.

3.7 Изменить программу

У Вас есть возможность добавлять или удалять отдельные программные компоненты установленной программы Avira (см. главу Установка и удаление > Установочные модули)

Если вы хотите добавить или удалить программные компоненты установленной программы, вы можете воспользоваться опцией **Программное обеспечение** для **изменения/удаления** программы в **Панели управления Windows**.

Выберите свою программу Avira и нажмите на **Изменить**. В диалоге *Добро пожаловать* программы выберите опцию **Изменить**. Вы пройдете через процедуру изменения установленной программы.

3.8 Установочные модули

При выборочной установке или изменении программы могут быть выбраны, добавлены или удалены следующие установочные модули:

- **Avira Internet Security**
  Этот модуль содержит все компоненты, необходимые для успешной установки вашего продукта Avira.
- **Real-Time Protection**
  Модуль Avira Real-Time Protection 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), продукт Avira автоматически проверяет файл. Avira Real-Time Protection не проверяет файл во время переименования.
- **Mail Protection**
  Mail Protection — это связующее звено между вашим компьютером и почтовым сервером, с которого ваша почтовая программа (почтовый клиент) загружает письма. Mail Protection играет роль так называемого прокси-сервера между почтовым клиентом и почтовым сервером. Все входящие письма перенаправляются через этот прокси-сервер, проверяются на наличие вирусов и вредоносных программ, а затем пересылаются на вашу почту. В зависимости от конфигурации, программа автоматически обрабатывает инфицированные письма и запрашивает пользователя о необходимых действиях. Кроме того, в модуле Mail Protection предусмотрена надежная защита от спама.
- **Avira FireWall**
  Avira FireWall контролирует входящий и исходящий трафик на вашем компьютере. Этот компонент разрешает или запрещает соединение, исходя из политики безопасности.

- **Rootkits Protection**
  Модуль Avira Rootkits Protection проверяет, содержится ли на вашем компьютере ПО, которое после проникновения в систему не может быть обнаружено обычными методами распознавания вредоносного ПО.
- **ProActiv**
  Компонент ProActiv контролирует действия приложений и сообщает об их подозрительном поведении. Это распознавание, основанное на поведении приложений, позволяет защитить ваш компьютер от неизвестных вредоносных программ. Компонент ProActiv встроен в модуль Avira Real-Time Protection.
- **Protection Cloud**
  Компонент Protection Cloud — это модуль для динамического онлайн-распознавания неизвестных вредоносных программ.
- **Backup**
  С помощью этого компонента можно вручную или в автоматическом режиме создавать полные резервные копии данных.
- **Web Protection**
  При работе в Интернете ваш веб-браузер получает данные с веб-сервера. Переданные веб-сервером данные (файлы HTML, скрипты и изображения, флэш-файлы, видео- и аудиопотоки) обычно сохраняются в кэш-памяти браузера и выполняются непосредственно в нем, делая невозможной проверку в режиме реального времени, обеспечиваемую Avira Real-Time Protection. Так вирусы и вредоносные программы могут попасть в вашу систему. Web Protection — это так называемый HTTP-прокси, который контролирует порты, используемые для передачи данных (80, 8080, 3128), и проверяет передаваемые данные на наличие вирусов и вредоносных программ. В зависимости от конфигурации, программа автоматически обрабатывает инфицированные файлы и запрашивает пользователя о необходимых действиях.
- **Расширение оболочки**
  Расширение оболочки создает в контекстном меню проводника Windows (вызов правой клавишей мыши) пункт *Проверить выбранные файлы с помощью Avira*. Этот пункт позволяет проверять отдельные файлы или папки.

3.9 Удаление

Если вы хотите удалить программу Avira, воспользуйтесь опцией **Программное обеспечение** для **Изменения/Удаления** программ через Панель управления Windows.

Так удаляется программа Avira (описано на примере Windows 7):

- Откройте пункт меню Windows **Пуск**, **Панель управления**.
- Дважды щелкните мышью по **Программы и функции**.
- Выберите свою программу Avira из списка и нажмите на **Удалить**.
  - ↪ Вы должны будете подтвердить, что действительно хотите удалить программу.

- Подтвердите кнопкой **Да**.
  - ↪ Появится запрос, следует ли снова активировать брандмауэр Windows (так как брандмауэр Avira FireWall деактивирован).
- Подтвердите кнопкой **Да**.
  - ↪ Удаляются все компоненты программы.
- Нажмите **Завершить** для завершения удаления.
  - ↪ В некоторых случаях может отобразиться окно с предложением перегрузить компьютер.
- Подтвердите кнопкой **Да**.
  - ↪ Программа Avira удалена. Компьютер при необходимости требуется перезагрузить. При этом будут удалены все папки, файлы и записи реестра программы.

Указание
Компонент Avira SearchFree Toolbar не входит в удаление программы, его необходимо удалить отдельно с помощью приведенных выше этапов. Для этого компонент Avira SearchFree Toolbar должен быть активирован через менеджер Add-On. После удаления поисковая панель больше не будет встроена в веб-браузер.

4. Обзор Avira Internet Security

главы содержится обзор функций и особенности использования программы Avira.

- См. главу Интерфейс и работа с программой
- см. главу Avira SearchFree Toolbar
- См. главу Это делается так

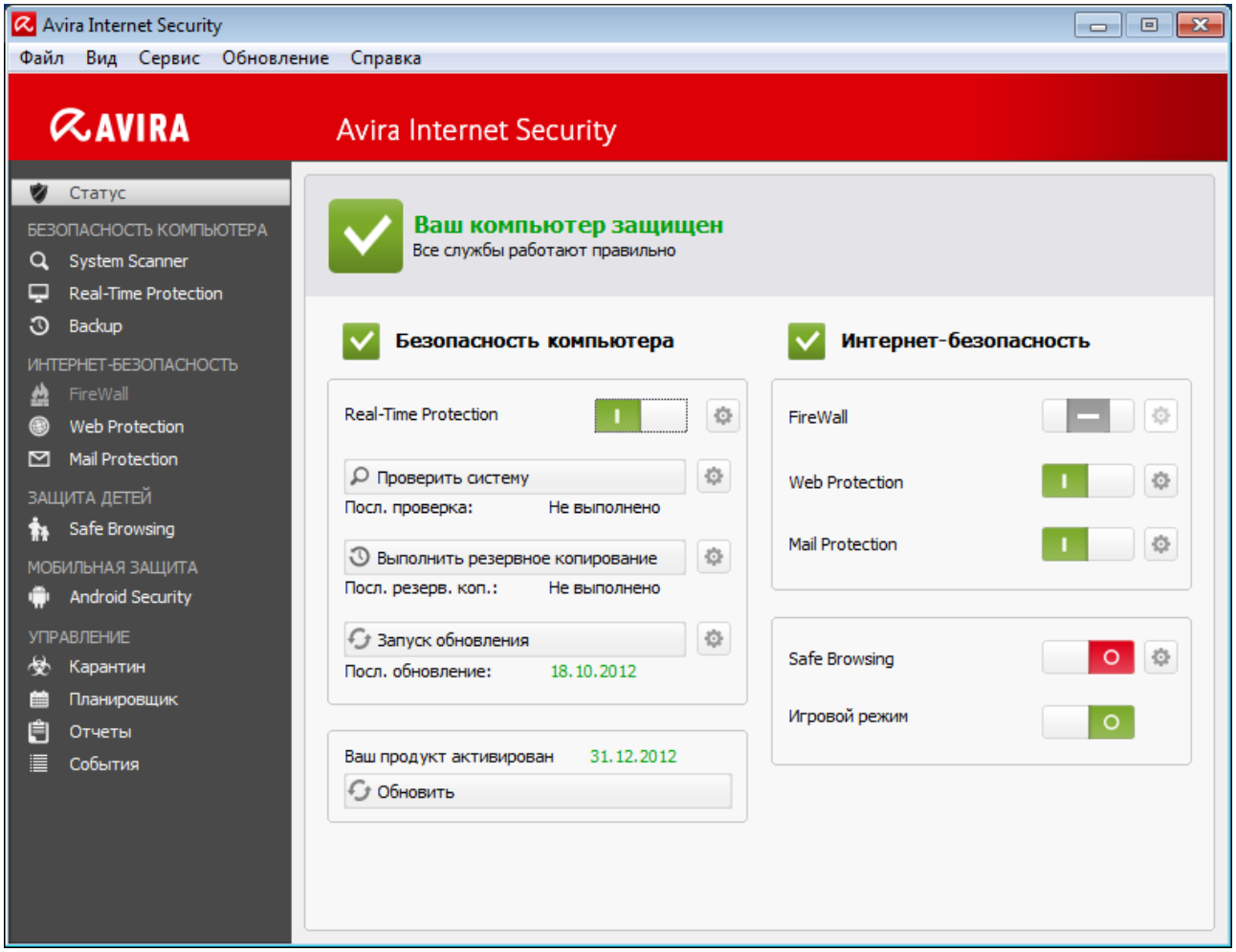
4.1 Интерфейс и работа с программой

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

- Центр управления: Контроль и управление программой Avira
- Настройка: Настройка программы Avira
- Значок в трее Системный трей панели задач: открытие центра управления и других функций

4.1.1 Control Center

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



Окно центра управления делится на три части: **меню**, **область навигации** и окно **состояние**:

- **Меню:** В меню центра управления вы можете открыть общие функции программы и получить информацию о программе.
- **Навигационное поле:** В навигационном поле можно быстро переключаться между отдельными вкладками центра управления. Отдельные вкладки содержат информацию и доступ к функциям программных компонентов, они расположены в строке меню по областям задач. Пример: Область задач *БЕЗОПАСНОСТЬ КОМПЬЮТЕРА* - вкладка **Real-Time Protection**.
- **Состояние:** На начальном экране **Состояние** можно увидеть, достаточно ли защищен компьютер, какие модули активны, когда создавалась последняя резервная копия и проводилась проверка системы. В окне **Состояние** находятся кнопки для выполнения функций или действий, например включение или отключение **Real-Time Protection**.

Запуск и завершение работы центра управления

У вас есть несколько возможностей запуска центра управления:

- Двойным щелчком по ярлыку на рабочем столе

- С помощью строки в меню **Пуск > Program Files**.
- Через Tray Icon вашей программы Avira.

Завершить работу центра управления можно с помощью команды меню **Завершить** в меню **Файл**, сочетанием клавиш **Alt+F4** или щелчком мыши по крестику в правом верхнем углу окна центра управления.

Работа с центром управления

Навигация в центре управления:

- Нажмите на область задач под вкладкой на навигационной панели.
  - ↪ Область задач отобразится с дополнительными возможностями настройки и функциями в окне.
- При необходимости нажмите на другую область задач для отображения этого раздела в окне.

> **Указание**
> Управление клавиатурой в меню можно включить с помощью клавиши [**Alt**]. Клавишей **Enter** можно выбрать выделенный пункт меню.
> Для открытия, закрытия и навигации в пунктах меню центра управления можно использовать сочетания клавиш: [**Alt**] + подчеркнутая буква в меню или команде меню. Удерживайте нажатой клавишу [**Alt**], 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.
- Нажмите кнопку в верхней части основного окна, чтобы обработать объект.

Обзор центра управления

- **Состояние**: На начальном экране **Состояние** представлены все вкладки, с помощью которых вы можете контролировать функции программы (см. Состояние).
  - Окно **Состояние** показывает, какие модули активны, предоставляет информацию о последних проведенных обновлениях.
- *БЕЗОПАСНОСТЬ КОМПЬЮТЕРА*: Здесь содержатся компоненты, с помощью которых вы можете проверить файлы на вашем компьютере на наличие вирусов и вредоносных программ.
  - Во вкладке **System Scanner** можно выполнить прямой поиск, т.е. настраивать поиск по собственному желанию и запускать его (см. System Scanner).

Предустановленные профили позволяют производить проверку с оптимальными стандартными настройками. Возможно также подстроить параметры проверки под ваши индивидуальные задачи с помощью Выборочной проверки (настройка сохраняется) или с помощью создания пользовательского профиля.

- Вкладка Real-Time Protection отображает информацию о проверенных файлах, а также другие статистические данные, которые в любое время могут быть обнулены и позволяет открыть файл отчета. Подробная информация о последнем обнаруженном вирусе или нежелательной программе вызывается "одним щелчком".
- Во вкладке **Backup** можно быстро и просто создавать резервные копии данных и устанавливать задачи по созданию резервных копий (см. Резервная копия).

- *ИНТЕРНЕТ-БЕЗОПАСНОСТЬ*: Здесь вы найдете компоненты, которые позволят защитить вашу систему от вирусов, вредоносных программ и сетевых атак.
  - В разделе **FireWall** можно изменять основные настройки брандмауэра Avira FireWall . Отображается также скорость передачи данных и все активные приложения, использующие сетевые соединения (см. FireWall).
  - Вкладка Web Protection отображает информацию о проверенных URL, обнаруженных вирусах, а также другие статистические данные, которые в любой момент можно обнулить, предоставляет возможность вызова файла отчета. Подробная информация о последнем обнаруженном вирусе или нежелательной программе вызывается "одним щелчком".
  - Вкладка **Mail Protection** показывает проверенные письма, их свойства и данные статистики. У вас есть возможность обучать фильтр AntiSpam и в будущем исключать адреса электронной почты из проверки на наличие вирусов или спама. Письма можно удалять из буфера модуля Mail Protection. (см. Mail Protection).
- *Child Protection*: Здесь представлены инструменты, с помощью которых вы можете обеспечить безопасность своих детей в сети.
  - Safe Browsing: Пользователям можно присвоить роли. Каждая роль настраивается и включает в себя набор правил со следующими критериями: запрещенные или разрешенные URL (адреса в Интернете), запрещенные категории содержимого, время работы в Интернете и при необходимости время работы в Интернете по будним дням
- *MOBILE PROTECTION*: С помощью категории Avira Free Android Security вы можете работать в сети на своих устройствах на базе Android.
  - Avira Free Android Security позволяет управлять всеми устройствами, работающими на операционной системе Android.
- *УПРАВЛЕНИЕ*: Здесь представлены инструменты, которые позволят вам 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 (см. Карантин). Кроме этого выбранный файл можно отправить по электронной почте в центр исследования вирусов компании Avira.

- Во вкладке **Планировщик** можно создавать выполняемые в определенное время задачи по проверке и обновлению или резервному копированию, а также согласовывать или удалять существующие задачи (см. Планировщик).
- Вкладка **Reports** позволяет вам получить информацию о результатах выполненных действий (см. Отчеты).
- Вкладка **Events** получает вам получить информацию о событиях, созданных модулями программы (см. События).

4.1.2 Игровой режим

Если вы запускаете на своем компьютере приложения, требующие полноэкранного режима, то активировав игровой режим, вы можете скрыть сообщения рабочего стола и указания, всплывающие окна и оповещения программ. В игровом режиме используются все правила адаптера и пользователя, которые вы установили в настройке Avira FireWall, без оповещения о событиях сети.

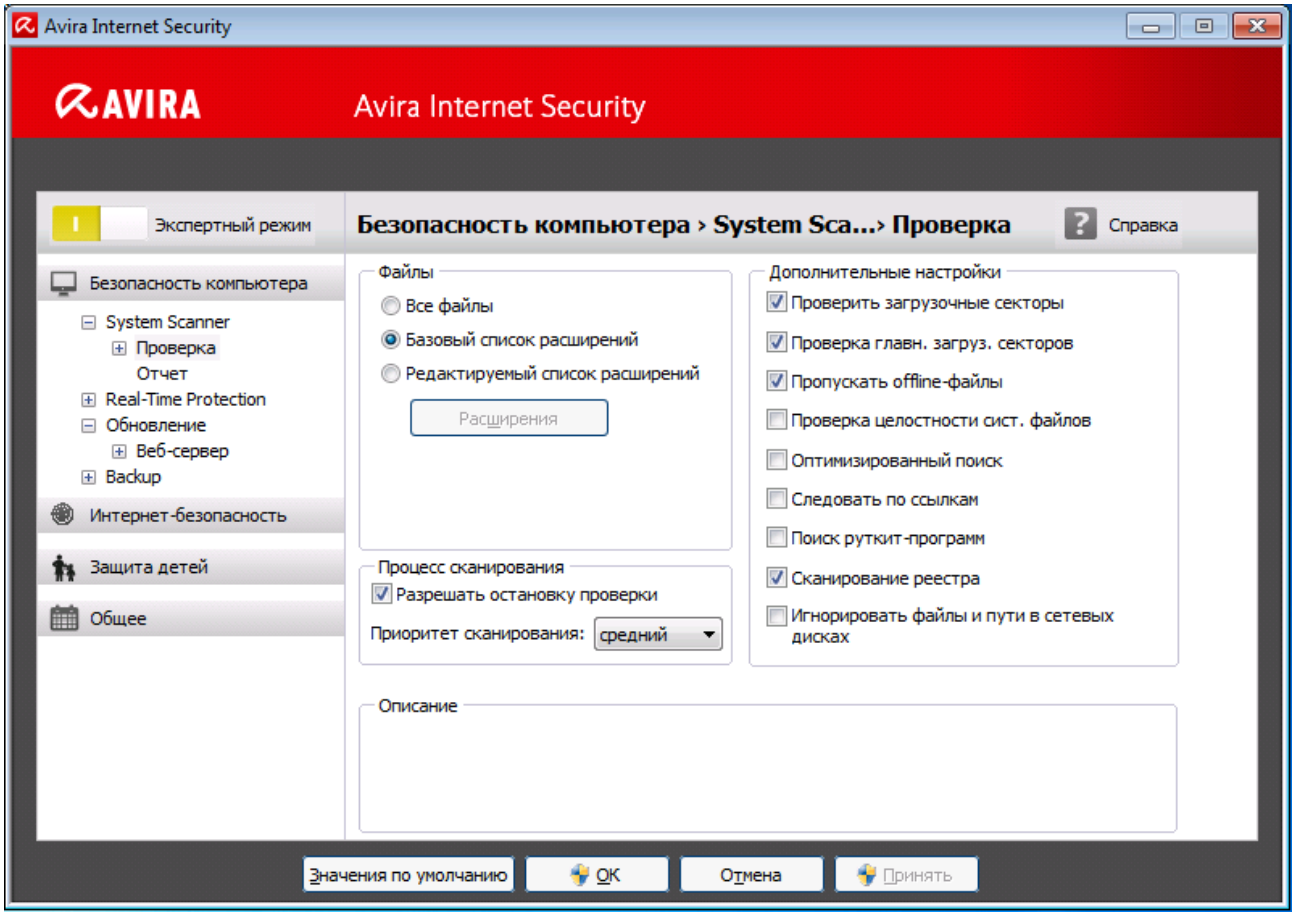
Вы можете активировать или включить автоматически игровой режим нажатием кнопки **ВКЛ/ВЫКЛ**. По умолчанию игровой режим установлен на **automatic** и отображается зеленым цветом. С этой настройкой ваша программа Avira автоматически переключается в игровой режим, если вы запускаете приложение в полноэкранном режиме.

- Чтобы активировать игровой режим, нажмите на кнопку слева от **ВЫКЛ**.
  - ↪ Игровой режим включен, кнопка отображается желтым цветом.

Указание
Мы рекомендуем изменять предварительно установленное состояние **ВЫКЛ** с автоматическим распознаванием приложений в полноэкранном режиме только временно, так как в игровом режиме вы не увидите сообщения рабочего стола и предупреждения о сетевом доступе, а также о возможных опасностях.

4.1.3 Настройка

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



Диалоговое окно настроек имеет следующую структуру: кнопки **OK** или **Принять** 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.

Открытие меню настроек

Вы можете запустить блок настроек несколькими способами:

- Через панель управления Windows.
- Через центра безопасности Windows - начиная с Windows XP SP 2.
- Через значок в трее вашей программы Avira.
- В центре управления в пункте меню Дополнительно > Настройки.
- В центре управления с помощью кнопки Настройки.

Указание
Если вы открываете настройки с помощью кнопки **Настройки** в центре управления, вы попадете в раздел настройки вкладки, которая активна в центре управления. Для выбора отдельных пунктов настройки должен быть включен **Режим эксперта**. В этом случае появится диалоговое окно, в котором необходимо включить **Режим эксперта**.

Работа с настройками

Навигация в окне настроек 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 соответствующей вкладкой настроек.

Указание
Для активации или деактивации опций в настройках и нажатия кнопок можно использовать комбинации клавиш: [**Alt**] + подчеркнутая буква в названии опции или обозначение кнопки.

Указание
Все вкладки настроек отображаются только в режиме эксперта. Включите **режим эксперта** для отображения вкладок настроек. **Режим эксперта** может быть защищен паролем, который необходимо указать при его включении.

Если вы хотите подтвердить сделанные настройки:

- Нажмите кнопку **OK**.
  - ↪ Окно настроек будет закрыто, настройки будут сохранены.

  - ИЛИ -

  Нажмите кнопку **Принять**.
  - ↪ Настройки сохраняются. 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 этом случае не сохраняются.

Обзор опций меню настройки

Предусмотрены следующие опции меню настройки:

- **System Scanner**: Настройка прямого поиска
  - Опции поиска
  - Действие при обнаружении
  - Опции проверки архивов
  - Исключения из прямого поиска
  - Эвристика прямого поиска
  - Настройка функции отчетов
- **Real-Time Protection**: Настройка модуля Real-Time Protection
  - Опции поиска
  - Действие при обнаружении
  - Дополнительные действия
  - Исключения постоянной защиты
  - Эвристика постоянной защиты
  - Настройка функции отчетов
- **Backup**:
  - Настройки компонентов резервного копирования (инкрементная резервная копия, поиск вирусов при создании резервной копии)
  - Исключения: Настройка файлов для резервного копирования
  - Настройка функции отчетов
- **Обновление**: Конфигурация настроек обновления
- **FireWall**: Настройка FireWall
  - Настройки правил адаптера
  - Добавление индивидуальных правил адаптера
  - Список надежных производителей (исключения при доступе приложений к сети)
  - Расширенные настройки: превышение по времени для правил, остановка Windows FireWall, оповещения
  - Настройка всплывающих окон (уведомления при доступе приложений к сети)
- **Web Protection**: Настройка модуля Web Protection
  - Опции поиска, активация и деактивация модуля Web Protection
  - Действие при обнаружении
  - Запрещенный доступ: Нежелательные типы файлов и MIME, веб-фильтры для известных нежелательных URL (вредоносные программы, фишинг и т. д.)
  - Исключения из поиска службой Web Protection: URL, типы файлов, MIME-типы
  - Эвристика службы Web Protection
  - Настройка функции отчетов
- **Mail Protection**: Настройка модуля Mail Protection

- Опции поиска: Активация контроля протоколов POP3, узлов IMAP, исходящих писем (SMTP)
- Действие при обнаружении
- Дополнительные действия
- Эвристика проверки модулем Mail Protection
- Функция AntiBot: Разрешенный сервер SMTP, разрешенный отправитель электронной почты
- Исключения из проверки модулем Mail Protection
- Настройка буфера памяти, очистка буфера
- Настройка учебной базы данных AntiSpam, очистить учебную базу данных
- Настройка строки примечания в отправленных письмах
- Настройка функции отчетов

- **Child Protection**:
  - Safe Browsing: Функция защиты детей с основанным на ролях фильтром и зависящим от роли ограничением времени доступа в Интернет
- **Общее**:
  - Расширенные категории угроз для прямой проверки и постоянной защиты
  - Расширенная защита: активация ProActiv и Cloud Protection
  - Фильтр приложений: блокировать или разрешать приложения
  - Защита паролем доступа к центру управления и настройкам
  - Безопасность: блокировка функций автозапуска, файлов Windows hosts, защита продукта
  - WMI: Активировать WMI-поддержку
  - Настройка протокола событий
  - Настройка функций отчетов
  - Настройка используемых папок
  - Настройка акустических сигналов при обнаружении вируса

4.1.4 Tray Icon

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

Пиктограмма	Описание
	Avira Real-Time Protection работает, FireWall работает
	Avira Real-Time Protection деактивирован, FireWall деактивирован

Значок в трее отображает состояние служб Real-Time Protection и FireWall .

Через контекстное меню значка в трее доступны основные функции программы Avira.

- Для вызова контекстного меню необходимо щелкнуть правой кнопкой мыши по значку в трее.

Пункты контекстного меню

- **Активировать Real-Time Protection**: активирует или деактивирует модуль Avira Real-Time Protection.
- **Активировать Mail Protection**: активирует или деактивирует модуль Avira Mail Protection.
- **Активировать Web Protection**: активирует или деактивирует модуль Avira Web Protection.
- **FireWall**:
  - **Активировать FireWall**: активирует или деактивирует Avira FireWall
  - **Блокировать весь трафик**: Включен: блокирует всю передачу данных за исключением передачи в собственной компьютерной системе (Local Host/IP 127.0.0.1).
- **Запустить Avira Internet Security**: Открывает Центр управления.
- **Настройка Avira Internet Security : открывает Настройку.**
- **Мои сообщения: Открывает список с последними сообщениями по вашей программе Avira.**
- **Мои настройки коммуникации: Открывает Центр сообщений о продукте**
- **Запустить обновление: Запускает Обновление.**
- **Справка: Открывает справочную онлайн-систему.**
- **Avira Internet Security: Открывает диалоговое окно с информацией о вашей программе Avira: информация о продукте, номер версии, лицензия.**

- **Avira в Интернете: Открывает веб-портал Avira в Интернете. Для этого необходимо иметь доступ к Интернету.**

4.2 Панель инструментов Avira SearchFree

Avira SearchFree Toolbar содержит два основных компонента: Avira SearchFree и уже известную панель инструментов.

Новое приложение Avira SearchFree Toolbar устанавливается в виде дополнения. При первом открытии браузера (в Internet Explorer и Firefox) вам необходимо будет ответить, разрешаете ли вы изменение своего браузера программой Avira SearchFree Toolbar. Чтобы выполнить установку Avira SearchFree Toolbar, вам необходимо дать согласие.

Avira SearchFree - это новая поисковая машина от Avira, она содержит логотип Avira, который при активации перенаправляет на сайт Avira, а также каналы изображений и веб-каналы. Она обеспечивает безопасный поиск для пользователей Avira.

Программа Toolbar встраивается в веб-браузер, она состоит из поискового поля, логотипа Avira, ведущего на сайт Avira, двух индикаций состояния, трех виджетов и меню **Options**.

- Поисковая панель
  Используйте поисковую панель, чтобы быстро и бесплатно осуществлять поиск в Интернете с помощью поисковой машины Avira SearchFree.
- Индикация состояния
  Индикаторы состояния сообщают о состоянии модуля Web Protection и текущее состояние обновления вашей программы Avira и помогают вам узнать, какие действия необходимо предпринять для защиты вашего компьютера.
- Виджеты
  Avira предоставляет вам прямой доступ к важным функциям в Интернете, например, сообщения в Facebook или электронная почта. Вы можете также установить безопасность своей системы с помощью виджета Web Protection (только Firefox и Internet Explorer).
- Опции
  С помощью меню **Options** вы получаете доступ к опциям панели инструментов, можете удалять прогресс поиска, вызывать справочную информацию по панели инструментов и удалять панель инструментов Avira SearchFree непосредственно через веб-браузер (только Firefox и Internet Explorer).

4.2.1 Использование

Avira SearchFree

С помощью поисковой панели Avira SearchFree вы можете осуществлять поиск в Интернете по одному или нескольким словам.

Введите слово в поисковое поле и нажмите кнопку **Enter**, или нажмите на **Search**. Поисковая машина Avira SearchFree осуществит для вас поиск в Интернете и покажет результаты в окне браузера.

Если вы хотите настроить Avira SearchFree в Internet Explorer, Firefox и Chrome в соответствии со своими предпочтениями, откройте **Options**.

Индикация состояния

Web Protection

Для определения статуса безопасности Вашего компьютера Вы можете использовать значки и сообщения:

Символ	Индикация состояния	Описание
	*Web Protection*	Если вы наведете указатель мыши над символом, то увидите следующее сообщение: *Avira Web Protection is active. Your browsing is protected.* Это означает, что другие действия не нужны.
	*Web Protection*	Если вы наведете указатель мыши над символом, то увидите следующее сообщение: *Avira Web Protection is off. Click to find out how to turn it on.* ↪ Вы будете перенаправлены на статью нашей базы знаний.

	*No Web Protection*	Если вы наведете указатель мыши над символом, то увидите следующее сообщение: • *You do not have Avira Web Protection installed. Click to find out how to protect your browsing.* Это означает, что вы удалили антивирус Avira или установили его неправильно. • *Web Protection is included for free with Avira Antivirus. Click to find out how to install it.* Это означает, что вы не установили Web Protection или удалили эту программу. ↪ В обоих случаях Вы будете перенаправлены на веб-сайт Avira, где Вы сможете загрузить программу Avira.
	*Error*	Если вы наведете указатель мыши над символом, то увидите следующее сообщение: *Avira reported an error. Click to contact Support for help.* ▸ Нажмите на серый символ или текст, чтобы перейти на страницу поддержки Avira.

Виджеты

Avira SearchFree Toolbar имеет 3 виджета с важнейшими функциями для работы в Интернете: Facebook, электронная почта и Browser Security.

Facebook

Эта функция позволяет вам получать сообщения непосредственно из Facebook и всегда быть в курсе событий.

Электронная почта

Если вы нажмете на символ электронной почты, появится выпадающий список, в котором вы можете выбрать наиболее частых адресатов.

Browser Security

Этот виджет был разработан Avira, чтобы сделать доступными все опции, связанные с безопасностью в Интернете. В настоящее время он доступен для Firefox и Internet Explorer. Предлагаются различные опции, которые в зависимости от браузера могут иметь разные названия:

- *Pop-up Blocker*

Если включена эта опция, то все всплывающие окна блокируются, когда вы работаете в Интернете.

