



Avira

Professional Security

Руководство пользователя

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 особыми знаками. Но это не означает, что их можно использовать без разрешения.

Информация об авторских правах

Для продукта Avira Professional Security используется код, предоставленный сторонней организацией. Мы благодарим обладателей авторских прав за предоставленный в наше распоряжение код.

Подробную информацию об авторском праве вы можете найти в разделе [Лицензии третьих лиц](#).

Лицензионное соглашение с конечным пользователем

<http://www.avira.com/ru/license-agreement>

Политика конфиденциальности

<http://www.avira.com/ru/general-privacy>

Содержание

1. Введение	10
1.1 Символы и способы выделения	10
2. Информация о продукте	12
2.1 Объем функций.....	12
2.2 Системные требования	13
2.2.1 Системные требования Avira Professional Security.....	13
2.2.2 Права администратора (начиная с Windows Vista).....	14
2.2.3 Удаление несовместимых программ	15
2.3 Лицензирование и обновление	15
2.3.1 Лицензирование	15
2.3.2 Продление лицензии	15
2.3.3 Управление лицензиями	16
3. Установка и удаление	17
3.1 Подготовка к установке.....	17
3.2 Установка с CD-диска при подключении к Интернету	18
3.3 Установка с CD-диска без подключения к Интернету.....	18
3.4 Установка программного обеспечения, загруженного с сайта Avira	18
3.5 Удаление несовместимых программ	19
3.6 Выбор типа установки.....	19
3.6.1 Выполнение быстрой установки.....	20
3.6.2 Выполнение выборочной установки	21
3.7 Установка Avira Professional Security.....	21
3.7.1 Выбор пути установки	22
3.7.2 Выбор компонентов установки	23
3.7.3 Создание ярлыков для Avira Professional Security	25
3.7.4 Активация Avira Professional Security.....	26
3.7.5 Настройка уровня эвристического обнаружения (AHeAD)	27
3.7.6 Выбор расширенных категорий опасности	28
3.7.7 Выбор настроек электронной почты	29
3.7.8 Запуск сканирования после установки.....	31
3.7.9 Установка и удаление в сети	32

3.8	Изменение компонентов установки.....	37
3.8.1	Изменение компонентов установки в системе Windows 8.....	37
3.8.2	Изменение компонентов установки в системе Windows 7.....	38
3.8.3	Изменение компонентов установки в системе Windows XP.....	38
3.9	Удаление.....	39
3.9.1	Удаление Avira Professional Security в системе Windows 8.....	39
3.9.2	Удаление Avira Professional Security в системе Windows 7.....	40
3.9.3	Удаление Avira Professional Security в системе Windows XP.....	41
3.9.4	Удаление из сети.....	41
4.	Обзор Avira Professional Security.....	42
4.1	Интерфейс и работа с программой.....	42
4.1.1	Control Center.....	42
4.1.2	Настройка.....	45
4.1.3	Tray Icon.....	50
4.2	Это делается так.....	51
4.2.1	Активация лицензии.....	51
4.2.2	Выполнить автоматизированное обновление.....	52
4.2.3	Запустить обновление вручную.....	54
4.2.4	Использование профиля сканирования для сканирования на наличие вирусов и вредоносного ПО.....	54
4.2.5	Прямой поиск: Поиск вирусов и вредоносного ПО с помощью Drag&Drop.....	56
4.2.6	Прямой поиск: Поиск вирусов и вредоносных программ с помощью контекстного меню.....	57
4.2.7	Прямой поиск: Автоматический поиск вирусов и вредоносного ПО.....	57
4.2.8	Целенаправленное сканирование руткитов и активного вредоносного ПО.....	59
4.2.9	Реагировать на найденные вирусы и вредоносное ПО.....	59
4.2.10	Карантин: Обращение с файлами (*.qua) на карантине.....	64
4.2.11	Восстановление файлов в карантине.....	66
4.2.12	Карантин: Поместить подозрительный файл на карантин.....	68
4.2.13	Профиль поиска: Добавить или удалить тип файла из профиля поиска.....	68
4.2.14	Профиль поиска: Создание ярлыка для профиля поиска.....	69
4.2.15	События: Фильтрация событий.....	69
4.2.16	Mail Protection: Исключить адреса из проверки.....	70
4.2.17	FireWall: выбор уровня безопасности в брандмауэре.....	71

5.	Обнаружение	72
5.1	Обзор	72
5.2	Интерактивный режим	72
5.2.1	Предупреждение	73
5.2.2	Обнаружения, ошибки, предупреждения	73
5.2.3	Контекстное меню действий	74
5.2.4	Особенности при обнаружении инфицированных загрузочных секторов, Rootkits и активного вредоносного ПО	75
5.2.5	Кнопки и ссылки	76
5.2.6	Особенности при обнаружении при отключенном модуле Web Protection	76
5.3	Автоматический режим	77
5.3.1	Предупреждение	77
5.3.2	Кнопки и ссылки	78
5.4	Отправка файлов в Protection Cloud	78
5.4.1	Отображаемая информация	78
5.4.2	Кнопки и ссылки	79
5.5	Real-Time Protection	79
5.6	Подозрительное поведение	80
5.6.1	Предупреждение модуля Real-Time Scanner: Обнаружено подозрительное поведение приложения	81
5.6.2	Имя и путь обнаруженной подозрительной программы	81
5.6.3	Возможности выбора	81
5.6.4	Кнопки и ссылки	82
5.7	Входящие письма	82
5.7.1	Предупреждение	83
5.7.2	Обнаружения, ошибки, предупреждения	83
5.7.3	Возможности выбора	84
5.7.4	Кнопки и ссылки	85
5.8	Исходящие письма	85
5.8.1	Предупреждение	86
5.8.2	Обнаружения, ошибки, предупреждения	86
5.8.3	Возможности выбора	87
5.8.4	Кнопки и ссылки	87
5.9	Отправитель	88
5.9.1	Предупреждение	88
5.9.2	Используемая программа, используемый сервер SMTP и адрес отправителя письма	88

5.10	Сервер	89
5.10.1	Предупреждение	89
5.10.2	Используемая программа, используемый сервер SMTP	89
5.11	Web Protection	90
6.	System Scanner	93
6.1	System Scanner	93
6.2	Luke Filewalker	93
6.2.1	Luke Filewalker: Окно состояния проверки	94
6.2.2	Luke Filewalker: Статистика проверки	97
7.	Control Center	99
7.1	Обзор	99
7.2	Файл	102
7.2.1	Закреть	102
7.3	Вид	102
7.3.1	Состояние	102
7.3.2	Режим презентации	114
7.3.3	System Scanner	115
7.3.4	Выборочная проверка	117
7.3.5	Real-Time Protection	121
7.3.6	FireWall	122
7.3.7	Web Protection	124
7.3.8	Защита электронной почты	125
7.3.9	Карантин	128
7.3.10	Scheduler	134
7.3.11	Отчеты	138
7.3.12	События	140
7.3.13	Обновить	143
7.4	Сервис	143
7.4.1	Проверка загрузочных секторов	143
7.4.2	Список вирусов	143
7.4.3	Download rescue CD	144
7.4.4	Настройка	145
7.5	Обновление	145
7.5.1	Запустить обновление	145
7.5.2	Ручное обновление	145

7.6	Справка	145
7.6.1	Темы	145
7.6.2	Помощь	145
7.6.3	Руководство по загрузке	146
7.6.4	Загрузка файла лицензии.....	146
7.6.5	Отправить сообщение обратной связи.....	146
7.6.6	О Avira Professional Security.....	146
8.	Настройка.....	148
8.1	Конфигурация.....	148
8.2	System Scanner	152
8.2.1	Поиск	152
8.2.2	Отчет	164
8.3	Real-Time Protection.....	165
8.3.1	Поиск	165
8.3.2	Отчет	178
8.4	Переменные: Исключения для Real-Time Protection и System Scanner	179
8.4.1	Переменные в Windows XP 32-Bit (**английский).....	179
8.4.2	Переменные в Windows 7 32-Bit/ 64-Bit (**английский)	180
8.5	Обновление	180
8.5.1	Файловый сервер.....	182
8.5.2	Веб-сервер.....	183
8.6	Firewall	185
8.6.1	Конфигурация FireWall.....	185
8.6.2	Avira FireWall	186
8.6.3	Avira FireWall в АМС.....	212
8.6.4	брандмауэр Windows.....	230
8.7	Web Protection	233
8.7.1	Поиск	233
8.7.2	Отчет	242
8.8	Mail Protection	243
8.8.1	Поиск	243
8.8.2	Общее.....	250
8.8.3	Отчет	253
8.9	Общее.....	254
8.9.1	Категории угроз.....	254
8.9.2	Расширенная защита	255
8.9.3	Пароль.....	259

8.9.4	Безопасность	261
8.9.5	WMI	263
8.9.6	События	263
8.9.7	Отчеты	264
8.9.8	Папки	264
8.9.9	Акустический сигнал предупреждения.....	266
8.9.10	Предупреждения	267
9.	Tray Icon	281
10.	FireWall.....	283
10.1	Avira FireWall.....	283
10.1.1	FireWall.....	283
10.1.2	Сетевое событие.....	284
10.2	брандмауэр Windows	287
11.	Обновления	288
11.1	Обновления	288
11.2	Модуль обновления.....	289
12.	Устранение проблемы, рекомендации	292
12.1	Помощь в случае возникновения проблем	292
12.2	Горячие клавиши	297
12.2.1	В диалоговых полях	297
12.2.2	В справке	298
12.2.3	В Центре управления	299
12.3	Центр обеспечения безопасности Windows	301
12.3.1	Общие сведения.....	302
12.3.2	Центр обеспечения безопасности Windows и ваш продукт Avira	302
12.4	Центр поддержки Windows	305
12.4.1	Общее	305
12.4.2	Центр поддержки Windows и ваш программный продукт Avira.....	306

13. Вирусы и другое	313
13.1 Категории угроз	313
13.2 Вирусы и вредоносные программы.....	317
14. Информация и сервис	321
14.1 Контакты.....	321
14.2 Техническая поддержка.....	321
14.3 Подозрительный файл.....	322
14.4 Сообщение о ложном срабатывании.....	322
14.5 Обратная связь для вашей безопасности.....	322

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
<i>Курсив</i>	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](#)

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 наблюдения за программой, управления ею и ее контроля
- Централизованная настройка в стандартном и экспертном режимах с контекстной справкой
- System Scanner (сканирование по требованию) с управляемой профилем и настраиваемым сканированием по всем известным типам вирусов и вредоносных программ
- Интегрированный в Windows контроль учетных записей пользователей позволяет вам выполнять задачи, требующие прав администратора.
- Real-Time Protection (On-Access Scan) для постоянного отслеживания попыток доступа к файлам

- Компонент ProActiv для постоянного наблюдения за действиями программ (только для 32-разрядных систем)
- Mail Protection (POP3-сканер, IMAP-сканер и SMTP-сканер) для постоянной проверки электронной почты на наличие вирусов и вредоносных программ, включая проверку вложений
- Web Protection для контроля данных и файлов, передаваемых из Интернета через HTTP-протокол (наблюдение за портами 80, 8080, 3128)
- Встроенный менеджер карантина для изоляции подозрительных файлов и работы с ними
- Защита от руткитов для обнаружения скрытого вредоносного ПО, установленного в системе вашего компьютера (руткитов) (недоступно в 64-разрядных версиях Windows XP)
- Прямой доступ к подробной информации об обнаруженных вирусах и вредоносном ПО через Интернет
- Простое и быстрое обновление программы, базы вирусных сигнатур, а также поисковой системы с помощью обновления одним файлом и инкрементного VDF-обновления с веб-сервера в Интернете или в сети интранет
- Удобная система управления лицензиями
- Встроенный планировщик для планирования таких однократных или повторяющихся задач, как обновление или сканирование
- Высочайший уровень обнаружения вирусов и вредоносных программ, гарантируемый новой технологией сканирования (антивирусное 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 компьютера от несанкционированного доступа из Интернета или локальной сети, а также от несанкционированного доступа к Интернету/локальной сети

2.2 Системные требования

2.2.1 Системные требования Avira Professional Security

Для использования Avira Professional Security ваша система должна соответствовать следующим требованиям.

Операционная система

- Windows 8, последний пакет обновлений (32 или 64-разрядная), или
- Windows 7, последний пакет обновлений (32 или 64-разрядная), или
- Windows XP, последний пакет обновлений (32 или 64-разрядная).

Аппаратное обеспечение

- Компьютер с процессором Pentium или выше, с тактовой частотой как минимум 1 ГГц
- Не менее 150 Мб свободного дискового пространства (больше, если используется карантин для временного хранения файлов)
- Не менее 1024 Мб ОЗУ для Windows 8, Windows 7
- Не менее 512 Мб ОЗУ для Windows XP

Прочие требования

- Для установки программы: права администратора
- Для всех установок: Windows Internet Explorer 6.0 или выше
- При необходимости: Интернет-соединение (см. раздел [Подготовка к установке](#))


2.2.2 Права администратора (начиная с Windows Vista)

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

Поэтому компания Microsoft ввела систему контроля учетных записей пользователей. Контроль учетных записей пользователей входит в следующие операционные системы:

- Windows Vista;
- Windows 7;
- Windows 8.

Контроль учетных записей обеспечивает больше защиты для пользователей, вошедших в систему как администраторы. Таким образом, первоначально администратор имеет только привилегии обычного пользователя. Действия, для которых необходимы права администратора, четко выделяются в операционной системе значком информации. Кроме того, пользователь должен явно подтвердить желаемое действие. Только после получения подтверждения производится повышение привилегий и операционная система выполняет задание администратора.

Программа Avira Professional Security требует прав администратора для некоторых действий. Эти действия обозначаются следующим символом: . Если этот символ также отображается на кнопке, для выполнения данного действия требуются права администратора. Если ваша текущая учетная запись не имеет прав администратора, то диалоговое окно контроля учетных записей Windows потребует ввода пароля администратора. Если у вас нет пароля администратора, вы не сможете выполнить это действие.

2.2.3 Удаление несовместимых программ

Программа Avira Professional Security выполнит поиск возможных несовместимых программ. При обнаружении таких программ будет сформирован список. Рекомендуется удалить эти программы, чтобы не нарушать стабильность работы компьютера.

- ▶ Выберите из списка программы, подлежащие автоматическому удалению с компьютера, и нажмите **Далее**.

Удаление некоторых компонентов необходимо подтвердить вручную.

Выберите такие программы и нажмите **Далее**.

Удаление одной или нескольких из выбранных программ может потребовать перезагрузки компьютера. После перезагрузки начнется процесс установки.

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 распространяется в виде цифрового лицензионного ключа (формат файла *.KEY*). Этот цифровой лицензионный ключ играет роль центра управления вашей персональной лицензией. Он содержит точные данные о том, на какие программы у вас есть лицензия и каков срок ее действия. Цифровой лицензионный ключ может включать в себя лицензии на несколько продуктов.

Цифровой лицензионный ключ высылается вам по электронной почте, если вы приобрели ваш продукт Avira в Интернете, или находится на CD/DVD с программой. Вы можете загрузить файл лицензии во время установки программы или после нее (через Службу управления 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.