- *Block Cookies*

Если включена эта опция, то файлы Cookies в браузере не сохраняются.

- *Private Browsing (Firefox) / InPrivate Browsing (Internet Explorer)*

Если включена эта опция, то вы не оставите следов своей работы в Интернете. Эта опция не представлена для Internet Explorer 7 и 8.

- *Clear Recent History (Firefox) / Delete Browsing History (Internet Explorer)*

Эта опция позволяет удалить все предыдущие действия в Интернете.

Website Safety Advisor

Website Safety Advisor предлагает вам разделение на ступени безопасности.
Вы сможете оценить, представляет ли сайт, на котором вы в данный момент находитесь, большой или маленький риск для вашей безопасности.
Этот виджет предоставляет дополнительную информацию о сайте, например кто является обладателем домена, почему сайт отнесен именно в эту определенную категорию.
Существует три категории: надежный, с небольшим риском, опасный.

Эти категории отображаются в приложении Toolbar и в ваших результатах поиска в виде значка Avira в трее с различными символами:

Символ	Индикация состояния	Описание
	*Safe*	Зеленая галочка для надежных веб-сайтов.
	*Low risk*	Желтый восклицательный знак для сайтов, представляющих небольшой риск.
	*High risk*	Красный значок "стоп" для веб-сайтов, представляющих большую опасность для вашей безопасности.
	*Unknown*	Серый знак вопроса для веб-сайтов, опасность которых не может быть определена.

	*Verifying*	Этот символ появляется во время проверки состояния.

Browser Tracking Blocker

С помощью блокировщика слежения для браузера можно остановить преследования, которые собирают о вас информацию, когда вы работаете в Интернете.
Виджет позволяет выбрать, какие преследования необходимо блокировать, а какие разрешить.

Предприятия делятся на три категории:

- Social Networks
- Ad Networks
- Other companies

4.2.2 Опции

Инструмент Avira SearchFree Toolbar совместим с Internet Explorer, Firefox и Google Chrome, его можно настроить в веб-браузере на ваше усмотрение:

- Internet Explorer, опции настройки
- Firefox, опции настройки
- Chrome, опции настройки

Internet Explorer

В браузере Internet Explorer в меню **Options** доступны следующие опции для Avira SearchFree Toolbar:

Toolbar options

Search

Avira search engine

В меню **Avira search engine** можно выбрать, какие поисковые машины будут использоваться для поиска. Доступны поисковые машины из США, Бразилии, Германии, Испании, Европы, Франции, Италии, Нидерландов, России и Великобритании.

Open searches in

В меню опции **Open searches in** можно выбрать, где будет отображаться результат поискового запроса: в текущем окне, в новом окне или в новой вкладке.

Display recent searches

Если включена опция **Display recent searches**, вы можете просматривать предыдущие результаты поиска под полем ввода панели поиска.

Auto clear recent search history when I close the browser

Активируйте опцию **Auto clear recent search history when I close the browser**, если вы не хотите сохранять процесс поиска, тогда при закрытии веб-браузера он будет удален.

More options

Select toolbar language

В меню **Select toolbar language** вы можете выбрать язык, на котором будет отображаться Avira SearchFree Toolbar. Доступны следующие языки: английский, немецкий, французский, итальянский, португальский и голландский.

> **Указание**
> Предварительно установленный язык панели Avira SearchFree Toolbar совпадает с языком вашей программы, если он доступен. Если Toolbar недоступен на вашем языке, то по умолчанию будет установлен английский.

Show button text labels

Отключите опцию **Show button text labels**, если вы хотите скрыть текст рядом со значком Avira SearchFree Toolbar.

Clear history

Активируйте опцию **Clear history**, если вы не хотите сохранять результат(ы) уже выполненного поиска, а хотите сразу его (их) удалить.

Help

Нажмите на **Help**, чтобы открыть сайт с часто задаваемыми вопросами (FAQ) по приложению Toolbar.

Uninstall

Вы можете удалить Avira SearchFree Toolbar непрсредственно в Internet Explorer: Удаление через веб-браузер.

About

Нажмите на **About**, чтобы посмотреть, какая версия Avira SearchFree Toolbar у вас установлена.

Firefox

В браузере Firefox в меню **Options** доступны следующие опции для Avira SearchFree Toolbar:

Toolbar options

Search

Select Avira search engine

В меню **Avira search engine** можно выбрать, какие поисковые машины будут использоваться для поиска. Доступны поисковые машины из США, Бразилии, Германии, Испании, Европы, Франции, Италии, Нидерландов, России и Великобритании.

Display recent searches

Если включена опция **Display recent searches**, вы можете просматривать предыдущие результаты поиска под полем ввода панели поиска, нажав на стрелку на панели поиска. Выберите один из терминов, если хотите увидеть результат еще раз.

Auto clear recent search history when I close the browser

Активируйте опцию **Auto clear recent search history when I close the browser**, если вы не хотите сохранять процесс поиска, тогда при закрытии веб-браузера он будет удален.

Display Avira search results when I type keywords or invalid URLs into the browser address bar

Если эта опция включена, то каждый раз, когда вы вводите ключевые слова или недействительные URL-адреса в адресную строку веб-браузера, то запускается поисковый запрос, отображается результат.

More options

Select toolbar language

В меню **Select toolbar language** вы можете выбрать язык, на котором будет отображаться Avira SearchFree Toolbar. Доступны следующие языки: английский, немецкий, французский, итальянский, португальский и голландский.

> **Указание**
> Предварительно установленный язык панели Avira SearchFree Toolbar совпадает с языком вашей программы, если он доступен. Если Toolbar недоступен на вашем языке, то по умолчанию будет установлен английский.

Show button text labels

Отключите опцию **Show button text labels**, если вы хотите скрыть текст рядом со значком Avira SearchFree Toolbar.

Clear history

Активируйте опцию **Clear history**, если вы не хотите сохранять результат(ы) уже выполненного поиска, а хотите сразу его (их) удалить.

Help

Нажмите на **Help**, чтобы открыть сайт с часто задаваемыми вопросами (FAQ) по приложению Toolbar.

Uninstall

Вы можете удалить Avira SearchFree Toolbar непрсредственно в Internet Explorer: Удаление через веб-браузер.

About

Нажмите на **About**, чтобы посмотреть, какая версия Avira SearchFree Toolbar у вас установлена.

Chrome

В браузере Google Chrome вы найдете все опции настроек с красным зонтиком Avira. Следующие опции доступны для Avira SearchFree Toolbar:

Help

Нажмите на **Help**, чтобы открыть сайт с часто задаваемыми вопросами (FAQ) по приложению Toolbar.

Uninstall instructions

Здесь вы найдете ссылки на инструкции по удалению Avira SeachFree Toolbar.

About

Нажмите на **About**, чтобы посмотреть, какая версия Avira SearchFree Toolbar у вас установлена.

Show/ Hide the Avira SearchFree Toolbar

Этот пункт меню включает и выключает Avira SeachFree Toolbar, находящийся в верхней части окна.

4.2.3 Удаление

Так удаляется панель инструментов Avira SearchFree (описано на примере Windows 7):

- Откройте пункт меню Windows **Пуск**, **Панель управления**.
- Дважды щелкните мышью по **Программы и функции**.
- Выберите **Avira SearchFree Toolbar plus Web Protection** из списка и нажмите **Удалить**.
  - ↪ Появится вопрос, действительно ли вы хотите удалить программу.
- Подтвердите кнопкой **Да**.
  - ↪ Приложение Avira SearchFree Toolbar plus Web Protection удалено, компьютер при необходимости требуется перезагрузить; при этом будут удалены все папки, файлы и записи реестра программы.

Удаление через веб-браузер

Вы можете удалить Avira SearchFree Toolbar в **Firefox и Internet Explorer**:

- Откройте в поисковой панели справа меню **Options**.
- Нажмите **Uninstall**.
  - ↪ Если веб-браузер еще открыт, то вам потребуется закрыть его.
- Закройте веб-браузер и нажмите **OK**.
  - ↪ Приложение Avira SearchFree Toolbar plus Web Protection удалено, компьютер при необходимости требуется перезагрузить; при этом будут удалены все папки, файлы и записи реестра программы.

Указание Для удаления Avira SearchFree Toolbar необходимо активировать панель инструментов в менеджере Add-On.

Удаление в качестве Add-On

Новая версия Avira SearchFree Toolbar устанавливается как дополнение Add-On, возможно управлять ей с помощью различных менеджеров.

Firefox

Нажмите на **Tools > Add-ons > Расширения**. Там возможно управление дополнением Avira: включение, выключение или удаление.

Internet Explorer

Нажмите на **Управление дополнениями > Панели управления и расширения**. Вы смоете включить, отключить и удалить дополнение Avira.

Google Chrome

Нажав на **Опции > Расширения** , вы сможете управлять дополнением Avira. Вы сможете включить, отключить или удалить Toolbar.

4.3 Это делается так

В разделах "Это делается так" представлена краткая информация об активации лицензии и программы, о важнейших функциях программы Avira. Краткие заметки служат для того, чтобы предоставить вам обзор функций программы Avira. Однако они не заменяют подробных разъяснений в отдельных главах данного руководства.

4.3.1 Активировать лицензию

Активация лицензии программы Avira:

Файл лицензии *.KEY* активирует вашу лицензию для программы Avira. Avira высылает лицензионный файл по электронной почте. В файле лицензии содержится лицензия для всей заказанной вами продукции.

Если вы еще не установили Avira:

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

Если вы уже установили Avira:

- Дважды щелкните в файловом менеджере или письме активации по файлу лицензии и следуйте указаниям управления лицензиями.

  - ИЛИ -

  В центре управления программы Avira выберите пункт меню **Справка > Менеджер лицензий**

> **Указание**
> 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.

4.3.2 Активировать продукт

Для активации продукта Avira у вас имеются следующие опции:

- Активация с помощью действующей полноценной лицензии

  Для активации полноценной лицензией вам необходим действующий активационный ключ, который содержит данные о вашей лицензии. Активационный ключ вы можете получить у нас по электронной почте или прочесть на упаковке продукта.

- Активация с помощью тестовой лицензии

  Программа Avira активируется созданной автоматически тестовой лицензией, которая позволяет вам в течение определенного времени опробовать функции Avira в полном объеме.

> **Указание**
> Для активации продукта или заказа тестовой лицензии вам потребуется активное Интернет-соединение.
> Если не создается соединение с серверами Avira, то проверьте настройки брандмауэра: при активации продукта используется соединение через HTTP-протокол и порт 80 (веб-коммуникация), а также зашифрованный протокол SSL и порт 443. Убедитесь в том, что ваш брандмауэр не блокирует входящие и исходящие данные. Сначала проверьте, можете ли вы вызвать веб-страницу через ваш браузер.

Активация программы Avira:

Если Вы еще не установили Avira:

- Установите программу Avira.
  - ↪ Во время установки вам потребуется выбрать способ активации
  - **Активация продукта** = Активация с помощью действующей полноценной лицензии
  - **Тестирование продукта** = Активация с помощью тестовой лицензии
- Для активации полноценной лицензией введите активационный ключ.
- Подтвердите выбор способа активации нажатием кнопки **Далее**.
- Укажите ваши данные для регистрации и подтвердите их нажатием кнопки **Далее**.
  - ↪ В следующем диалоговом окне отображаются данные вашей лицензии. Ваш продукт Avira активирован.
- Продолжите установку.

Если вы уже установили Avira:

- В центре управления выберите пункт меню **Справка > Менеджер лицензий**.
  - ↪ Откроется ассистент лицензий, где вы можете выбрать способ активации. Активируйте продукт, следуя приведенной выше схеме.

4.3.3 Выполнить автоматизированное обновление

С помощью планировщика Avira создается задача, с помощью которой автоматически обновляется ваша программа Avira:

- В центре управления выберите вкладку *Управление* **> Планировщик**.
- Нажмите пиктограмму **Создать новую задачу, используя мастер**.
  - ↪ Появится диалоговое окно **Имя и описание задачи**.
- Введите имя и описание задачи.
- Нажмите **Далее**.
  - ↪ Появится диалоговое окно **Тип задачи**.
- Выберите **Задача обновления** из списка.
- Нажмите **Далее**.
  - ↪ Появится диалоговое окно **Время задачи**.
- Выберите время проведения обновления:

- **Немедленно**
- **Ежедневно**
- **Еженедельно**
- **Интервал**
- **Однократно**
- **Логин**

> **Указание**
> Мы рекомендуем регулярно проводить обновления. Рекомендуемый интервал между обновлениями: 2 часа.

- В зависимости от выбора задайте время.
- При необходимости выберите дополнительные опции (в зависимости от типа задачи):

- **Повторить задачу, даже если выполнения закончено**
  Выполняются задачи, срок выполнения которых уже прошел, но они не могли быть запущены в назначенное время, например если компьютер был выключен.
- **Дополнительно запускать задачу при установлении Интернет-соединения**
  Помимо выполнения задач с установленной частотой осуществляется

дополнительный запуск задач при каждом установленном Интернет-соединении.

- Нажмите **Далее**.
  - ↪ Появится диалоговое окно **Выбор режима отображения**.
- Выберите режим отображения задачи:

- **невидимый**: нет окна задачи
- **минимум**: только прогресс выполнения
- **максимум**: все окно задачи

- Нажмите кнопку **Завершить**.
  - ↪ Новое задание будет отмечено галочкой как активированное на стартовой странице раздела *Управление* **> Планировщик**.
- Деактивируйте задачи, которые не должны выполняться.

Используя следующие символы, вы можете обработать задания:

Просмотреть свойства задания

Изменение задачи

Удаление задачи

Запустить задачу

Остановить задачу

4.3.4 Запустить обновление вручную

У вас есть несколько возможностей запустить обновление вручную: При выполнении обновления вручную производится обновление файла вирусных сигнатур и поискового движка.

Так запускается обновление программы Avira вручную:

- Щелкните правой кнопкой мыши по значку Avira в трее на панели задач и выберите **Начать обновление**.

  - ИЛИ -

- Выберите в центре управления вкладку **Статус**, затем нажмите в **Последнее обновление** ссылку **Начать обновление**.

  - ИЛИ -

В центре управления в меню **Обновление** выберите команду меню **Начать обновление**.

↪ Появится диалоговое окно **Модель обновления**.

Указание
Мы рекомендуем регулярно проводить автоматические обновления. Рекомендуемый интервал между обновлениями: 2 часа.

Указание
Вы можете выполнить обновление вручную через Центр безопасности Windows.

4.3.5 Прямой поиск: Поиск вирусов и вредоносного ПО с помощью профиля поиска

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:

- В Windows XP:

   Нажатием на эту пиктограмму запускается поиск с помощью профиля.
- В Windows Vista:

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

   Нажатием на эту пиктограмму запускается ограниченный поиск с помощью профиля. Проверяются только те папки и файлы, доступ к которым разрешен Windows Vista.

 Нажатием на эту пиктограмму запускается поиск 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 выберите вкладку *PC PROTECTION* **> System Scanner**.
  - ↪ Появятся предустановленные профили поиска.
- Выберите один из предустановленных профилей поиска.

  -ИЛИ-

  Настройте профиль поиска **Выбор вручную**.

  -ИЛИ-

  Создайте новый профиль поиска
- Нажмите на символ (Windows XP:  или Windows Vista: ).
- Появится окно **Luke Filewalker** и запустится прямой поиск.
  - ↪ По окончании проверки будут показаны результаты.

Если Вы хотите настроить профиль поиска:

- В профиле поиска **Manual Selection** 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 (черная галочка)
- Только подкаталоги в каталоге (серая галочка, у подкаталогов галочка черная)
- Не выделять (галочка отсутствует)

Если вы хотите создать новый профиль поиска:

- Нажмите пиктограмму  **Создать новый профиль.**
  - ↪ Среди имеющихся профилей появится *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 (черная галочка)
- Только подкаталоги в каталоге (серая галочка, у подкаталогов галочка черная)
- Не выделять (галочка отсутствует)

4.3.6 Прямой поиск: Поиск вирусов и вредоносного ПО с помощью Drag&Drop

Поиск вирусов и вредоносного ПО с помощью Drag&Drop:

✓ Откройте Центр управления программы Avira.

▸ Выделите файл или каталог, который необходимо проверить.

▸ Перетяните левой кнопкой мышки выделенный файл или выделенный каталог на Центре управления.

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

↳ По окончании проверки будут показаны результаты.

4.3.7 Прямой поиск: Поиск вирусов и вредоносных программ с помощью контекстного меню

Искать с помощью контекстного меню вирусы и вредоносное ПО:

▸ Щелкните правой кнопкой мыши (например, в проводнике Windows, на рабочем столе или в открытом каталоге Windows) по файлу или каталогу, который вы хотите проверить.

↳ Появится контекстное меню проводника Windows.

▸ В контекстном меню выберите **Проверить выбранные файлы с помощью Avira**.

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

↳ По окончании проверки будут показаны результаты.

4.3.8 Прямой поиск: Автоматический поиск вирусов и вредоносного ПО

Указание
После установки в планировщике устанавливается задача *Complete system scan*: через рекомендуемые промежутки времени автоматически проводится полная проверка системы.

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

▸ В центре управления нажмите во вкладке *Administration* > Scheduler.

▸ Нажмите пиктограмму  **Insert new job**.

↳ Появится диалоговое окно **Name and description of the job**.

- Введите имя и описание задачи.
- Нажмите **Next**.

↳ Появится диалоговое окно **Type of job**.

- Выберите строку **Scan job**.
- Нажмите **Next**.

↳ Появится диалоговое окно **Selection of the profile**.

- Выберите профиль для проверки.
- Нажмите **Next**.

↳ Появится диалоговое окно **Time of the job**.

- Выберите время проведения проверки:

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Single**
- **Login**

- В зависимости от выбора задайте время.
- При необходимости выберите следующую дополнительную опцию (доступна в зависимости от задачи): **Repeat job if time has expired**

↳ Выполняются задачи, срок выполнения которых уже прошел, но они не могли быть запущены в назначенное время, например если компьютер был выключен.

- Нажмите **Next**.

↳ Появится диалоговое окно **Selection of the display mode**.

- Выберите режим отображения задачи:

- **invisible**: нет окна задачи
- **minimized**: только прогресс выполнения
- **maximized**: все окно задачи

- Выберите опцию **Shut down computer if job is done**, если вы хотите автоматически отключить компьютер, как только задача будет выполнена и завершена.

  Опция доступна в минимизированном и максимизированном режиме отображения.

- Нажмите кнопку **Finish**.

↳ Новое установленное задание будет отмечено галочкой как активированное на стартовой странице раздела *Administration* > Scheduler.

- Деактивируйте задачи, которые не должны выполняться.

Используя следующие символы, вы можете обработать задания:

 Просмотреть свойства каждого задания

 Изменение задачи

 Удаление задачи

 Запустить задачу

Остановить задачу

4.3.9 Прямой поиск: Целенаправленный поиск активных Rootkits

Для поиска активных Rootkits используйте предустановленный профиль поиска **Поиск Rootkits и активного вредоносного ПО**.

Прямой поиск активных Rootkits:

- В центре управления выберите вкладку *PC PROTECTION* **> System Scanner**.
  - ↪ Появятся предустановленные профили поиска.
- Выберите предустановленный профиль поиска **Поиск Rootkits и активного вредоносного ПО**.
- Отметьте дополнительные узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле.
- Нажмите на символ (Windows XP:  или Windows Vista: ).
  - ↪ Появится окно **Luke Filewalker** и запустится прямой поиск.
  - ↪ По окончании проверки будут показаны результаты.

4.3.10 Реагировать на найденные вирусы и вредоносное ПО

Для отдельных компонентов защиты программы Avira в настройках можно настроить **Действия при обнаружении**, это значит, как будет реагировать Avira при обнаружении вируса или вредоносной программы.

Для компонента ProActiv Real-Time Protection не существует настраиваемых опций действия: обнаружение всегда отображается в окне **Real-Time Protection: подозрительное поведение приложения**.

Опции действия для System Scanner:

- **Интерактивный**

  В интерактивном режиме обнаруженные System Scanner объекты показываются в диалоговом окне. Эта настройка включена по умолчанию.
  При проверке **System Scanner** 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 System Scanner.

- **Автоматический**

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

Опции действия для модуля Real-Time Protection:

- **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 System Scanner для дополнительной обработки вируса. System Scanner сообщает об обнаружении в окне, в котором вам в контекстном меню доступны различные опции для обработки соответствующего файла (см. Обнаружение > System Scanner).

- **Автоматический**

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

Опции действия для Mail Protection, Web Protection:

- **Интерактивный**

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

- **Автоматический**

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

Интерактивный режим

- В интерактивном режиме при обнаружении вирусов или вредоносных программ в уведомлении вы можете выбрать **Действие с инфицированными объектами** и подтвердить свой выбор нажатием кнопки **Подтвердить**.

Вы можете выбрать одно из следующих действий:

> **Указание**
> Предлагаемые действия зависят от операционной системы, от защитных компонентов (Avira System Scanner, Avira Real-Time Protection, Avira Mail Protection, Avira Web Protection), которые сообщают об обнаруженных вирусах и вредоносных программах.

Действия модуля System Scanner и Real-Time Protection (без обнаружений ProActiv):

- **Лечить**

  Файл будет вылечен.
  Эту опцию можно выбрать, если лечение файла возможно.

- **Переименовать**

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

- **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.

- **Удалить**

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

- **Пропустить**

  Другие действия не выполняются. Инфицированный файл будет активен в вашей системе.

- **Переписать и удалить**

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

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

- **Всегда игнорировать**

  Действия при обнаружении вируса модулем Real-Time Protection: другие действия не выполняются. Доступ к файлу разрешается. Другой доступ к этому

файлу будет разрешен, о нем не будет сообщаться до перезапуска системы или до обновления файла вирусных сигнатур.

- **Копировать в карантин**

  Действие при обнаружении Rootkits: программа копируется в карантин.

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

  Действия при обнаружении инфицированных загрузочных секторов: доступен ремонт инфицированных дисков. Если восстановление с помощью программы Avira невозможно, можно загрузить специальную программу для обнаружения и удаления вирусов загрузочного сектора.

> **Указание**
> Используемые действия не могут быть применены к работающим процессам.

Действия модуля Real-Time Protection при обнаружении компонента 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. Фильтр приложения: Исключенные 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. Фильтр приложений: Блокируемые приложения).

- **Пропустить**

  Выполнение программы продолжается. Компонент ProActiv продолжает контролировать действия программы.

Действия модуля Mail Protection: Входящие письма

- **Поместить на карантин**

  Письмо со всеми приложениями помещается на Карантин. Инфицированное письмо удаляется. Тело письма и приложения к нему, если они есть, заменяются Стандартным текстовым шаблоном.

- **Удалить письмо**

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 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, ни в коем случае не запускайте приложения двойным щелчком!

Действия модуля Mail Protection: 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. В почтовой программе будет выдано сообщение об ошибке. При каждой последующей отправке с вашего адреса это письмо будет проверяться на вирусы.

- **Блокировать почту (не отправлять)**

  Письма не будут отправляться, оставаясь в папке с исходящей корреспонденцией. В почтовой программе будет выдано сообщение об ошибке. При каждой последующей отправке с вашего адреса это письмо будет проверяться на вирусы.

- **Пропустить**

  Инфицированное письмо будет отправлено.

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

Действия модуля Web Protection:

- **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.

- **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 отправляются модулем Web Protection вашему веб-браузеру.

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

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

Указание
Отправьте нам для проверки файлы, отмеченные эвристикой.
Загрузите их на наш сайт: http://www.avira.ru/sample-upload
Файлы, обнаруженные эвристикой, отмечены обозначением *HEUR/* или *HEURISTIC/* перед именем файла, напр.: *HEUR/testdatei.**.

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

Обращение с файлами, помещенными на карантин:

- В центре управления нажмите 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 Avira 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  .
- Подтвердите кнопкой **Да**.

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

- Отметьте файл, который вы хотите загрузить.
- Нажмите  .
  - ↳ Откроется диалог *Выгрузка файла* с формуляром для ваших контактных данных.
- Введите полные данные.
- Выберите тип **Подозрительный файл**, **Подозрение на** или **Ложное срабатывание**.
- Выберите формат ответа: **HTML**, **Text**, **HTML & Text**.
- Нажмите кнопку **OK.**
  - ↳ Файл загружается в заархивированном виде на веб-сервер в центр исследований вирусов компании Avira.

Указание
В следующих случаях рекомендуется анализ центра Avira Malware Research Center:
Эвристическое совпадение (подозрительный файл): во время проверки программа Avira распознала файл как подозрительный и поместила его в карантин: в диалоговом окне или в файле отчета о проверке была рекомендована проверка файла центром Avira Malware Research Center.
Подозрительный файл: Вы определили файл как подозрительный и поэтому поместили его на карантин, однако проверка файла на вирусы говорит об обратном.

Подозрение на Ложное срабатывание: Вам кажется, что при обнаружении вируса имеет место ложное срабатывание: ваша программа Avira сообщает об обнаружении вируса с высокой вероятностью того, что файл не поврежден вредоносной программой.

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

Указание
Вы можете загрузить только один файл.

Для копирования объекта из карантина в другой каталог:

- Выделите объект карантина и нажмите  .
  - ↪ Откроется диалог *Search folder*, в котором можно выбрать нужную папку.
- Выберите папку, в которую необходимо скопировать объект карантина и подтвердите выбор нажатием**OK**.
  - ↪ Выделенный объект карантина сохраняется в указанном каталоге.

Указание
Объект карантина не будет идетничным 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 в карантине можно восстановить (см. главу: Карантин: Восстановление файлов в карантине).

4.3.12 Карантин: Восстановление файлов в карантине

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

- **Windows XP и 2000**:

 С помощью этого символа вы восстановите файл в первоначальную папку.

 С помощью этого символа вы восстановите файл в указанную папку.

- **В Windows Vista**:

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

   С помощью этого символа вы восстановите файл в указанную папку.

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

Восстановление файлов из карантина:

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

✓ Повторно проверить и вылечить файл.

▸ В центре управления нажмите выберите во вкладке *Управление* **> Карантин**.

Указание

Электронные письма и вложения восстанавливаются только с опцией  и расширением **.eml*.

Если вы хотите восстановить файл в его прежнюю папку:

▸ Отметьте файл и нажмите кнопку с символом (Windows XP:  , Windows Vista ).

Эта функция недоступна для электронных писем.

Указание

Электронные письма и вложения восстанавливаются только с опцией  и 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.

4.3.13 Карантин: Поместить подозрительный файл на карантин

Вы можете поместить подозрительный файл на карантин вручную:

- В центре управления нажмите выберите во вкладке *Управление* **> Карантин**.
- Нажмите  .
  - ↪ Появится стандартное окно выбора файлов Windows.
- Выберите необходимый файл и подтвердите свой выбор **Открыть**.
  - ↪ Файл переместится в папку карантина.

Файлы в карантине можно проверить программой Avira System Scanner (см. главу: Карантин: Обращение с файлами (*.qua), помещенными на карантин).

4.3.14 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):

- ✓ Вы находитесь в центре управления на вкладке *Безопасность компьютера* **> System Scanner**.
- Щелкните правой кнопкой мыши по профилю поиска, который вы хотите обработать.
  - ↪ Появится контекстное меню.
- Выберите строку **Фильтр файла**.
- Разверните контекстное меню, нажав на маленький треугольник на правой стороне контекстного меню.
  - ↪ Появятся пункты **По умолчанию**, **Проверить все файлы** и **Настраивается пользователем**.

- Выберите строку **Настраивается пользователем**.
  - ↪ Появится диалоговое окно **Расширения** 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 типа файлов.

  Максимальная длина расширения не может превышать 10 символов, не ставьте точку перед расширением. Допустимы специальные символы (* и ?).

4.3.15 Профиль поиска: Создание ярлыка для профиля поиска

С помощью ярлыка прямой поиск можно запускать непосредственно с рабочего стола, не открывая центр управления программы Avira.

Создать ярлык к выбранному профилю на рабочем столе:

- ✓ Вы находитесь в центре управления на вкладке *Безопасность компьютера* **> System Scanner**.
- Выберите профиль поиска, для которого вы хотите создать ярлык.
- Нажмите пиктограмму  .
  - ↪ Появится ярлык на рабочем столе.

4.3.16 События: Фильтрование событий

В центре управления в *УПРАВЛЕНИЕ* **> События** показываются все события, созданные компонентами программы Avira (по аналогии с индикацией событий вашей операционной системы Windows). Ниже представлены компоненты программы:

- Backup
- Web Protection
- Real-Time Protection
- Mail Protection
- FireWall
- Helper Service
- Scheduler
- Safe Browsing

- System Scanner
- Модуль обновления

Отображаются следующие типы событий:

- *Information*
- *Warning*
- *Error*
- *Detection*

Фильтрация отображаемых событий:

- В центре управления выберите вкладку *Управление* **> 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.

4.3.17 Mail Protection: Исключить адреса из проверки

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

- В центре управления выберите вкладку *ИНТЕРНЕТ-БЕЗОПАСНОСТЬ* **> Mail Protection**.

  ↪ В списке вы увидите входящие письма.
- Отметьте письма, которые вы хотите исключить из проверки Mail Protection.
- Нажмите на необходимый символ, чтобы исключить письмо из проверки Mail Protection:

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

   Выделенный адрес в дальнейшем не будет проверяться на наличие спама.

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

Предупреждение
Поэтому исключайте из проверки Mail Protection только надежные адреса.

Указание
В конфигурации Mail Protection > Общее > Исключения вы можете внести дополнительные адреса в список исключений или удалить оттуда адреса.

4.3.18 Mail Protection: Тренировать модуль AntiSpam

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

Сортировка электронных писем для учебной базы данных:

- В центре управления выберите вкладку *ИНТЕРНЕТ-БЕЗОПАСНОСТЬ* > **Mail Protection**.
  - ↪ В списке вы увидите входящие письма.
- Отметьте письма, которые вы хотите сортировать.
- Нажмите на необходимый символ, чтобы обозначить письмо, например, как *спам*  или как *"чистое"* письмо  .
  - ↪ Письмо будет сохранено в учебной базе данных и в следующий раз будет использовано для распознавания спама.

Указание
Вы можете удалить учебную базу данных здесь: **Mail Protection > Общее > AntiSpam**.

Указание
Исключение избранных Email-адресов из процедуры проверки на наличие вредоносного ПО касается только входящих писем. Функции обучения модуля AntiSpam и исключений AntiSpam также касаются исключительно входящей почты. Для отключения проверки исходящих писем отключите ее в настройках Mail Protection > Поиск.

4.3.19 FireWall: выбор уровня безопасности в брандмауэре

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

Доступны следующие уровни безопасности:

Низкий

Распознается сканирование портов и флудинг.

Средний

Запрещаются подозрительные TCP- и UDP-пакеты.

Предотвращается сканирование портов и флудинг.

(стандартная настройка)

Высокий

Компьютер невидим в сети.

Блокируются соединения извне.

Предотвращается сканирование портов и флудинг.

Пользователь

Правила, установленные пользователем: Программа автоматически переключается на этот режим, если вы изменили правила адаптера.

Блокировать все

Завершает все текущие сетевые соединения.

> **Указание**
> Стандартная настройка уровня безопасности для всех предопределенных правил модуля Avira FireWall - **Средний**.

Уровень безопасности брандмауэра выбирается следующим образом:

- В центре управления выберите вкладку *PC PROTECTION* **> FireWall**.
- Установите ползунковый регулятор на необходимый уровень безопасности.
  - ↪ Уровень безопасности становится активным.

4.3.20 Backup: Создание Backups вручную

С помощью инструментов Backup в центре управления можно быстро и просто создать резервную копию своих данных. С помощью модуля Avira Backup можно создавать так называемые зеркальные копии, позволяющие сохранять текущее состояние ваших данных, не используя большое количество системных ресурсов. При создании резервной копии с помощью Avira Backup сохраняемые данные можно проверять на наличие вирусов и вредоносного ПО. Инфицированные файлы не сохраняются.

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

Указание
При использовании Avira Backup с настройками по умолчанию сохраняются только измененные файлы и проводится проверка на наличие вирусов и вредоносного ПО. Вы можете изменять эту настройку здесь: Backup > Настройки.

Так можно создать резервную копию при помощи инструментов Backup:

- В центре управления выберите вкладку *Безопасность компьютера* **> Backup**.
  - ↪ Появятся предустановленные профили Backup.
- Выберите один из предустановленных профилей Backup.

  -ИЛИ-

  Примените профиль Backup **Выбор вручную**.

  -ИЛИ-

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

  Вы можете указать в качестве папки для Backup папку на Вашем компьютере, сетевой диск или сменный носитель, например, USB.
- Нажмите пиктограмму  .
  - ↪ Появится окно **Avira Backup** и начнется создание резервной копии. Состояние и результаты Backup отобразятся в окне Backup.

Если вы хотите настроить профиль Backup:

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

Возможны следующие варианты резервного копирования:

- Каталог с подкаталогами (черная галочка)
- Только отдельные подкаталоги внутри каталога (серая галочка, у подкаталогов галочка черная)
- Не выделять (галочка отсутствует)

Если вы хотите создать новый профиль Backup:

- Нажмите пиктограмму **Создать новый профиль**.
  - ↪ Среди имеющихся профилей появится *Новый профиль*.
- При необходимости переименуйте профиль Backup, нажав пиктограмму .
- Отметьте узлы и папки, для которых вы создаете резервную копию, поставив флажок в соответствующем поле.

Возможны следующие варианты резервного копирования:

- Каталог с подкаталогами (черная галочка)
- Только отдельные подкаталоги внутри каталога (серая галочка, у подкаталогов галочка черная)
- Без каталогов (галочка отсутствует)

4.3.21 Автоматическое создание резервных копий

Как инициировать автоматическое резервное копирование:

- В центре управления выберите вкладку *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 **Задача резервирования**.
- Нажмите **Далее**.
  - ↪ Появится диалоговое окно **Выбор профиля**.
- Выберите профиль для проверки.

Указание
Отобразятся только профили резервирования, для которых задавалась папка резервирования.

- Нажмите **Далее**.
  - ↪ Появится диалоговое окно **Время задачи**.
- Выберите время проведения проверки:

- **Немедленно**
- **Ежедневно**
- **Еженедельно**
- **Интервал**
- **Однократно**
- **Логин**
- **Plug&Play**

  При событии **Plug&Play** резервирование происходит тогда, когда сменный носитель, выбранный в качестве хранилища профиля резервирования, подключается к компьютеру. Для события **Plug&Play** необходимо, чтобы в качестве места хранения резервной копии было указано USB-устройство.

- В зависимости от выбора задайте время.
- При необходимости выберите следующую дополнительную опцию (доступна в зависимости от 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:

- **минимум**: только прогресс выполнения
- **максимум**: все окно резервирования
- **невидимый**: нет окна резервирования

- Нажмите кнопку **Завершить**.
  - ↪ Новое задание будет отмечено галочкой как активированное на стартовой странице раздела *Управление* **> Планировщик**.
- Деактивируйте задачи, которые не должны выполняться.

Используя следующие символы, вы можете обработать задания:

 Просмотреть свойства каждого задания

 Изменение задачи

 Удаление задачи

 Запустить задачу

 Остановить задачу

5. System Scanner

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

- **Прямой поиск с помощью контекстного меню**
  Прямой поиск с помощью контекстного меню (правая клавиша мышки - пункт **Проверить выбранные файлы с помощью Avira**) рекомендуется, например, 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 не требуется запуск Центра управления.
- **Прямой поиск с помощью Drag&Drop**
  При перетягивании файла или папки в окно программы Центр управления компонент System Scanner проверяет файл или каталог, а также все существующие подкаталоги. Эта процедура рекомендуется, если вы хотите проверить отдельные файлы и папки, которые, например, находятся на вашем рабочем столе.
- **Прямой поиск через профили**
  Эта процедура рекомендуется, если вы хотите регулярно проверять определенные папки и диски (например, Ваш рабочий стол или диски, на которые вы регулярно сохраняете новые файлы). Вам не нужно выбирать эти папки и диски перед каждой проверкой, просто сделайте выбор с помощью соответствующего профиля. См. Проверка через профиль.
- **Проверка через планировщик**
  Планировщик позволяет запускать проверки в заданное время. См. Прямой поиск с помощью планировщика.

При поиске Rootkits, вирусов загрузочных секторов и при проверке активных процессов необходимы специальные методы. Вы располагаете следующими опциями настройки:

- Поиск Rootkits с помощью профиля поиска **Поиск Rootkits и активного вредоносного ПО**
- Проверка активных процессов через профиль поиска **Активные процессы**
- Поиск вирусов загрузочных секторов через команду **Проверка загрузочных записей** в меню **Дополнительно**

6. Обновления

Эффективность антивирусного ПО напрямую зависит от актуальности состояния программы, особенно VDF-файла и движка. Для выполнения обновления модуль обновления встроен в программу Avira. Модуль обновления отвечает за то, чтобы программа Avira всегда находилась на самом актуальном уровне и могла обнаруживать ежедневно появляющиеся вирусы. Этот модуль обновляет следующие компоненты:

- Файл вирусных сигнатур:

  VDF-файл содержит шаблоны вредоносных кодов, используемых Avira при проверке на вирусы и вредоносное ПО или лечении файлов.

- Поисковый движок:

  Поисковый движок Avira применяет различные методы обнаружения вирусов и вредоносных программ.

- Программные файлы (обновление продукта):

  Пакеты обновлений продукта предоставляют в распоряжение отдельные программные компоненты.

При выполнении обновлений VDF-файл и поисковый движок проверяются на актуальность и при необходимости обновляются. После обновления программы может потребоваться перезапуск компьютера. Если обновляется только файл VDF и поисковый движок, перезагрузка не требуется.

Если после обновления продукта необходима перезагрузка, то Вы можете решить самостоятельно, продолжать обновление или дождаться, когда Вам об этом напомнят позже. Если Вы решили продолжать обновление, то Вы можете решить, когда должна состояться перезагрузка.

Если Вы хотите обновить продукт позже, то, несмотря на это, обновляется файл вирусных сигнатур и поисковый движок, но не программные файлы.

Указание
Обновление продукта не будет завершено, пока не состоится перезагрузка.

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

Обновление автоматически выполняется через рекомендованный промежуток 2 часа.

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 вкладке **Состояние**
- С помощью контекстного меню значка в трее

Вы загружаете обновления из Интернет с веб-сервера разработчика. По умолчанию используется существующее сетевое соединение с сервером Avira. Вы можете изменить эти настройки в меню Настройка > Обновление.

7. FireWall

Avira Internet Security позволяет контролировать и регулировать входящие и исходящие потоки данных в соответствии с настройками Вашего компьютера:

- Avira FireWall

В операционных системах до Windows 7 брандмауэр Avira FireWall содержится в Avira Internet Security.

8. Резервное копирование

У вас есть различные возможности для создания резервной копии данных:

С помощью инструмента резервного копирования

С помощью инструмента резервного копирования вы можете выбрать или создать профиль резервного копирования и вручную запустить процесс резервного копирования для выбранного профиля .

Резервное копирование с помощью задания резервного копирования в планировщике

Планировщик дает возможность создавать реагирующие на время или на конкретное событие задачи резервного копирования. Планировщик автоматически выполняет задания резервного копирования. Этот метод удобен, если нужно регулярно создавать резервные копии определенных файлов .

9. Устранение проблемы, рекомендации

В этой главе содержатся важные указания по устранению проблем и другие советы по работе с вашим продуктом Avira.

- См. главу Помощь в сложных случаях
- См. главу Горячие клавиши
- см. главу Центр обеспечения безопасности Windows (для Windows XP и Vista) или Центр поддержки Windows (начиная с Windows 7)

9.1 Помощь в случае возникновения проблем

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

- Появляется сообщение об ошибке *Не удается открыть файл лицензии*.
- Сообщение об ошибке *Соединение было разорвано при загрузке файла ...* появляется при попытке запустить обновление.
- Вирусы и вредоносные программы невозможно удалить или переместить.
- Значок в трее свидетельствует об отключении программы.
- Компьютер работает очень медленно, когда я произвожу резервное копирование данных.
- Мой Firewall при включении сразу же выдает сообщение о Avira Real-Time Protection и Avira Mail Protection, как только они включаются
- Avira Mail Protection не работает.
- В виртуальных машинах сетевое соединение недоступно, если Avira FireWall установлен в главной операционной системе и для Avira FireWall установлен *средний* или *высокий* уровень безопасности.
- Соединение Virtual Private Network (VPN) блокируется, если в Avira FireWall установлен *средний* или *высокий* уровень безопасности.
- Письмо, отправленное через TLS-соединение, было заблокировано приложением Mail Protection.
- Веб-чат не работает: сообщения чата не отображаются.

Появляется сообщение об ошибке *Не удается открыть файл лицензии*.

Причина: файл зашифрован.

- Для активации лицензии не нужно открывать файл, достаточно сохранить его в программной директории.

Сообщение об ошибке *Соединение было разорвано при загрузке файла ...* появляется при попытке запустить обновление.

Причина: Ваше Интернет-соединение неактивно. Поэтому невозможно установить связь с веб-сервером.

- Проверьте, работают ли другие Интернет-службы, например, WWW или электронная почта. Если они не работают, восстановите соединение с Интернетом.

Причина: Прокси-сервер недоступен.

- Проверьте, не изменился ли логин для входа на прокси-сервер, в случае необходимости скорректируйте настройки.

Причина: Ваш Firewall не полностью разрешает выполнение файла *update.exe*.

- Убедитесь в том, что выполнение файла *update.exe* полностью разрешено вашим Firewall.

В противном случае:

- Проверьте параметры в настройках (режим эксперта) в Безопасность ПК > Обновление.

Вирусы и вредоносные программы невозможно удалить или переместить.

Причина: Файл загружен Windows и находится в активном состоянии.

- Обновите свой продукт Avira.
- Если вы используете операционную систему Windows XP, отключите восстановление системы.
- Запустите компьютер в безопасном режиме.
- Откройте настройки продукта Avira (режим эксперта).
- Выберите **System Scanner > Поиск**, активируйте в поле *Файлы* опцию **Все файлы** и подтвердите изменения нажатием на **OK**.
- Запустите проверку всех локальных дисков.
- Запустите компьютер в обычном режиме.
- Проверьте систему в обычном режиме.
- Если другие вирусы или вредоносные программы не обнаружены, активируйте восстановление системы, если оно имеется и должно использоваться.

Значок в трее свидетельствует об отключении программы.

Причина: приложение Avira Real-Time Protection отключено.

- Щелкните в Центре управления по пункту **Статус** и активируйте в области *Безопасность ПК* **Real-Time Protection**.

- ИЛИ-

- Щелкните правой кнопкой мыши по значку в трее на панели задач. Откроется контекстное меню. Щелкните по кнопке **Активировать Real-Time Protection**.

Причина: приложение Avira Real-Time Protection блокируется Firewall.

- Установите в настройках вашего Firewall общее разрешение для Avira Real-Time Protection. Приложение Avira Real-Time Protection работает только с адресом 127.0.0.1 (local host). Соединение с Интернетом не устанавливается. То же верно для Avira Mail Protection.

В противном случае:

- Проверьте способ запуска службы Avira Real-Time Protection. При необходимости включите эту службу: выберите на панели задач **Пуск > Настройки > Панель управления**. Откройте окно настроек двойным щелчком по кнопке **Службы** (в Windows XP приложение находится в поддиректории *Администрирование*). Найдите запись *Avira Real-Time Protection*. Для способа запуска выберите `автоматически`, для статуса `запущен`. При необходимости запустите приложение вручную, выбрав соответствующую строку и нажав клавишу **Пуск**. Если возникает сообщение об ошибке, проверьте список событий.

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

Причина: Avira Real-Time Protection проверяет во время процесса резервного копирования все файлы, с которыми работает служба резервного копирования.

- Выберите в пункте Настройки (Режим эксперта) **Real-Time Protection > Поиск > Исключения** и укажите имя процесса программы резервного копирования.

Мой Firewall при включении сразу же выдает сообщение о Avira Real-Time Protection и Avira Mail Protection, как только они включаются.

Причина: Связь с Avira Real-Time Protection и Avira Mail Protection осуществляется через протокол TCP/IP. Брандмауэр отслеживает все соединения, производящиеся по этому протоколу.

- Установите в настройках вашего Firewall общее разрешение для Avira Real-Time Protection и Avira Mail Protection. Приложение Avira Real-Time Protection работает только с адресом 127.0.0.1 (local host). Соединение с Интернетом не устанавливается. То же верно для Avira Mail Protection.

Avira Mail Protection не работает.

✓ Проверьте работоспособность Avira Mail Protection по следующим пунктам, если возникают проблемы с Avira Mail Protection.

Пункты проверки

- ✓ Проверьте, связывается ли почтовый клиент с сервером через Kerberos, APOP или RPA. Эти методы аутентификации в настоящее время не поддерживаются.
- ✓ Проверьте, использует ли ваш почтовый клиент SSL (также часто называется TLS - Transport Layer Security) на сервере. Avira Mail Protection не поддерживает SSL и поэтому завершает работу зашифрованных соединений SSL. Если вы хотите использовать зашифрованные соединения SSL без защиты Avira Mail Protection, вам следует использовать другой, не контролируемый Avira Mail Protection, порт для соединения. Контролируемые модулем Mail Protection порты можно изменить в настройках **Avira Mail Protection > Поиск**.
- ✓ Включена ли служба Avira Mail Protection? При необходимости включите эту службу: выберите на панели задач **Пуск > Настройка > Панель управления**. Откройте окно настроек двойным щелчком по кнопке **Службы** (в Windows XP приложение находится в поддиректории *Администрирование*). Найдите запись *Avira Mail Protection*. Для способа запуска выберите `автоматически`, для статуса `запущен`. При необходимости запустите приложение вручную, выбрав соответствующую строку и нажав клавишу **Пуск**. Если возникает сообщение об ошибке, проверьте *список событий*. Если не удалось исправить положение, необходимо полностью удалить продукт Avira через **Пуск > Настройка > Панель управления > Программы**, перезагрузить компьютер и вновь установить продукт Avira.

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.
- Ваш продукт Avira не проверяет при отправке письма на вирусы и вредоносные программы.

> **Примечание**
> Мы рекомендуем вам регулярно производить обновление продуктов Microsoft для того, чтобы закрыть возможные бреши в системе безопасности.

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

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

Причина: Виртуальная машина эмулирует программными средствами сетевую карту. За счет эмуляции пакеты данных гостевой системы помещаются в специальные пакеты данных (так называемые guest system) и направляются через внешний шлюз в хост-систему. Начиная с уровня безопасности *средний*, Avira FireWall блокирует эти пакеты, поступающие извне.

Чтобы этого избежать, проделайте следующее:

- В центре управления выберите вкладку *ИНТЕРНЕТ-БЕЗОПАСНОСТЬ* > **FireWall**.
- Щелкните по ссылке **Настройки**.
- Появится диалоговое окно *Настройки*. Вы находитесь в разделе настроек *правил приложений*.
- Включите **Режим эксперта**.
- Выберите раздел настроек **Правила адаптера**.
- Нажмите кнопку **Добавить**.
- Выберите во *Входящих правилах* **UDP**.
- Укажите *имя* правила в поле **Имя правила**.
- Нажмите кнопку **OK**.
- Проверьте, имеет ли данное правило приоритет перед правилом **Запрещать все IP-пакеты**.

Предупреждение
Это правило является потенциально опасным, так как пропускает UDP-пакеты без фильтрации! Установите после работы с виртуальной машиной исходный уровень безопасности.

Соединение Virtual Private Network (VPN) блокируется, если в Avira FireWall установлен *средний* или *высокий* уровень безопасности.

Причина: Как правило, все пакеты, не соответствующие правилам, установленным по умолчанию, не разрешаются. Отправленные через VPN пакеты проверяются на соответствие этим правилам, так как они на основании своего типа (так называемых пакетов GRE) не могут быть отнесены ни к одной другой категории.

- Добавьте к **Правилам адаптера** настройки Avira FireWall **Разрешить VPN-соединения**, чтобы разрешить все пакеты, относящиеся к VPN.

Электронное письмо, отправленное через TLS-соединение, было заблокировано приложением Mail Protection.

Причина: Transport Layer Security (TLS: зашифрованный протокол передачи данных в Интернете) в настоящее время не поддерживается приложением Mail Protection. У вас есть несколько возможностей отправить электронное письмо:

- Используйте другой порт, чем используемый SMTP порт 25. Так вы сможете избежать проверки модулем Mail Protection.
- Откажитесь от закодированного TLS-соединения и отключите поддержку TLS в своем почтовом клиенте.
- Отключите (временно) проверку исходящих писем с помощью Mail Protection в настройках **Mail Protection > Поиск**.

Веб-чат не работает: сообщения чата не отображаются.

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

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

- В настройках введите URL веб-чата в качестве исключения (см. настройки: Web Protection > Поиск > Исключения).

9.2 Горячие клавиши

Горячие клавиши позволяют быстро перемещаться в программе, вызывать отдельные модули и выполнять действия.

Ниже приводится список доступных горячих клавиш. Подробную информацию о функциях и их доступности найдете в соответствующих разделах справочной системы.

9.2.1 В диалоговых полях

Горячие клавиши	Описание
Ctrl + Tab **Ctrl + Page Down**	Навигация в центре управления Переход к следующему разделу.
Ctrl +Shift + Tab **Ctrl + Page Down**	Навигация в центре управления Переход к предыдущему разделу.

←↑→↓	Навигация по вкладкам настроек Сначала установите курсор мыши на раздел настроек. Переключение между опциями в выделенном выпадающем списке или в одной группе опций.
Tab	Переход к следующей опции / группе опций.
Shift + Tab	Переход к предыдущей опции / группе опций.
Пробел	Включение / выключение кнопки-флажка, если активная опция представляет собой кнопку-флажок.
Alt + буква с подчеркиванием	Выбор опции или выполнение команды.
Alt + ↓ **F4**	Открыть выбранный раскрывающийся список.
Esc	Закрыть выбранный раскрывающийся список. Прервать выполнение команды и закрыть диалоговое окно.
Enter	Выполнение команды активной опции или кнопки.

9.2.2 В справке

Горячие клавиши	Описание
Alt + Пробел	Отображение системного меню.
Alt + Tab	Переключение между окном справки и другими открытыми окнами.
Alt + F4	Закрыть окно справки.
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 выше текущей в оглавлении, индексе или списке результатов поиска.
Page down	Переход к теме, расположенной в содержании, индексе или списке результатов поиска ниже текущей.
Page up **Page down**	Пролистывание страниц 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	Запуск обновления

Раздел **System Scanner**

Горячие клавиши	Описание
F2	Переименование выбранного профиля
F3	Запуск проверки с выбранным профилем

F4	Создание ярлыка на рабочем столе для выбранного профиля
Ins	Создать новый профиль
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...
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 **Отчеты**

Горячие клавиши	Описание
F3	Показать файл отчета
F4	Печатать файл отчета
Enter	Отображение отчета
Del	Удалить отчет(ы)

Раздел **События**

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

9.3 Центр безопасности Windows

- от Windows XP Service Pack 2 до Windows Vista -

9.3.1 Общее

Центр обеспечения безопасности Windows проверяет статус компьютера с точки зрения важнейших аспектов безопасности.

Если обнаруживается проблема в отношении одного из этих пунктов (напр., устаревшая антивирусная программа), Центр обеспечения безопасности выдает соответствующее предупреждение и дает рекомендации по более качественной организации защиты компьютера.

9.3.2 Центр обеспечения безопасности Windows и ваш продукт Avira

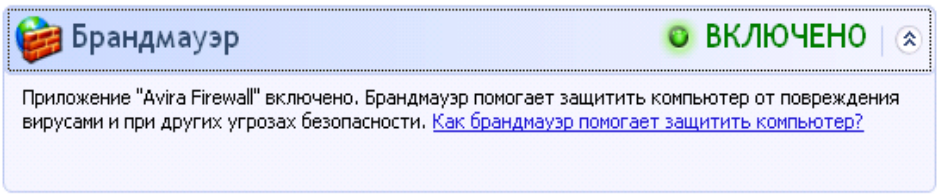
FireWall

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

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

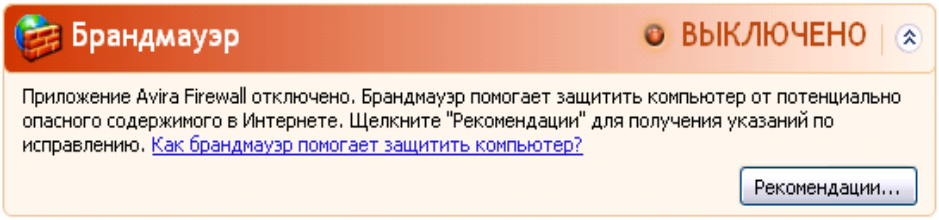
Брандмауэр АКТИВИРОВАН / Брандмауэр включен

После установки вашего продукта Avira и отключения брандмауэра Windows вы получите следующее уведомление:



Брандмауэр ДЕАКТИВИРОВАН / Брандмауэр выключен

При деактивации Avira FireWall выдается следующее сообщение:



Указание
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.

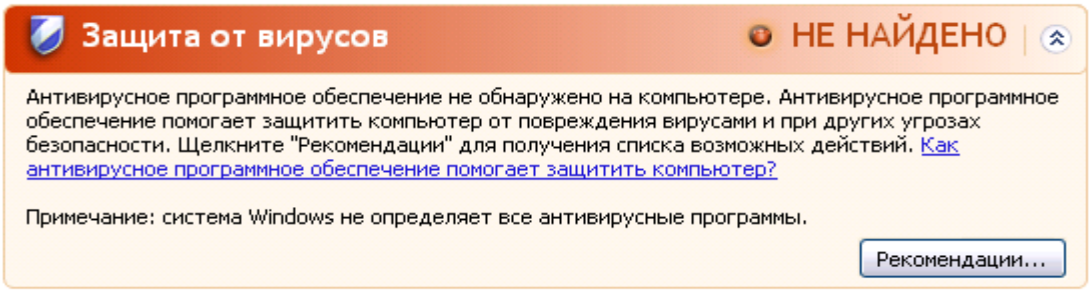
Антивирусное ПО / Защита от вредоносных программ

Вы можете получить от Центра обеспечения безопасности Windows 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

Антивирусных программ НЕ ОБНАРУЖЕНО

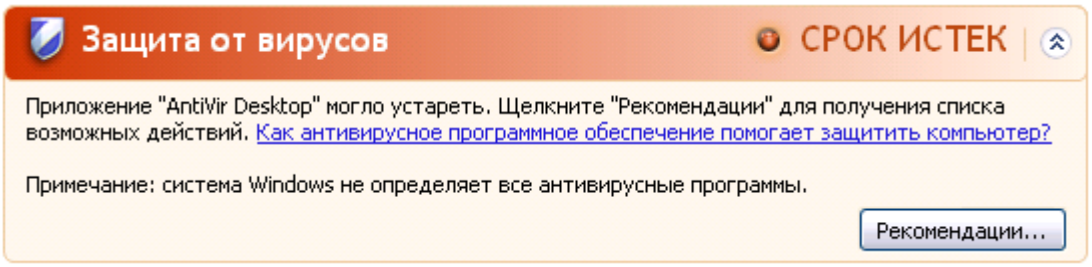
Это сообщение выдается Центром обеспечения безопасности Windows, если на компьютере не было обнаружено антивирусных программ.



Примечание
Установите программный продукт Avira на компьютер, чтобы защитить его от вирусов и иных вредоносных программ!

Антивирусные базы УСТАРЕЛИ

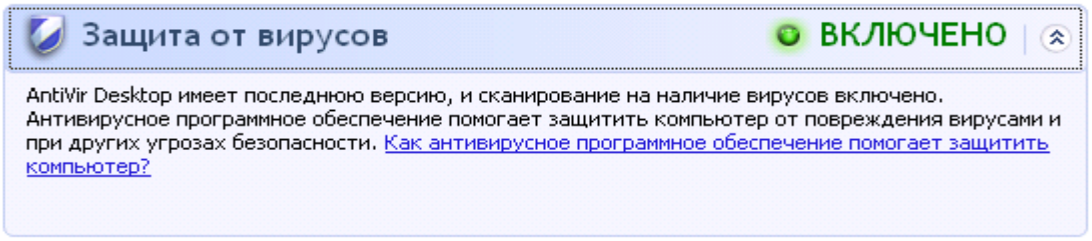
Если вы уже установили Windows XP Service Pack 2 или Windows Vista, а теперь устанавливаете продукт Avira или устанавливаете Windows XP Service Pack 2 или Windows Vista в систему, в которой уже установлен продукт Avira, будет выдано следующее сообщение:



Указание
Чтобы Центр обеспечения безопасности Windows счел продукт Avira актуальным, после установки программы необходимо произвести обновление. Обновить систему можно с помощью функции Обновление.

Защита от вирусов ВКЛЮЧЕНА

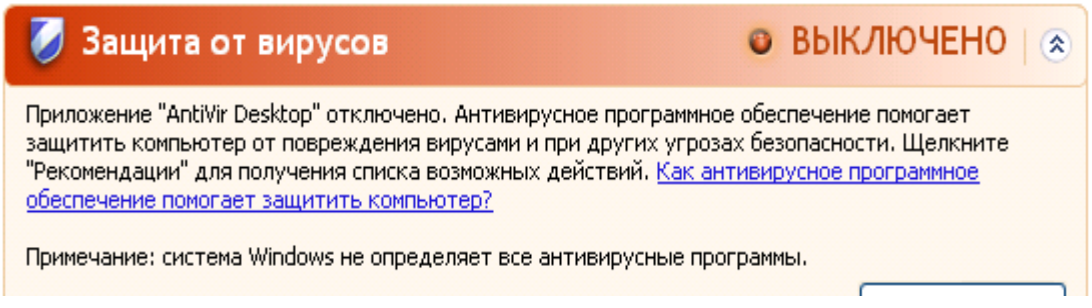
После установки продукта Avira и последующего обновления программы вы получите следующее уведомление:



Ваш продукт Avira обновлен до последней версии, модуль Avira Real-Time Protection активен.

Защита от вирусов ВЫКЛЮЧЕНА

Следующее уведомление выдается при отключенном сканере в режиме реального времени Avira или при остановке его работы.

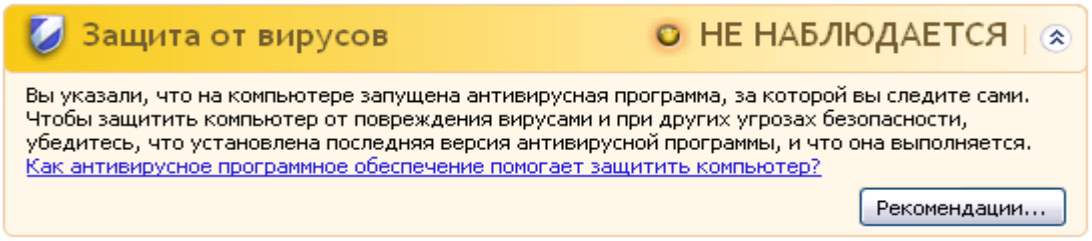


Указание
Активировать или отключить службу Avira Real-Time Protection можно в

разделе **Статус Центра управления**. О включении Avira Real-Time Protection свидетельствует раскрытый красный зонтик на панели задач.