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

Указание

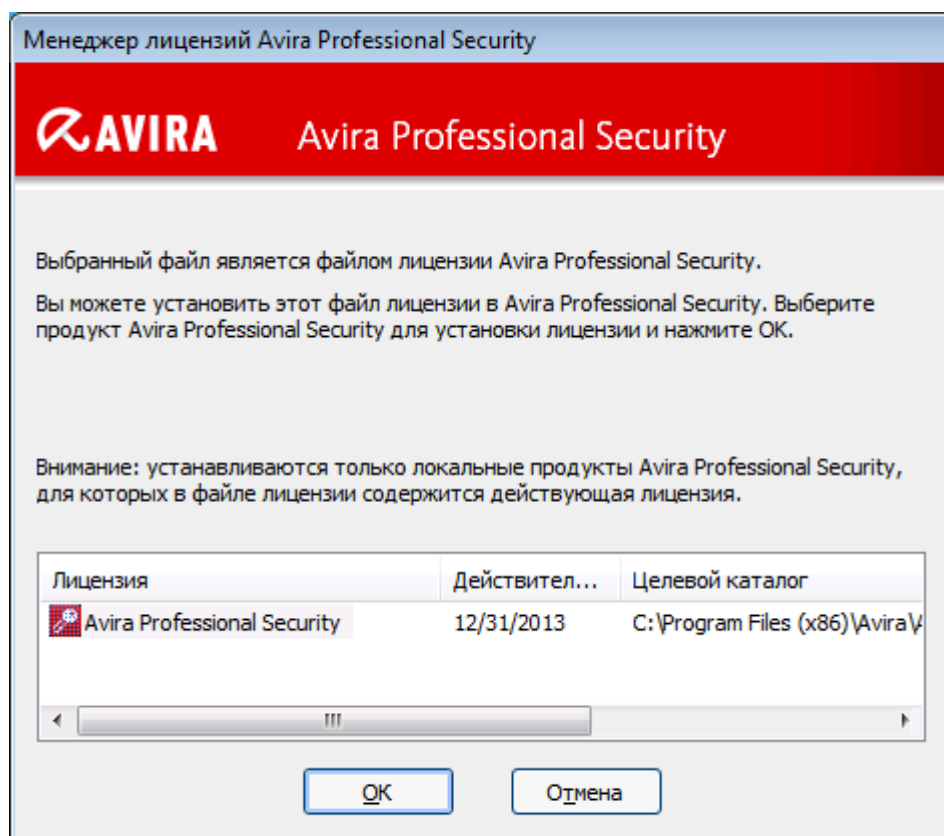
Если ваш продукт Avira администрирует АМС, то обновление будет выполнено администратором. Вам будет предложено сохранить данные и

перезагрузить компьютер, в противном случае компьютер не будет защищен в достаточной степени.

2.3.3 Управление лицензиями

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

Менеджер лицензий Avira Professional Security



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

Указание

Менеджер лицензий Avira Professional 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 этом разделе собрана информация, относящаяся к установке программы Avira Professional Security.

- [Подготовка к установке](#)
- [Установка с CD-диска при подключении к Интернету](#)
- [Установка с CD-диска без подключения к Интернету](#)
- [Установка загруженного программного обеспечения](#)
- [Удаление несовместимых программ](#)
- [Выбор типа установки](#)
- [Установка Avira Professional Security](#)
- [Изменение компонентов установки](#)
- [Удаление Avira Professional Security](#)

3.1 Подготовка к установке

- ✓ Перед установкой проверьте, соблюдены ли минимальные системные требования.
- ✓ Закройте все работающие приложения.
- ✓ Убедитесь в том, что не установлены другие антивирусные решения. Автоматические функции защиты различных систем безопасности могут мешать друг другу (автоматические параметры см. в разделе [Удаление несовместимых программ](#)).
- ✓ Если в вашей системе установлены другие панели инструментов поиска, удалите их перед установкой Avira SearchFree Toolbar. В противном случае установка панели Avira SearchFree Toolbar будет невозможна.
- ✓ Установите подключение к Интернету.
- Подключение необходимо для следующих этапов установки.
 - Загрузка актуальных программных файлов и ядра сканирования, а также последних файлов вирусных сигнатур с помощью программы установки (при установке через Интернет).
 - Активация программы.
 - Регистрация пользователя.
 - При необходимости выполнение обновления по завершении установки.
- ✓ Подготовьте код активации или файл лицензии для программы Avira Professional Security, если вы хотите активировать её.
- ✓ Для активации или регистрации программа Avira Professional Security соединяется с серверами Avira через HTTP-протокол и порт 80 (веб-коммуникация), а также через зашифрованный протокол SSL и порт 443. Если вы используете брандмауэр, убедитесь в том, что он не блокирует указанные

порты и входящий/исходящий трафик.

3.2 Установка с CD-диска при подключении к Интернету

- ▶ Вставьте CD-диск Avira Professional Security в дисковод.

При активации автозапуска выберите **Открыть папку** для просмотра файлов.
ИЛИ

Перейдите к дисководу CD-дисков, щелкните правой кнопкой название диска (AVIRA) и выберите **Открыть** для просмотра файлов.

Дважды щелкните файл *autorun.exe*.

В меню CD-диска выберите установку онлайн-версии.

Программа проведет поиск несовместимых программ (подробнее см. раздел [Удаление несовместимых программ](#)).

Нажмите кнопку **Далее** в окне *Добро пожаловать*.

Выберите нужный язык и нажмите **Далее**. С сервера Avira будут загружены все файлы, необходимые для установки.

Перейдите к разделу [Выбор типа установки](#).

3.3 Установка с CD-диска без подключения к Интернету

- ▶ Вставьте CD-диск Avira Professional Security в дисковод.

При активации автозапуска выберите **Открыть папку** для просмотра файлов.
ИЛИ

Перейдите к дисководу CD-дисков, щелкните правой кнопкой название диска (AVIRA) и выберите **Открыть** для просмотра файлов.

Дважды щелкните файл *autorun.exe*.

В меню CD-диска выберите установку автономной версии (без подключения к сети).

Программа проведет поиск несовместимых программ (подробнее см. раздел [Удаление несовместимых программ](#)).

Выполнится распаковка установочного файла. Запустится процедура установки.

Перейдите к разделу [Выбор типа установки](#).

3.4 Установка программного обеспечения, загруженного с сайта Avira

- ▶ Перейдите на сайт www.avira.com/download.

Выберите нужный продукт и нажмите **Скачать**.

Сохраните загруженный файл в своей системе.

Дважды щелкните установочный файл `avira_professional_security_ru.exe`.

Если откроется окно контроля учетных записей, нажмите «Да».

Программа проведет поиск несовместимых программ (подробнее см. раздел [Удаление несовместимых программ](#)).

Выполнится распаковка установочного файла. Запустится процедура установки.

Продолжение см. в разделе [Выбор типа установки](#).

3.5 Удаление несовместимых программ

Программа Avira Professional Security выполнит поиск возможных несовместимых программ. При обнаружении таких программ будет сформирован список. Рекомендуется удалить эти программы, чтобы не нарушать стабильность работы компьютера.

- ▶ Выберите из списка программы, подлежащие автоматическому удалению с компьютера, и нажмите **Далее**.

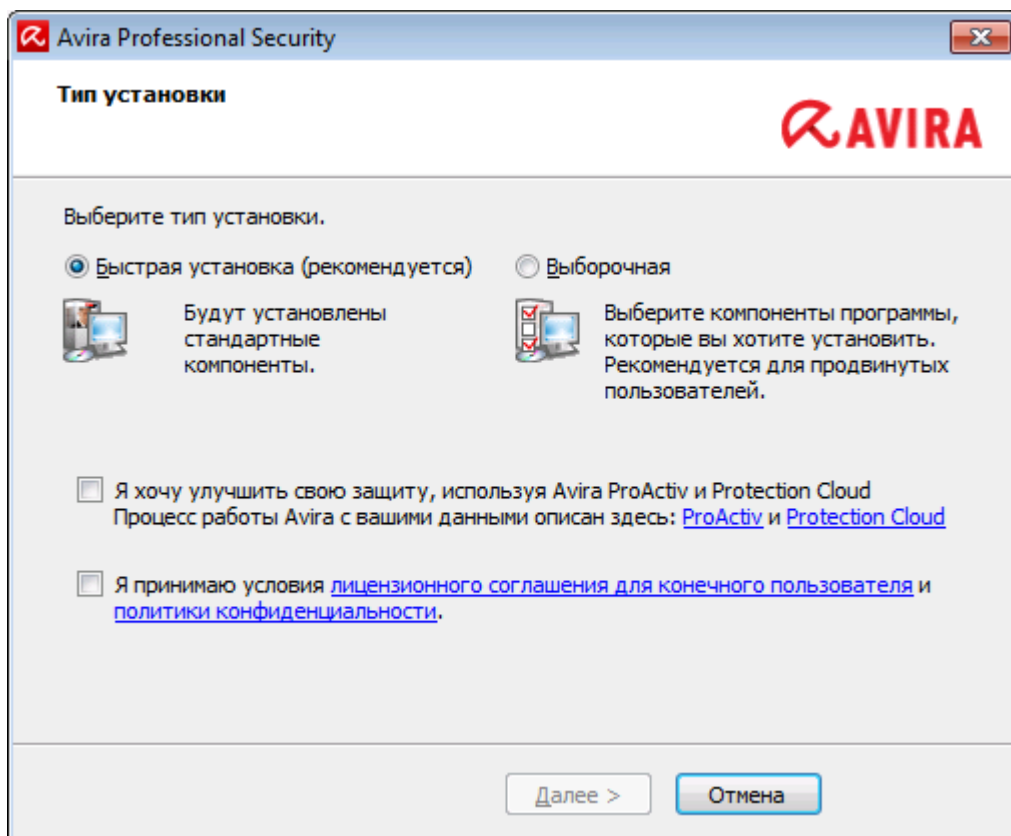
Удаление некоторых компонентов необходимо подтверждать вручную.

Выберите такие программы и нажмите **Далее**.

Удаление одной или нескольких из выбранных программ может потребовать перезагрузки компьютера. После перезагрузки начнется процесс установки.

3.6 Выбор типа установки

Вы можете выбрать тип установки в мастере установки. Мастер установки предназначен для того, чтобы поэтапно и доступно провести вас через всю процедуру.



Схожие темы:

- Раздел [Выполнение быстрой установки](#)
- Раздел [Выполнение выборочной установки](#)

3.6.1 Выполнение быстрой установки

Быстрая установка является рекомендуемой процедурой установки.

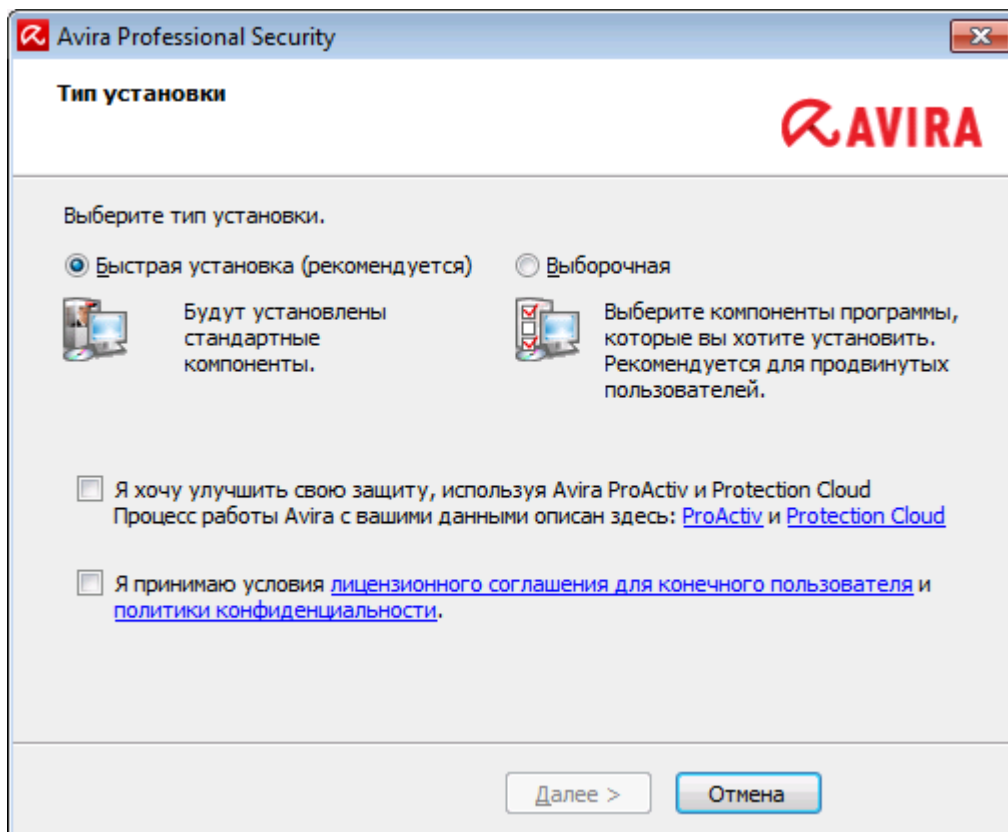
- Она устанавливает все стандартные компоненты пакета Avira Professional Security. При этом используются рекомендованные компанией Avira параметры уровня безопасности.
- В качестве пути установки выбирается один из следующих путей:
 - `C:\Program Files\Avira` (для 32-разрядных версий Windows) или
 - `C:\Program Files (x86)\Avira` (для 64-разрядных версий Windows).
- В этой папке размещаются все файлы, относящиеся к Avira Professional Security.
- Выбрав этот тип установки, вам потребуется всего лишь нажать кнопку **Далее**, и установка будет полностью выполнена.
- Этот тип установки разработан специально для тех пользователей, которые чувствуют себя не в своей тарелке при настройке программных средств.

3.6.2 Выполнение выборочной установки

Выборочная установка позволяет задать собственную конфигурацию при установке пакета. Она рекомендуется только продвинутым пользователям, хорошо знакомым с вопросами аппаратного и программного обеспечения, а также информационной безопасности.

- Есть возможность установить отдельные программные компоненты.
- Можно выбрать папку, в которую будет произведена установка.
- Вы сможете установить, необходимо ли **создавать ярлык на рабочем столе и/или новую группу программ в меню Пуск**.
- В ассистенте настроек можно установить собственные параметры для пакета Avira Professional Security. Кроме того, можно выбрать комфортный для вас уровень безопасности.
- В конце можно отменить быстрое сканирование системы, обычно выполняемое автоматически после установки.

3.7 Установка Avira Professional Security



- ▶ Если вы не желаете принимать участия в Avira Community, снимите флажок **Я хочу улучшить свою защиту, используя Avira ProActiv и Protection Cloud**, установленные по умолчанию.

Если вы подтвердите свое согласие на участие в Avira Community, Avira Professional Security будет отправлять данные о подозрительных программах в исследовательский 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.

3.7.1 Выбор пути установки

Выборочная установка позволяет выбрать папку, в которую будет установлен пакет Avira Professional Security.