Защита от вирусов НЕ КОНТРОЛИРУЕТСЯ

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



Указание
Эта функция не поддерживается системой Windows Vista.

Указание
Центр обеспечения безопасности Windows поддерживается вашим продуктом Avira. Вы можете включить эту опцию в любое время с помощью кнопки **Рекомендации...**.

Указание
Даже если вы установили на своей системе Windows XP Service Pack 2 или Windows Vista, вам все же требуется антивирусная система. Хотя Windows контролирует ваше антивирусное ПО, сама ОС не обладает функциями антивирусной защиты. Без дополнительных средств антивирусной защиты ваша система не защищена от вирусов и вредоносного ПО!

9.4 Центр поддержки Windows

- Windows 7 и Windows 8 -

9.4.1 Общее

Примечание:
Начиная с Windows 7, **Центр обеспечения безопасности Windows** стал называться **Центром поддержки Windows**. В этом разделе программы содержится статус всех опций безопасности.

Центр поддержки Windows проверяет статус компьютера с точки зрения важнейших аспектов безопасности. Вы можете напрямую войти в Центр поддержки, щелкнув по маленькому флажку в панели задач или через меню **Управление системой > Центр поддержки**.

Если обнаруживается проблема в отношении одного из этих пунктов (напр., устаревшая антивирусная программа), Центр поддержки выдает соответствующее предупреждение и дает рекомендации по более качественной организации защиты компьютера. Это значит, что при правильной работе компьютера Центр поддержки не будет выдавать сообщения. Тем не менее, статус безопасности компьютера можно отслуживать в **Центре поддержки** в рубрике **Безопасность**.
Также существует возможность управления установленными пользователем программами (например, *просмотреть антивирусные программы, установленные на компьютере*).

Предупреждающие сообщения можно отключить в **Центр поддержки > Изменить настройки** (например, *деактивировать сообщения о защите от шпионских программ и других вредоносных программ*).

9.4.2 Центр поддержки Windows и ваш программный продукт Avira

Сетевой брандмауэр

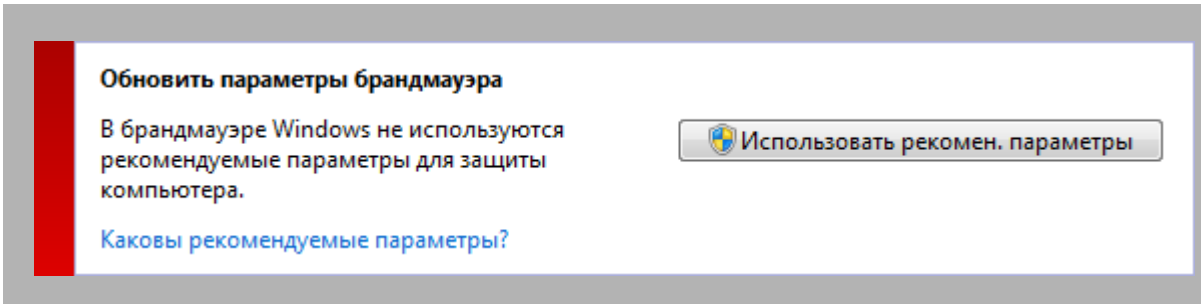
Вы можете получить из Центра поддержки следующую информацию о состоянии FireWall:

- Модуль Avira FireWall сообщил об активации
- Как брандмауэр Windows, так и Avira FireWall сообщили, что выключены
- брандмауэр Windows деактивирован или неправильно настроен

Модуль Avira FireWall сообщил об активации

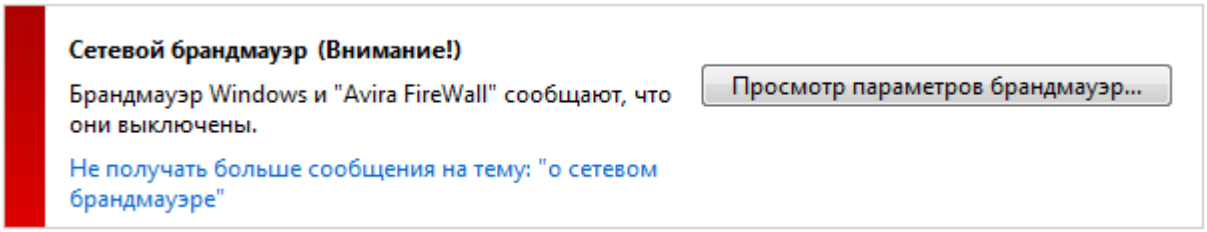
После установки вашего продукта Avira и отключения брандмауэра Windows вы получите следующее уведомление в **Центр поддержки > Безопасность > Сетевой брандмауэр**: *Модуль Avira FireWall сообщил об активации*. Это означает, что Avira FireWall является выбранным вами брандмауэром (следует различать Firewall (продукт Windows) и FireWall (продукт Avira)).

Предупреждение
Под **брандмауэром Windows не** подразумевается ваш **Avira FireWall**. Поэтому не следует беспокоиться, если вы получите следующие сообщения: *Обновить настройки брандмауэра* или ***Рекомендованные для защиты компьютера настройки не используются брандмауэром Windows.*** **Ваш продукт Avira исправно работает, и компьютер в безопасности**. Windows просто информирует вас о том, что отключены его собственные программы.



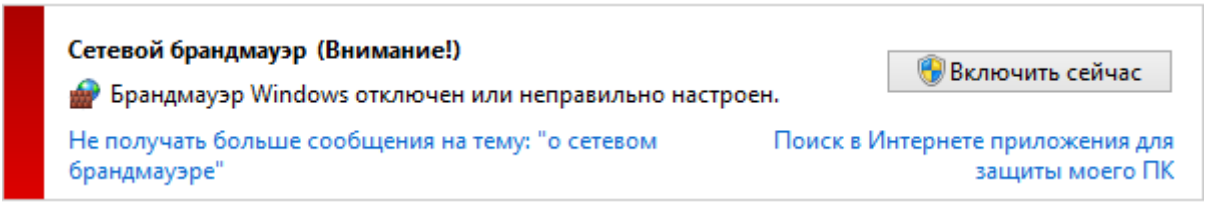
Как брандмауэр Windows, так и Avira FireWall сообщили, что выключены

При деактивации Avira FireWall выдается следующее сообщение:



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

Брандмауэр брандмауэр Windows деактивирован или неправильно установлен.



Это означает, что ни **брандмауэр Windows**, ни **Avira FireWall** не активированы.

- **В Windows 7**

  Avira FireWall деактивирован или неправильно настроен. Avira FireWall должен автоматически определяться Центром поддержки. Выполните перезагрузку. Если решить проблему не удалось, переустановите продукт Avira.

Защита от вирусов

Вы можете получить от Центра поддержки Windows следующую информацию, касающуюся защиты от вирусов:

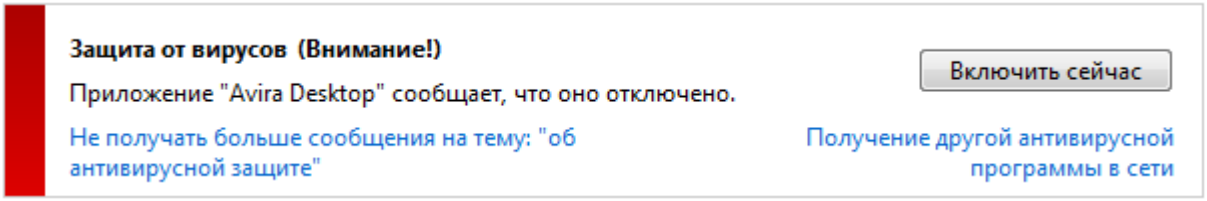
- Приложение Avira Desktop сообщает, что оно обновлено до новейшей версии и поиск вирусов включен
- Приложение Avira Desktop деактивировано

Приложение Avira Desktop сообщает, что оно обновлено до новейшей версии и поиск вирусов включен

После установки продукта Avira и последующего обновления программы вы сначала не получите от Центра поддержки Windows никаких уведомлений. Тем не менее, в разделе **Центр поддержки > Безопасность** будет можно найти следующее примечание: *Приложение Avira Desktop сообщает, что оно обновлено до новейшей версии и поиск вирусов включен*. Это значит, что ваш продукт Avira обновлен до последней версии, сканер в режиме реального времени Avira активен.

Приложение Avira Desktop деактивировано

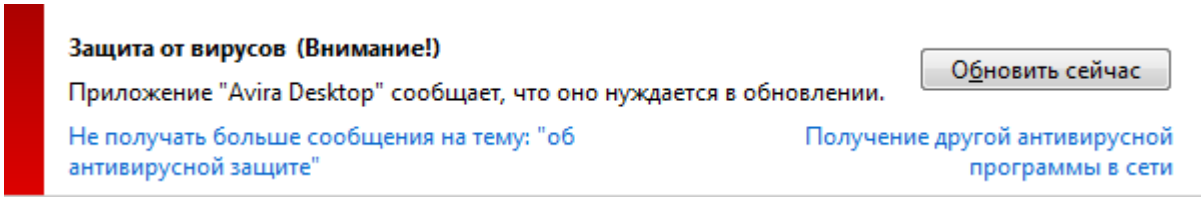
Следующее уведомление выдается при отключенном сканере в режиме реального времени Avira или при остановке его работы.



Примечание
Активировать или отключить **Avira Real-Time Protection** можно в разделе **Статус Центра Управления Avira**. О включении **Avira Real-Time Protection** свидетельствует раскрытый красный зонтик в панели задач. Отдельные компоненты Avira также можно включить щелчком по клавише *Включить сейчас* в Центре поддержки. При получении сообщения, требующего подтверждения продолжения работы программы Avira, щелкните по кнопке *Разрешить*, Avira Real-Time Protection будет включен.

Приложение Avira Desktop устарело

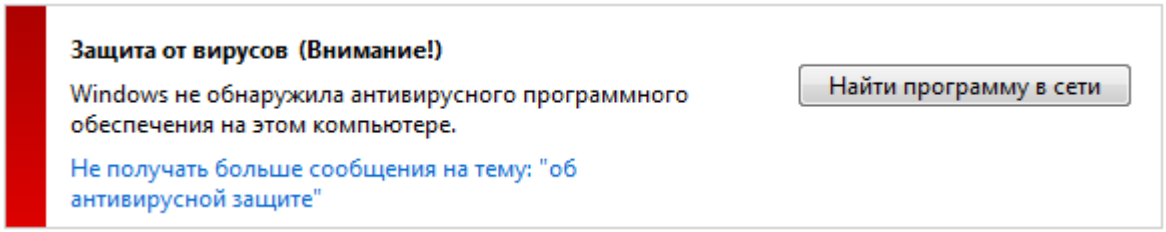
Если вы только что установили Avira или если по какой-либо причине файл вирусных сигнатур, поисковая система или программные файлы вашего продукта Avira не были автоматически обновлены (например при переходе с более ранней версии операционной системы Windows с уже установленным программным продуктом Avira к более поздней версии), вы получите следующее сообщение:



Примечание
Чтобы Центр поддержки Windows счел продукт Avira актуальным, после установки программы необходимо произвести обновление. Обновить систему можно с помощью функции Обновление.

На компьютере не обнаружено ни одной антивирусной программы

Это сообщение выдается Центром поддержки Windows, если Центр поддержки не обнаружил на компьютере антивирусных программ.

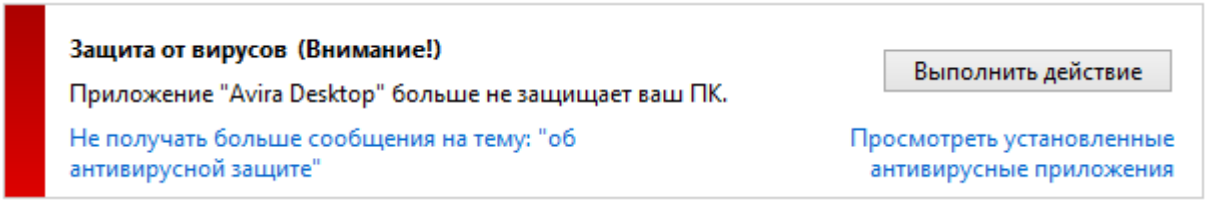


Примечание
Обратите внимание, что эта опция недоступна в Windows 8. Windows Defender, начиная с этой операционной системы, является предустановленной компанией Microsoft функцией защиты от вирусов.

Примечание
Установите программный продукт Avira на компьютер, чтобы защитить его от вирусов и иных вредоносных программ!

Ваш компьютер больше не защищен приложением Avira Desktop

Это примечание Центра поддержки Windows появляется, если срок действия вашей лицензии на продукт Avira истек.
Если щелкнуть по клавише **Выполнить действие**, вы будете перенаправлены на вебсайт Avira, где можно прибрести новую лицензию.



Примечание
Обратите внимание, что эта опция доступна только для Windows 8.

Защита от шпионских программ и других нежелательных программ

Вы можете получить от Центра поддержки Windows следующую информацию, касающуюся защиты от шпионских программ и других нежелательных программ:

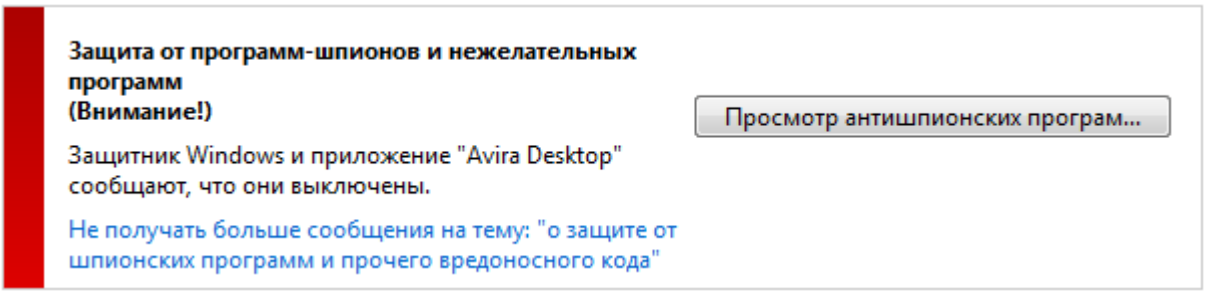
- Приложение Avira Desktop сообщает, что оно включено
- Как Windows Defender, так и Avira Desktop сообщили, что выключены
- Приложение Avira Desktop устарело
- Приложение Windows Defender устарело
- Приложение Windows Defender отключено

Приложение Avira Desktop сообщает, что оно включено

После установки продукта Avira и последующего обновления программы вы сначала не получите от Центра поддержки Windows никаких уведомлений. Тем не менее, в разделе **Центр поддержки > Безопасность** будет можно найти следующее примечание: *Приложение Avira Desktop сообщает, что оно включено*. Это значит, что ваш продукт Avira теперь обновлен до последней версии, сканер в режиме реального времени Avira активен.

Как Windows Defender, так и Avira Desktop сообщили, что выключены

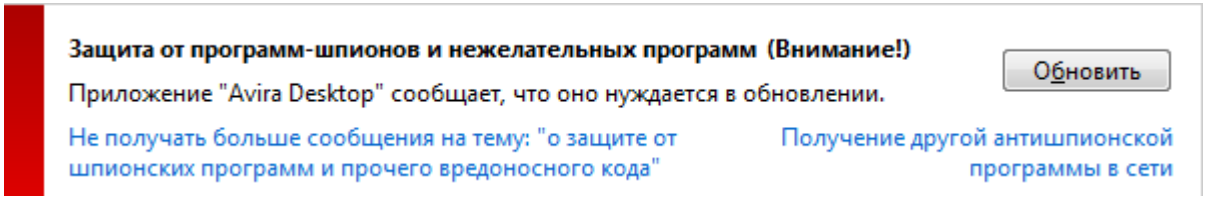
Следующее уведомление выдается, если сканер в режиме реального времени Avira выключен или его работа остановлена.



Примечание
Активировать или отключить **Avira Real-Time Protection** можно в разделе **Статус Центра Управления Avira**. О включении **Avira Real-Time Protection** свидетельствует раскрытый красный зонтик в панели задач. Отдельные компоненты Avira также можно включить щелчком по клавише *Включить сейчас* в Центре поддержки. При получении сообщения, требующего подтверждения продолжения работы программы Avira, щелкните по кнопке *Разрешить*, Avira Real-Time Protection будет включен.

Приложение Avira Desktop устарело

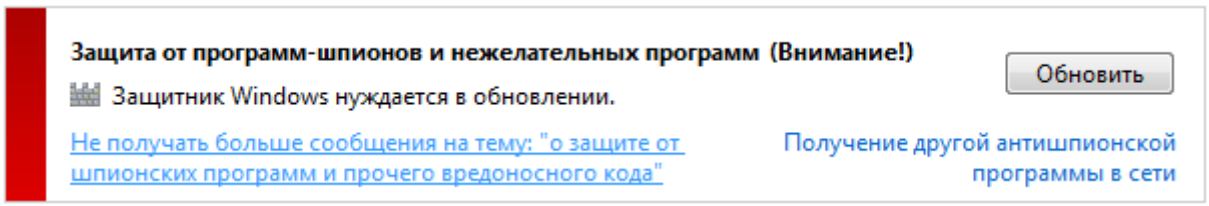
Если Вы только что установили Avira, или по какой-либо причине файл VDF, поисковый движок или программные файлы Вашего продукта Avira не были автоматически обновлены (например, если они в более старой ОС Windows, на которую был уже установлен продукт Avira, обновляются до следующей версии), то Вы получите следующее сообщение:



Примечание
Чтобы Центр поддержки Windows счел продукт Avira актуальным, после установки программы необходимо произвести обновление. Обновить систему можно с помощью функции Обновление.

Приложение Windows Defender устарело

Следующее сообщение может появиться после активации Windows Defender. Это может означать, что ваш продукт Avira установлен неправильно. Проверьте установку.

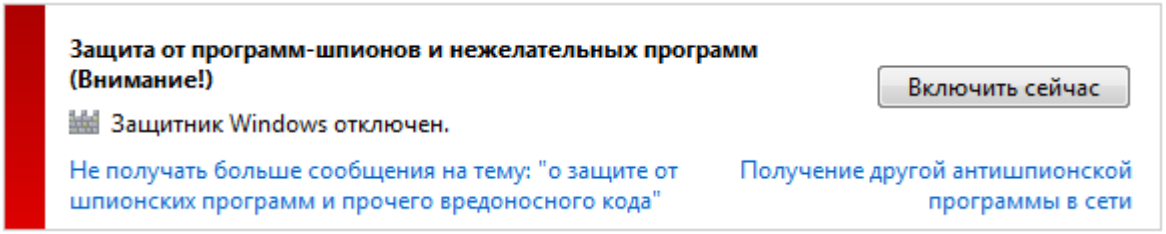


Примечание
Windows Defender – это предусмотренное приложение Windows для защиты от шпионских программ и вирусов.

Приложение Windows Defender отключено

Вы получите сообщение от центра поддержки Windows *Windows Defender отключен*, если на вашем компьютере на найдено другого антишпионского ПО. Windows Defender (Защитник Windows) — программный продукт Microsoft, по умолчанию встроенный в операционную систему для распознавания шпионского ПО. Если вы уже установили на своем компьютере другое антивирусное ПО, то приложение деактивируется.
Если продукт Avira установлен правильно, вы не должны получать это сообщение,

так как центр поддержки распознает продукты Avira автоматически. Проверьте, правильно ли работает Avira.



10. Вирусы и другое

10.1 Вирусы и другое

Avira Internet Security распознает не только вирусы и вредоносные программы, программа может защитить вас и от других угроз. В данной главы представлен обзор видов вредоносных прогармм и других угроз. Здесь описано их происхождение, особенности и неприятные последствия, к которым они могут привести.

Соответствующие темы:

- Категории угроз
- Вирусы и вредоносные программы

10.2 Категории угроз

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 во время действия влияют на работу компьютера и являются проблемными с точки зрения безопасности данных.

Ваш продукт Avira распознает такие программы. Если в настройках в разделе Категории угроз включена опция **Рекламные программы**, пользователь получает уведомление об обнаружении программой Avira рекламных программ.

Рекламное ПО/шпионское ПО

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

Ваш продукт Avira распознает рекламные/шпионские программы. Если в настройках в разделе Категории угроз включена опция **рекламные и шпионские программы**, пользователь получает уведомление об обнаружении программой Avira рекламных и шпионских программ.

Приложение

Под приложением подразумеваются программы, запуск которых может быть связан с определенным риском, или источник их происхождения не внушает доверия. Ваш продукт Avira распознает такие "приложения" (APPL). Если в настройках в пункте Категории угроз включена опция **Приложение**, вы получаете

соответствующее предупреждение, если программа Avira замечает подобное поведение.

Backdoor-программы

Для организации кражи 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 (Client) может управляться третьими лицами. Avira распознает backdoor-утилиты удаленного администрирования. Если в настройках в разделе Категории угроз с помощью галочки включена опция **Backdoor-программы**, пользователь получает уведомление об обнаружении программой Avira таких программ программ.

Файлы со скрытыми расширениями

Исполняемые файлы, скрывающие настоящие расширения файлов. Этот метод сокрытия часто используется вредоносным ПО.
Программа Avira распознает файлы с двойным расширением. Если в настройках в разделе Категории угроз с помощью галочки включена опция **Файлы с двойным расширением** , пользователь получает уведомление в случае обнаружения программой Avira подобных объектов.

Программа дозвона на платные номера

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 получению счетов на гораздо более высокие суммы.

Для качественной защиты от нежелательных дайлеров (0190/0900), мы рекомендуем поместить используемые ими номера в черный список.

По умолчанию Avira обнаруживает наиболее распространенные программы-дайлеры.

Если в настройках в разделе Категории угроз включена опция **Программы дозвона на платные номера** , 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.

Фишинг

Фишинг, известный как brand spoofing, является специфической формой кражи данных, нацеленной на реальных или потенциальных клиентов Интернет-провайдеров, банков, различных служб и учреждений.
При передачи своего электронного адреса в Интернете, заполнения онлайн-формуляров, вступлении в новые группы или регистрации на веб-сайтах ваши данные могут попадать к так называемым "Internet crawling spiders" и использоваться без вашего разрешения в целях обмана или других преступлений.

Ваш продукт Avira распознает фишинговые программы. Если в настройках в пункте Категории угроз включена опция **Фишинг**, вы получаете соответствующее предупреждение, если программа Avira замечает подобное поведение.

Программы, нарушающие частную сферу

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

Программа Avira распознает программы, несущие риск вторжения в приватную сферу. Если в настройках в разделе Категории угроз включена опция **Программы, нарушающие частную сферу**, пользователь получает уведомление об обнаружении программой Avira таких приложений.

Программы-шутки

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

Но, внимание! Все симптомы таких развлекательных программ могут быть также имитированы вирусами или троянами. В конце концов, эти программы могут просто

испугать пользователя, или могут помочь ему самому стать инициатором действий, причиняющих вред.

Avira 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** , пользователь извещается об обнаружении таких объектов.

Игры

Мы не против компьютерных игр, но совсем не обязательно играть в них в рабочее время (может быть, за исключением обеденных перерывов). Тем не менее, многие сотрудники посвящают массу своего рабочего времени различным компьютерным играм и развлечениям. Через Интернет можно загрузить массу игр. Игры по электронной почте также пользуются популярностью: от шахмат до "морского боя", существует большое количество таких игр, где ходы в игре отправляются участнику через электронную почту.

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.

Ваш продукт Avira распознает компьютерные игры. Если в настройках в разделе Категории угроз включена опция **Игры**, пользователь получает уведомление об обнаружении программой Avira таких приложений. После чего игры, в прямом смысле слова, заканчиваются, так как у вас появляется возможность удалять их очень легко.

Обманная программа

"Поддельные антивирусы" (Scareware) или "ложные антивирусы" (Rogueware) - это поддельные программы, которые сообщают о вирусном заражении и опасности и при этом внешне очень похожи на профессиональные антивирусные программы. Поддельные антивирусы предназначены для запугивания пользователей и придания им неуверенности. Если жертва попалась на удочку и считает себя подверженной угрозе, зачастую за отдельную плату ей предлагается устранение несуществующей опасности. В других случаях жертва, поверившая в нападение на нее, принуждается к определенными действиям, вследствие которых действительно будет совершено нападение.

Если в настройках в разделе Категории угроз включена опция **Обманные программы**, вы получите уведомление об обнаружении активности такой программы.

Нестандартные паковщики

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

Avira распознает деятельность нестандартных паковщиков. Если в настройках в разделе Категории угроз включена опция **Необычные паковщики (PCK)**, пользователь получает предупреждение в случае, если Avira обнаружит подобные объекты.

10.3 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 во время действия влияют на работу компьютера и являются проблемными с точки зрения безопасности данных.

Утилиты удаленного администрирования

Backdoor (задняя дверь, черный ход) может, 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 может быть инфицирован загрузочными вирусами. Эти вирусы изменяют важную информацию, необходимую для запуска системы. Одно из неприятных последствий: невозможность загрузки операционной системы...

Bot-сети

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. Формой эксплойта считаются атаки из Интернета с помощью управляемых пакетов данных, которые используют уязвимости сетевого ПО. Так в систему могут проникать программы, с помощью которых могут быть получены расширенные права доступа.

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 перенаправить их как можно большему количеству пользователей и коллег для того, чтобы предостеречь всех от "опасности".

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 проверяет 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. По сравнению с обычными вирусами макровирусы нападают не на исполняемые файлы, а на документы соответствующих приложений.

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. Ясно, 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.

Rootkits

Rootkits - набор программных средств, которые устанавливаются в систему, обеспечивая сокрытие входа в систему злоумышленника, сокрытие процессов и копирования данных - попросту говоря: делая злоумышленника невидимым. Вы пытаетесь обновить уже установленную шпионскую программу или установить удаленное шпионское ПО.

Скрипт-вирусы и черви

Эти вирусы очень просты в написании и при наличии необходимых технологий могут быть распространены по всему миру всего за несколько часов.

Скриптовые вирусы и черви используют скриптовые языки, такие как, например, Javascript, VBScript и др., чтобы добавлять себя к новым скриптам или распространяться через вызов функций операционной системы. 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.

Шпионские программы

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 (кратко: трояны)

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 особым видом троянской программы. Эта программа рассаживает вирусы в системе.

Обманная программа

"Поддельные антивирусы" (Scareware) или "ложные антивирусы" (Rogueware) - это поддельные программы, которые сообщают о вирусном заражении и опасности и при этом внешне очень похожи на профессиональные антивирусные программы. Поддельные антивирусы предназначены для запугивания пользователей и придания им неуверенности. Если жертва попалась на удочку и считает себя подверженной угрозе, зачастую за отдельную плату ей предлагается устранение несуществующей опасности. В других случаях жертва, поверившая в нападение на нее, принуждается к определенными действиям, вследствие которых действительно будет совершено нападение.

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

В этой главе размещены контактные данные для связи с нами.

- См. главу Контакты
- См. главу Техническая поддержка
- См. главу Подозрительный файл
- См. главу Уведомление о ложном срабатывании
- См. главу Обратная связь

11.1 Контакты

Мы с удовольствием поможем вам, если у вас есть вопросы и пожелания, касающиеся продукции Avira. Наши контакты указаны в центре управления в **Справка > О Avira Internet Security**.

11.2 Техническая поддержка

Служба техподдержки Avira Support всегда готова помочь, если у вас есть вопросы или технические проблемы.

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

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 Avira Internet Security > Информация о лицензии**. См. Информация о лицензии.
- **Информация о версии**. Информацию о версии вы найтете в меню программы в пункте **Справка > О Avira Internet Security > Информация о версии**. См. Информация о версии.
- **Версия операционной системы** и при необходимости установленные пакеты обновления.
- **Установленные программы**, например антивирусные программы других 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 необходимый файл в заархивированном виде (WinZIP, PKZip, Arj, и т.д.) во вложении письма по следующему адресу:
  virus-premium-suite@avira.ru
  Так как некоторые почтовые шлюзы работают с антивирусным ПО, защитите файл(ы) паролем и не забудьте сообщить его нам.
- У вас есть также возможность отправить подозрительные файлы через наш сайт:
  http://www.avira.ru/sample-upload

11.4 Сообщить о ложном срабатывании

Если вы считаете, что программа Avira определила заведомо чистый, по вашему мнению, файл инфицированным, отправьте этот файл в запакованном (WinZIP, PKZIP, Arj и пр.) виде на адрес:
virus-premium-suite@avira.ru

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

11.5 Обратная связь для вашей безопасности

Avira считает безопасность клиентов самой главной своей задачей. Для этого каждое отдельное решение Avira и каждое отдельное обновление до публикации тщательно проверяются нашими экспертами относительно 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-premium-suite@avira.ru

12. Информация: Опции меню настройки

В информации о настройке содержатся все доступные опции меню Настройка.

12.1 System Scanner

Раздел **System Scanner** Настройки отвечает за настройку параметров прямого поиска, т.е. за проверку по требованию пользователя. (Эти опции доступны только при включенном экспертном режиме.)

12.1.1 Поиск

Здесь вы можете задать принципиальный метод при поиске (Эти опции доступны только при включенном экспертном режиме). Если Вы выбираете определенные папки для проверки, System Scanner осуществляет проверку в зависимости от настроек:

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

Файлы

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

Все файлы

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

> **Указание**
> Если включена опция **Все файлы**, кнопка **Расширения файлов** недоступна.

Интеллектуальный выбор файлов

Если эта опция включена, то программа автоматически выбирает файлы для проверки. Это означает, что продукт Avira принимает решение о необходимости проверки файла на наличие вирусов и вредоносных программ, основываясь на его содержании. Эта процедура длится 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.

Указание
Если включена опция **Интеллектуальный выбор файлов**, кнопка **Расширения файлов** недоступна.

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.

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

Расширения файлов

С помощью этой кнопки вызывается диалоговое окно, в котором отображаются все расширения файлов, проверяемых при поиске в режиме "**Использовать список расширений файлов"**. В списке уже приведены некоторые расширения файлов, но вы можете добавлять новые или удалять их.

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

Дополнительные настройки

Проверить загрузочные секторы

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

Проверка главных загрузочных секторов

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

Пропустить оффлайн-файлы

Если эта опция включена, при прямом поиске полностью игнорируются так называемые оффлайн-файлы. Это значит, что эти файлы не проверяются на наличие вирусов и вредоносных программ. Оффлайн файлы - это файлы, которые были физически перенесены с помощью так называемой иерархической

системы управления носителями (HSM) с жесткого диска, например, на магнитную ленту. Эта настройка активирована по умолчанию.

Проверка целостности системных файлов

Если эта опция включена, то при каждом прямом поиске важнейшие системные файлы Windows особенно тщательно проверяются на изменения, внесенные вредоносными программами. При обнаружении измененного файла появится сообщение о подозрительном объекте. Для этой функции необходимо много ресурсов. Поэтому по умолчанию эта опция отключена.

Указание
Эта функция доступна только начиная с Windows Vista.

Указание
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 System Scanner будет распределяться оптимально. Из соображений производительности протоколирование при оптимальной проверке осуществляется не подробнее, чем при опции по умолчанию.

Указание
Опция доступна только для многопроцессорных компьютеров.

Следовать по ссылкам

Если опция включена, то System Scanner при проверке следует по всем ссылкам поискового профиля или выбранной папки, чтобы проверить файлы на вирусы.

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

Поиск Rootkits при запуске поиска

Если эта опция включена, System Scanner проверяет при запуске поиска путем так называемого быстрого поиска системную папку Windows на активные Rootkits. Таким методом ваш компьютер проверяется не так тщательно на активные Rootkits, как специальный профиль "**Поиск Rootkits"**, но проверка занимает существенно меньше времени. Эта опция меняет только настройки созданных Вами профилей.

Указание
Поиск Rootkits в Windows XP 64 бит недоступен!

Сканирование реестра

Если эта опция включена, то при проверке реестр сканируется на наличие вредоносных программ. Эта опция меняет только настройки созданных Вами профилей.

Пропустить 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 проверки

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 неактивной. Остановка проверки до ее окончания станет невозможной! Эта настройка активирована по умолчанию.

Приоритет сканера

System Scanner имеет три уровня приоритета. Это возможно только в том случае, если на компьютере запущено одновременно несколько процессов. Выбор оказывает влияние на скорость поиска.

низкий

System Scanner получает от операционной системы процессорное время только в том случае, если оно не требуется другим процессам. Т.е. до тех пор, пока System Scanner работает в одиночку, скорость является максимальной. В целом это позволяет ускорить работу с другими программами: Компьютер работает быстрее, если другие программы используют процессорное время, когда System Scanner продолжает работать в фоновом режиме.

средний

Проверка System Scanner выполняется с нормальным приоритетом. Все процессы получают от операционной системы одинаковое количество процессорного времени. Эта опция включена по умолчанию и рекомендована. При определенных обстоятельствах затрудняется работа с другими приложениями.

высокий

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

Действие при обнаружении

Вы можете определить операции, которые будут выполняться, если System Scanner обнаружит вирус или вредоносную программу. (Эти опции доступны только при включенном экспертном режиме.)

Интерактивный

Если опция включена, то об обнаружении вирусов при проверке System Scanner сообщается в диалоговом окне. При проверке System Scanner 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 System Scanner.

Указание
По умолчанию в диалоговом окне по обработке вирусов стоит **Карантин**. С помощью контекстного меню можно выбирать другие действия.

Автоматический

Если эта опция включена, при обнаружении вируса или вредоносной программы не открывается диалоговое окно для выбора действия. System Scanner работает автоматически в соответствии с выбранными Вами настройками.

Копировать файл перед выполнением действия в карантин

Если эта опция включена, System Scanner создает резервную копию перед осуществлением первичного или вторичного действия. Резервная копия хранится в карантине, откуда можно восстановить файл, если он имеет ценность. Кроме того, вы можете отправить резервную копию в Avira Malware Research Center для дальнейшего изучения.

Первичное действие

Первичное действие выполняется, если System Scanner обнаруживает вирус или вредоносную программу. Если выбрана опция "**Лечить**", но лечение

инфицированного файла невозможно, выполняется операция, определенная в пункте **"Вторичное действие"**.

Указание
Опция **Вторичное действие** доступна только в том случае, если для **Первичного действия** выбрано действие **Лечить**.

Лечить

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

Указание
Разработчик рекомендует автоматическое лечение, но это означает, что System Scanner изменяет файлы на вашем компьютере.

Переименовать

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

Карантин

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

Удалить

Если эта опция включена, файл удаляется. Эта процедура значительно быстрее, чем **Переписать и удалить** (см. ниже).

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 существенный вред вашему компьютеру!

Переписать и удалить

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

Вторичное действие

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

Переименовать

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

Карантин

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

Удалить

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

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 существенный вред вашему компьютеру!

Переписать и удалить

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

Указание
Если в качестве первичного или вторичного действия выбрано **Удалить** или **Переписать и удалить** , помните следующее: при обнаружении системой эвристического поиска инфицированные файлы не удаляются, а перемещаются в карантин.

Архивы

При проверке архивов System Scanner применяет рекурсивный поиск: архивы в архивах распаковываются и проверяются на вирусы и вредоносные программы. Файлы проверяются, затем они распаковываются и вновь проверяются. (Эти опции доступны только при включенном экспертном режиме.)

Просмотреть архивы

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

Все типы архивов

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

Базовый список расширений

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

Указание
Проверяются только отмеченные в списке архивов типы архивов.

Ограничить уровень рекурсии

Распаковка и проверка архивов с высокой степенью вложенности 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 компьютера.

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

Максимальная глубина рекурсии

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 параметры поиска в архивах.

Список архивов

В этой области вы можете указать, какие архивы должны проверяться модулем System Scanner. Для этого необходимо отметить соответствующие строки.

Исключения

Файловые объекты, исключенные из проверки модулем System Scanner (Эти опции доступны только при включенном экспертном режиме.)

Список в этом окне содержит файлы и пути, которые нужно исключить из проверки на наличие вирусов или вредоносных программ службой System Scanner.

Вносите как можно меньше исключений, это должны быть только файлы, которые по определенным причинам действительно не должны проверяться в ходе обычной проверки. Рекомендуется в любом случае проверить эти файлы на наличие вирусов и вредоносных программ перед включением их в список!

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

Предупреждение
Эти файлы не проверяются при сканировании!

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, поскольку причины, по которым файл был исключен из проверки, могут потерять актуальность. В этом случае удалите имя этого файла из списка.

Поле ввода

В этом поле укажите имя файлового объекта, который должен быть исключен из прямого поиска. По умолчанию список не содержит объектов.

Нажатием на эту кнопку открывается окно, в котором вы можете выбрать желаемый файл или путь.
Если вы указали имя файла и полный путь к нему, только этот файл не будет проверяться на наличие вирусов. Если вы указали имя файла, но не указали путь к нему, ни один из файлов с этим именем (вне зависимости от папки и диска) не будет проверяться.

Добавить

С помощью этой кнопки можно перенести введенный в поле ввода файл в окно исключений.

Удалить

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

> **Указание**
> Если вы добавите к списку исключенных из проверки файловых объектов целый раздел, из проверки исключаются только файлы, сохраненные непосредственно в этом разделе, но не файлы, находящиеся в размещенных в разделе папках:
> пример: исключаемый файловый объект: `D:\` = `D:\file.txt` исключается из проверки модулем System Scanner, а `D:\folder\file.txt` не исключается.

Эвристика

Этот раздел настроек содержит параметры эвристического поиска. (Эти опции доступны только при включенном экспертном режиме.)

Продукты Avira содержат 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, например, основываясь на имеющейся у него информации о надежности источника происхождении файла.

Эвристическое обнаружение макровирусов

Эвристическое обнаружение макровирусов

Ваш продукт Avira имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, альтернативно можно ограничиться уведомлением пользователя о подозрительных документах. Эта опция включена по умолчанию и рекомендована.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Благодаря технологии AHeAD ваша программа Avira содержит очень мощную эвристическую систему для определения даже неизвестных (новых) вредоносных программ. Если эта опция включена, вы можете установить уровень "резкости" эвристики. Эта настройка включена по умолчанию.

Низкий уровень распознавания

Если эта опция включена, программа обнаруживает меньше неизвестного вредоносного ПО, опасность ложных обнаружений при этом невелика.

Средний уровень распознавания

При включении этой опции обеспечивается сбалансированная защита с небольшим количеством ложных обнаружений. Эта настройка определена по умолчанию, если вы используете эвристический поиск.

Высокий уровень распознавания

При включении этой опции обнаруживается существенно больше неизвестного вредоносного ПО, но число ложных обнаружений также возрастает.

12.1.2 Отчет

Модуль System Scanner имеет функцию подробного протоколирования. С ее помощью вы получите точную информацию о результатах проверки. Файл отчета содержит все записи системы, а также предупреждения и сообщения службы прямого поиска. (Эти опции доступны только при включенном экспертном режиме.)

> **Указание**
> Чтобы определить, какие действия выполнил модуль System Scanner при обнаружении вируса или вредоносной программы, необходимо всегда составлять файл отчета.

Протоколирование

Выкл

Если эта опция включена, System Scanner не составляет отчет о выполнении действий и результатах прямого поиска.

По умолчанию

Если эта опция включена, System Scanner протоколирует имя соответствующих файлов с указанием пути. Кроме того, в файл отчета записываются параметры настройки текущего поиска, информация о версии и лицензии.

Дополнительно

Если эта опция включена, System Scanner протоколирует также все предупреждения и примечания. В файле отчета будет отображаться "(Cloud)"-суффикс для идентификации предупреждений Cloud Protection.

Полный

Если установлена эта опция, System Scanner дополнительно протоколирует все проверенные файлы. Кроме того, в файл отчета включаются имена всех инфицированных файлов, все предупреждения и примечания.

Указание
Если вы собираетесь направить нам файл отчета (например, для поиска ошибок), просим создавать отчет в этом режиме.

12.2 Real-Time Protection

Раздел Real-Time Scanner в Настройке отвечает за настройку постоянной защиты в режиме реального времени. (Эти опции доступны только при включенном экспертном режиме.)

12.2.1 Поиск

Обычно пользователи включают постоянную защиту своей системы. Для этого используется служба Real-Time Protection (поиск в реальном времени = On-Access-Scanner). Это позволяет "на лету" проверять все копирующиеся или открываемые на компьютере файлы на наличие вирусов или нежелательных программ. (Эта опция доступна только при включенном экспертном режиме.)

Файлы

Real-Time Protection может использовать фильтр, чтобы проверять только файлы с определенным расширением (типом).

Все файлы

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

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

Интеллектуальный выбор файлов

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

Указание
Если включена опция **Интеллектуальный выбор файлов**, кнопка **Расширения файлов** недоступна.

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.

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

Расширения файлов

С помощью этой кнопки вызывается диалоговое окно, в котором отображаются все расширения файлов, проверяемых при поиске в режиме **"Использовать список расширений файлов"**. В списке уже приведены некоторые расширения файлов, но вы можете добавлять новые или удалять их.

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

Режим поиска

Здесь задается время проверки файла.

Проверить при считывании

Если эта опция включена, Real-Time Protection проверяет файлы до того, как они считываются или выполняются каким-нибудь приложением или операционной системой.

Проверить при записи

Если эта опция включена, Real-Time Protection проверяет файл в момент записи. К файлу можно обратиться только после завершения этой операции.

Проверить при записи и считывании

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

Диски

Проверка сетевых дисков

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

Указание
Чтобы не загружать слишком сильно ваш компьютер, опцию **Проверка сетевых дисков** 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!

Указание
Если файлы, находящиеся на сетевых дисках, выполняются, то они **проверяются** модулем Real-Time Protection независимо от установки опции **Сетевые диски**. В некоторых случаях файлы проверяются на сетевых дисках при открытии, хотя опция **Проверка сетевых дисков** отключена. Это происходит потому, что к этим файлам обращаются с полномочием "Выполнить файл". Если вы хотите исключить эти или выполняемые файлы на сетевых дисках из проверки службой Real-Time Protection, внесите эти файлы в список файловых объектов, которые необходимо исключить (см.: Исключения).

Активировать кэшинг

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

Архивы

Просмотреть архивы

При включении этой опции будет осуществляться проверка архивов. Проверяются сжатые файлы, затем они распаковываются и вновь проверяются. По умолчанию эта 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.

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

Макс. глубина рекурсии

При проверке архивов Real-Time Protection применяет рекурсивный поиск: архивы в архивах распаковываются и проверяются на вирусы и вредоносные программы. Можно задать глубину рекурсии. Стандартное рекомендуемое значение для глубины рекурсии составляет 1 и является рекомендованным: проверяются все файлы, которые находятся непосредственно в главном архиве.

Макс. количество файлов

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

Макс. размер (КБ)

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

Действие при обнаружении

Вы можете определить операции, которые должен выполнять модуль Real-Time Protection при обнаружении вируса или вредоносной программы. (Эти опции доступны только при включенном экспертном режиме.)

Интерактивный

Если эта опция активирована, то при обнаружении вируса модулем Real-Time Protection выдается сообщение на рабочий стол. Вы можете удалить обнаруженную вредоносную программу или выбрать другие действия для обработки вирусов нажатием кнопки "**Подробно**". Действия отображаются в диалоговом окне. Эта опция включена по умолчанию.

Лечить

Real-Time Protection вылечит инфицированный файл, если это будет возможно.

Переименовать

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

Карантин

Real-Time Protection помещает файлы в карантин. Файл может быть восстановлен из менеджера карантина, если в этом возникнет необходимость, или его можно отправить разработчику в центр исследования вирусов компании Avira Malware Research Center. В зависимости от типа файла есть возможность выбора других действий (см. в Менеджере карантина).

Удалить

Файл удаляется. Эта процедура значительно быстрее, чем **переписать и удалить** (см. ниже).

Пропустить

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

Переписать и удалить

Real-Time Protection переписывает файл, заменяя его стандартным шаблоном, а затем удаляет файл. Он не может быть восстановлен.

Предупреждение
Если в Real-Time Protection включена опция **Проверить при записи**, инфицированный файл не записывается.

По умолчанию

С помощью этой кнопки вы можете выбрать действие, которое должно быть активировано по умолчанию в диалоговом окне при обнаружении вируса. Выделите действие, которое должно быть по умолчанию активно, и нажмите кнопку "**По умолчанию**".

Указание
В качестве действия по умолчанию невозможно выбрать **Лечение**.

Более подробную информацию можно получить по ссылке.

Автоматический

Если эта опция включена, при обнаружении вируса или вредоносной программы не открывается диалоговое окно для выбора действия. Real-Time Protection реагирует автоматически в соответствии с выбранными вами настройками.

Копировать файл перед выполнением действия в карантин

Если эта опция включена, Real-Time Protection создает резервную копию (Backup) перед осуществлением первичного или вторичного действия. Резервная копия сохраняется в Карантине. Она может быть восстановлена из Менеджера Карантина, если она имеет информационное значение. Кроме того, вы можете отправить резервную копию в Avira Malware Research Center. В зависимости от типа файла в менеджере карантина есть возможность выбора других действий (см. Менеджер карантина)

Первичное действие

Первичное действие выполняется, если Real-Time Protection обнаруживает вирус или вредоносную программу. Если выбрана опция "**Лечить**", но лечение инфицированного файла невозможно, выполняется операция, определенная в пункте "**Вторичное действие**".

Указание
Опция **Вторичное действие** доступна только в том случае, если для **Первичного действия** выбрано действие **Лечить**.

Лечить

Если эта опция включена, Real-Time Protection автоматически пытается лечить инфицированный файл. Если Real-Time Protection не может вылечить инфицированный файл, выполняется операция, предусмотренная **Вторичным действием**.

Указание
Разработчик рекомендует автоматическое лечение, но это означает, что Real-Time Protection изменяет файлы на вашем компьютере.

Переименовать

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

Карантин

Если эта опция включена, Real-Time Protection помещает файл в папку карантина. Файлы из этой папки могут быть позже вылечены или, в случае необходимости, отправлены разработчику, в центр исследования вирусов Avira Malware Research Center.

Удалить

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

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 существенный вред вашему компьютеру!

Переписать и удалить

Если эта опция включена, Real-Time Protection заменяет файл стандартным шаблоном, а затем удаляет его.Если эта опция включена, Real-Time Protection заменяет файл стандартным шаблоном, а затем удаляет его. Он не может быть восстановлен.

Запретить доступ

Если эта опция включена, Real-Time Protection вносит информацию об обнаружении подозрительного объекта в файл отчета, только если функция отчетов включена. Если эта опция включена, Real-Time Protection также вносит запись в протокол событий.

Предупреждение
Если в Real-Time Protection включена опция **Проверить при записи**, инфицированный файл не записывается.

Вторичное действие

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

Переименовать

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

Карантин

Если эта опция включена, Real-Time Protection перемещает файл в карантин. Файлы могут быть позже вылечены или, в случае необходимости, отправлены в Avira Malware Research Center.

Удалить

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

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 существенный вред вашему компьютеру!

Переписать и удалить

Если эта опция включена, Real-Time Protection заменяет файл стандартным шаблоном, а затем удаляет его.Если эта опция включена, Real-Time Protection заменяет файл стандартным шаблоном, а затем удаляет его. Он не может быть восстановлен.

Запретить доступ

Если эта опция включена, инфицированный файл не записывается. Real-Time Protection вносит информацию об обнаружении подозрительного объекта в файл отчета, только если функция отчетов включена. Если эта опция включена, Real-Time Protection также вносит запись в протокол событий.

Указание
Если в качестве первичного или вторичного действия выбрано **Удалить** или **Переписать и удалить** , помните следующее: при обнаружении системой эвристического поиска инфицированные файлы не удаляются, а перемещаются в карантин.

Дополнительные действия

Запись в протокол событий

Если эта опция включена, информация о каждом обнаружении сохраняется в журнале регистрации событий Windows. События можно просмотреть с помощью индикации событий Windows. Эта настройка включена по умолчанию. (Эти опции доступны только при включенном экспертном режиме.)

Исключения

С помощью этих опций вы можете задать объекты, исключенные из проверки модулем Real-Time Protection (постоянная защита). Данные объекты не будут проверяться в режиме реального времени. Real-Time Protection может игнорировать при постоянной проверке обращения этих объектов к файлам в соответствии со списком исключенных процессов. Это, в частности, целесообразно для баз данных или программ резервного копирования. (Эти опции доступны только при включенном экспертном режиме.)

При указании исключенных из проверки процессов и файловых объектов необходимо помнить следующее: список обрабатывается сверху вниз. Чем длиннее список, тем больше времени процессора требует обработка списка для каждого доступа. Поэтому список должен быть как можно короче.

Процессы, исключенные из проверки службой Real-Time Protection

Любой доступ к файлам со стороны процессов, указанных в этом списке, не будет отслеживаться службой Real-Time Protection.

Поле ввода

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

Заданный путь и имя файла процесса не должны превышать 255 символов. Вы можете ввести до 128 процессов. Совокупная длина записей в списке не должна превышать 6000 знаков.

При указании процесса можно использовать символы Unicode. Поэтому можно вводить имена процессов или папок, содержащие специальные символы.

Диски указываются следующим образом: `[Буква, обозначающая диск]:\`

Двоеточие (:) можно указывать только при указании диска.

При указании процесса можно использовать символ-заполнитель * (произвольное количество знаков) и ? (один знак):

```
C:\Program Files\приложение\приложение.exe
C:\Program Files\приложение\прилож?.exe
C:\Program Files\приложение\прилож*.exe
C:\Program Files\приложение\*.exe
```

Чтобы не все процессы были исключены из проверки службой Real-Time Protection, недействительными считаются записи, состоящие только из следующих символов: * (звездочка), ? (знак вопроса), / (косая черта), \ (обратная косая черта), . (точка), : (двоеточие).

Вы можете исключить процессы из проверки службой Real-Time Protection, не указывая полностью путь к ним: `приложение.exe`

Но это касается только процессов, исполняемые файлы которых находятся на жестком диске.

Для процессов, исполняемые файлы которых находятся на подключенных дисках, например на сетевых дисках, путь нужно вводить полностью. При этом соблюдайте общие указания для ввода Исключений на подключенных сетевых дисках.

Не задавайте исключения для процессов, исполняемые файлы которых находятся на динамических дисках. Динамические диски используются для сменных носителей, таких как CD, DVD или USB-накопители.

Предупреждение
Помните, что все обращения к файлам, инициированные процессами и указанные в этом списке, будут исключены из поиска вирусов или нежелательных программ!

Нажатием на эту 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 проверки службой Real-Time Protection

Любой доступ файлов к объектам, указанным в этом списке, не будет отслеживаться службой Real-Time Protection.

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.

Совокупная длина записей в списке не должна превышать 6000 знаков.

При указании исключенных файловых объектов можно использовать символ-заполнитель * (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
```

Имя папки должно заканчиваться на обратный слеш \.

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

На один диск можно задать не более 20 исключений с полным путем (начиная с буквенного обозначения диска).

Пример: `C:\Program Files\Приложение\Имя.log`

Максимальное количество исключений без полного пути составляет 64. Пример:

```
*.log
\компьютер1\C\папка1
```

Для динамических дисков, смонтированных как том на другом диске, в списке исключений необходимо использовать альтернативное имя операционной системы для смонтированного диска:
например
`\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
При использовании самой точки монтирования (mount point), например `C:\DynDrive`, динамический диск все равно будет проверяться. Альтернативное имя операционной системы можно узнать в файле отчета Real-Time Protection.

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

Добавить

С помощью этой кнопки можно перенести введенный в поле ввода файловый объект в окно просмотра.

Удалить

С помощью кнопки Удалить можно удалить отмеченный файловый объект из окна просмотра.

При создании исключений помните следующее

Для исключения объектов, обращение к которым осуществляется с помощью коротких имен файлов DOS (DOS name convention 8.3), необходимо добавить в список также соответствующее короткое имя файла.

К имени файла, содержащего символы-заполнители, нельзя добавлять в конце обратный слеш.
Пример:
`C:\Program Files\приложение\прилож*.exe\`
Эта запись недействительна и не будет рассматриваться как исключение!

При работе с **исключениями на подключенных сетевых дисках** необходимо помнить следующее: если вы используете букву диска связанного сетевого диска, указанные файлы и папки НЕ будут исключены из проверки службой Real-Time Protection. 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 проверки службой Real-Time Protection. Используемый UNC-путь можно узнать в файле отчета Real-Time Protection:
\\<Имя компьютера>\<Разрешение>\ -ИЛИ- \\<IP-адрес>\<Разрешение>\

На основании файла отчета Real-Time Protection вы можете указать пути, которые будет использовать модуль Real-Time Protection при поиске инфицированных файлов. Всегда используйте в списке исключений те же пути. Установите параметр протоколирования Real-Time Protection в настройках: Отчет на **Полный**. Обратитесь с помощью активированного модуля Real-Time Protection к файлам, папкам, к подключенным дискам или к подключенным сетевым дискам. Вы можете найти используемый путь в файле отчетов Real-Time Protection. Файл отчета можно вызвать в Центре управления в разделе Real-Time Protection.

Эвристика

Этот раздел настроек содержит параметры эвристического поиска. (Эта опция доступна только при включенном экспертном режиме.)

Продукты Avira содержат 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, например, основываясь на имеющейся у него информации о надежности источника происхождении файла.

Эвристическое обнаружение макровирусов

Эвристическое обнаружение макровирусов

Ваш продукт Avira имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, альтернативно можно ограничиться уведомлением пользователя о подозрительных документах. Эта опция включена по умолчанию и рекомендована.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Благодаря технологии AHeAD ваша программа Avira содержит очень мощную эвристическую систему для определения даже неизвестных (новых) вредоносных программ. Если эта опция включена, вы можете установить уровень "резкости" эвристики. Эта настройка включена по умолчанию.

Низкий уровень распознавания

Если эта опция включена, программа обнаруживает меньше неизвестного вредоносного ПО, опасность ложных обнаружений при этом невелика.

Средний уровень распознавания

При включении этой опции обеспечивается сбалансированная защита с небольшим количеством ложных обнаружений. Эта настройка определена по умолчанию, если вы используете эвристический поиск.

Высокий уровень распознавания

При включении этой опции обнаруживается существенно больше неизвестного вредоносного ПО, но число ложных обнаружений также возрастает.

12.2.2 Отчет

Модуль Real-Time Protection обладает обширными функциями протоколирования, которые могут предоставить пользователю или администратору точные сведения о виде и характере найденного объекта. (Эта опция доступна только при включенном экспертном режиме.)

Протоколирование

В этой группе определяется объем файла отчета.

ВЫКЛ

Если эта опция включена, то Real-Time Protection 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 Real-Time Protection записывает в файле отчета важную информацию (о найденном объекте, предупреждениях и ошибках), менее важная информация не включаются из соображений лучшей наглядности. Эта настройка активирована по умолчанию.

Дополнительно

Если эта опция включена, то Real-Time Protection вносит в отчет и менее значимую информацию.

Полный

Если опция включена, Real-Time Protection включает в файл отчета все данные, в том числе, тип, размер и дату файла.

Ограничить файл отчета

Ограничить размер до n МБ

Если выбрана эта опция, размер файла отчета можно ограничить, возможные значения: от 1 до 100 МБ. При ограничении размера файла отчета предоставляется лимит около 50 КБ, чтобы уменьшить нагрузку на компьютер. Если размер файла отчета превышает установленный лимит на 50 КБ, старые записи автоматически удаляются до тех пор, пока размер не сократится на 50 КБ.

Защитить файл отчета от сокращения

Включив эту опцию, можно сохранить файл отчета перед сокращением.

Записать конфигурацию в файл отчета

Если эта опция активна, используемые настройки поиска в режиме реального времени записываются в файл отчета.

Указание
Если ограничение для файла отчета не указано, новый файл отчета автоматически создается после того, как файл отчета достигнет размера 100 МБ. Для старого файла сохраняется резервная копия. Может существовать до трех резервных копий старых файлов отчета. Самые старые копии удаляются.

12.3 Обновление

В разделе **Обновление** вы можете настроить автоматическое выполнение обновления. У вас есть возможность настроить различные интервалы между обновлениями.

Автоматическое обновление

каждые n дня(ей) / час(ов) / минут(ы)

В этом поле можно указать интервал, с которым должно выполняться автоматическое обновление. Чтобы изменить частоту обновлений, выберите одну из временных характеристик в этом поле и измените ее при помощи кнопок со стрелками, расположенных 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. (Эта опция доступна только при включенном экспертном режиме.)

Запуск задачи, даже если установленное время запуска прошло

Если эта опция включена, задача обновления выполняется, даже если срок выполнения уже прошел, если она не могла быть запущена в назначенное

время, например, из-за того, что компьютер был выключен. (Эта опция доступна только при включенном экспертном режиме.)

12.3.1 Webserver

Веб-сервер

Обновление можно выполнить непосредственно через веб-сервер в Интернете внутренней сети. (Эти опции доступны только при включенном экспертном режиме.)

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 доступны. 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 выбранной учетной записи.

Пароль

Введите пароль для этой учетной записи. Для безопасности вводимые в это поле знаки заменяются звездочками (*).

Примечание
Если вы забыли имя пользователя или пароль существующей учетной записи, обратитесь к провайдеру.

Указание
Автоматический вызов обновления с помощью так называемого инструмента набора (например, SmartSurfer, Oleco, ...) пока не предусмотрен.

Разорвать модемное соединение, установленное для обновления

Если эта функция включена, то установленное для обновления модемное соединение будет автоматически разорвано сразу же после успешного завершения загрузки.

Указание
Эта функция доступна только при Windows XP. Начиная с Windows Vista открытое для обновления dial-up соединение всегда автоматически разрывается сразу же после успешного завершения загрузки.

Настройки прокси-сервера

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 функция включена, то для соединения с веб-сервером через прокси-сервер будут использоваться текущие системные настройки Windows. Задать системные настройки Windows для использования прокси-сервера можно здесь: **Панель управления > Сеть и Интернет > Подключения > Настройки сети**. В Internet Explorer в меню **Дополнительно** также можно выполнить настройку доступа в Интернет.

Предупреждение
При использовании прокс-сервера, требующего аутентификации, полностью введите необходимые данные в разделе **Подключение через это прокси**. Опцию **Использовать системные настройки Windows** можно применять только для прокси-серверов 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 хотели бы 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.

Пароль

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

Примеры:

Адрес: `proxy.domain.de` порт: `8080`

Адрес: `192.168.1.100` порт: `3128`

12.4 Backup

В пункте меню **Настройка > Интернет-безопасность > Резервное копирование** вы можете настроить параметры компонента Резервное копирование. (Эти опции доступны только при включенном экспертном режиме.)

12.4.1 Настройки

В меню **Настройки** можно задать параметры компонента Резервное копирование.

Создавать резервную копию только для измененных файлов

Если эта опция включена, то создается инкрементная резервная копия: в профиле резервного копирования сохраняются только те файлы, которые были изменены с момента последнего резервного копирования. Если эта опция отключена, при каждом резервном копировании профиля создается полная резервная копия: сохраняются все файлы. Эта опция по умолчанию активирована и рекомендуется, так как инкрементные копии создаются быстрее полных, не так сильно загружая систему.

Проверять на наличие вредоносного ПО перед резервным копированием

Если опция включена, файлы перед резервным копированием проверяются на вирусы и вредоносное ПО. Инфицированные файлы не сохраняются. Эта опция по умолчанию включена и рекомендуется.

12.4.2 Исключения

В **Исключениях** вы можете определить, какие файловые объекты и типы файлов подлежат резервному копированию, а какие нет.

Файловые объекты, исключенные из резервного копирования

Список в этом окне содержит файлы и папки, которые не подлежат резервному копированию.

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

Примечание
Содержащиеся в этом списке файлы фиксируются в файле отчета.

Поле ввода

В этом поле укажите имя файлового объекта, который не надо сохранять. По умолчанию указан путь к временной папке для локальных настроек активного пользователя.

Нажатием на эту кнопку открывается окно, в котором вы можете выбрать желаемый файл или путь.
Если вы указали имя файла и полный путь к нему, именно этот файл не подлежит резервному копированию. Если вы указали имя файла, но не указали путь к нему, ни один из файлов с этим именем (вне зависимости от папки и диска) не будет добавлен к резервной копии.

Добавить

С помощью этой кнопки можно перенести введенный в поле ввода файловый объект в окно просмотра.

Удалить

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

Сбросить список

Эта кнопка восстанавливает настройки по умолчанию.

Обратите внимание на следующее

- Символ-заполнитель * (произвольное количество знаков) - и ? (один знак) допустимы только в именах файлов.
- Список обрабатывается сверху вниз.
- Если исключается папка, автоматически исключаются и папки, находящиеся внутри нее.
- Можно исключать из проверки и отдельные расширения файлов (включая символы-заполнители).
- Для исключения объектов, обращение к которым осуществляется с помощью коротких имен файлов DOS (DOS name convention 8.3), необходимо добавить в список также соответствующее короткое имя файла.

Примечание
К имени файла, содержащего символы-заполнители, нельзя добавлять в конце обратный слеш. Пример:
`C:\Program Files\Приложение\Прилож*.exe\`
Эта запись недействительна и не будет рассматриваться как исключение!

Примеры

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

Списки расширений файлов

Включать все расширения файлов

Если эта опция включена, все файлы сохраняются в профиле резервного копирования.

Активировать список исключаемых расширений файлов

Если эта опция включена, то в профиле резервного копирования сохраняются все файлы, за исключением тех, расширения которых были внесены в список исключаемых.

Расширения файлов

Кнопка вызывает диалоговое окно, отображающее все расширения файлов, которые не включаются в резервное копирование при активной опции "**Активировать список исключаемых расширений файлов**". В списке уже приведены некоторые расширения файлов, но вы можете добавлять новые или удалять их.

Активировать список включаемых расширений файлов

Если эта опция включена, то в резервное копирование включаются только те файлы, расширения которых внесены в список.

Расширения файлов

Кнопка вызывает диалоговое окно, отображающее все расширения файлов, которые включаются в резервное копирование при активной опции "**Активировать список включаемых расширений файлов**". В списке уже приведены некоторые расширения файлов, но вы можете добавлять новые или удалять их.

12.4.3 Отчет

Компонент Резервное копирование имеет функцию протоколирования.

Протоколирование

В этой группе можно задать степень детализации файла отчета.

ВЫКЛ

Если опция включена, то компонент Резервное копирование не создает протокол. Отказывайтесь от протоколирования только в исключительных случаях.

По умолчанию

Компонент Резервное копирование добавляет к отчету важную информацию (резервное копирование, поиск вирусов, предупреждения и ошибки), менее важная информация для удобства работы с отчетом игнорируется. Эта настройка активирована по умолчанию.

Дополнительно

Если опция включена, то компонент Резервное копирование добавляет в файл отчета и менее важную информацию.

Полный

Если опция включена, то компонент Резервное копирование включает в отчет всю информацию о ходе резервного копирования и поиске вирусов.

12.5 FireWall

12.5.1 Конфигурация FireWall

Avira Internet Security позволяет конфигурировать брандмауэр Avira FireWall:

- Avira FireWall

12.5.2 Avira FireWall

Раздел **FireWall** в **Конфигурация > Безопасность** отвечает за настройку компонента Avira FireWall в операционных системах до Windows 7.

Правила адаптера

Под адаптером в Avira FireWall подразумевается любая 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. (Эти опции доступны только при включенном экспертном режиме.)

- ICMP-протокол
- Сканирование порта TCP
- Сканирование порта UDP
- Входящие правила
- Исходящие правила
- Кнопки

Предустановленное правило адаптера зависит от уровня безопасности. Вы можете изменять *уровень безопасности* в разделе **Интернет-безопасность > FireWall** центра управления или согласовывать правила адаптера со своими потребностями. Если Вы настроили правила адаптера под Ваши потребности, в разделе FireWall центра управления регулятор в поле *Уровень безопасности* будет перемещен в положение **Пользователь**.

> **Указание**
> Стандартная настройка Уровня безопасности для всех предопределенных правил модуля Avira FireWall - **Средний**.

ICMP-протокол

Internet Control Message Protocol (ICMP) служит для сетевого обмена информационными сообщениями и сообщениями об ошибках. Протокол применяется также для статусных сообщений Ping или Tracert.
Это правило позволяет задать 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	Правила
Низкий	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**.
Средний	Те же правила, что и для настройки *Низкий*.
Высокий	Блокирует входящие типы: **различные типы**. Блокирует входящие типы: **различные типы**. Подозрение на флудинг, если задержка между пакетами составляет менее **50** миллисекунд. Фрагментированные ICMP-пакеты **отклонять**.

Заблокированные входящие типы: ни один тип/разные типы

Щелчком мыши по этой 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 / разные типы

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

Предположить флудинг

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

Фрагментированные ICMP-пакеты

Щелчком мыши по ссылке Вы можете выбрать "**отклонять**" или "**не отклонять**" фрагментированные ICMP-пакеты.

Сканирование порта TCP

При помощи этого правила вы можете определить, когда FireWall должен предполагать сканирование порта TCP и как он должен действовать в этом случае.

Правило для предотвращения так называемых атак сканирования портов TCP, с помощью которых можно определить 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 сканирования порта TCP

Установка	Правила
Низкий	Подозрение на сканирование портов TCP, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении сканирования портов TCP записывать IP-адрес злоумышленника **в банк событий** и **не добавлять** к правилам для блокирования атаки.
Средний	Подозрение на сканирование портов TCP, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении сканирования портов TCP записывать IP-адрес злоумышленника **в банк событий** и **добавлять** к правилам для блокировки атаки.
Высокий	Те же правила, что при настройке *Средний*.

Порты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести число сканируемых портов, при достижении которого принимается решение об обнаружении сканирования портов TCP.

Временные параметры сканирования портов

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

Банк событий

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

Правило

Щелчком по этой ссылке можно решить, нужно ли добавлять правило для блокировки атаки сканирования портов TCP.

Сканирование порта UDP

При помощи этого правила можно определить, когда FireWall принимает решение об обнаружении сканирования портов UDP, а также задать 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 сканирования портов UDP

Установка	Правила
Низкий	Подозревать сканирование портов UDP, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении сканирования портов UDP записывать IP-адрес злоумышленника **в банк событий** и **не добавлять** к правилам для блокирования атаки.
Средний	Подозревать сканирование портов UDP, если **50** или более портов сканируются за **5000** миллисекунд. При обнаружении сканирования портов TCP записывать IP-адрес злоумышленника **в банк событий** и **добавлять** к правилам для блокировки атаки.
Высокий	Те же правила, что при настройке *Средний*.

Порты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести число сканируемых портов, при достижении которого принимается решение об обнаружении сканирования портов UDP.

Временные параметры сканирования портов

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

Банк событий

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

Правило

Щелчком по этой ссылке можно решить, нужно ли добавлять правило для блокировки атаки сканирования портов UDP.

Входящие правила

Посредством входящих правил Avira FireWall контролирует входящий трафик.

Предупреждение
Так как при фильтрации пакетов определенные правила применяются друг за другом, их последовательность имеет важнейшее значение. Изменяйте последовательность только тогда, когда вы точно знаете, какие последствия это вызовет.

Предустановленные правила мониторинга TCP-трафика

Установка	Правила
Низкий	Avira FireWall не блокирует входящий трафик.
Средний	• **Разрешить установленное TCP-соединение по порту 135** TCP-пакеты **Разрешить**, от адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в **{135}** и удаленный порт находится в **{0-65535}**. Применять для **Пакетов существующих соединений**. **Не вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**. • **Запрещать TCP-пакеты на порт 135** TCP-пакеты **Отклонить**, с адреса **0.0.0.0** с маской **0.0.0.0**, если локальны порт находится в **{135}**, а удаленный порт в **{0-65535}**. Применять ко **всем пакетам**. **Не вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**. • **Контроль трафика, соответствующего TCP** TCP-пакеты **Разрешить**, с адреса **0.0.0.0** с маской **0.0.0.0**, если локальный порт находится в **{0-65535}**, а удаленный порт в **{0-65535}**. Применять к **началу установления соединения и к пакетам существующих соединений.**. **Не вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**. • **Запрещать все TCP-пакеты** TCP-пакеты **Отклонять**, 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 вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**.

Высокий	**Контролировать разрешенный TCP-трафик** Разрешить TCP-пакеты от 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 для **Пакетов существующих соединений**. **Не вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**.

Разрешить / запретить TCP-пакеты

Щелчком по этой ссылке можно установить, разрешать или отклонять определенные TCP-пакеты.

IP-адрес

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести адрес IPv4 или IPv6.

IP-маска

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести маску IPv4 или IPv6.

Локальные порты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести один или несколько локальных портов, а также целые диапазоны портов.

Удаленные порты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести один или несколько удаленных портов, а также целые диапазоны портов.

Метод применения

Щелчком по этой ссылке можно определить необходимость применения правила к пакетам существующих соединений, к началу установления соединения и пакетами имеющихся соединений или ко всем соединениям.

Банк событий

Щелчком по этой ссылке можно определить необходимость сохранения информации в базе данных событий, если пакет соответствует правилу.

Дополнительно

Опция **Расширенный** позволяет фильтровать на основании содержимого. Вы можете, например, отклонять пакеты, содержащие специальные данные с

определенным оффсет. Если вы не хотите использовать эту опцию, не выбирайте файл или выберите пустой файл.

Фильтрация по содержимому: байты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Щелчком по этой ссылке открывается диалоговое окно, в котором можно выбрать специальную маску.

Фильтрация по содержимому: оффсет

Щелчком по этой ссылке открывается диалоговое окно, в котором можно указать оффсет для фильтра содержимого. Оффсет рассчитывается с конца заголовка TCP.

Предустановленные правила мониторинга UDP-трафика

Установка	Правила
Низкий	-
Средний	• **Контроль трафика в соответствии с UDP** UDP-пакеты **Разрешить**, 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 правило к **открытым портам** для **всех потоков данных**. **Не записывать в банк событий,** , если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**. • **Запрещать все UDP-пакеты** UDP-пакеты **Отклонять**, 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** для **всех потоков данных**. **Не вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**.

Высокий	**Контролировать разрешенный UDP-трафик** UDP-пакеты **Разрешить**, 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, 88,...}**. Применять правило к **открытым портам** для **всех потоков данных**. **Не вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**.

Разрешить / запретить UDP-пакеты

Щелчком по этой ссылке можно установить, разрешать или отклонять определенные UDP-пакеты.

IP-адрес

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести адрес IPv4 или IPv6.

IP-маска

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести маску IPv4 или IPv6.

Локальные порты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести один или несколько локальных портов, а также целые диапазоны портов.

Удаленные порты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести один или несколько удаленных портов, а также целые диапазоны портов.

Метод применения

Порты

Щелчком по этой ссылке можно определить необходимость применения правила ко всем портам или только ко всем открытым портам.

Потоки данных

Щелчком по этой ссылке можно определить необходимость применения правила ко всем потокам данных или только ко всем исходящим потокам данных.

Банк событий

Щелчком по этой ссылке можно определить необходимость сохранения информации в базе данных событий, если пакет соответствует правилу.

Дополнительно

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

Фильтрация по содержимому: байты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Щелчком по этой ссылке открывается диалоговое окно, в котором можно выбрать специальную маску.

Фильтрация по содержимому: оффсет

Щелчком по этой ссылке открывается диалоговое окно, в котором можно указать оффсет для фильтра содержимого. Оффсет рассчитывается с конца заголовка UDP.

Предустановленные правила мониторинга ICMP-трафика

Установка	Правила
Низкий	-
Средний	**Не отменять ICMP-пакеты на базе IP-адреса** ICMP-пакеты **Разрешить** с адреса **0.0.0.0** с маской **0.0.0.0**. **Не вносить в банк событий**, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты **<пусто>** с маской **<пусто>** при оффсете **0**.
Высокий	Те же правила, что при настройке *Средний*.

Разрешить / запретить ICMP-пакеты

Щелчком по этой ссылке можно установить, разрешать или отклонять определенные ICMP-пакеты.

IP-адрес

Щелчком по ссылке откройте диалоговое окно, в котором Вы можете указать желаемый IPv4-адрес.

IP-маска

Щелчком по ссылке откройте диалоговое окно, в котором Вы можете указать желаемую IPv4-маску.

Банк событий

Щелчком по этой ссылке можно определить необходимость сохранения информации в базе данных событий, если пакет соответствует правилу.

Дополнительно

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

Фильтрация по содержимому: байты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно выбрать файл, который содержит специальный буфер.

Фильтрация по содержимому: маска

Щелчком по этой ссылке открывается диалоговое окно, в котором можно выбрать специальную маску.

Фильтрация по содержимому: оффсет

Щелчком по этой ссылке открывается диалоговое окно, в котором можно указать оффсет для фильтра содержимого. Оффсет рассчитывается с конца заголовка ICMP.

Предустановленное правило для IP-пакетов

Установка	Правила
Низкий	-
Средний	-
Высокий	**Запретить IP-пакеты** **Отклонить IPv4**- пакеты с адреса **0.0.0.0** с маской **0.0.0.0**. **Не записывать в банк событий**, если пакет соответствует правилу.

Разрешить / запретить

Щелчком по ссылке Вы можете определить необходимость разрешения или запрета определенных IP-пакетов.

IPv4 / IPv6

Щелчком по ссылке выберите IPv4 или IPv6.

IP-адрес

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести адрес IPv4 или IPv6.

IP-маска

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести маску IPv4 или IPv6.

Банк событий

Щелчком по этой ссылке можно определить необходимость сохранения информации в базе данных событий, если пакет соответствует правилу.

Исходящие правила

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

Предупреждение
Так как при фильтрации пакетов определенные правила применяются друг за другом, их последовательность имеет важнейшее значение. Изменяйте последовательность только тогда, когда вы точно знаете, какие последствия это вызовет.

Кнопки

Кнопка	Описание
Добавить	Позволяет создать новое правило. Щелкните на этой кнопке для отображения окна "Добавить правило". В этом диалоговом окне Вы можете выбрать новые правила.
Удалить	Удалить выбранное правило.
Наверх	Переместить выбранное правило на одну позицию вверх, благодаря чему приоритет данного правила повысится.
Вниз	Перемещение выбранного правила на одну позицию вниз, в результате чего приоритет данного правила понизится.

Переименовать	Переименовать выбранное правило.

Указание
Вы можете добавлять новые правила для отдельных адаптеров или для всех адаптеров компьютера. Чтобы добавить правило для всех адаптеров, выберите **Рабочее место** в представленной структуре адаптеров и нажмите кнопку **Добавить**. См. Добавить новое правило.

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

Добавить новое правило

В этом окне вы можете выбрать новые входящие и исходящие правила. Выбранное правило переносится с настройками по умолчанию в окно **Правила адаптера**, в котором можно вносить в него дальнейшие изменения. Наряду с входящими и исходящими правилами в вашем распоряжении имеются и другие правила.

Возможные правила

Разрешить пиринговую сеть

Разрешает пиринговые соединения: входящее TCP-соединение по порту 4662 и входящее UDP-соединение по порту 4672

Порт TCP

Щелчком мыши по этой ссылке открывается диалоговое окно, в котором можно ввести разрешенный порт TCP.

Порт UDP

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести разрешенный порт UDP.

Разрешить VMWARE-соединения

Разрешает связь между VMWare-системами

Блокировать IP-адрес

Блокирует весь трафик с определенным IP-адресом

IP-Версия

Щелчком по ссылке выберите IPv4 или IPv6.

IP-адрес

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести адрес IPv4 или IPv6.

Блокировать подсеть

Блокирует весь трафик с определенным IP-адресом и маской подсети

IP-Версия

Щелчком по ссылке выберите IPv4 или IPv6.

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести нужный IP-адрес.

Маска подсети

Щелчком по ссылке открывается диалоговое окно, в котором можно ввести маску подсети.

Разрешить IP-адрес

Разрешает весь трафик с определенным IP-адресом

IP-Версия

Щелчком по ссылке выберите IPv4 или IPv6.

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести нужный IP-адрес.

Разрешить подсеть

Разрешает весь трафик с определенным IP-адресом и маской подсети

IP-Версия

Щелчком по ссылке выберите IPv4 или IPv6.

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести нужный IP-адрес.

Маска подсети

Щелчком по ссылке открывается диалоговое окно, в котором можно ввести маску подсети.

Разрешать веб-сервер

Разрешает соединение с веб-сервером по порту 80: входящее TCP-соединение по порту 80

Порт

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести порт, используемый веб-сервером.

Разрешить VPN-соединения

Разрешает VPN-соединения (Virtual Private Network) с определенным IP: Входящий UDP-трафик по x портам, входящий TCP-трафик по x портам, входящий IP-трафик с протоколами ESP(50), GRE (47)

IP-Версия

Щелчком по ссылке выберите IPv4 или IPv6.

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести нужный IP-адрес.

Разрешить соединение с удаленным рабочим столом

Разрешает соединение с "Удаленным рабочим столом" (Remote Desktop Protocol) по порту 3389

Порт

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести порт, используемый для разрешенного соединения с удаленным рабочим столом.

Разрешать VNC-соединение

Разрешает VNC-соединения (Virtual Network Computing) по порту 5900

Порт

Щелчком по ссылке открывается диалоговое окно, в которое вы можете ввести порт, используемый для разрешенного VNC-соединения.

Разрешить общие сетевые папки и принтеры

Разрешает доступ к общим принтерам и файлам: Входящий TCP-трафик по порту 137, 139 и входящий UDP-трафик по порту 445 с любого IP-адреса.

Возможные входящие правила

- **Входящее IP-правило**
- **Входящее ICMP-правило**
- **Входящее UDP-правило**
- **Входящее TCP-правило**
- **Входящее правило IP-протоколов**

Возможные исходящие правила

- **Исходящее IP-правило**
- **Исходящее ICMP-правило**
- **Исходящее UDP-правило**
- **Исходящее TCP-правило**
- **Исходящее правило IP-протоколов**

> **Примечание**
> Опции для возможных входящих и исходящих правил идентичны опциям предустановленных правил соответствующих протоколов, как описано в FireWall > Правила адаптера.

Кнопки

Кнопка	Описание
ОК	Отмеченное правило принимается как новое правило адаптера.
Прервать	Окно закрывается без добавления нового правила.

Правила приложения

Правила приложения для пользователя

В этом списке перечислены все пользователи системы. Если вы зарегистрированы с правами администратора, вы можете выбрать пользователя, для которого хотите создать правила. Если вы не являетесь пользователем с привилегированными правами, вы увидите в списке только имя текущего пользователя.

Приложение

В этой таблице приведен список приложений, для которых определены правила. Список содержит настройки для каждого приложения, которое было запущено после того, как был установлен Avira FireWall, и для которого создано правило.

Стандартный вид

Столбец	Описание
Приложение	Имя приложения
Активные соединения	Количество активных соединений, открытых приложениями
Действие	Отображает действие, которое Avira FireWall выполнит автоматически, если приложение каким-либо образом использует сеть. Щелчком по этой ссылке можно сменить тип выполняемого действия. На выбор предлагаются следующие варианты действий: **Спрашивать**, **Разрешить** или **Отклонить**. Настройка по умолчанию - **Спрашивать.**

Расширенная настройка

Если вы хотите индивидуально регулировать сетевые доступы приложения, так же как для правил адаптера, вы можете создавать определенные правила приложения, основанные на фильтрах пакетов.

- Для перехода к расширенным настройкам правил приложения включите **режим эксперта**.
- Теперь в **Настройка > Интернет-безопасность > FireWall > Настройки** измените настройку для *Правил приложения*: включите опцию **Расширенные настройки** и сохраните настройку нажатием на **Применить** или **OK**.
  - ↳ Теперь в окне **Настройка > Интернет-безопасность > FireWall > Правила приложения** в списке правил приложения появится новый столбец **Фильтр** с записью **Простой**.

Столбец	Описание
Приложение	Имя приложения.
Активные соединения	Количество активных соединений, открытых приложениями

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 следующие варианты действий: **Спрашивать**, **Разрешить** или **Отклонить**. При установке **Фильтр - расширенный** отображается тип выполняемого действия **Правила**. Ссылка **Правила** открывает окно **Расширенные правила приложений**, в котором вы можете сохранить подробные правила для приложения.
Фильтр	Отображает тип фильтра. Щелчком мыши по ссылке можно сменить тип фильтра. **Простой**: При простой фильтрации указанное действие выполняется для всей типов сетевой активности приложения программы. **Расширенный**: при фильтрации выполняются правила, сохраненные в расширенной настройке.

- Если для приложения нужно задать особые правила приложения, в разделе **Фильтр** выберите запись **Расширенные**.
  - ↪ В столбце **Действие** отобразится запись **Правила**.
- Щелкните мышью по записи **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. Предлагаются следующие опции:

Отклонить / разрешить 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). Технология кодовых инъекций используется разработчиками вредоносных программ для выполнения кода под прикрытием другой программы. Например, таким образом можно скрыть доступ к Интернету от FireWall. По умолчанию кодовые инъекции разрешены для всех подписанных приложений.

Разрешить или запретить пассивное прослушивание приложением 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 можно создать любое количество правил приложения. Правила приложения выполняются в отображенной последовательности (более подробную информацию вы найдете в разделе Расширенные правила приложения).

Примечание
Если изменить **Расширенный** фильтр на **Простой** для правила приложения, то заданные ранее правила приложения в расширенной настройке не будут окончательно удалены, а будут отключены. Если вы снова переключитесь на **Расширенный** фильтр, 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.

- *Имя* - Имя приложения.
- *Путь* - Путь к исполняемому файлу приложения.

Кнопки

Кнопка	Описание
Добавить приложение	Позволяет вам создать новое правило приложения. После щелчка по этой кнопке отображается диалоговое окно. Вы можете выбрать приложение, для которого необходимо создать правило.
Удалить правило	Удалить выбранное правило приложения.

Показать подробности	В окне *Свойства* отображается детальная информация о приложении, выбранном вами в списке приложений. (Эта опция доступна только при включенном экспертном режиме.)
Обновить	Обновление списка приложений с одновременной отменой всех изменений, сделанных в правилах приложения.

Расширенные правила приложения

В окне **Расширенные правила приложения** можно создать определенные правила для трафика приложений и прослушивания портов. Новое правило создается нажатием на кнопку **Добавить**. В нижней области окна Вы можете осуществить дальнейшее определение правила. Для каждого приложения можно создать любое количество правил. Правила выполняются в отображенной последовательности. С помощью кнопок **Вверх** и **Вниз** можно изменить последовательность правил.

> **Примечание**
> Чтобы изменить позицию правила приложения, перетащите его в нужную позицию с помощью мыши.

Информация о приложении

В разделе Подробности отображается детальная информация о выбранном приложении:

- *Имя* - Имя приложения.
- *Путь* - Путь к исполняемому файлу приложения.

Опции правила

Запретить / разрешить кодовую инъекцию

Щелчком мыши можно разрешить или запретить кодовые инъекции при работе с выбранным приложением