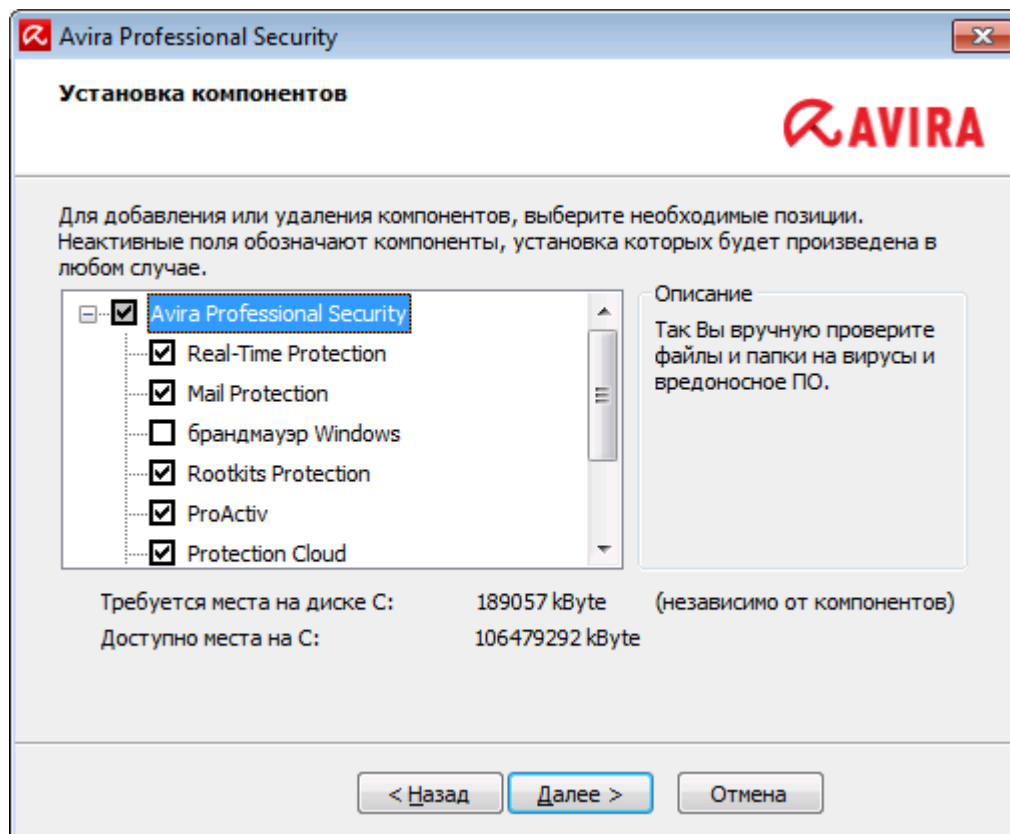
- ▶ Нажмите **Обзор** и перейдите к местоположению, в которое вы хотите установить Avira Professional Security.

Выбор папки для установки пакета Avira Professional Security производится в окне **Путь установки**.

Нажмите **Далее**.

3.7.2 Выбор компонентов установки

При выборочной установке или при изменении компонентов установки могут быть выбраны, добавлены или удалены следующие установочные модули.



Установите или снимите флажки в списке диалогового окна «Компоненты установки».

- **Avira Professional Security**

Этот модуль содержит все компоненты, необходимые для успешной установки вашего продукта Avira Professional Security.

- **Real-Time Protection**

Программа Avira Real-Time Protection работает в фоновом режиме. Она контролирует доступ к файлам и по возможности восстанавливает их при таких операциях, как открытие, закрытие и копирование. Когда пользователь производит операцию с файлом (загрузку документа, исполнение, копирование), программа Avira Professional Security автоматически проверяет этот файл. Однако файл не проверяется модулем Avira Real-Time Protection при переименовании.

- **Mail Protection**

Mail Protection — это связующее звено между вашим компьютером и почтовым сервером, с которого ваш почтовый клиент загружает письма. Mail Protection играет роль так называемого прокси-сервера между почтовым клиентом и почтовым сервером. Все входящие письма направляются через этот прокси-сервер, проверяются на наличие вирусов и нежелательных программ, а затем

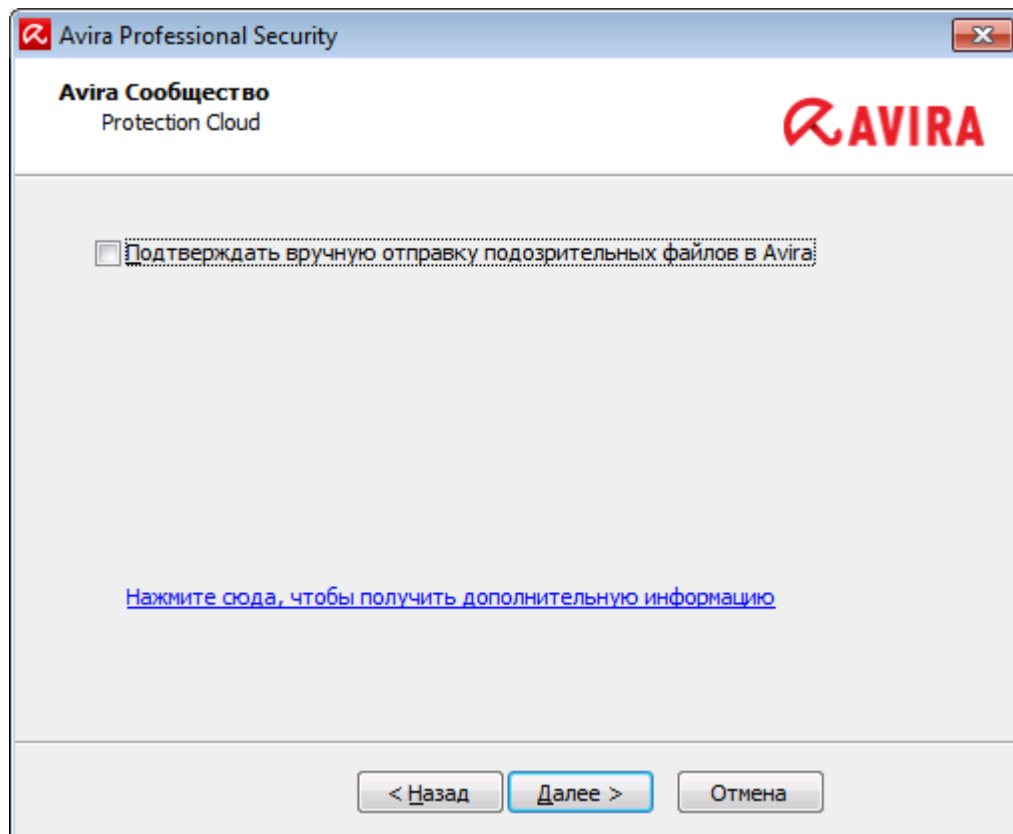
пересылаются на вашу почту. В зависимости от конфигурации программа либо автоматически обрабатывает вредоносные письма, либо запрашивает вас о необходимых действиях.

- **Avira FireWall** (вплоть до Windows XP) Avira FireWall контролирует входящий и исходящий трафик на вашем компьютере. Этот компонент разрешает или запрещает соединение, исходя из политики безопасности.
- **Windows Firewall** (начиная с Windows 7)
Этот компонент позволяет управлять брандмауэром Windows Firewall через интерфейс Avira Professional Security.
- **Rookits Protection**
Модуль Avira Rookits 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 уведомляет пользователя о подозрительном поведении. Такой поведенческий анализ позволяет защитить ваш компьютер от неизвестных вредоносных программ. Компонент ProActiv встроен в пакет Avira Real-Time Protection.
- **Protection Cloud**
Компонент Protection Cloud служит для динамического обнаружения пока неизвестных вредоносных программ с помощью Интернета. При этом файлы загружаются на удаленный сервер и сравниваются как с известными файлами, так и с другими файлами, загружаемыми и анализируемыми в реальном времени (без перерывов и задержек). Таким образом, база данных постоянно обновляется, что еще более повышает уровень безопасности.
Если вы выбрали компонент Cloud Protection, но хотите каждый раз вручную подтверждать отправку файлов на анализ, установите флажок **Подтверждать ручную отправку подозрительных файлов в центр Avira**.
- **Web Protection**
При работе в Интернете ваш браузер получает данные с веб-серверов. Переданные веб-сервером данные (HTML-файлы, скрипты и картинки, флэш, видео- и аудиопотоки и т. д.) обычно попадают сразу в кэш браузера для отображения в браузере, делая невозможной проверку в момент доступа по технологии 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 либо автоматически обрабатывает вредоносные файлы, либо запрашивает пользователя о необходимых действиях.
- **Расширение оболочки**
Модуль «Расширение оболочки» создает запись **Проверить выбранные файлы с помощью Avira** в контекстном меню Проводника Windows (которое открывается правым щелчком мыши). Это позволяет вам без труда сканировать файлы и папки.

Схожие темы:

[Изменение компонентов установки](#)

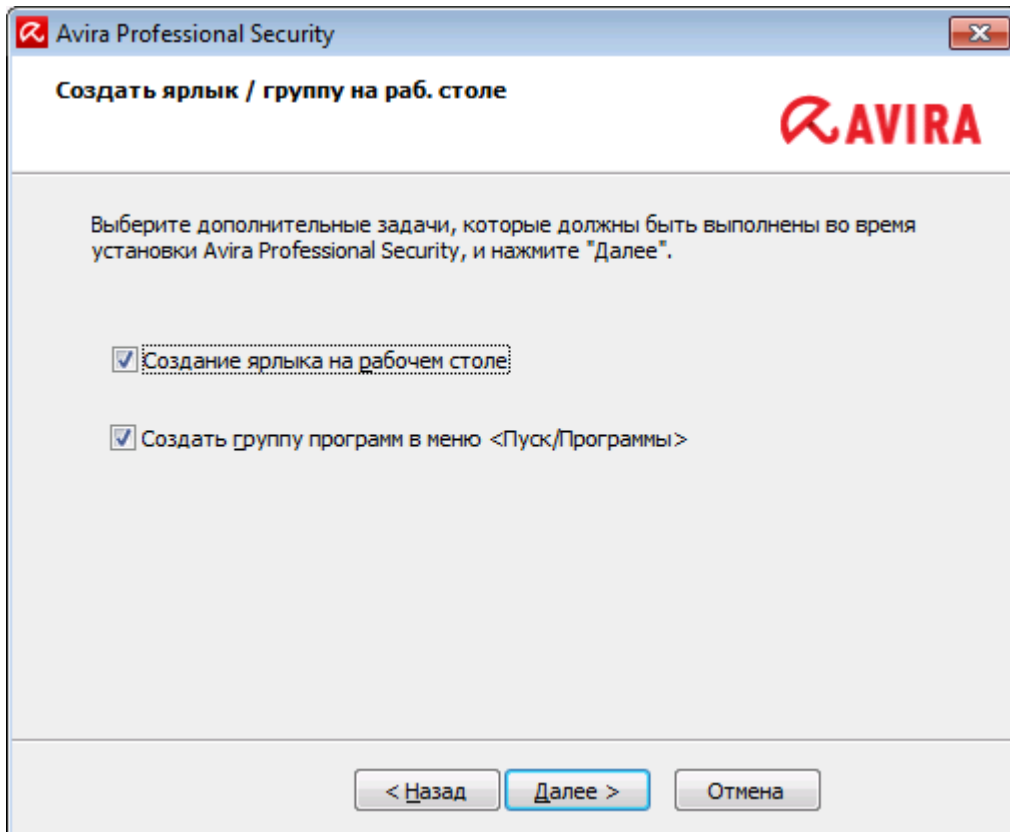
Если вы решили принять участие в сообществе Avira, вы можете выбрать подтверждение отправки файла в Avira Malware Research Center вручную в любое время.



- ▶ Чтобы Avira Professional Security запрашивал подтверждение каждый раз, включите опцию **Confirm manually when sending suspicious files to Avira**.

3.7.3 Создание ярлыков для Avira Professional Security

Ярлык на рабочем столе и группа программ в меню «Пуск» позволяют быстрее и проще получать доступ к пакету Avira Professional Security.



- ▶ Чтобы создать ярлык на рабочем столе и/или группу программ в меню **Пуск** для Avira Professional Security, не снимайте установленные флажки.

3.7.4 Активация Avira Professional Security

Для активации пакета Avira Professional Security есть несколько способов.



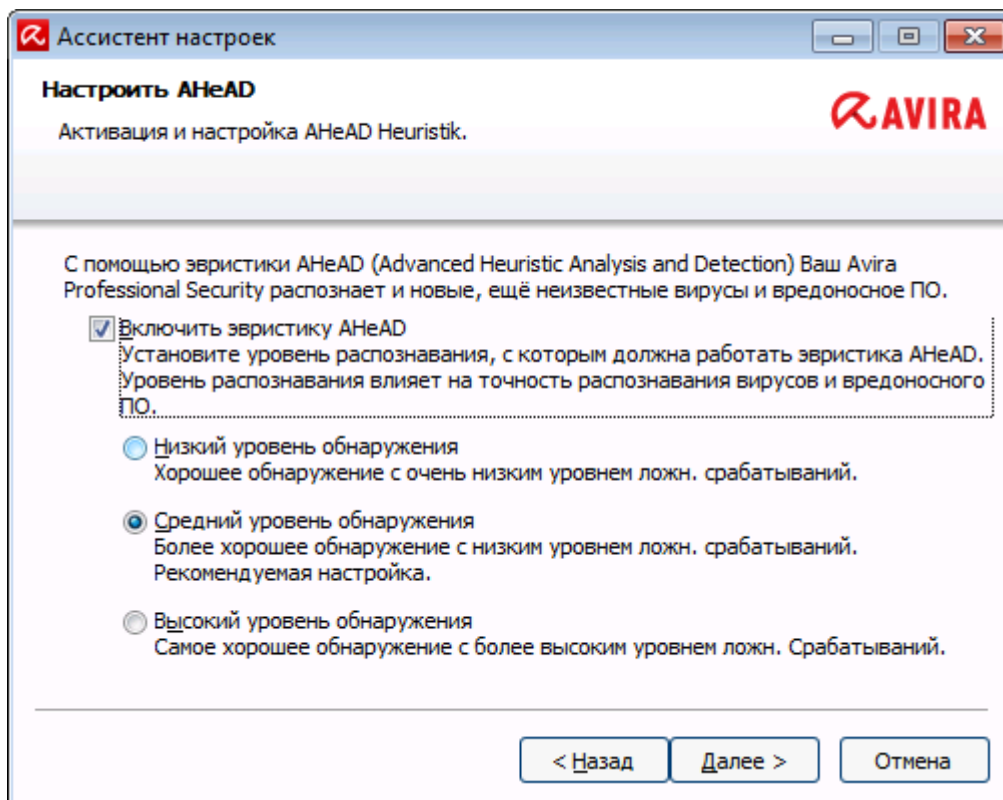
Если у вас уже есть код активации, введите его в соответствующие поля.