Тип правила: Трафик / Прослушивание

Здесь Вы можете определить щелчком мыши необходимость создания правила для трафика данных или для прослушивания портов.

Действие: Разрешить / запретить

Щелчком по этой ссылке можно указать, какое действие выполняется правилом.

Порт

Здесь Вы можете щелчком мыши выбрать диалоговое окно для ввода локального порта, к которому относится правило прослушивания. Также Вы можете ввести несколько портов или диапазонов портов.

Исходящие, входящие, все пакеты

Щелчком по этой ссылке можно указать, какие пакеты будут контролировать правила для трафика: все пакеты, только исходящие или только входящие.

IP-пакеты / TCP-пакеты / UDP-пакеты

Щелчком по этой ссылке можно указать, какой протокол контролирует правило для трафика.

Опции для IP-пакетов

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести нужный IP-адрес.

IP-маска

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести нужную IP-маску.

Опции для TCP-пакетов / UDP-пакетов

Локальный IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести локальный IP-адрес.

Локальная IP-маска

Щелчком по ссылке можно открыть диалоговое окно, в которое Вы можете ввести желаемую локальную IP-маску.

Удаленный IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести удаленный IP-адрес.

Удаленная IP-маска

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести удаленную IP-маску.

Локальный порт

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести один или несколько локальных портов, а также целые диапазоны портов.

Удаленный порт

Щелчком по этой ссылке открывается диалоговое окно, в котором можно ввести один или несколько удаленных портов, а также целые диапазоны портов.

Не записывать в файл отчета / Записать в файл отчета

Щелчком по этой ссылке можно указать, вносить ли запись в файл отчета программы при соответствии правилу.

Кнопки

Кнопка	Описание
Добавить	Создается новое правило приложения.
Удалить	Удаление выбранного правила приложения.
Наверх	Выбранное правило перемещается на одну позицию вверх, благодаря чему приоритет правила повышается.
Вниз	Выбранное правило приложения перемещается на одну позицию вниз, благодаря чему приоритет правила понижается.
Переименовать	Выбранное правило редактируется, можно ввести новое имя правила.
Применить	Avira FireWall принимает и сразу же применяет внесенные изменения.

ОК	Изменения принимаются. Окно для настройки правил приложения закрывается.
Прервать	Окно для настройки правил приложения закрывается без сохранения изменений.

Надежные разработчики

В разделе *Надежные разработчики* показывается список надежных производителей программного обеспечения. (Эти опции доступны только при включенном экспертном режиме.)

Вы можете добавить разработчика к списку или удалить его, используя опцию **Всегда доверять этому разработчику** во всплывающем окне **Сетевое событие**. Вы можете разрешить по умолчанию сетевой доступ для приложений, которые подписаны разработчиками из списка, активировав опцию **Автоматически разрешать приложения от надежных разработчиков**.

Надежные разработчики для пользователей

Если вы зарегистрированы с правами администратора, вы можете выбрать пользователя, список надежных разработчиков которого вы хотите просмотреть или отредактировать. 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.

Разработчики

Список содержит всех разрабочиков, 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	Внесенные изменения отменяются: загружается последний сохраненный список.

Примечание
Если вы удалите разработчиков 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
Для FireWall правила приложений имеют больший приоритет, чем список надежных производителей: если вы создали правило приложения и разработчик приложения находится в списке надежных поставщиков, то правило приложения выполняется.

Настройки

Эти опции доступны только при включенном экспертном режиме.

Расширенные настройки

Отключать при загрузке брандмауэр Windows

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

Превышено время ожидания для правила

Всегда блокировать

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

Удалять правило через n секунд

Если эта опция включена, созданные автоматически правила, например, при сканировании портов, удаляются по истечении указанного вами времени. Эта опция включена по умолчанию. В этом поле можно задать, через сколько секунд следует удалить правило.

Уведомления

Определите в разделе уведомлений, при каких событиях вы хотите получать уведомление FireWall в виде всплывающего окна.

Сканирование портов

Если эта опция включена, вы получите уведомление в виде всплывающего окна, если FireWall обнаружит сканирование портов.

Флудинг

Если эта опция включена, вы получите уведомление в виде всплывающего окна, если FireWall обнаружит флуд-атаку.

Приложения заблокированы

Если эта опция включена, вы получите уведомление в виде всплывающего окна, если FireWall запретит, т.е. заблокирует сетевую активность приложения.

IP заблокирован

Если эта опция включена, вы получите уведомление в виде всплывающего окна, если FireWall запретит 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

Если эта опция включена, у вас есть возможность индивидуальной настройки различных сетевых доступов приложения.

Основные настройки

Если эта опция включена, может быть задано единственное действие для различных сетевых доступов приложения.

Настройки всплывающего окна

Эти опции доступны только при включенном экспертном режиме.

Настройки всплывающего окна

Проверить стартовый блок процесса

Если эта опция включена, происходит более точная проверка списка процессов. FireWall исходит из того, что каждый процесс из списка, не классифицированный как надежный, 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 всплывающее окно. Альтернативно информация выдается только после первой попытки установить соединение. Эта опция по умолчанию отключена.

Сохранять действие для приложения

Всегда включена

Если эта опция включена, по умолчанию активна опция "**Сохранить действие для этого приложения**" диалогового окна "**Сетевое событие**".

Всегда отключена

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

Разрешить подписанные приложения

Если опция включена, при получении подписанным приложением определенного разработчика доступа к сети автоматически включается опция "**Сохранять действие для приложения**" диалогового окна "**Сетевое событие**". Эти подписанные приложения предоставляются так называемыми "Надежными разработчиками" (см. Надежные разработчики).

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 сетевом событии. Если при последнем сетевом событии опция "**Сохранять действие для приложения**" была отключена, она будет неактивна также при следующем сетевом событии.

Отображать подробности

В этой группе опций настройки Вы можете настроить отображение подробной информации в окне **Сетевое событие**.

Отображать подробности по запросу

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

Всегда отображать подробности

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

Запомнить последнее состояние

Если опция включена, сохраняется статус отображения подробностей при последнем сетевом событии. 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 следующем событии отображаться не будут.

12.6 Web Protection

Раздел **Web Protection** в **Настройка > Интернет-безопасность** отвечает за настройку функции Web Protection.

12.6.1 Поиск

Модуль Web Protection помогает защитить ваш компьютер от вирусов и вредоносных программ, которые загружаются из Интернета через браузер. В разделе **Поиск** Вы можете настроить действия модуля Web Protection. (Эти опции доступны только при включенном экспертном режиме.)

Поиск

Поддержка IPv6

Если выбрана эта опция, то модуль Web Protection поддерживает версию 6 Интернет-протокола. Эта опция не доступна для новых установок или измененных программ на Windows 8.

Защита Drive-By

Защита *Drive-By* позволяет настроить блокировку элементов I-Frame, также называемых вложенными фреймами. I-Frame - это элементы HTML, т.е. элементы Интернет-страниц, которые ограничивают участок веб-страницы. С помощью I-Frame можно загрузить и отобразить другой веб-контент, часто имеющий отличные URL, как отдельные документы в отдельном окне браузера. Чаще всего I-Frame используются для баннерной рекламы. Иногда I-Frame используются для маскировки вредоносных программ. В таком случае область I-Frame в браузере почти не видна или совсем не видна. С помощью опции **Блокировать**

подозрительные I-Frame вы можете контролировать и блокировать загрузку I-Frame.

Блокировать подозрительные I-Frame

Если эта опция включена, то I-Frame на запрошенных страницах будут проверяться по определенным критериям. Если на запрошенной веб-странице будут обнаружены подозрительные I-Frame, они будут заблокированы. В окне I-Frame отобразится сообщение об ошибке.

Действие при обнаружении

Вы можете определить действия, которые будут выполняться, если модуль Web Protection обнаружит вирус или вредоносную программу. (Эти опции доступны только при включенном экспертном режиме.)

Интерактивный

Если включен интерактивный режим, при обнаружении вируса или вредоносной программы отображается окно, предлагающее выбор действий с инфицированным файлом. Эта настройка активирована по умолчанию.

Показать степень выполнения

Если эта опция включена, на рабочем столе возникает индикатор выполнения, если время ожидания загрузки файла или открытия сайта превышает 20 секунд. Этот индикатор предназначен для контроля процесса загрузки сайтов с большим объемом информации: при поиске в Интернете с включенным модулем Web Protection содержимое веб-сайтов загружается в Интернет-браузер не последовательно, так как перед отображением в браузере оно проверяется на наличие вирусов и вредоносного ПО. Эта опция по умолчанию отключена.

Более подробную информацию можно получить по ссылке.

Автоматический

Если эта опция включена, при обнаружении вируса или вредоносной программы не открывается диалоговое окно для выбора действия. Web Protection работает автоматически в соответствии с выбранными вами настройками.

Первичное действие

Первичное действие - это действие, выполняемое в случае, когда Web Protection 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. Web Protection заносит сведения об обнаруженном объекте в файл отчета, если включена Функция отчетов.

Поместить на карантин

Запрошенная веб-сервером страница или переданные данные и файлы при обнаружении вируса или вредоносной программы помещаются в 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 отправляются модулем Web Protection вашему веб-браузеру. Доступ к файлу разрешается, никаких действий с ним не выполняется.

Предупреждение
Инфицированный файл все еще активен в вашей системе! Это может причинить существенный вред вашему компьютеру!

Запрет доступа

В пункте **Запрет доступа** вы можете указывать типы файлов и MIME (типы содержимого передаваемых данных), которые должны блокироваться модулем Web Protection. С помощью веб-фильтра вы можете заблокировать известные, нежелательные URL, например, URL фишинг-программ или вредоносных программ. Web Protection препятствует передаче данных из Интернета на ваш компьютер. (Эти опции доступны только при включенном экспертном режиме.)

Типы файлов / типы MIME, которые должны блокироваться модулем Web Protection

Web Protection блокирует все приведенные в списке типы данных и MIME-типы (типы содержимого передаваемых данных).

Поле ввода

Укажите в этом поле имя типов MIME и файлов, которые должен блокировать модуль Web Protection. Для типов файлов укажите расширение, например, **.htm**. Для типов MIME укажите тип носителя и, при необходимости, подтип. Оба типа данных 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 модулем Web Protection, но могут быть загружены локально из Интернет-браузера вашим компьютером. Временные Интернет-файлы - это файлы, которые сохраняются Интернет-браузером для более быстрой загрузки веб-страниц.

Примечание
Список блокируемых типов файлов / MIME игнорируется, если имеются записи в списке не подлежащих проверке типов файлов и MIME в виде исключений.

Примечание
При указании типов файлов и типов MIME нельзя применять специальные символы (символ-заполнитель * для любого числа символов и ? для замены одного символа).

Типы MIME: примеры типов носителей

- `text`= для текстовых файлов
- `image` = для графических файлов
- `video` = для видеофайлов
- `audio` = для аудиофайлов
- `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 модулем Web Protection.
- `application/olescript` = файлы MIME-типа application/olescript (скрипт-файлы ActiveX *.axs) блокируются модулем Web Protection.
- `.exe` = все файлы с расширением .exe (исполняемые файлы) блокируются модулем Web Protection.
- `.msi` = все файлы с расширением .msi (файлы Windows Installer) блокируются модулем Web Protection.

Добавить

С помощью этой кнопки вы можете перенести введенный в поле ввода MIME-тип или тип файла в окно индикации.

Удалить

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

Веб-фильтр

Веб-фильтр имеет внутреннюю, ежедневно пополняемую базу данных, в которой URL расположены в соответствии с характеристиками содержания.

Активировать веб-фильтр

Если эта функция включена, то все адреса URL, которые относятся к выбранным категориям в списке Web-фильтра, блокируются.

Список веб-фильтра

В списке веб-фильтра вы можете выбрать категории содержания, адреса URL которых должны блокироваться модулем Web Protection.

Примечание
Веб-фильтр игнорируется для объектов, включенных в список исключенных из проверки URL как Исключения.

Примечание
К группе **Спам-URL** относятся URL, через которые распространяются спам-письма. Категория **Обман / дезинформация** включает в себя Интернет-страницы с "абонементами-ловушками" и различными услугами, стоимость которых скрывается поставщиком.

Исключения

С помощью этих опций вы можете исключить из проверки модуля Web Protection MIME-типы (типы содержимого передаваемых файлов) и типы файлов для URL (Интернет-адреса). Указанные MIME-типы и URL не будут проверяться модулем Web Protection на наличие вирусов или вредоносных систем при пересылке в вашу компьютерную систему. (Эти опции доступны только при включенном экспертном режиме.)

MIME-типы, исключенные из проверки модулем Web Protection

В этом поле вы можете выбрать MIME-типы (тип содержимого переданных данных), которые должны быть исключены из проверки модулем Web Protection.

Исключенные из проверки модулем Web Protection типы файлов / MIME (определены пользователем)

Все типы файлов и MIME-типы (тип содержимого переданных данных), указанные в списке, исключаются из проверки модулем Web Protection.

Поле ввода

В этом поле укажите имена MIME-типов и типов файлов, которые должны быть исключены из проверки модулем Web Protection. Для типов файлов укажите расширение, например, `.htm`. Для типов MIME укажите тип носителя и, при необходимости, подтип. Оба типа данных отделяются друг от друга обычной косой чертой, например `,video/mpeg` или `audio/x-wav`.

Указание
При указании типов файлов и типов MIME нельзя применять специальные символы (символ-заполнитель * для любого числа символов и ? для замены одного символа).

Предупреждение
Все типы файлов и содержимого, указанные в списке исключений, загружаются в Интернет-браузер без дополнительной проверки заблокированного доступа (список блокируемых типов файлов и MIME в разделе Запрет доступа) или модуля Web Protection: Для всех объектов, входящих в список исключений, записи в списке блокируемых типов файлов и MIME игнорируются. Поиск на наличие вирусов и вредоносного ПО не производится.

Типы MIME: примеры типов носителей

- `text` для текстовых файлов
- `image` = для графических файлов
- `video` = для видеофайлов
- `audio` = для аудиофайлов
- `application` = для файлов, связанных с определенной программой

Примеры: Исключенные из проверки типы файлов и MIME

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

Добавить

С помощью этой кнопки вы можете перенести введенный в поле ввода MIME-тип или тип файла в окно индикации.

Удалить

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

URL, исключенные из проверки модулем Web Protection

Все URL из этого списка исключаются из проверки модулем Web Protection.

Поле ввода

Укажите в этом поле URL (Интернет-адреса), которые необходимо исключить из проверки модулем Web Protection, например, **www.domainname.com**. Вы можете задать части URL, указав уровень домена со стоящими перед ним или после него точками: .domainname.ru для всех страниц и всех субдоменов домена. Веб-страница с любым доменом первого уровня (.com или .net) должна заканчиваться точкой: **домен.**. Если вы записываете набор символов без точки в начале или в конце, такая последовательность интерпретируется как домен первого уровня, например, **net** для всех доменов зоны NET (www.domain.net).

Указание
При вводе URL можно использовать специальный символ * для любого количества знаков. Используйте в сочетании со специальными символами точки для обозначения уровня домена перед его именем или после него:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (действительно, но не рекомендовано)
Адреса без точек, например `*name*`, будут рассматриваться как части домена первого уровня, поэтому их ввод нецелесообразен.

Предупреждение
Все веб-сайты, указанные в списке разрешенных URL, загружаются в Интернет-браузер без дополнительной проверки с помощью Web-фильтра или модуля Web Protection: Для всех объектов, входящих в список разрешенных URL, записи в списке веб-фильтра (см. запрет доступа) игнорируются. Поиск на наличие вирусов и вредоносного ПО не производится. Поэтому исключайте из проверки модулем Web Protection только надежные URL.

Добавить

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

Удалить

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

Пример: Разрешенные URL

- `www.avira.com` -ИЛИ- `www.avira.com/*`
  = Все URL с доменом www.avira.com исключаются из проверки модулем Web Protection: 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.ru не исключаются из проверки модулем Web Protection.

- `avira.com` -ИЛИ- `*.avira.com`
  = = Все URL с доменом второго и первого уровня 'avira.com' исключаются из проверки модулем Web Protection. Указанный диапазон включает все существующие субдомены ".avira.com": www.avira.com, forum.avira.com,...
- `avira.` -ИЛИ- `*.avira.*`
  = Все URL с доменом второго уровня "avira" исключаются из проверки модулем Web Protection. Указанный диапазон включает все существующие домены первого уровня и субдомены ".avira.": www.avira.com, www.avira.ru, forum.avira.com,...
- `.*domain*.*`
  = Все URL, содержащие домен второго уровня с цепочкой символов "domain", исключаются из проверки модулем Web Protection: www.domain.com, www.new-domain.ru, www.sample-domain1.ru, ...
- `net` -ИЛИ- `*.net`
  = Все URL с доменом первого уровня "net" исключаются из проверки модулем Web Protection: www.name1.net, www.name2.net,...

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

Эвристика

Этот раздел настроек содержит параметры эвристического поиска. (Эти опции доступны только при включенном экспертном режиме.)

Продукты Avira содержат 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, например, основываясь на имеющейся у него информации о надежности источника происхождении файла.

Эвристическое обнаружение макровирусов

Ваш продукт Avira имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, альтернативно можно ограничиться уведомлением пользователя о

подозрительных документах. Эта опция включена по умолчанию и рекомендована.

Эвристика AHeAD (Advanced Heuristic Analysis and Detection)

Активировать AHeAD

Благодаря технологии AHeAD ваш продукт Avira содержит очень мощную эвристическую систему для определения даже неизвестных (новых) вредоносных программ. Если эта опция включена, вы можете установить уровень "резкости" эвристики. Эта настройка активирована по умолчанию.

Низкий уровень распознавания

Если эта опция включена, программа обнаруживает меньше неизвестного вредоносного ПО, опасность ложных обнаружений при этом невелика.

Средний уровень распознавания

При включении этой опции обеспечивается сбалансированная защита с небольшим количеством ложных обнаружений. Эта настройка определена по умолчанию, если вы используете эвристический поиск.

Высокий уровень распознавания

При включении этой опции обнаруживается существенно больше неизвестного вредоносного ПО, но число ложных обнаружений также возрастает.

12.6.2 Отчет

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

Протоколирование

В этой группе определяется объем файла отчета.

ВЫКЛ

Если выбрана эта опция, то модуль Web Protection 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 включена эта опция, модуль Web Protection записывает важную информацию (обнаружения, предупреждения и ошибки) в файл отчета, а менее значимая информация для удобства работы с отчетом в него не включается. Эта настройка активирована по умолчанию.

Расширенный

Если эта опция включена, модуль Web Protection вносит в отчет и менее значимую информацию.

Полный

Если эта опция включена, модуль Web Protection включает в файл отчета все данные, в том числе, тип, размер и дату создания файла.

Ограничить файл отчета

Ограничить размер до n МБ

Если выбрана эта опция, размер файла отчета можно ограничить, возможные значения: от 1 до 100 МБ. При ограничении размера файла отчета предоставляется лимит около 50 КБ, чтобы уменьшить нагрузку на компьютер. Если размер файла отчета превышает установленный лимит на 50 КБ, старые записи автоматически удаляются до тех пор, пока размер не сократится на 20%.

Записать конфигурацию в файл отчета

Если эта опция активна, используемые настройки поиска в режиме реального времени записываются в файл отчета.

> **Указание**
> Если ограничение для файла отчета не указано, старые записи автоматически удаляются после того, как файл отчета достигнет размера 100 МБ. Записи удаляются до тех пор, пока размер файла отчета не составит 80 МБ.

12.7 Mail Protection

Раздел Mail Protection в Настройке отвечает за настройку защиты модуля.

12.7.1 Поиск

Модуль Mail Protection используется для проверки входящей почты на наличие вирусов, вредоносного ПО и спама. Mail Protection может проверять исходящие письма на наличие вирусов и вредоносного ПО. Модуль Mail Protection может блокировать исходящие письма, отправленные неизвестным ботом для рассылки спама с вашего компьютера.

Проверять входящую почту

Если эта опция активирована, то входящие письма проверяются на вирусы, вредоносные программы, а также на спам. Mail Protection поддерживает протоколы POP3 и IMAP. Активируйте протокол входящих писем, который

использует ваш почтовый клиент для получения электронной почты, для контроля службой Mail Protection.

Контролировать аккаунты POP3

Если опция включена, проверяются аккаунты POP3 на указанных портах.

Контролируемые порты

В это поле необходимо ввести порт, который будет использоваться для протокола входящих писем POP3. Несколько портов разделяются между собой запятыми. (Эта опция доступна только при включенном экспертном режиме.)

По умолчанию

Кнопка возвращает заданные порты к стандартному порту для POP3. (Эта опция доступна только при включенном экспертном режиме.)

Контролировать аккаунты IMAP

Если опция включена, то проверяются аккаунты IMAP на указанных портах.

Контролируемые порты

В это поле необходимо ввести порт, который будет использоваться для протокола IMAP. Несколько портов разделяются между собой запятыми. (Эта опция доступна только при включенном экспертном режиме.)

По умолчанию

Кнопка возвращает настройки по умолчанию для порта IMAP. (Эта опция доступна только при включенном экспертном режиме.)

Проверять исходящую почту (SMTP)

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

Контролируемые порты

В это поле необходимо ввести порт, который будет использоваться для исходящих писем протокола SMTP. Несколько портов разделяются между собой запятыми. (Эта опция доступна только при включенном экспертном режиме.)

По умолчанию

Кнопка возвращает заданные порты к стандартному порты для SMTP. (Эта опция доступна только при включенном экспертном режиме.)

Указание
Для верификации используемых протоколов и портов откройте в вашей почтовой программе свойства учетной записи. Как правило, используются стандартные порты.

Поддержка IPv6

Если выбрана эта опция, то модуль Mail Protection поддерживает версию 6 Интернет-протокола. (Эта опция доступна только при включенном экспертном режиме и не может быть использована для новых установок или измененных программ на Windows 8.)

Действие при обнаружении

В этом разделе настроек содержатся данные о том, какие действия будут выполнены, если Mail Protection обнаружит в письме или вложении вирус или вредоносную программу. (Эти опции доступны только при включенном экспертном режиме.)

> **Указание**
> Заданные здесь действия выполняются как при обнаружении вируса во входящем, так и в исходящем письме.

Интерактивный

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

Показать степень выполнения

Если эта опция включена, Mail Protection 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. Mail Protection работает автоматически в соответствии с настройками, выбранными в этом разделе.

Инфицированные письма

Выбранное в меню "*Инфицированные письма*" действие будет в первую очередь выполняться в случае, если Mail Protection обнаруживает в письме вирус или вредоносную программу. Если установлена опция **"Пропустить"**, в меню "*Инфицированные вложения*" можно дополнительно определить, какие действия должны выполняться в случае обнаружения подозрительных объектов в приложении.

Удалить

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

Пропустить

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

Поместить на карантин

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

Инфицированные вложения

Опция "**Инфицированные вложения**" может быть выбрана только в том случае, если в меню "*Инфицированные письма*" определена операция "**Пропустить**". 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 и заменяется текстовым шаблоном.

Пропустить

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

Предупреждение
Если вы выбираете эту опцию, Mail Protection 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 не запускайте приложения двойным щелчком!

Поместить на карантин

Если выбрана эта опция, инфицированное вложение помещается в Карантин, а затем удаляется (заменяется текстовым шаблоном). Позже, если потребуется, приложение можно восстановить.

Другие действия

Здесь содержатся данные о том, какие дополнительные действия необходимо выполнить, если Mail Protection обнаружит в письме или вложении вирус или вредоносную программу. (Эти опции доступны только при включенном экспертном режиме.)

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

Шаблон для удаленных и перемещенных писем

Текст в этом поле добавляется в тело письма вместо инфицированного сообщения. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующая комбинация клавиш может использоваться для форматирования:

Ctrl + Ввод = Вставляет разрыв строки.

По умолчанию

Кнопка позволяет добавить заданный текстовый шаблон в текстовое поле.

Шаблон для удаленных и перемещенных вложений

Текст в этом поле вставляется в письмо вместо инфицированного вложения. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующая комбинация клавиш может использоваться для форматирования:

Ctrl + Ввод = Вставляет разрыв строки.

По умолчанию

Кнопка позволяет добавить заданный текстовый шаблон в текстовое поле.

Эвристика

Этот раздел настроек содержит параметры эвристического поиска. (Эти опции доступны только при включенном экспертном режиме.)

Продукты Avira содержат 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, например, основываясь на имеющейся у него информации о надежности источника происхождении файла.

Эвристическое обнаружение макровирусов

Ваш продукт Avira имеет очень мощный блок макроэвристики. Если эта опция включена, при попытке лечения макросы в инфицированном документе удаляются, альтернативно можно ограничиться уведомлением пользователя о

подозрительных документах. Эта опция включена по умолчанию и рекомендована.

Advanced Heuristic Analysis and Detection (AHeAD)

Активировать AHeAD

Благодаря технологии AHeAD ваш продукт Avira содержит очень мощную эвристическую систему для определения даже неизвестных (новых) вредоносных программ. Если эта опция включена, вы можете установить уровень "резкости" эвристики. Эта настройка включена по умолчанию.

Низкий уровень распознавания

Если эта опция включена, программа обнаруживает меньше неизвестного вредоносного ПО, опасность ложных обнаружений при этом невелика.

Средний уровень распознавания

При включении этой опции обеспечивается сбалансированная защита с небольшим количеством ложных обнаружений. Эта настройка определена по умолчанию, если вы используете эвристический поиск.

Высокий уровень распознавания

При включении этой опции обнаруживается существенно больше неизвестного вредоносного ПО, но число ложных обнаружений также возрастает.

AntiBot

С помощью функции AntiBot модуля Mail Protection можно воспрепятствовать тому, чтобы ваш компьютер использовался как часть так называемой бот-сети для распространения спама по электронной почте: При распространении спама с помощью бот-сетей злоумышленник инфицирует большое количество компьютеров ботом, который подключается к IRC-серверу, занимает определенный канал и переходит в режим ожидания команды на рассылку спама. Для того чтобы отличать спам-письма неизвестного бота от писем пользователя, модуль Mail Protection проверяет, указаны ли используемый SMTP-сервер и отправитель исходящего письма в списке разрешенных серверов и отправителей. Если сервера или адреса нет в списке, исходящее письмо блокируется и не будет отправлено. О заблокированном письме сообщается в диалоговом окне. (Эти опции доступны только при включенном экспертном режиме.)

Указание
Функция AntiBot может быть использована только, если в Mail Protection включена проверка исходящих писем (см. опцию **Проверять исходящие письма** в разделе Mail Protection > Поиск).

Разрешенные серверы

Модуль Mail Protection разрешает отправку электронных писем всем серверам в этом списке: отправляемые на эти сервера письма **не** блокируются модулем Mail Protection. Если в списке не указано ни одного сервера, при отправке писем используемый SMTP-сервер не проверяется. Если в списке есть записи, Mail Protection блокирует письма, отправленные на SMTP-сервер, не содержащийся в списке.

Поле ввода

В этом поле можно указать имя хоста или IP-адрес SMTP-сервера, который вы используете для отправки своих писем.

> **Указание**
> Параметры SMTP-серверов, применяемых для отправки ваших писем, вы найдете в своей почтовой программе среди параметров учетных записей.

Добавить

Кнопка добавляет указанный в поле ввода сервер к списку разрешенных серверов.

Удалить

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

Удалить все

Кнопка удаляет все строки списка разрешенных серверов.

Разрешенные отправители

Модуль Mail Protection разрешает получение электронных писем от всех отправителей в этом списке: отправляемые с этих адресов письма **не** блокируются модулем Mail Protection. Если в списке не указан ни один отправитель, разрешенные адреса для исходящих писем не проверяются. Если в списке есть записи, Mail Protection блокирует письма отправителей, не содержащихся в списке.

Поле ввода

В этом поле укажите адрес(а) отправителя.

Добавить

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

Удалить

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

Удалить все

Кнопка удаляет все строки списка разрешенных отправителей.

12.7.2 Общее

Исключения

Адреса, не подвергающиеся проверке

В этой таблице содержится список адресов, исключенных из проверки модулем Avira Mail Protection (белый список).

> **Указание**
> Список исключений применяется модулем Mail Protection только для входящих писем.

Адреса, не подвергающиеся проверке

Поле ввода

В этом поле укажите адрес, который вы хотите добавить к списку адресов, не подвергающихся проверке. В дальнейшем, в зависимости от ваших настроек, адрес не будет проверяться модулем Mail Protection.

> **Указание**
> При указании адресов электронной почты можно применять специальные символы: символ-заполнитель ***** для любого числа символов и **?**. Заменители могут использоваться только в адресах, которые не проверяются модулем AntiSpam. Вы получите сообщение об ошибке, если попытаетесь добавить адрес с заменителем символов в список исключений, активирую в списке исключений Checkbox **Вредоносное ПО**. При вводе адресов с заменителями символов следите за соблюдением структуры адреса электронной почты(*@*.*).

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

Примеры: Использование заменителей в адресах электронной почты (белый список)

- `virus@avira.* /` = охватывает все письма с этим адресом и любым доменом первого уровня: virus@avira.de, virus@avira.com, virus@avira.net,...
- `*@avira.com` = охватывает все письма, отправленные с домене **avira.com**: info@avira.com, virus@avira.com, contakt@avira.com, employee@avira.com
- `info@*.com` = охватывает все письма доменом первого уровня **com** и адресом **info**: Домен второго уровня произволен: info@name1.com, info@name2.com,...

Добавить

С помощью этой кнопки вы можете добавить к списку не подвергающихся проверке адресов адрес, указанный в поле ввода.

Удалить

Кнопка удаляет выделенный адрес из списка.

Адрес электронной почты

Адрес электронной почты, который больше не должен подвергаться проверке.

Вредоносное ПО

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

Спам

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

наверх

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

вниз

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

Импортировать адресную книгу Outlook

С помощью этой кнопки вы можете импортировать адреса электронной почты из адресной книги MS Outlook в список исключений. Импортированные почтовые адреса не проверяются на наличие спама.

Импортировать адресную книгу Outlook Express (Windows XP) / Импортировать адресную книгу Windows Mail (Windows Vista, Windows 7)

С помощью этой кнопки вы можете импортировать адреса электронной почты из адресной книги MS Outlook Express или Windows Mail в список исключений. Импортированные почтовые адреса не проверяются на наличие спама.

Буфер

Буферная память модуля Mail Protection содержит данные о проверенных письмах, которые отображаются в статистике в Центре управления в разделе **Mail Protection**. (Эти опции доступны только при включенном экспертном режиме.)

Кроме того, копии входящих писем сохраняются в буферной памяти. Письма используются для целей обучения модуля AntiSpam (*Снять отметку спам – использовать для обучения*, *Отметить письмо как спам – использовать для обучения*).

> **Указание**
> Для сохранения входящих писем в буферной памяти необходимо активировать модуль AntiSpam.

Максимальное число писем в буферной памяти

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

Максимальная продолжительность хранения письма в днях

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

Очистить буфер

Нажатием на эту кнопку из буфера удаляются хранящиеся в нем письма.

Нижний колонтитул

В разделе **Нижний колонтитул** вы можете настроить нижний колонтитул письма, который будет отображаться в отправляемых вами письмах. (Эти опции доступны только при включенном экспертном режиме.)

Эта функция может быть использована только при активации проверки Mail Protection для исходящих писем; см. опцию **Сканировать исходящую почту (SMTP)** в разделе **Настройка > Mail Protection > Поиск**. Вы можете использовать заданный нижний колонтитул Avira Mail Protection, 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 сначала будет идти пользовательский текст нижнего колонтитула Avira Mail Protection.

Нижний колонтитул в отправляемых письмах

Присоединить нижний колонтитул Mail Protection

Если эта опция активирована, то в тексте отправляемого письма будет отображаться нижний колонтитул Avira Mail Protection. Нижним колонтитулом Avira Mail Protection вы подтверждаете, что отправленное письмо было проверено на вирусы и вредоносные программы модулем Avira Mail Protection и не составлено неизвестным ботом. Нижний колонтитул Avira Mail Protection содержит следующий текст: "*Проверено антивирусной программой Avira Mail Protection [версия программы] [сокращенное название и номер версии поисковой машины] [сокращенное название и номер версии файла вирусных сигнатур]*".

Присоединить этот нижний колонтитул

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

Поле ввода

В этом поле задается текст, который будет отображаться в отправленных письмах как нижний колонтитул.

AntiSpam

Avira Mail Protection проверяет письма на вирусы и вредоносные программы. Кроме того, этот модуль обеспечивает надежную защиту от спама. (Эти опции доступны только при включенном экспертном режиме.)

Включить модуль AntiSpam

Если опция включена, функция AntiSpam в модуле Mail Protection активна.

Отметить тему письма

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

Просто

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

Подробно

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

Протоколирование

Если опция включена, Mail Protection создает специальный AntiSpam-отчет.

Использовать черные списки реального времени (RBL)

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

Тайм-аут: n секунд(ы)

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

Очистить учебную базу данных

Нажатием на эту кнопку удаляется учебная база данных.

Автоматически добавлять получателей исходящих писем в белый список

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

Указание
Эта опция может быть выбрана, если у Mail Protection активирована функция проверки исходящих писем (см. опцию **Проверять исходящие письма** в Mail Protection > Проверка).

12.7.3 Отчет

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

Протоколирование

В этой группе определяется объем файла отчета.

ВЫКЛ

Если выбрана эта опция, то модуль Mail Protection 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 включена эта опция, модуль Mail Protection записывает важную информацию (обнаружения, предупреждения и ошибки) в файл отчета, а менее значимая информация для удобства работы с отчетом в него не включается. Эта настройка активирована по умолчанию.

Расширенный

Если эта опция включена, модуль Mail Protection вносит в отчет и менее значимую информацию.

Полный

Если эта опция включена, модуль Mail Protection вносит в отчет всю информацию.

Ограничить файл отчета

Ограничить размер до n МБ

Если выбрана эта опция, размер файла отчета можно ограничить, возможные значения: от 1 до 100 МБ. При ограничении размера файла отчета предоставляется лимит около 50 КБ, чтобы уменьшить нагрузку на компьютер. Если размер файла отчета превышает установленный лимит на 50 КБ, старые записи автоматически удаляются до тех пор, пока размер не сократится на 50 КБ.

Защитить файл отчета от сокращения

Включив эту опцию, можно защитить файл отчета от сокращения.

Записать конфигурацию в файл отчета

Если эта опция включена, применяемые настройки Mail Protection записываются в файл отчета.

> **Указание**
> Если ограничение для файла отчета не указано, новый файл отчета автоматически создается после того, как файл отчета достигнет размера 100 МБ. Для старого файла сохраняется резервная копия. Может существовать до трех резервных копий старых файлов отчета. Самые старые копии удаляются.

12.8 Child Protection

Используйте функции программы Avira *Защита детей*, чтобы обеспечить безопасность проведения времени в Интернете для своих детей и других людей, использующих ваш компьютер.

- С помощью функции **Safe Browsing** вы можете присвоить роли пользователям Windows. Для каждой роли вы можете определить, какие URL или категории содержимого должны быть разрешены или запрещены, а также длительность работы в Интернете или разрешенные промежутки времени использования.

Соответствующие темы:

- Что такое Safe Browsing

12.8.1 Safe Browsing

Программа Avira оснащена функцией **Safe Browsing** для фильтрации нежелательных или нелегальных Интернет-услуг и для ограничения использования Интернета по времени. Функция **Safe Browsing** является частью компонента *Защита детей*.

Пользователю может быть присвоена роль. Роль пользователя может настраиваться, она содержит набор правил со следующими критериями:

- Запрещенные или разрешенные URL-ссылки (адреса)
- Запрещенные категории содержимого
- Длительность пользования Интернетом и при необходимости разрешенные интервалы использования по будним дням

При блокировке содержимого по определенным категориям используются мощные списки фильтров URL, которые фильтруют URL-адреса исходя из контента веб-страниц.. Списки фильтров URL-ссылок обновляются и расширяются ежечасно. Роли **Ребенок**, **Молодой человек**, **Взрослый** сконфигурированы соответствующим образом.

Использование Интернета по времени определяется по запросам, осуществляемым за минимальный интервал в 5 минут.

Если функция **Safe Browsing** активирована, то при навигации в Интернет все открываемые в браузере страницы будут проверяться в соответствии с ролью пользователя. При запрещенных страницах адрес будет блокироваться, в браузере появится сообщение. При превышении разрешенного интервала пользования или пользования за пределами разрешенного времени блокируются следующие веб-страницы. В браузере появится сообщение.

Предупреждение
Обратите внимание на то, что вам необходимо активировать"**Web Protection**", чтобы воспользоваться функцией "**Safe Browsing**".

Предупреждение
Защитите конфигурацию своей программы Avira паролем, если вы активируете функцию **Safe Browsing**. Если конфигурация не защищена паролем, то все пользователи компьютера смогут изменять или отключать настройки в **Safe Browsing** . Пароль можно активировать здесь: Настройка > Общее > Пароль.

Соответствующие темы:

- Активировать Safe Browsing

- Присвоить роль
- Safe Browsing Настройка

Активировать Safe Browsing

- Откройте центр управления Avira и нажмите на **Status** на навигационной панели.

  Активируйте **Web Protection**, чтобы воспользоваться функцией **Safe Browsing**.
- Если модуль **Safe Browsing** отключен, активируйте его, нажав в виде **Status** в разделе *Internet Protection* красный выключатель рядом с **Safe Browsing**.

  Если модуль активен, то кнопка рядом с **Safe Browsing** станет зеленой ("ВКЛ").

  Активируйте функцию **Safe Browsing**, нажав в виде **Status** красный выключатель рядом с **Safe Browsing**.

  Если модуль активен, то кнопка рядом с Safe Browsing станет зеленой ("ВКЛ").
- Для настройки роли ребенка или другого человека в **Safe Browsing** нажмите в виде **Status** кнопку настройки рядом с **Safe Browsing**.

Соответствующие темы:

- Что такое Safe Browsing
- Присвоить роль
- Safe Browsing Настройка

Присвоить роль

Условия:

✓ Убедитесь в том, что для каждого человека, использующего ваш компьютер, создана своя учетная запись в Windows. В программа Avira вы можете каждой учетной записи в Windows присвоить роль Safe Browsing.
✓ Активируйте функцию **Safe Browsing** в своей программе Avira.
✓ Проверьте свойства роли перед тем, как присвоить роль пользователю.

- В виде **Status** нажмите на кнопку настройки рядом с **Safe Browsing**.
- Выберите пользователя, которому вы хотите присвоить роль из списка **User selection**.

  Список содержит учетные записи Windows, созданные на вашем компьютере.
- Нажмите кнопку **Add**.

  ↪ Пользователь будет добавлен в список.

  В Avira Internet Security настроены следующие роли пользователей:

- **Child**
- **Young person**
- **Adult**

Если вы добавляете учетную запись к списку, то по умолчанию ей присвоится роль **Child**.

- Вы можете присвоить другую роль, щелкнув по роли пользователя несколько раз.

> **Указание**
> Пользователи компьютера, которым не присвоена роль в настройках **Safe Browsing**, по умолчанию получают от программы учетную запись **Standard** с ролью **Child**. Вы можете изменить роль пользователя **Standard**.

- Нажмите на **Accept**, чтобы сохранить настройку.

Соответствующие темы:

- Изменить свойства роли
- Добавить или удалить роль

Изменить свойства роли

- В виде **Status** нажмите на кнопку настройки рядом с **Safe Browsing**.
- Если она не активна, нажмите на зеленую кнопку рядом с **Expert mode**.

  Если она активна, то кнопка рядом с **Expert mode** станет желтой ("ВКЛ").

  ↪ Опции **Roles** отображаются в окне настройки функции **Safe Browsing**.
- Нажмите на имя роли, которую вы хотите изменить (например **Young person**) и нажмите **Change**.

  ↪ Появится окно со свойствами роли **Properties**.
- Выполните изменения и нажмите **OK**.

Соответствующие темы:

- Свойства роли
- Safe Browsing Настройка

Добавить или удалить роль

- В виде **Status** нажмите на кнопку настройки рядом с **Safe Browsing**.
- Если она не активна, нажмите на зеленую кнопку рядом с **Expert mode**.

  Если она активна, то кнопка рядом с **Expert mode** станет желтой ("ВКЛ").

  ↪ Опции **Roles** отображаются в окне настройки функции **Safe Browsing**.
- Чтобы удалить роль (например **Young person**), нажмите **Delete**.

Указание
Вы не сможете удалить роль, пока она присвоена пользователю.

- Чтобы добавить роль, введите ее имя (не более 30 символов) в поле ввода и нажмите **Add**.
- Чтобы назначить свойства новой роли, выберите новую роль из списка и нажмите **Change**.

Соответствующие темы:

- Safe Browsing Настройка
- Свойства роли
- Присвоить роль

Если вы задали пароль для функции **Safe Browsing**, окно настроек модуля **Safe Browsing** скрывается и возникает кнопка **Защищено паролем**.

Защищено паролем

Нажмите кнопку "**Защищено паролем**" и введите пароль для модуля "**Safe Browsing**" в окне "**Введите пароль**", чтобы получить доступ к настройкам модуля **Safe Browsing**.

Активировать Safe Browsing

Если эта опция включена, то при навигации в Интернете все открываемые в браузере страницы будут проверяться в соответствии с ролью зарегистрировавшегося в **Safe Browsing** пользователя. Будут блокироваться те страницы, которые в пределах данной роли считаются запрещенными.

Примечание
Пользователи компьютера, которым в рамках функции **Safe Browsing** не была присвоена роль, при активированной функции **Safe Browsing** будут *по умолчанию* идентифицироваться как **Ребенок**. Вы можете изменить роль пользователя по умолчанию.
После инсталляции определены роли пользователей **Ребенок**, **Подросток** и **Взрослый**. В заранее сконфигурированных ролях временные ограничения использования Интернета отключены.

Выбор пользователя

Пользователь

Этот список содержит имена всех пользователей системы.

Добавить

С помощью этой кнопки вы можете добавить выбранного пользователя к списку защищаемых пользователей.

Удалить

Кнопка удаляет из списка выделенную строку.

Список "ролей пользователей"

В списке отображаются все добавленные пользователи с присвоенными им ролями. При добавлении пользователя программа по умолчанию приписывает ему роль **Ребенок**. Щелкнув мышью по роли, вы можете сменить роль.

Примечание
Пользователя *по умолчанию* удалить невозможно.

Роли (Эти опции доступны только при включенном экспертном режиме.)

Поле ввода

В это поле вводится имя роли, которую вы хотите добавить к ролям пользователей.

Изменить

Нажав кнопку "**Изменить**", вы можете настроить выбранную роль. Откроется диалоговое окно, в котором можно указать запрещенные и разрешенные URL, а также выбрать запрещенное содержание в зависимости от категории. (См. Свойства роли.)

Добавить

С помощью этой кнопки введенную в окне ввода роль можно добавить к списку доступных ролей.

Удалить

Кнопка удаляет из списка выделенную роль.

Список

Список отображает все созданные роли. Двойным щелчком по роли открывается диалог свойств роли.

Примечание
Уже присвоенные пользователям роли не могут быть удалены.

Соответствующие темы:

Свойства роли

В окне **Свойства роли** вы можете определить выбранную роль для использования Интернета. (Эти опции доступны только при включенном экспертном режиме.)

Вы можете явным образом запретить или разрешить доступ к URL. Вы можете на основании выбора определенных категорий блокировать содержание сайтов. Вы можете ограничивать по времени использование Интернета.

Контролировать доступ к следующим URL

В списке отображаются все внесенные URL с приписанными правилами *Блокировать* или *Разрешить*. При добавлении URL по умолчанию приписывается правило *Блокировать*. Щелкнув по правилу, вы можете изменить его.

Добавить URL

В это поле необходимо ввести URL, которые должны контролироваться функцией защиты детей. Вы можете задать части URL, указав уровень домена со стоящими перед ним или после него точками: **.domainname.de** для всех страниц и всех субдоменов домена. Веб-страница с любым доменом первого уровня (.com или .net) будет заканчиваться точкой: domainname.. Если вы записываете набор символов без точки в начале или в конце, такая последовательность интерпретируется как домен первого уровня, например, **net** для всех доменов зоны NET (www.domain.net).Вы можете применять специальный символ ***** для любого количества знаков. Используйте в сочетании со специальными символами точки для обозначения уровня домена перед его именем или после него.

Примечание
Правила URL имеют приоритет, исходя из количества частей имени (Labels) домена. Чем больше частей указано в имени домена, тем выше приоритет правила. Пример:
URL: www.avira.com - правило: Разрешить
URL: .avira.com - Заблокировать
Этот набор правил разрешает все URL домена www.avira.com. URL "forum.avira.com" будет заблокирован.

Примечание
Указанные . или * относятся ко всем URL. Используйте эти символы, если вы хотите, например, для роли *Ребенок* разблокировать только некоторые, явным образом указанные сайты, как, например, в следующем наборе правил:
URL***** или **.** - правило: блокировать
URL: kids.yahoo.com - правило: разрешить
URL: kids.nationalgeographic.com - правило: разрешить
Набор правил блокирует все URL, кроме URL с доменами "kids.yahoo.com" и "kids.nationalgeographic.com".

Добавить

С помощью этой кнопки вы можете добавить заданный URL к списку контролируемых URL.

Удалить

Кнопка удаляет отмеченный URL из списка контролируемых URL.

Блокировать доступ к URL-ссылкам, которые относятся к следующим категориям

Если эта опция включена, то содержание веб-страниц, относящееся к выбранным категориям в списке категорий, блокируется.

Разрешенная длительность использования

При нажатии на кнопку **Разрешенная длительность использования** откроется диалог, в котором вы можете установить временные ограничения на использование Интернета для роли, которую вы настраиваете. Время работы в Интернете для роли можно задать на одну неделю, месяц или отдельно для рабочих дней и выходных. Определить точные интервалы использования в определенный день недели можно в следующем диалоге. См. Длительность использования.

Примеры: контролируемые URL

- `www.avira.com` -ИЛИ- `www.avira.com/*`
  = Включает все URL с доменом `www.avira.com`:
  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 включены.
- `avira.com` -ИЛИ- `*.avira.com`
  = Включает все URL с доменами второго и первого уровня `avira.com`. Указанный диапазон включает все существующие домены первого уровня и поддомены `.avira.com`: *www.avira.com*, *forum.avira.com*,...
- `avira.` -ИЛИ- `*.avira.*`
  = включает в себя все URL домена второго уровня `avira`. Указанный диапазон

включает все существующие домены первого уровня и поддомены `.avira.`: *www.avira.com, www.avira.de, forum.avira.com*,...

- `.*domain*.*`
  Включает все URL, содержащие домен второго уровня с цепочкой символов "`domain`": *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...
- `net` -ИЛИ- `*.net`
  =Включает все URL с доменом первого уровня "`net`": *www.name1.net*, *www.name2.net*,...

Соответствующие темы:

- Что такое Safe Browsing
- Safe Browsing Настройка
- Длительность использования
- Интервал использования

Длительность использования

В окне **Длительность использования** вы можете установить максимальную длительность использования Интернета для определенной роли пользователя. Использование Интернета по времени определяется по запросам, осуществляемым за минимальный интервал в 5 минут. Необходимое максимальное время работы в Интернете для роли можно задать на одну неделю, месяц или отдельно для рабочих дней и выходных.

Ограничить Интернет-доступ по времени

С помощью этой опции вы можете ограничить время использования Интернета для всех пользователей, которым присвоена роль. При превышении разрешенного времени использования веб-страницы, вызываемые пользователем, будут блокироваться. В браузере появится предупреждающее сообщение.

Ограничение по времени в неделю, месяц, день (пн – пт, сб, вс)

Необходимую длительность использования можно задать с помощью ползункового регулятора или кнопок-стрелок справа, рядом с полями ввода. Вы также можете ввести длительность использования вручную в соответствующее поле. Учитывайте формат времени.

Если для времени использования введены разные значения, программа их не корректирует. Программа использует соответствующее минимальное значение для ограничения длительности использования.

Точный интервал использования

Нажатием на кнопку **Точный интервал использования** открывается диалог, в котором можно определить время для определенной максимальной длительности использования. См. Интервал использования.

Соответствующие темы:

- Что такое Safe Browsing
- Safe Browsing Настройка
- Свойства роли
- Интервал использования

Интервал использования

В окне **Интервал использования** укажите разрешенное время использования для заданной максимальной длительности пользования Интернета роли: для каждого дня недели можно разрешить определенный период работы в Интернете.

Использование Интернета разрешено только в указанное время

С помощью этой опции вы можете установить время суток для использования Интернета для всех пользователей, которым присвоена роль. Если Интернет используется дольше, чем установлено для данной роли, то вызываемые страницы будут блокироваться. В браузере появится соответствующее сообщение.

- Для выделения времени работы в Интернете, отметьте нужные временные интервалы.

  Предусмотрены следующие возможности для разрешения или запрета работы в определенное время:

  - **Для разрешения работы в Интернете в определенное время:** щелкните по нужным неотмеченным полям с указанием времени или переместите курсор мыши при нажатой левой клавише по неотмеченным полям времени.
  - **Для запрещения работы в Интернете в определенное время:** щелкните по нужным отмеченным полям с указанием времени или переместите курсор мыши при нажатой левой клавише по отмеченным полям времени.

- Щелкните правой клавишей мыши по полю времени нужного дня, чтобы отобразить указанные промежутки времени в диалоговом окне. Пример: *Доступ в Интернет запрещен с 00:00 до 11:00.*

Соответствующие темы:

- Что такое Safe Browsing
- Safe Browsing Настройка
- Свойства роли
- Длительность использования

Avira защищает от вредоносных программ и вирусов не только ваш компьютер, но и мобильные телефоны и смартфоны, работающие на операционной системе Android, от кражи и/или утери. С помощью компонента Avira Free Android Security вы можете блокировать нежелательные звонки и SMS. Просто добавьте телефонные номера из

своего списка звонков, сообщений или контактов в список для блокировки или создайте контакты, которые вы хотите блокировать, вручную.

Дополнительную информацию вы можете посмотреть на нашем веб-сайте:

http://www.avira.com/android

12.9 Общее

12.9.1 Категории угроз

Выбор расширенных категорий угроз (Эти опции доступны только при включенном экспертном режиме)

Ваш продукт Avira защищает вас от компьютерных вирусов. Кроме того, у вас есть возможность дифференцированного поиска следующих дополнительных категорий угроз.

- Рекламные программы
- Рекламное ПО/шпионское ПО
- Приложения
- Backdoor-программы
- Файлы со скрытыми расширениями
- Программы дозвона на платные номера
- Фишинг
- Программы, нарушающие частную сферу
- Программы-шутки
- Игры
- Обманная программа
- Необычные паковщики

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.

12.9.2 Расширенная защита

Расширенная защита

ProActiv (Эта опция доступна только при включенном экспертном режиме.)

Включить ProActiv

Если эта опция включена, программы контролируются вашей системой и проверяются на наличие подозрительной активности. При возникновении типичного для вредоносного ПО поведения вы получаете сообщение. Вы можете блокировать программу или, выбрав "**Игнорировать"**, продолжить выполнение программы. Из проверки 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.

Используя функцию ProActiv, вы защищаете себя от новых и неизвестных угроз, для которых еще нет описания вирусов и эвристических методов. Технология ProActiv интегрирована в компонент Real-Time Protection, она наблюдает за выполняемыми программами действиями и анализирует их. Поведение программ исследуется на наличие активности, типичной для вредоносного ПО: вид действия и очередность действий. Если программа осуществляет действия, типичные для вредоносного ПО, она идентифицируется как обнаруженный вирус : Вы можете заблокировать выполнение программы или проигнорировать сообщение и продолжить ее выполнение. 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 типичного для вредоносного ПО поведения компонент ProActiv использует наборы правил, разработанные центром исследований вирусов компании Avira. Наборы правил поставляются банками данных Avira. Для сбора информации в банках данных компании Avira приложение ProActiv пересылает информацию о найденных подозрительных программах. В процессе установки ПО Avira вы можете отключить передачу данных в базы данных компании Avira.

Указание
Технология ProActiv пока недоступна для 64-битных систем!

Cloud Protection (Эти опции доступны только при включенном экспертном режиме.)

Включить Cloud Protection

Отпечатки всех подозрительных файлов передаются для динамического распознавания в онлайн режиме на Avira Cloud. Файлы приложений сразу же идентифицируются как чистые, инфицированные или неизвестные.

Система Cloud Protection действует как центральный узел, распознающий кибер-атаки на сообщество Avira. Файлы, к которым обращается ваш компьютер, сравниваются с образцами файлов, сохраненными в облачной системе. Поскольку основная работа выполняется в облаке, локальной программе защиты требуется меньше ресурсов.

При каждой **быстрой проверке системы** создается список мест хранения файлов, подверженных угрозе воздействия вредоносных программ. В этом списке, в частности, находятся текущие процессы, программы запуска и служебные программы. Для каждого файла составляется контрольная сумма ("отпечаток") и отправляется в облачную систему безопасности, после этого файл идентифицируется как "чистый" или "вредоносный". Неизвестные программные файлы загружаются для проверки в систему Cloud Protection.

Вручную подтверждать отправку подозрительных файлов в компанию Avira

Вы можете проверить список подозрительных файлов, которые нужно загрузить в Cloud Protection, и решить самостоятельно, какие файлы вы хотите загрузить.

В разделе *Блокируемые приложения* можно добавить приложения, которые вы классифицируете как вредоносные и которые по умолчанию должны блокироваться AntiVir ProActiv. Добавленные приложения не будут выполняться вашей системой. Вы можете добавлять программы к фильтру приложений для блокируемых приложений также при помощи сообщений Real-Time Protection о подозрительном поведении программ, используя опцию **Всегда блокировать эту программу**.

Блокируемые приложения

Приложение

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

Поле ввода

Укажите в этом поле 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.

Нажатием этой кнопки открывается 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.

> **Указание**
> Приложения, необходимые для работы операционной системы, не могут быть добавлены.

Удалить

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

В разделе *Исключаемые приложения* перечислены приложения, исключенные из проверки компонентом ProActiv: подписанные программы, которые по умолчанию содержатся в списке разрешенных приложений, все приложения, сочтенные надежными и внесенные в фильтр приложений: в настройках к списку разрешенных приложений можно добавить новые приложения. Вы также можете с помощью сообщений Real-Time Protection о подозрительных программах добавить приложения, используя в сообщении Real-Time Protection опцию **Высоконадежный поставщик**.

Исключаемые приложения

Приложение

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 сообщений Real-Time Protection. Компонент ProActiv идентифицирует приложения на основании пути, имени файла и содержания. Проверка содержания необходима, так как в процессе изменения, например, обновлений, к программе можно добавить вредоносный код. Задав **Тип**, вы можете указать, нужно ли проверять содержание: при типе "*Содержание*" заданные с путем и именем файла приложения проверяются на изменения содержания файлов до того, они будут исключены из проверки компонента ProActiv. При измененном содержании файлов приложение снова будет проверяться компонентом ProActiv. Если указан тип "*Путь*", проверка содержания не осуществляется до тех пор, пока

приложение не будет исключено из проверки модулем Real-Time Protection. 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.

Указание
Некоторые надежные приложения, например, все компоненты вашего продукта Avira, 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 компонентом 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.

Нажатием кнопки открывается 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 приложение из списка приложений, которые необходимо исключить.

12.9.3 Пароль

Вы можете защитить свой продукт Avira в различных областях паролем. В этом случае пароль будет запрашиваться каждый раз при попытке открыть защищенную область.

Пароль

Введите пароль

Задайте свой 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".

Подтверждение

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

> **Примечание**
> Большие и маленькие буквы различаются!

Защищенные паролем области (Эти опции доступны только при включенном экспертном режиме.)

Ваш продукт Avira может защищать паролем отдельные разделы. Щелчком по соответствующему флажку можно по желанию включить или выключить запрос пароля для отдельных разделов.

Защищенная паролем область	Функция
Центр управления	Если опция включена, для запуска модуля Центр управления потребуется установленный пароль.
Включить / отключить Real-Time Protection	Если эта опция включена, требуется установленный пароль для включения / отключения Avira Real-Time Protection.
Включить / отключить Mail Protection	Если эта опция включена, требуется установленный пароль для включения / отключения Mail Protection.
Включить / отключить FireWall	Есть эта опция включена, требуется установленный пароль для включения / отключения FireWall.
Включить/отключить Web Protection	Если эта опция включена, требуется установленный пароль для включения / отключения Web Protection.
Safe Browsing включить / отключить	Если опция включена, требуется установленный пароль для включения/отключения функции Защита детей.

Карантин	Если эта опция включена, требуется установленный пароль для включения / отключения всех областей менеджера карантина. Щелчком по соответствующему флажку можно по желанию включить или выключить запрос пароля.
Восстановление инфицированных объектов	Если эта опция включена, для восстановления объектов требуется установленный пароль.
Повторная проверка затронутых объектов	Если эта опция включена, для повторной проверки объекта требуется установленный пароль.
Свойства поврежденных объектов	Если эта опция включена, то для просмотра свойств объекта необходим установленный пароль.
Удаление поврежденных объектов	Если эта опция включена, то для удаления объекта необходим установленный пароль.
Отправить электронное письмо в компанию Avira	Если эта опция включена, то для отправки объекта для проверки в центр исследования вирусов компании Avira требуется установленный пароль.
Копирование поврежденных объектов	Если эта опция включена, для копирования поврежденных объектов требуется установленный пароль.
Добавление и изменение заданий	Если эта опция включена, требуется установленный пароль для добавления и изменения задач в планировщике.

Настройка	Если опция включена, настройка программы возможна только после ввода установленного пароля.
Установка / Удаление	Если эта опция включена, для установки или удаления программы требуется установленный пароль.

12.9.4 Безопасность

Эти опции доступны только при включенном экспертном режиме.

Autorun

Блокировать функцию автозапуска

Если эта опция активирована, то выполнение функции автозапуска Windows на всех подключаемых дисках, например, USB-накопителях, CD и DVD дисках, сетевых дисках, блокируется. Благодаря функции автозапуска Windows файлы на носителях или сетевых дисках при подключении сразу считываются, поэтому файлы могут быть запущены автоматически. 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, если вы уверены, что используете исключительно надежные носители информации.

Защита системы

Защита файла Windows hosts от внесения изменений

Если эта опция включена, файл Windows hosts защищен от записи. Какие-либо манипуляции с файлом более невозможны. В этом случае вредоносное ПО не может перенаправлять ваши запросы на нежелательные страницы. Эта опция включена по умолчанию.

Защита продукта

Примечание
Опции по защите продукта недоступны, если Real-Time Protection не был установлен в ходе выборочной установки.

Защита процессов от нежелательного завершения

Если эта опция включена, все процессы программы защищены от нежелательного завершения вредоносными программами, а также от "неконтролируемого" завершения пользователем, например, через диспетчер задач. Эта опция включена по умолчанию.

Расширенная защита процессов

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

Примечание
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 включения опции потребуется перезапустить компьютер.

Предупреждение
Помните, что при отключении этой опции возможны проблемы с лечением систем, инфицированных определенными видами вредоносного ПО.

Примечание
Если эта опция включена, то изменения в конфигурации, а также в

заданиях на проверку и обновление возможны только через интерфейс пользователя.

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

12.9.5 WMI

Эти опции доступны только при включенном экспертном режиме.

Поддержка для инструментария управления Windows (WMI)

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. Ваш продукт Avira поддерживает WMI и предоставляет в интерфейсе различные данные (информация о статусе, статистические данные, отчеты, запланированные задания и т. д.), события . С помощью WMI можно вызывать оперативные данные программы.

Активировать WMI-поддержку

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

12.9.6 События

Эти опции доступны только при включенном экспертном режиме.

Ограничить размер банка событий

Установить максимальный размер не более n записей

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

Удалять все записи о событиях через n дней (день)

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

Без ограничений

При включении этой опции размер банка данных событий не ограничен. Однако в интерфейсе программ в разделе События отображается не более 20 000 записей.

12.9.7 Отчеты

Эти опции доступны только при включенном экспертном режиме.

Ограничение отчетов

Ограничить количество до n шт.

Если эта опция включена, можно ограничить максимальное количество отчетов, определенным числом; допустимы следующие значения: от 1 до 300. Если количество отчетов превысит указанное, самые старые отчеты будут удалены.

Удалять все отчеты старше через n дней

Если эта функция включена, отчеты будут автоматически удаляться через определенное количество дней; допустимы следующие значения: от 1 до 90 дней. По умолчанию эта опция включена со значением 30 дней.

Без ограничений

Если эта опция включена, количество отчетов не ограничено.

12.9.8 Папки

Эти опции доступны только при включенном экспертном режиме.

Временный путь

Использовать системные настройки

Если эта функция включена, для работы с временными файлами используются настройки системы.

Примечание
Узнать, где ваша система сохраняет временные файлы, можно на примере von Windows XP: **Пуск > Настройки > Панель управления > Система >** вкладка "**Дополнительно**" > кнопка "**Переменные окружения**". 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 ввода.

Поле ввода

В этом поле ввода нужно указать путь к папке, в которой система должна хранить временные файлы.

Нажатием на кнопку открывается окно, в котором можно выбрать нужный путь для временных файлов.

По умолчанию

Нажатием на эту кнопку восстанавливается предустановленная папка для временного пути.

12.9.9 Акустический сигнал предупреждения

Эти опции доступны только при включенном экспертном режиме.

При обнаружении вируса или вредоносного ПО с помощью модуля System Scanner или Real-Time Scanner в интерактивном режиме раздается предупреждающий сигнал. У вас есть возможность отключить или включить предупреждающий сигнал, а также выбрать в качестве предупреждающего сигнала другой Wave-файл.

> **Примечание**
> Режим действий модуля System Scanner задается в настройках следующим образом: Безопасность ПК > System Scanner > Поиск > Действие при обнаружении. Режим действий Real-Time Scanner задается в настройках следующим образом: Безопасность ПК > Real-Time Scanner > Поиск > Действие при обнаружении.

Без предупреждения

При включении этой опции акустический сигнал не подается при обнаружении вируса с помощью System Scanner или Real-Time Scanner.

Воспроизводить через громкоговоритель компьютера (только при интерактивном режиме)

При включении этой опции подается акустический сигнал со стандартным звуковым предупреждением при обнаружении вируса с помощью модуля System Scanner или Real-Time Scanner. Предупреждающий сигнал воспроизводится внутренним громкоговорителем компьютера.

Использовать следующий Wave-файл (только при интерактивном режиме)

При включении этой опции при обнаружении вируса модулем System Scanner или Real-Time Scanner выдается акустический сигнал с помощью выбранного

Wave-файла. Выбранный Wave-файл воспроизводится через подключенный внешний громкоговоритель.

Wave-файл

В этом поле ввода можно указать имя выбранного вами аудио-файла для воспроизведения и путь к нему. Стандартный предупреждающий сигнал программы задан по умолчанию.

Нажатием на кнопку открывается окно, в котором вы можете с помощью Проводника выбрать требуемый файл.

Тест

Эта кнопка предназначена для тестового запуска выбранного Wave-файла.

12.9.10 Предупреждения

При наступлении определенных событий ваш продукт Avira создает уведомления на рабочем столе, так называемые всплывающие окна, чтобы проинформировать вас об угрозе, а также об успешно выполненных или не удавшихся программах, например, о выполнении обновления. В разделе **Предупреждения** вы можете включить или отключить уведомление при наступлении определенных событий.

Для уведомлений на рабочем столе есть возможность отключить уведомление непосредственно во всплывающем окне. Вы можете отменить отключение уведомлений в разделе **Предупреждения**.

Обновление

Предупреждать, если последнее обновление было более n дня(ей) назад

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

Показывать предупреждение, если устарел файл вирусных сигнатур

Если эта функция включена, вы получите предупреждающее сообщение, когда файл вирусных сигнатур устареет. С помощью опции "Предупреждать, если последнее обновление было более n дня(ей) назад" можно сконфигурировать временной интервал между предупреждающими сообщениями.

Предупреждения / указания в следующих ситуациях

Используется Dial-up соединение

Если эта функция активирована, уведомления в виде всплывающих окон будут предупреждать вас, о том, что программа дозвона на вашем компьютере устанавливает селекторную связь по телефонной сети или сети ISDN.

Существует опасность того, что программа дозвона представляет собой неизвестную и вредоносную программу, которая устанавливает платное соединение. (См. Категории угроз: Программа дозвона на платные номера)

Файлы были успешно обновлены

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

Не удалось выполнить обновление

Если эта опция включена, вы получаете уведомление в виде всплывающего окна, если обновление не состоялось: Не удалось установить соединение с сервером загрузки или установить файлы обновления.

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.

Техническая информация по состоянию на 2-й квартал 2013 г.

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