- ▶ Если вам еще предстоит приобрести код активации, нажмите на ссылку «Получить активационный код».
- Вы будете перенаправлены на сайт Avira, где сможете приобрести код активации.
- ▶ Если вы просто желаете опробовать программу, выберите вариант **Тестировать продукт** и введите свои данные в необходимые регистрационные поля.
- Тестовая лицензия действительна в течение 31 дня.
- ▶ Если вы ранее уже активировали продукт Avira и хотите его переустановить, выберите вариант **У меня уже есть действующий файл лицензии**.

Откроется окно обзора, в котором нужно будет найти свой файл *hbedv.key*.

3.7.5 Настройка уровня эвристического обнаружения (AHeAD)

Пакет Avira Professional Security содержит очень мощное средство защиты — технологию Avira AHeAD (*Advanced Heuristic Analysis and Detection* — расширенный эвристический анализ и обнаружение). Эта технология применяет методики распознавания моделей для обнаружения неизвестных (новых) вредоносных программ на основе анализа старых.

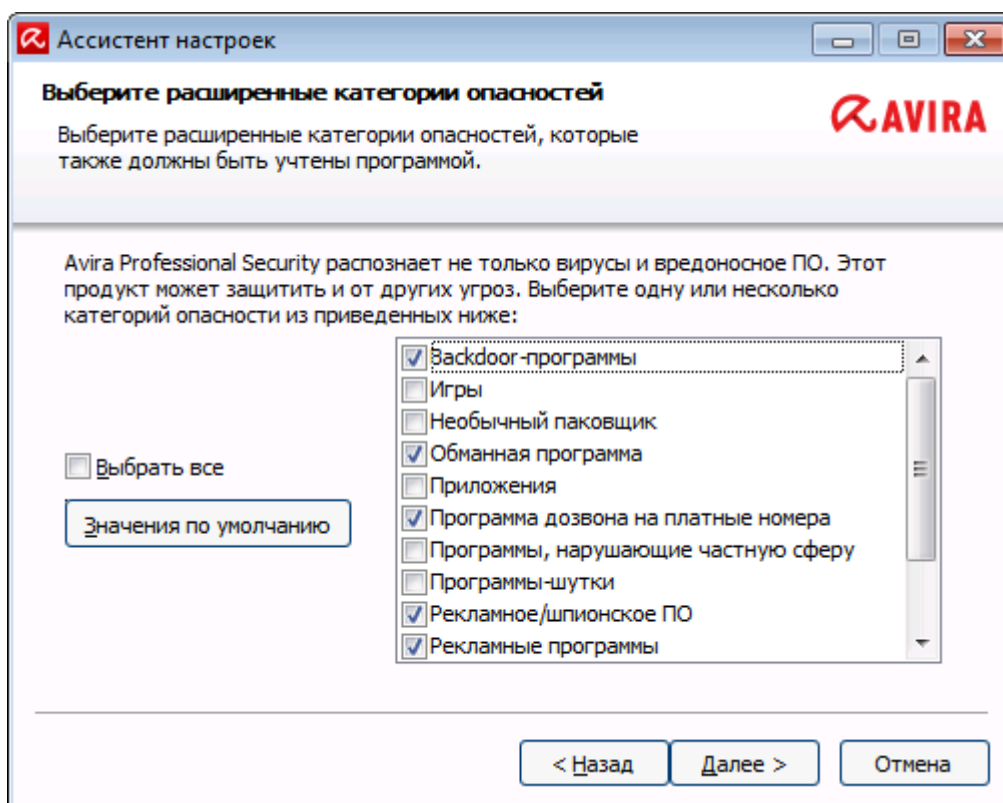


- ▶ Выберите уровень обнаружения в окне **Настройка AHeAD** и нажмите **Далее**.

Выбранный уровень обнаружения будет использован для конфигурации технологии AHead модуля System Scanner (прямая проверка) и модуля Real-Time Protection (проверка в реальном времени).

3.7.6 Выбор расширенных категорий опасности

Вирусы и вредоносные программы — не единственные угрозы для системы вашего компьютера. Нами составлен целый список элементов риска, который отсортирован в виде расширенных категорий опасности.



- ▶ Ряд категорий опасности уже выбран заранее по умолчанию.

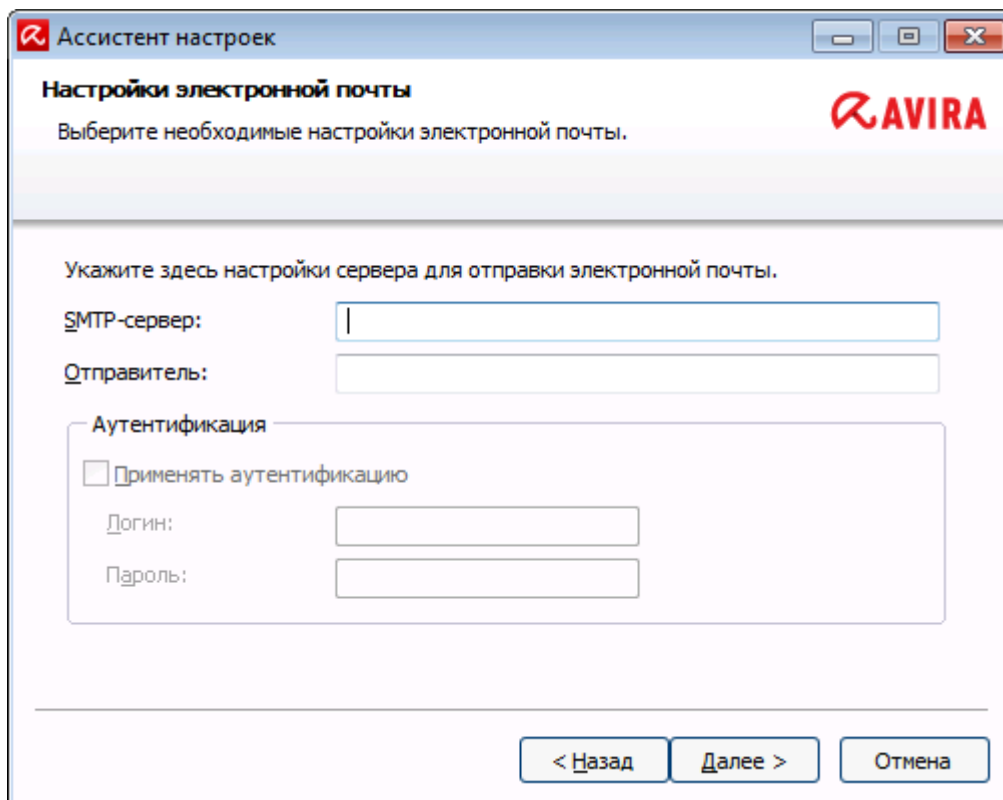
По необходимости можно активировать и другие категории в диалоговом окне **Выберите расширенные категории опасности**.

Если вы передумаете, можно вернуть рекомендуемые значения с помощью кнопки **Значения по умолчанию**.

Продолжите установку кнопкой **Далее**.

3.7.7 Выбор настроек электронной почты

Программа Avira Professional Security использует SMTP-протокол для направления подозрительных объектов из карантина в исследовательский центр Avira Malware Research Center, а также для отправки писем и предупреждений по электронной почте.



- ▶ Если вы хотите иметь возможность автоматически отправлять почту по SMTP-протоколу, следует задать параметры сервера для отправки почты в окне **Настройки электронной почты**.

SMTP-сервер

Укажите имя компьютера или IP-адрес нужного SMTP-сервера.

Примеры

Адрес: smtp.company.com

Адрес: 192.168.1.100

Адрес отправителя

Укажите адрес электронной почты отправителя.

Аутентификация

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

Использовать аутентификацию

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

Логин:

Укажите здесь свое имя пользователя.

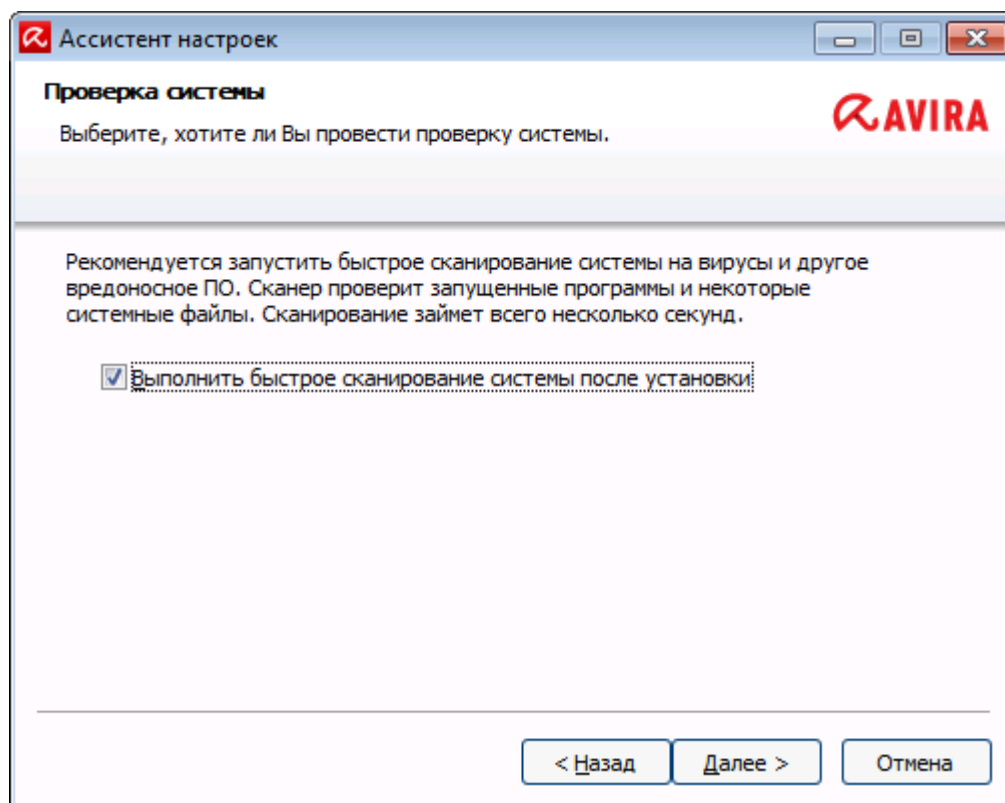
Пароль:

Укажите здесь соответствующий пароль. Пароль сохраняется в закодированном виде. Для безопасности вводимые в это поле знаки заменяются звездочками (*).

Нажмите **Далее**.

3.7.8 Запуск сканирования после установки

Для проверки текущего состояния безопасности компьютера после настройки конфигурации и перед перезагрузкой компьютера можно выполнить быстрое сканирование системы. Модуль System Scanner проверяет работающие программы и большую часть важных системных файлов на наличие вирусов и вредоносных программ.



- ▶ Если вы хотите выполнить быстрое сканирование системы, оставьте на месте флажок **Быстрое сканирование системы**.

Нажмите **Далее**.

Завершите настройку конфигурации кнопкой **Готово**.

Если флажок **Быстрое сканирование системы** не был снят, откроется окно *Luke Filewalker*.

Модуль System Scanner выполняет быстрое сканирование системы.

3.7.9 Установка и удаление в сети

Чтобы упростить администратору установку Avira в сеть с большим количеством клиентских машин, Avira предлагает специальную технологию для первичной установки и установки изменений.

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

Указание

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

Указание

Обратите внимание на то, что для установки по сети вам потребуется инсталляционный пакет Avira. Установочный файл для установки через Интернет не обязателен.

Программа Avira устанавливается в сети с помощью логин-скрипта сервера или через SMC.

Здесь содержится информация по установке и удалению в сети:

- См. главу: [Параметры командной строки для установщика](#)
- См. главу: [Аргумент файла *setup.inf*](#)
- см. главу: [Установка в сети](#)
- см. главу: [Удаление в сети](#)

Указание

Еще одна удобная возможность установки и удаления программы в сети предлагается Avira Management Console (AMC). Avira Management Console служит для дистанционной установки и обслуживания продуктов Avira в сети. Дополнительную информацию вы можете посмотреть на нашем веб-сайте:

<http://www.avira.ru>

Установка в сети

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

Установка подходит для следующих случаев:

- Первичная установка через сеть (необслуживаемая установка)
- Установка персональных компьютеров
 - ▶ Установка изменений или обновление

Указание

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

Указание

При установке на операционной системе сервера функции Real-Time Protection и защита данных недоступны.

Так устанавливаются программы Avira в сети:

- ✓ Требуются права администратора (в т.ч. и в Batch-режиме)
- ▶ Настройте параметры файла *setup.inf* и сохраните файл.
- ▶ Запустите установку с аргументом */inf* или добавьте аргумент к скрипту сервера.

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

→ Установка производится автоматически.

Параметры командной строки для установщика

Указание

Параметры, содержащие данные о расположении или имени файла, должны заключаться в кавычки (пример:
`InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

Возможные параметры для установки:

- `/inf`

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

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

Возможные параметры для удаления:

- `/remove`

Установщик удаляет программу Avira.

Пример: `presetup.exe /remove`

- `/remsilent`

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

Пример: `presetup.exe /remsilent`

- `/remsilentaskreboot`

Установщик удаляет программу Avira, не показывая диалоговые окна, спрашивает после установки, необходимо ли перезагрузить компьютер.

Пример: `presetup.exe /remsilentaskreboot`

Для протоколирования удаления возможен следующий параметр:

- `/unsetuplog`

Фиксируются все действия при удалении.

Пример: `presetup.exe /remsilent`

`/unsetuplog="c:\logfile\unsetup.log"`

Параметры файла *setup.inf*

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

Указание

Параметры, содержащие данные о расположении или имени файла, должны заключаться в кавычки (пример:

`InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\").`

- `DestinationPath`

Папка, в которую устанавливается программа. Она должна быть указана в скрипте. Помните, что программа установки автоматически прикрепляет название компании и продукта. Могут использоваться переменные среды.

Пример: `DestinationPath=%PROGRAMFILES%`

означает путь установки *C:\Program Files\Avira\AntiVir Desktop*

- `ProgramGroup`

Создает в меню «Пуск» Windows группу программ для всех пользователей.

1: создать группу программ

0: не создавать группу программ

Пример: `ProgramGroup=1`

- `DesktopIcon`

Создает на рабочем столе ярлык для всех пользователей.

1: создать ярлык на рабочем столе

0: не создавать ярлык на рабочем столе

Пример: `DesktopIcon=1`

- `ShellExtension`

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

1: создать расширение оболочки

0: не создавать расширение оболочки

Пример: `ShellExtension=1`

- Guard

Устанавливает Avira Real-Time Protection (On-Access-Scanner).

1: установить Avira Real-Time Protection

0: не устанавливать Avira Real-Time Protection

Пример: `Guard=1`

- MailScanner

Устанавливает Avira Mail Protection.

1: установить Avira Mail Protection

0: не устанавливать Avira Mail Protection

Пример: `MailScanner=1`

- KeyFile

Указывает путь к файлу лицензии, который копируется при установке.

Требуется при первой установке. Имя файла необходимо указывать полностью. (При изменении программы опционально.)

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

- ShowReadMe

Отображает файл `readme.txt` после установки.

1: показать файл

0: не показывать файл

Пример: `ShowReadMe=1`

- RestartWindows

Перезагружает компьютер после установки. Эта строка имеет более высокий приоритет, чем `ShowRestartMessage`.

1: перезагрузить компьютер

0: не перезагружать компьютер

Пример: `RestartWindows=1`

- ShowRestartMessage

Отображает информацию об автоматической перезагрузке в процессе установки

0: не показывать информацию

1: показать информацию

Пример: `ShowRestartMessage=1`

- SetupMode

Не требуется при первой установке. Программа установки распознает, выполнена ли установка в первый раз. Определяет вид установки. Если

продукт уже установлен, необходимо выбрать режим установки: обновление, изменение или удаление.

Update: выполняет обновление имеющейся установки. При этом параметры конфигурации, такие как `Guard`, игнорируются.

Modify: выполняет модификацию существующей установки. При этом файлы не копируются в целевую папку.

Remove: удаляет продукт Avira из системы.

Пример: `SetupMode=Update`

- `AVWinIni` (опционально)

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

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

- `Password`

Эта опция передает процессу установки пароль, требуемый для установки (изменения) или удаления программы. Строка проверяется процессом установки только в случае указания пароля. Если пароль был определен, но не был указан в виде параметра или был указан неверно, процедура установки будет прервана.

Пример: `Password>Password123`

- `WebGuard`

Устанавливает Avira Web Protection.

1: установить Avira Web Protection

0: не устанавливать Avira Web Protection

Пример: `WebGuard=1`

- `RootKit`

Устанавливает модуль Avira Rootkits Protection. Без модуля Avira Rootkits Protection сканер не сможет искать руткиты в системе!

1: установить модуль Avira Rootkits Protection

0: не устанавливать модуль Avira Rootkits Protection

Пример: `RootKit=1`

- `ProActiv`

Устанавливает компонент Avira ProActiv. Avira ProActiv — это основанная на ролях технология распознавания, с помощью которой выявляется еще не известное вредоносное ПО.

1: установить ProActiv

0: не устанавливать ProActiv

Пример: `ProActiv=1`

- `FireWall`

Устанавливает брандмауэр Avira FireWall (до Windows 7). Avira FireWall контролирует и управляет входящим и исходящим трафиком на вашем компьютере и защищает компьютер от угроз из Интернета и иных видов сетевого окружения.

1: установить FireWall

0: не устанавливать FireWall

Пример: FireWall=1

- MgtFirewall

Устанавливает компоненты управления Windows FireWall. Начиная с Windows 8, брандмауэр Avira FireWall не входит в Avira Professional Security. Вместо этого брандмауэром Windows FireWall можно управлять с помощью Центра управления сетями и общим доступом.

1: установить компоненты управления Windows FireWall

0: не устанавливать компоненты управления Windows FireWall

Пример: MgtFirewall=1

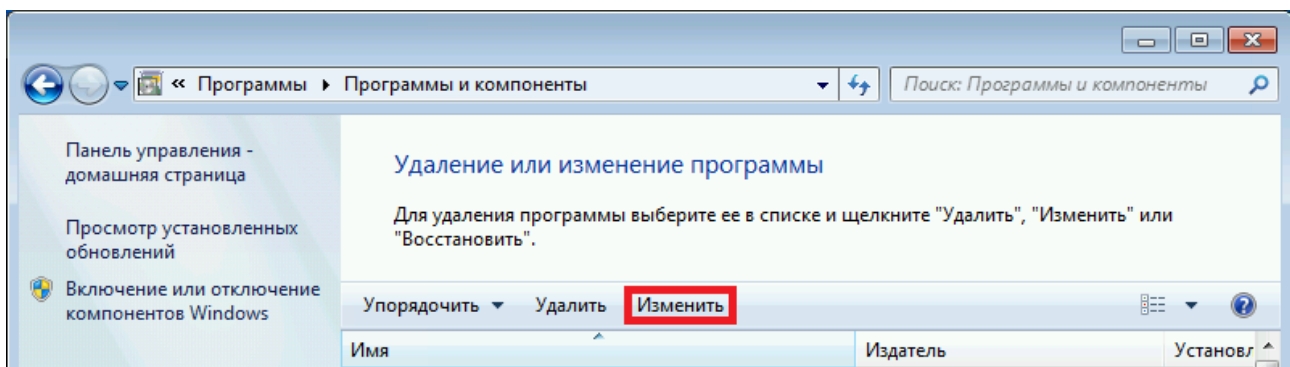
3.8 Изменение компонентов установки

Если нужно добавить или удалить модули уже установленного программного обеспечения, можно сделать это без полного удаления Avira Professional Security. Нужные действия описаны здесь:

- Изменение компонентов установки в системе Windows 8
- [Изменение компонентов установки в системе Windows 7](#)
- [Изменение компонентов установки в системе Windows XP](#)

3.8.1 Изменение компонентов установки в системе Windows 8

Есть возможность добавлять или удалять отдельные программные компоненты установленного продукта Avira Professional Security (см. раздел [Выбор компонентов установки](#)).



Если вы хотите добавить или удалить модули после установки, вы можете воспользоваться функцией **Удаление программ** на **Панели управления Windows** для **изменения/удаления** программы.

- ▶ Щелкните правой кнопкой мыши по экрану.

Появится символ **Все приложения**.

Нажмите символ и найдите в разделе *Приложения — Система Windows* пункт **Панель управления**.

Дважды щелкните символ **Панели управления**.

Выберите **Программы — Удалить программу**.

Щелкните **Программы и компоненты — Удалить программу**.

Выберите в списке Avira Professional Security и нажмите **Изменить**.

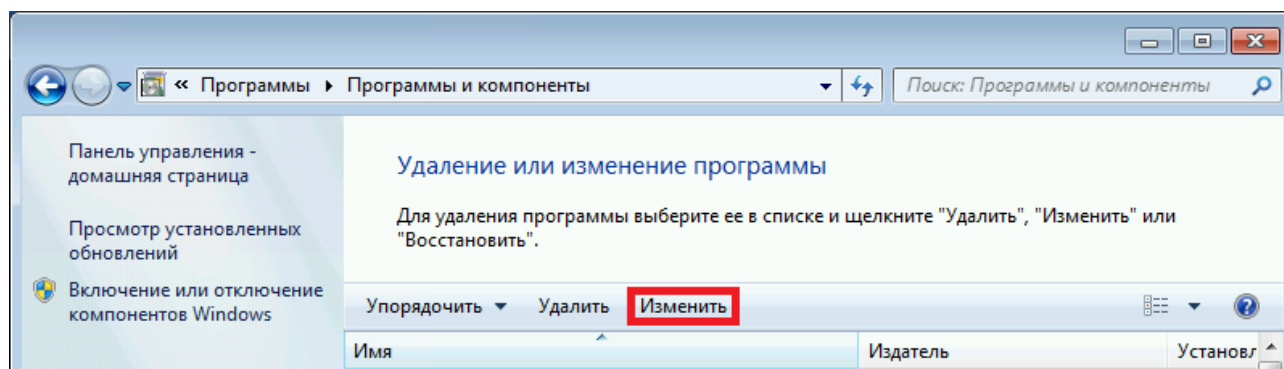
В диалоговом окне **Добро пожаловать** выберите пункт **Изменить**. Вы пройдете через процедуру изменения компонентов установки.

Схожие темы:

[Выбор компонентов установки](#)

3.8.2 Изменение компонентов установки в системе Windows 7

Есть возможность добавлять или удалять отдельные программные компоненты установленного продукта Avira Professional Security (см. раздел [Выбор компонентов установки](#)).



Если вы хотите добавить или удалить модули после установки, вы можете воспользоваться функцией **Установка и удаление программ** на **Панели управления Windows** для **изменения/удаления** программы.

- ▶ Откройте пункт **Панель управления** в меню Windows **Пуск**.

Дважды щелкните мышью **Программы и компоненты**.

Выберите в списке Avira Professional Security и нажмите **Изменить**.

В диалоговом окне **Добро пожаловать** выберите пункт **Изменить**. Вы пройдете через процедуру изменения компонентов установки.

Схожие темы:

[Выбор компонентов установки](#)

3.8.3 Изменение компонентов установки в системе Windows XP

Есть возможность добавлять или удалять отдельные программные компоненты установленного продукта Avira Professional Security (см. раздел [Выбор компонентов установки](#)).

Если вы хотите добавить или удалить модули после установки, вы можете воспользоваться функцией **Установка и удаление программ** на **Панели управления Windows** для **изменения/удаления** программы.

- ▶ Откройте пункт **Панель управления** в меню Windows **Пуск > Настройки**.

Дважды щелкните компонент **Установка и удаление программ**.

Выберите в списке Avira Professional Security и нажмите **Изменить**.

В диалоговом окне **Добро пожаловать** выберите пункт **Изменить**. Вы пройдете через процедуру изменения компонентов установки.

Схожие темы:

[Выбор компонентов установки](#)

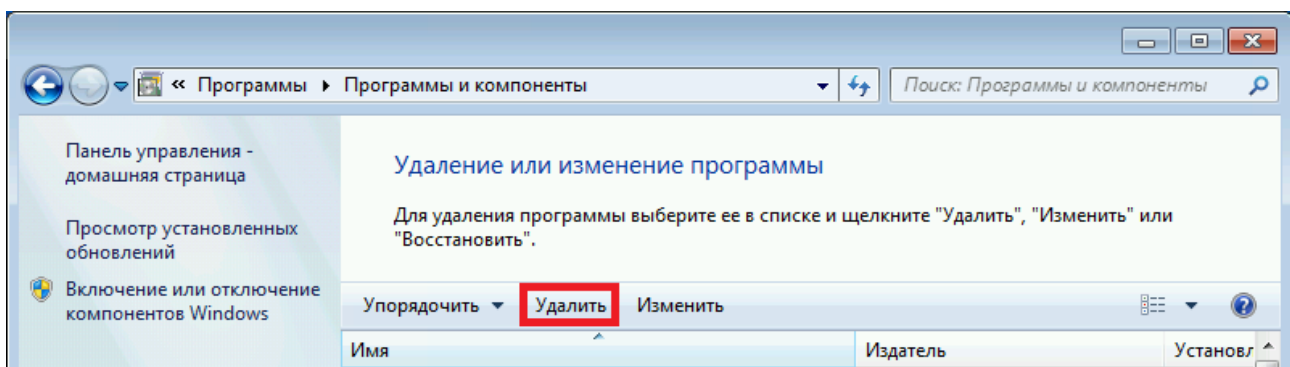
3.9 Удаление

Если когда-нибудь возникнет необходимость в удалении пакета Avira Professional Security, вот как это можно сделать:

- [Удаление Avira Professional Security в системе Windows 8](#)
- [Удаление Avira Professional Security в системе Windows 7](#)
- [Удаление Avira Professional Security в системе Windows XP](#)

3.9.1 Удаление Avira Professional Security в системе Windows 8

Для удаления пакета Avira Professional Security с компьютера воспользуйтесь функцией **Программы и компоненты** на **Панели управления Windows**.



- ▶ Щелкните правой кнопкой мыши по экрану.

Появится символ **Все приложения**.

Нажмите символ и найдите в разделе *Приложения — Система Windows* пункт **Панель управления**.

Дважды щелкните символ **Панели управления**.

Выберите **Программы — Удалить программу**.

Щелкните **Программы и компоненты — Удалить программу**.

Выберите Avira Professional Security из списка и нажмите кнопку **Удалить**.

На запрос об удалении приложения и всех его компонентов нажмите **Да** для подтверждения.

На запрос об активации брандмауэра Windows (перед удалением Avira FireWall) нажмите **Да** — это позволит хотя бы частично защитить систему.

Удаляются все компоненты программы.

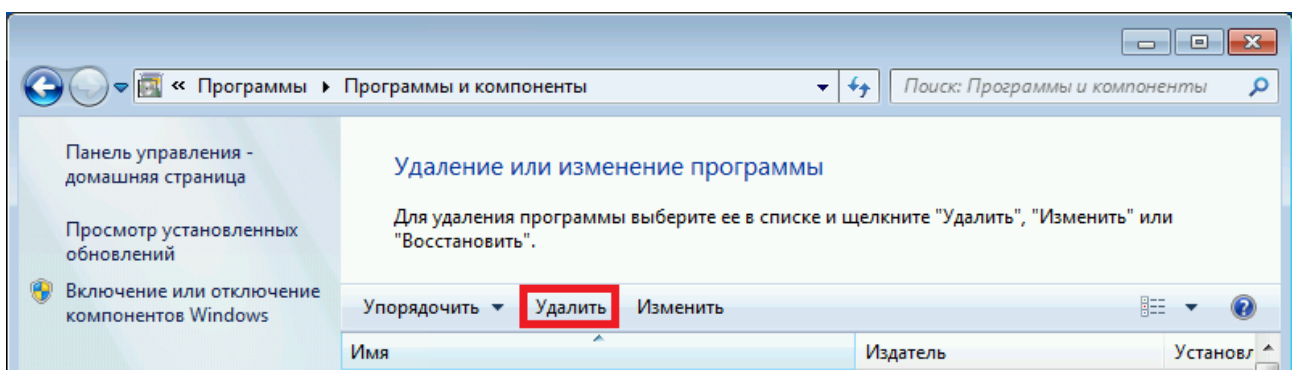
Нажмите **Завершить** для завершения удаления.

Если отобразится окно с предложением перезагрузить компьютер, нажмите **Да** для подтверждения.

Теперь пакет Avira Professional Security удален. Все папки, файлы и записи реестра этой программы будут удалены после перезагрузки компьютера.

3.9.2 Удаление Avira Professional Security в системе Windows 7

Для удаления пакета Avira Professional Security с компьютера воспользуйтесь функцией **Программы и компоненты** на Панели управления Windows.



- ▶ Откройте пункт **Панель управления** в меню Windows **Пуск**.

Щелкните **Программы и компоненты**.

Выберите Avira Professional Security из списка и нажмите кнопку **Удалить**.

На запрос об удалении приложения и всех его компонентов нажмите **Да** для подтверждения.

На запрос об активации брандмауэра Windows (перед удалением Avira FireWall) нажмите **Да** — это позволит хотя бы частично защитить систему.

Удаляются все компоненты программы.

Нажмите **Завершить** для завершения удаления.

Если отобразится окно с предложением перезагрузить компьютер, нажмите **Да** для подтверждения.

Теперь пакет Avira Professional Security удален. Все папки, файлы и записи реестра этой программы будут удалены после перезагрузки компьютера.

3.9.3 Удаление Avira Professional Security в системе Windows XP

Для удаления пакета Avira Professional Security с компьютера воспользуйтесь функцией **Установка и удаление программ** на Панели управления Windows.

- ▶ Откройте пункт **Панель управления** в меню Windows **Пуск > Настройки**.

Дважды щелкните компонент **Установка и удаление программ**.

Выберите Avira Professional Security из списка и нажмите кнопку **Удалить**.

На запрос об удалении приложения и всех его компонентов нажмите **Да** для подтверждения.

Удаляются все компоненты программы.

Нажмите **Завершить** для завершения удаления.

Если отобразится окно с предложением перезагрузить компьютер, нажмите **Да** для подтверждения.

Теперь пакет Avira Professional Security удален. Все папки, файлы и записи реестра этой программы будут удалены после перезагрузки компьютера.

3.9.4 Удаление из сети

Так Вы можете автоматически удалить программы Avira из сети:

- ✓ Требуется права администратора (в т.ч. и в Batch-режиме)
- ▶ Запустите удаление с параметром `/remsilent` или `/remsilentaskreboot` или добавьте параметр в логин-скрипт сервера.

Дополнительно можно указать аргумент для протоколирования процесса удаления.

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

→ Удаление происходит автоматически.

Указание

Не запускайте программу установки для удаления на открытом сетевом диске, это должно выполняться на локальном диске, на котором требуется удаление Avira.

4. Обзор Avira Professional Security

главы содержится обзор функций и особенности использования программы Avira.

- См. главу [Интерфейс и работа с программой](#)
- См. главу [Это делается так](#)

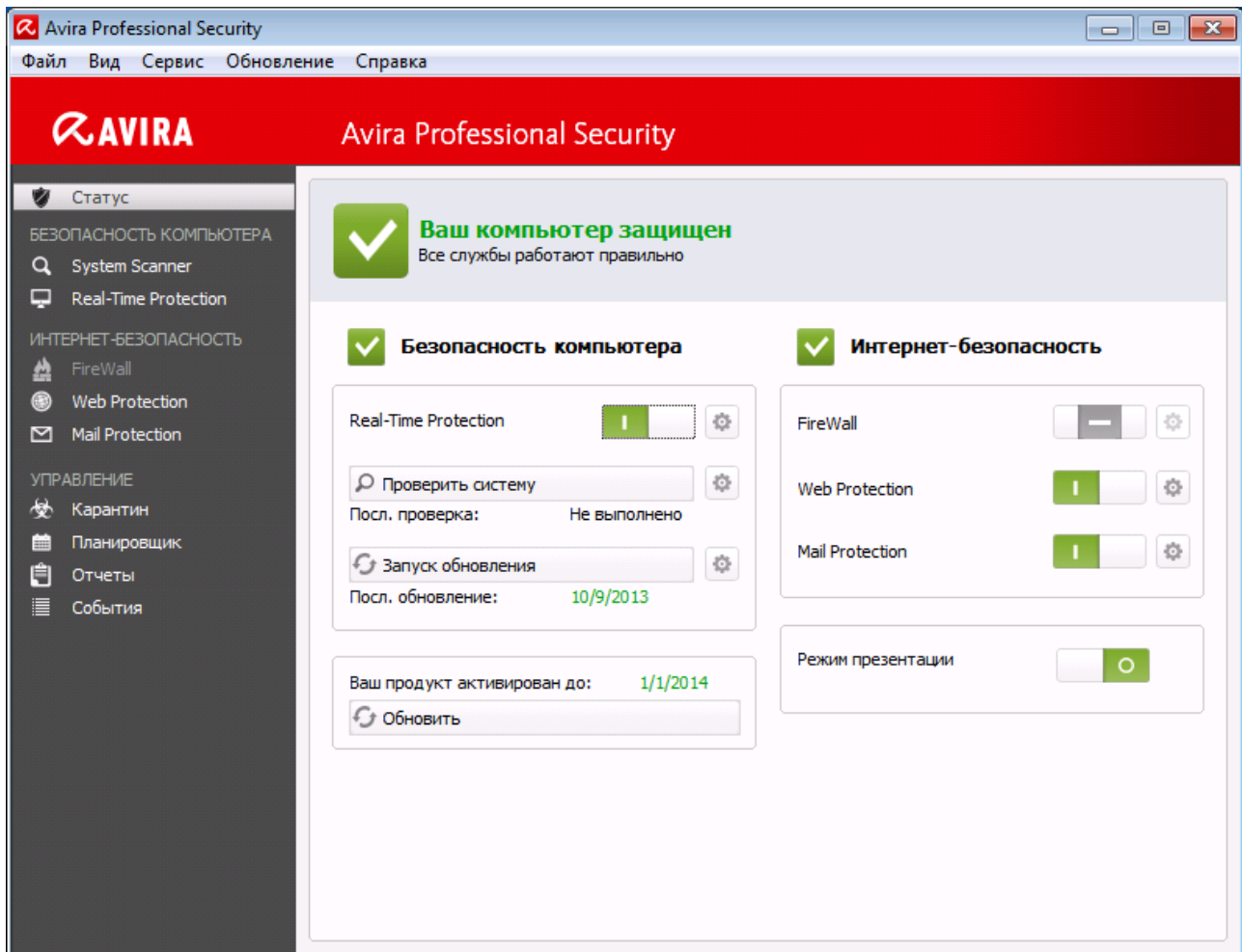
4.1 Интерфейс и работа с программой

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

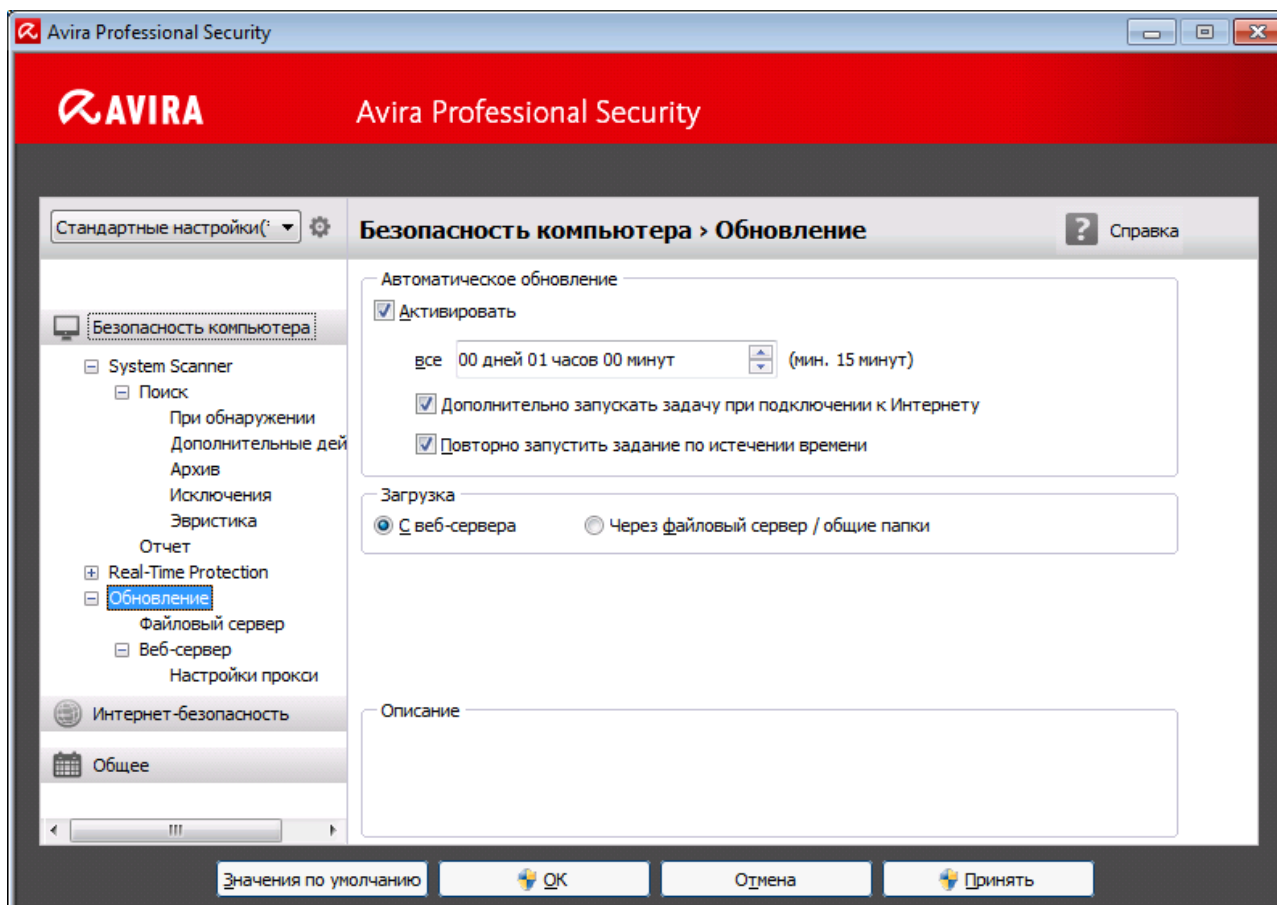
- **Состояние:** На начальном экране **Состояние** представлены все вкладки, с помощью которых вы можете контролировать функции программы (см. **Состояние**).
 - Окно **Состояние** показывает, какие модули активны, предоставляет информацию о последних проведенных обновлениях.
- **БЕЗОПАСНОСТЬ КОМПЬЮТЕРА:** 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".
- **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 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. Письма можно удалять из буфера модуля Mail Protection. (см. Mail Protection).
- **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** позволяет вам получить информацию о событиях, созданных модулями программы (см. События).

4.1.2 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 **ОК** 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.

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.

Если вы хотите подтвердить сделанные настройки:

- ▶ Нажмите кнопку **ОК**.
 - 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.

Профили меню настройки

Вы можете сохранить свои настройки в профиле настройки. В профиле настройки сохраняются все опции, относящиеся к одной группе. Настройки отображаются в строке меню в виде дерева каталогов. Вы можете добавить свои настройки к стандартным. Вы можете определять правила для переключения на определенную настройку:

При переключении настройки, основанном на правиле, настройки могут связываться с использованием соединения LAN или Интернета (идентификация через

стандартный шлюз): Вы можете создавать профили настроек для различных сценариев использования компьютера:

- использование в сети фирмы: обновление через сервер Intranet, функция Web Protection деактивирована
- использование дома: обновление через веб-сервер Avira Standard, функция Web Protection активирована

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

Указание

Системе контроля учетных записей пользователей (UAC) требуется ваше разрешение на включение или отключение служб Real-Time Protection, FireWall, Web Protection и Mail Protection (в операционных системах, начиная с Windows Vista).

Обзор опций меню настройки

Предусмотрены следующие опции меню настройки:

- **System Scanner:** Настройка прямого поиска
 - Опции поиска
 - Действие при обнаружении
 - Дополнительные действия
 - 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
- **Обновление:** Конфигурация настроек обновления
 - Загрузка с файлового сервера
 - Загрузка с веб-сервера
 - Настройки прокси-сервера

- **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 строки примечания в отправленных письмах
 - Настройка функции отчетов
- **Общее:**
 - Настройка отправки писем через SMTP
 - 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
 - Предупреждения:

Конфигурация сетевых уведомлений компонента(ов):

- System Scanner
- Real-Time Protection

Конфигурация почтовых уведомлений компонента(ов):

- System Scanner
- Real-Time Protection
- Модуль обновления
- Настройка акустических сигналов при обнаружении вируса

4.1.3 Tray Icon

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

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

- **Активировать брандмауэр Windows:** активирует или деактивирует брандмауэр Windows (эта функция доступна только, начиная с Windows 8).
- **Блокировать весь трафик:** Включен: блокирует всю передачу данных за исключением передачи в собственной компьютерной системе (Local Host/IP 127.0.0.1).
- **Запустить Avira Professional Security:** Открывает [Центр управления](#).
- **Настройка Avira Professional Security :** открывает [Настройку](#).
- **Запустить обновление:** Запускает [Обновление](#).
- **Выбор настроек:** Открывает подменю с доступными профилями настроек. Нажмите на настройку, чтобы активировать ее. Команда меню деактивируется, если вы уже определили правила для автоматического переключения на настройку.
- **Справка:** Открывает справочную онлайн-систему.
- **Avira Professional 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 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.

4.2.1 Активация лицензии

Порядок активации лицензии продукта Avira:

Активируйте лицензию на продукт Avira с помощью файла лицензии *.KEY*. Файл лицензии можно получить от Avira по электронной почте. В файле лицензии содержится лицензия для всех продуктов, заказанных вами в одном процессе заказа.

Если вы еще не установили продукт Avira:

- ▶ Сохраните файл лицензии в папке на локальном диске компьютера.
- ▶ Установите продукт Avira.
- ▶ При установке укажите путь к сохраненному файлу лицензии.

Если вы уже установили продукт Avira:

- ▶ Дважды щелкните файл лицензии в файловом менеджере или электронном письме активации и следуйте инструкциям на экране управления лицензиями.

- ИЛИ -

В центре управления программы Avira выберите элемент меню **Справка > Загрузить файл лицензии**


Примечание

В Windows Vista отображается диалоговое окно контроля учетных записей. Войдите в систему как администратор, если это необходимо. Щелкните **Далее**.

- ▶ Выделите файл лицензии и щелкните **Открыть**.
 - ↳ Отображается сообщение.
- ▶ Щелкните **ОК** для подтверждения.
 - ↳ Лицензия активирована.
- ▶ При необходимости перезагрузите систему.

4.2.2 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: 60 минут.

- ▶ 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

4.2.3 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: 60 минут.

Указание

Вы можете выполнить обновление вручную через Центр безопасности Windows.

4.2.4 Использование профиля сканирования для сканирования на наличие вирусов и вредоносного ПО

Профиль сканирования — это набор дисков и папок, которые необходимо сканировать.

Существует несколько способов сканирования через профиль сканирования:

Использование предустановленного профиля сканирования

Если предустановленные профили соответствуют вашим требованиям.

Адаптация и использование профиля сканирования (выборочная проверка)

При необходимости сканирования с пользовательским профилем.

Создание и использование нового профиля сканирования

Если вы хотите создать собственный профиль сканирования.

В зависимости от операционной системы для запуска профиля сканирования доступны различные значки.

- В Windows XP:



Этот значок запускает сканирование с помощью профиля сканирования.

- В Windows Vista:

В Microsoft Windows Vista через Центр управления доступны только ограниченные права, например, для доступа к папкам и файлам. Определенные действия и доступ к файлам доступны через Центр управления при наличии расширенных прав администратора. Эти расширенные права администратора необходимо предоставлять в начале каждого сканирования через профиль сканирования.





- Этот значок запускает ограниченное сканирование с помощью профиля сканирования. Проверяются только те папки и файлы, доступ к которым разрешен операционной системой.



- Этот значок запускает сканирование с расширенными правами администратора. После подтверждения будут проверены все папки и файлы выбранного профиля сканирования.



Порядок сканирования на вирусы и вредоносное ПО с помощью профиля сканирования:

- ▶ Перейдите в центр управления и выберите раздел **БЕЗОПАСНОСТЬ КОМПЬЮТЕРА > System Scanner**.
 - Отображаются предустановленные профили сканирования.
- ▶ Выберите один из предустановленных профилей сканирования.
 - ИЛИ-
 - Настройте профиль сканирования **Выборочная проверка**.
 - ИЛИ-
 - Создайте новый профиль сканирования
- ▶ Щелкните значок (Windows XP: , Windows Vista: ).
- ▶ Появится окно **Luke Filewalker** и запустится сканирование системы.
 - По окончании сканирования отображаются результаты.

Если вы хотите настроить профиль сканирования:

- ▶ В профиле сканирования **Выборочная проверка** разверните дерево каталогов настолько, чтобы были видны все диски и папки, которые необходимо сканировать.
- Щелкните значок **+**. Отобразится следующий уровень каталогов.
- Щелкните значок **-**. Следующий уровень каталогов будет скрыт.
- ▶ Выделите узлы и папки для сканирования, устанавливая соответствующие флажки на требуемом уровне каталогов:
Возможны следующие варианты выбора каталогов:
 - Каталог с подкаталогами (черный флажок)
 - Только отдельные подкаталоги внутри каталога (серый флажок, у подкаталогов черные флажки)
 - Без каталогов (без флажков)

Если вы хотите создать новый профиль сканирования:

- ▶ Щелкните значок  **Создать новый профиль**.
 - ↳ Среди имеющихся профилей появляется **Новый профиль**.
- ▶ При необходимости переименуйте профиль сканирования, щелкнув значок .
- ▶ Отметьте узлы и папки, которые необходимо проверить, поставив флажок в соответствующем поле.
Возможны следующие варианты выбора каталогов:
 - Каталог с подкаталогами (черный флажок)
 - Только отдельные подкаталоги внутри каталога (серый флажок, у подкаталогов черные флажки)
 - Без каталогов (без флажков)

4.2.5 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.
- ▶ Перетащите левой кнопкой мышки выделенный файл или выделенный каталог на Центр управления.
 - ↳ Появится окно **Luke Filewalker** и запустится прямой поиск.
 - ↳ По окончании проверки будут показаны результаты.

4.2.6 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.

4.2.7 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

4.2.8 Целенаправленное сканирование руткитов и активного вредоносного ПО

Для сканирования активных руткитов используйте предустановленный профиль сканирования **Поиск "руткитов" и активного вредоносного ПО**.

Порядок систематического сканирования на наличие активных руткитов:

- ▶ В центре управления выберите раздел *Безопасность компьютера* > **System Scanner**.
 - Появятся предустановленные профили сканирования.
- ▶ Выберите предустановленный профиль сканирования **Поиск "руткитов" и активного вредоносного ПО**.
- ▶ При необходимости выделите другие узлы и папки для сканирования, установив флажок на уровне папки.
- ▶ Щелкните значок (Windows XP: , Windows Vista: ).
 - Появится окно **Luke Filewalker** и запустится сканирование системы.
 - По окончании сканирования отображаются результаты.

4.2.9 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. При активации опции **Показывать предупреждение** при

обнаружении вируса вы будете получать предупреждение, в котором будет показано выполненное действие.

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 **Подробнее** 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. При активации опции **Показывать предупреждение** при обнаружении вируса вы будете получать уведомление на рабочем столе.

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. При активации опции **Показывать прогресс** при обнаружении вируса вы будете получать предупреждение, в котором можно будет подтвердить выполняемое действие.

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](#)).

- **Единой 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.**.

4.2.10 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 **ОК**.
 - 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 одновременно отправить несколько файлов, выделив их и нажав кнопку **Отправить объект**.


Для копирования объекта из карантина в другой каталог:

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

Указание

Объект карантина не будет идентичным 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](#)).



4.2.11 Восстановление файлов в карантине

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

- В Windows XP:
 -  С помощью этого значка выполняется восстановление файлов в первоначальную папку.
 -  С помощью этого значка файлы восстанавливаются в указанную папку.

- В Windows Vista:

В Microsoft Windows Vista через Центр управления доступны только ограниченные права, например, для доступа к папкам и файлам. Определенные действия и доступ к файлам доступны через Центр управления при наличии расширенных прав администратора. Эти расширенные права администратора необходимо предоставлять в начале каждого сканирования через профиль сканирования.

-  С помощью этого значка файлы восстанавливаются в указанную папку.
-  С помощью этого значка выполняется восстановление файлов в первоначальную папку. Если для доступа к этой папке необходимы расширенные права администратора, отображается соответствующий запрос.


Восстановление файлов из карантина:

Предупреждение

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

- ✓ Файл проверен повторно и вылечен.
- ▶ В центре управления выберите раздел **УПРАВЛЕНИЕ > Карантин**.

Примечание


Электронные письма и вложения восстанавливаются только с помощью функции , если файл имеет расширение **.eml*.

Порядок восстановления файла в его прежнюю папку:

- ▶ Выделите файл и щелкните значок (Windows XP: , Windows Vista: )


Эта функция недоступна для электронных писем.

Примечание

Электронные письма и вложения восстанавливаются только с помощью функции , если файл имеет расширение **.eml*.


- Отображается вопрос, хотите ли вы восстановить файл.
- ▶ Щелкните **Да**.
 - Файл будет восстановлен в папку, из которой он был помещен на карантин.

Порядок восстановления файла в определенную папку:

- ▶ Выделите файл и щелкните .
 - ↳ Отображается вопрос, хотите ли вы восстановить файл.
- ▶ Щелкните **Да**.
 - ↳ Отображается стандартное окно Windows *Сохранить как* для выбора папки.
- ▶ Выберите папку, в которую необходимо восстановить файл, подтвердите выбор.
 - ↳ Файл будет восстановлен в указанную папку.

4.2.12 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](#)).

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

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

- ✓ 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 ?).

4.2.14 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.

4.2.15 События: Фильтрация 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:

- Web Protection
- Real-Time Protection
- Mail Protection
- FireWall
- Helper Service
- Scheduler
- System Scanner
- Модуль обновления
- ProActiv

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.

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

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.

4.2.17 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 predetermined 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.

5. Обнаружение

5.1 Обзор

При обнаружении вирусов продукт Avira автоматически может выполнять определенные действия или реагировать интерактивно. В интерактивном режиме при обнаружении вируса откроется диалог, в котором вы можете выбрать, какое действие применить к вирусу (удалить, пропустить и т.д.), или инициировать это действие. В автоматическом режиме существует возможность при обнаружении вируса выводить уведомление. В уведомлении отображается действие, которое автоматически было применено к объекту.

этой главы вы найдете подробную информацию об уведомлениях об обнаружении подозрительных объектов, упорядоченную по модулям.

- см. главу [System Scanner](#): Интерактивный режим
- см. главу [System Scanner](#): Автоматический режим
- см. главу [System Scanner](#): Отправка файлов в Protection Cloud
- см. главу [Real-Time Scanner](#)
- см. главу [Real-Time Scanner](#) Подозрительное поведение
- см. главу [Mail Protection](#): Входящие письма
- см. главу [Mail Protection](#): Исходящие письма
- см. главу [Отправка почты](#): Сервер
- см. главу [Отправка почты](#): Отправитель
- см. главу [Web Protection](#)

5.2 Интерактивный режим

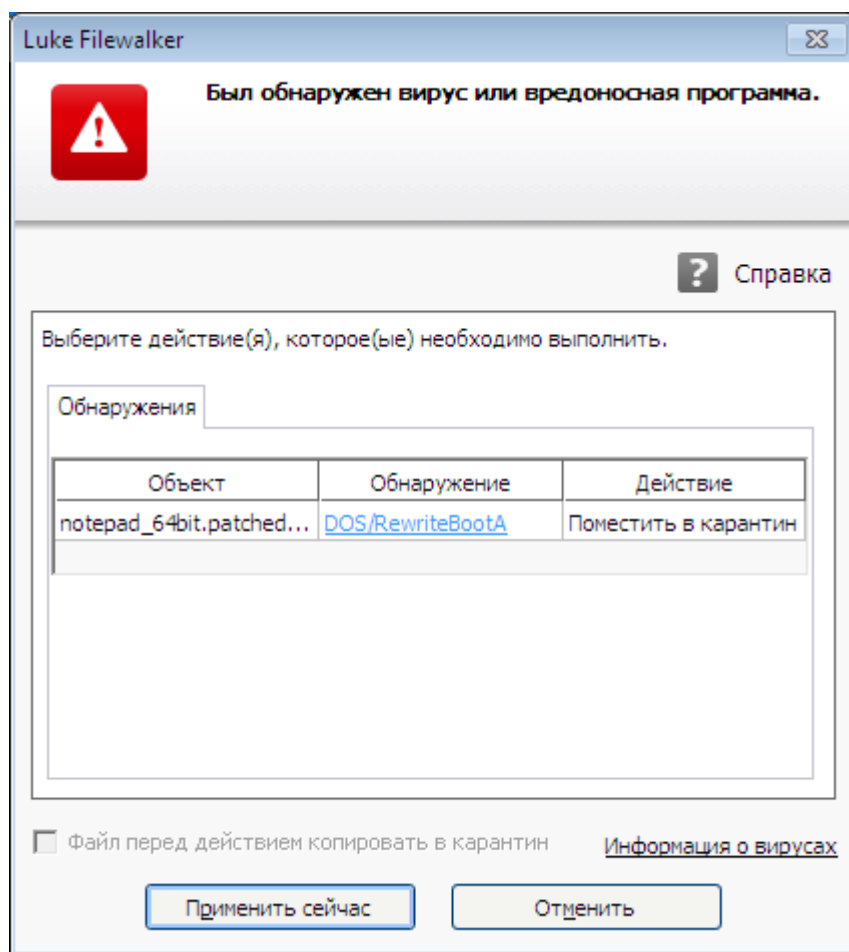
После завершения проверки модулем System Scanner выдается предупреждение со списком инфицированных файлов, если для обнаружения вирусов был выбран режим *интерактивный* (см. вкладку настроек [System Scanner > Поиск > Действия при обнаружении](#)).

С помощью контекстного меню вы можете выбрать действие для каждого обнаруженного файла. Вы можете применить выбранное действие ко всем файлам или завершить работу сканера System Scanner.

Примечание

При [включенном протоколировании](#) модуль System Scanner записывает каждое обнаружение вируса в [файл отчета](#).

5.2.1 Предупреждение



5.2.2 Обнаружения, ошибки, предупреждения

В вкладках **Обнаружение**, **Ошибки** и **Предупреждения** показываются сообщения, подробная информация и опции действий для обнаруженных вирусов:

- **Обнаружение:**
 - *Объект:* Имя инфицированного файла
 - *Обнаружение:* Имя обнаруженного вируса или вредоносной программы
 - *Действие:* Выбранное действие, которое будет применяться к инфицированному файлу
В контекстном меню для выбранного действия можно выбрать дополнительные варианты обработки вредоносного ПО.
- **Ошибки:** Сообщения об ошибках, которые возникли во время проверки
- **Предупреждения:** Предупреждения касательно обнаруженных вирусов

Примечание

В строке-подсказке для объекта отображается следующая информация:

имя инфицированного файла и полный путь к нему, имя вируса, действие, выполняемое при нажатии кнопки **Применить сейчас**.

Указание

В качестве выполняемого действия по умолчанию отображается стандартное действие модуля System Scanner. Действие сканера по умолчанию при работе с инфицированными файлами можно настроить во вкладке настроек [System Scanner > Поиск > Действие при обнаружении](#) в области *Разрешенные действия*.

5.2.3 Контекстное меню действий

Примечание

Если обнаруженный объект был определен системой эвристического поиска (HEUR/), был создан необычным паковщиком (PSK/) или является файлом со скрытым расширением (HEUR-DBLEXT/), то в [интерактивном режиме](#) доступны только опции [Поместить в карантин](#) и [Пропустить](#). В [автоматическом режиме](#) обнаруженный инфицированный или вредоносный объект автоматически помещается в [Карантин](#). Это ограничение препятствует тому, чтобы обнаруженные файлы, которые, возможно, были ошибочно отнесены к вредоносным программам, сразу же удалялись из вашего компьютера. Файл может быть в любое время восстановлен с помощью [менеджера карантина](#). В зависимости от настроек пользователю предлагаются различные опции.

Лечить

Если эта опция включена, System Scanner пытается вылечить инфицированный файл.

Указание

Опцию **Лечить** можно выбрать только, если лечение файла возможно.

Карантин

При включенной опции System Scanner перемещает файл в [карантин](#). Файл может быть восстановлен [менеджером карантина](#), если он имеет информативную ценность, или его можно отправить в центр исследования вирусов компании Avira. В зависимости от типа файла в [менеджере карантина](#) есть возможность выбора разных действий.

Удалить

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

Переписать и удалить

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

Переименовать

Если эта опция включена, System Scanner переименовывает файл. Прямой доступ к этому файлу (например, с помощью двойного щелчка) становится невозможен. Файл может быть позднее вылечен и переименован обратно.

Пропустить

Если эта опция включена, файл не подвергается изменениям.

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.

Предупреждение

При выборе опции Игнорировать или Всегда игнорировать соответствующие файлы будут находиться в системе в активном состоянии! Это может причинить существенный вред вашему компьютеру!

5.2.4 Особенности при обнаружении инфицированных загрузочных секторов, Rootkits и активного вредоносного ПО

При обнаружении инфицированных загрузочных секторов возможно исправление загрузочных секторов:

722 КБ | 1,44 МБ | 2,88 МБ | 360 КБ | 1,2 МБ исправление загрузочных секторов


Эти опции доступны для дисководов для дискет.

Загрузить восстановления CD

Выбрав эту опцию, вы попадете на веб-сайт компании Avira, где можно загрузить специальный инструмент для обнаружения и удаления вирусов из загрузочных секторов.

Если эти действия нужно применить к работающим процессам, то эти процессы будут завершены до выполнения действия.

5.2.5 Кнопки и ссылки

Кнопка/ссылка	Описание
Применить сейчас	Выбранные действия применяются для всех инфицированных файлов.
Прервать	System Scanner закрывается без выполнения дополнительных действий. Инфицированные файлы остаются в системе.
	Эта кнопка или ссылка открывает страницу справочной онлайн-системы.

Предупреждение

Выбирайте действие *Прервать* только в исключительных случаях. В случае прерывания инфицированные файлы останутся в активном состоянии в вашей системе! Это может причинить существенный вред вашему компьютеру!

5.2.6 Особенности при обнаружении при отключенном модуле Web Protection

Если вы отключили модуль Web Protection, Real-Time Protection сообщает об обнаруженном, активном вредоносном ПО с помощью всплывающего окна в процессе проверки системы. Вы можете создать точку восстановления системы перед исправлением.

- ✓ Функция восстановления системы должна быть включена в вашей операционной системе Windows.
- ▶ Щелкните по кнопке **Отображать подробности** во всплывающем окошке.
 - ↪ Откроется окно *Идет проверка системы*.
- ▶ Включите опцию **Создать точку восстановления системы перед исправлением**.
- ▶ Нажмите **Применить**.
 - ↪ Была создана точка восстановления системы. Теперь при необходимости можно инициировать в операционной системе Windows восстановление системы.

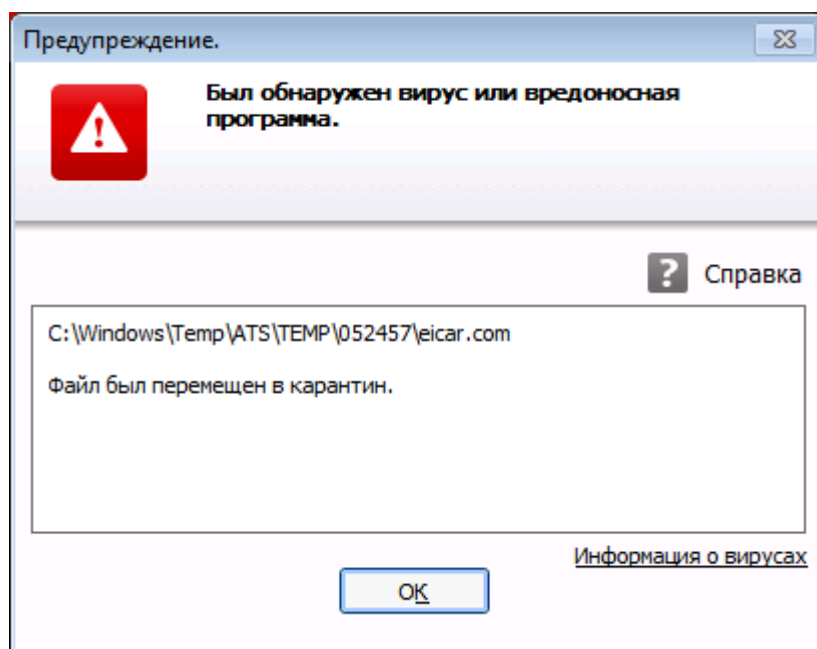
5.3 Автоматический режим

Во время проверки файла модулем System Scanner при каждом обнаружении вируса вы получаете предупреждение, если для обнаружения вирусов выбран режим *автоматический* с опцией **Показывать предупреждение** (см. вкладку настроек [System Scanner > Поиск > Действия при обнаружении](#)). В автоматическом режиме с уведомлением нет возможности выбора действий с вирусом. Выполняется действие, выбранное в настройках для обработки вирусов. В уведомлении отображается действие, которое автоматически было применено к объекту.


Примечание

При [включенном протоколировании](#) модуль System Scanner записывает каждое обнаружение вируса в [файл отчета](#).

5.3.1 Предупреждение



5.3.2 Кнопки и ссылки

Кнопка / Ссылка	Описание
	Эта кнопка или ссылка открывает соответствующую страницу справочной online-системы.

5.4 Отправка файлов в Protection Cloud

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. Неизвестные программные файлы загружаются для проверки в систему Protection Cloud.

Если в процессе выборочной установки или настройки **расширенной защиты** вы выбрали опцию **Подтверждать вручную, если Avira отправляются подозрительные файлы**, вы можете проверить список подозрительных файлов и выбрать самостоятельно файлы, которые нужно загрузить в Protection Cloud. По умолчанию для загрузки помечаются все подозрительные файлы.

Примечание

Если вы активировали **расширенное** протоколирование при настройке модуля System Scanner, в файле отчета отобразится *(Cloud)*-суффикс для идентификации Protection Cloud.

5.4.1 Отображаемая информация

Список подозрительных файлов, которые нужно загрузить в Protection Cloud.

- *Отправить?:* Вы можете выбрать, какие файлы нужно загрузить в Protection Cloud.
- *Файл:* Имя подозрительного файла.
- *Путь:* Путь подозрительного файла.

Всегда отправлять файлы автоматически

Пока эта опция активна, после каждой **быстрой проверки** подозрительные файлы автоматически, без подтверждения вручную, отправляются на проверку в Protection Cloud.

5.4.2 Кнопки и ссылки

Кнопка / Ссылка	Описание
Отправить	Отмеченные файлы отправляются в Avira Protection Cloud.
Отмена	System Scanner закрывается без выполнения дополнительных действий. Инфицированные файлы оставляются в вашей системе.
Справка	Открывается эта страница справочной онлайн-системы.
Что такое Protection Cloud?	Открывается веб-сайт с информацией о Cloud Protection.

Соответствующие темы:

- [Настройка расширенной защиты](#)
- [Выборочная установка](#)
- [Настройка отчета](#)
- [Вид отчетов](#)

5.5 Real-Time Protection

При обнаружении вируса модулем Real-Time Protection запрещается доступ к файлу и показывается уведомление, если для обнаружения вирусов выбран режим *интерактивный* или режим *автоматический* с опцией **Показывать предупреждение** (см. вкладку настроек [Real-Time Protection > Поиск > Действия при обнаружении](#)).

Уведомление

В уведомлении отображается следующая информация:

- Дата и время обнаружения
- Путь и имя инфицированного или подозрительного файла
- Имя вредоносной программы

Указание

Выбор режима запуска по умолчанию для Real-Time Protection (обычный запуск) и быстрая регистрация счета пользователя при запуске

компьютера, в частности, приводят к тому, что программы, автоматически запускаемые при загрузке системы не проверяются, так как они запускаются еще до полной загрузки модуля Real-Time Protection.

В интерактивном режиме доступны следующие опции:

Удалить

Соответствующий файл передается на компонент **System Scanner** и удаляется компонентом System Scanner. Дополнительное сообщение не показывается.

Подробности

Соответствующий файл передается компоненту **System Scanner**. System Scanner сообщает об обнаружении в окне, в котором доступны различные опции для обработки соответствующего файла.

Указание

Соблюдайте указания по обработке вирусов в [Обнаружение > System Scanner](#).

Указание

Для обработки вируса предлагается действие, которое вы выбрали в качестве действия по умолчанию в [Real-Time Protection > Поиск > Действие при обнаружении](#). С помощью контекстного меню можно выбирать другие действия.

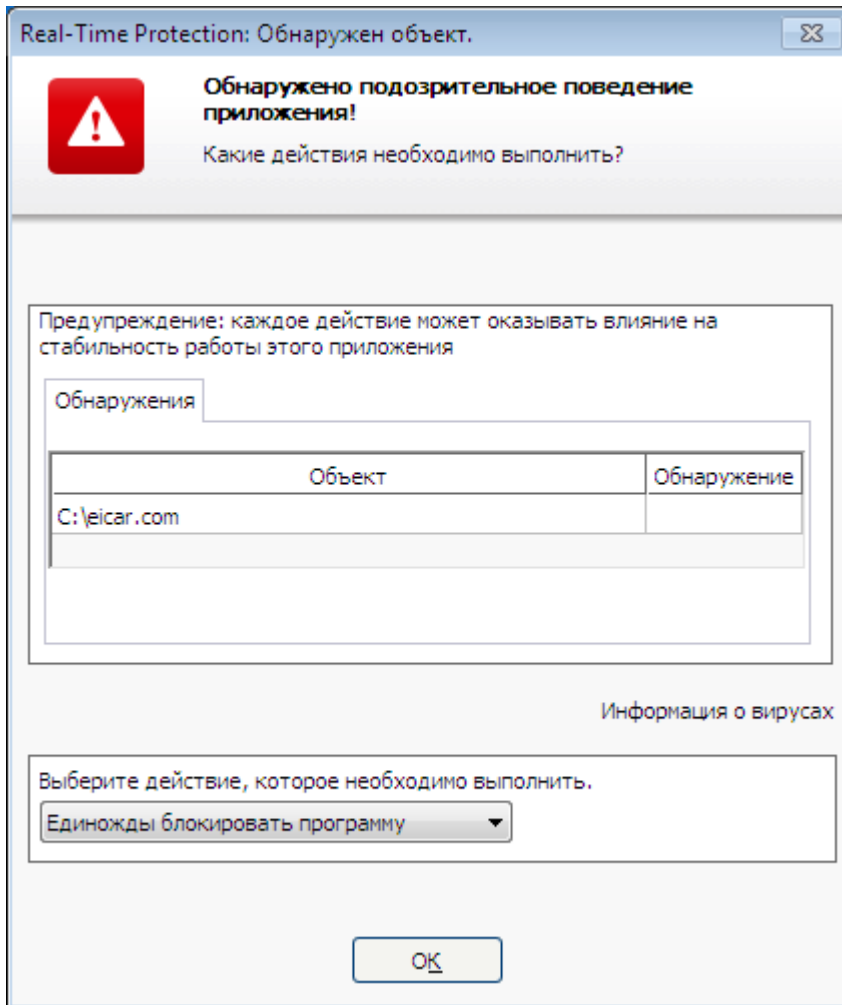
Закрыть

Сообщение закрывается. Обработка вирусов прекращается.

5.6 Подозрительное поведение

При активации компонента ProActiv в модуле Real-Time Scanner осуществляется контроль за действиями приложений и проверка на наличие подозрительного, типичного для вредоносного ПО поведения. При возникновении типичного для вредоносного ПО поведения выдается предупреждение. Вы можете среагировать на обнаружение различными способами.

5.6.1 Предупреждение модуля Real-Time Scanner: Обнаружено подозрительное поведение приложения



5.6.2 Имя и путь обнаруженной подозрительной программы

В среднем окне сообщения отображается имя и путь приложения, выполняющего подозрительные действия.

5.6.3 Возможности выбора

Высоконадежный поставщик

Если эта опция включена, 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 приложений: Разрешенные приложения](#)).

Единожды блокировать программу

Если эта опция включена, программа блокируется, т.е. выполнение программы завершается. Компонент ProActiv продолжает контролировать действия программы.

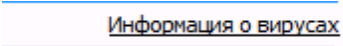

Всегда блокировать эту программу

Если эта опция включена, программа блокируется, т.е. выполнение программы завершается. Программа добавляется в список блокируемых приложений и больше не будет выполняться (см. [Фильтр приложений: Блокируемые приложения](#)).

Пропустить

Если эта опция включена, выполнение программы продолжается. Компонент ProActiv продолжает контролировать действия программы.

5.6.4 Кнопки и ссылки

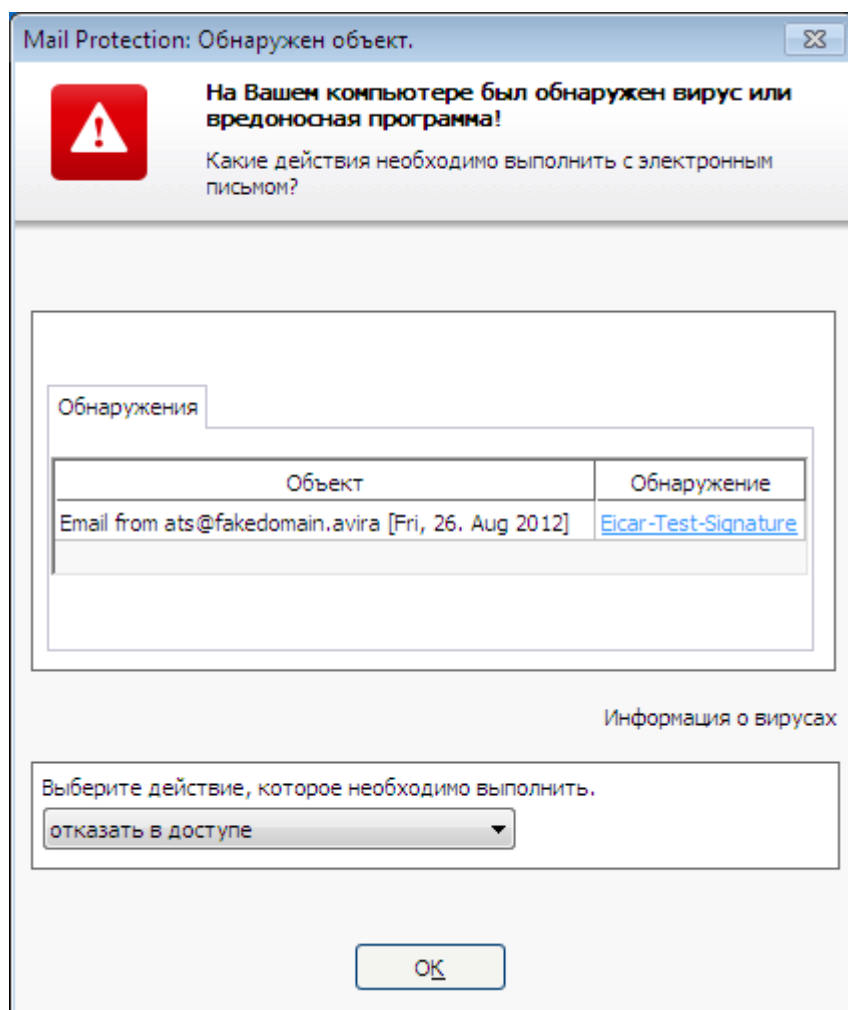
Кнопка / Ссылка	Описание
	<p>По этой ссылке вы попадаете при установленном Интернет-соединении на веб-страницу, содержащую подробную информацию о вирусе или вредоносной программе.</p>
	<p>Эта кнопка или ссылка открывает соответствующую страницу справочной online-системы.</p>

5.7 Входящие письма

При обнаружении вируса модулем Mail Protection вы получаете предупреждение, если для обнаружения вирусов выбран режим *интерактивный* (см. вкладку настроек [Mail Protection > Поиск > Действия при обнаружении](#)). В интерактивном режиме вы можете выбрать в окне диалога, что делать с инфицированным письмом или приложением.

Размещенное ниже уведомление вы получите при обнаружении вируса во входящем письме.

5.7.1 Предупреждение



5.7.2 Обнаружения, ошибки, предупреждения

Во вкладках **Обнаружения**, **Ошибки** и **Предупреждения** показываются сообщения и подробная информация о подозрительных или инфицированных письмах:

- **Обнаружения:** Объект: Соответствующее письмо с указанием отправителя и времени отправки письма
Обнаружение: Имя обнаруженного вируса или вредоносной программы
- **Ошибка:** Сообщения об ошибках, которые возникли во время проверки модулем Mail Protection
- **Предупреждения:** Предупреждения, относящиеся к поврежденным объектам

5.7.3 Возможности выбора

Примечание

Если обнаруженный объект был определен системой эвристического поиска (HEUR/), был создан необычным паковщиком (PSK/) или является файлом со скрытым расширением (HEUR-DBLEXT/), то в [интерактивном режиме](#) доступны только опции [Поместить в карантин](#) и [Пропустить](#). В [автоматическом режиме](#) обнаруженный инфицированный или вредоносный объект автоматически помещается в [Карантин](#). Это ограничение препятствует тому, чтобы обнаруженные файлы, которые, возможно, были ошибочно отнесены к вредоносным программам, сразу же удалялись из вашего компьютера. Файл может быть в любое время восстановлен с помощью [менеджера карантина](#).

Поместить на карантин

Если эта опция включена, письмо со всеми приложениями помещается в [Карантин](#). Оно может быть позже доставлено через [Менеджер карантина](#). Инфицированное письмо удаляется. Тело письма и приложения к нему, если они есть, заменяются [Стандартным текстовым шаблоном](#).

Удалить письмо

Если эта опция включена, инфицированное письмо при обнаружении вируса / вредоносной программы удаляется. Тело письма и возможные приложения заменяются [Стандартным текстовым шаблоном](#).

Удалить приложение

Если эта опция включена, инфицированное приложение заменяется [текстовым шаблоном](#). Если поврежден текст письма, то оно удаляется и заменяется [текстовым шаблоном](#). Письмо доставляется адресату.

Поместить приложение на карантин

Если выбрана эта опция, инфицированное вложение помещается в [Карантин](#), а затем удаляется (заменяется [текстовым шаблоном](#)). Текст письма доставляется адресату. Инфицированное приложение может быть позже доставлено адресату из [Менеджера карантина](#).

Пропустить

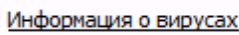

Если эта опция включена, инфицированное письмо доставляется адресату, несмотря на обнаружение в нем вируса или вредоносной программы.

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!

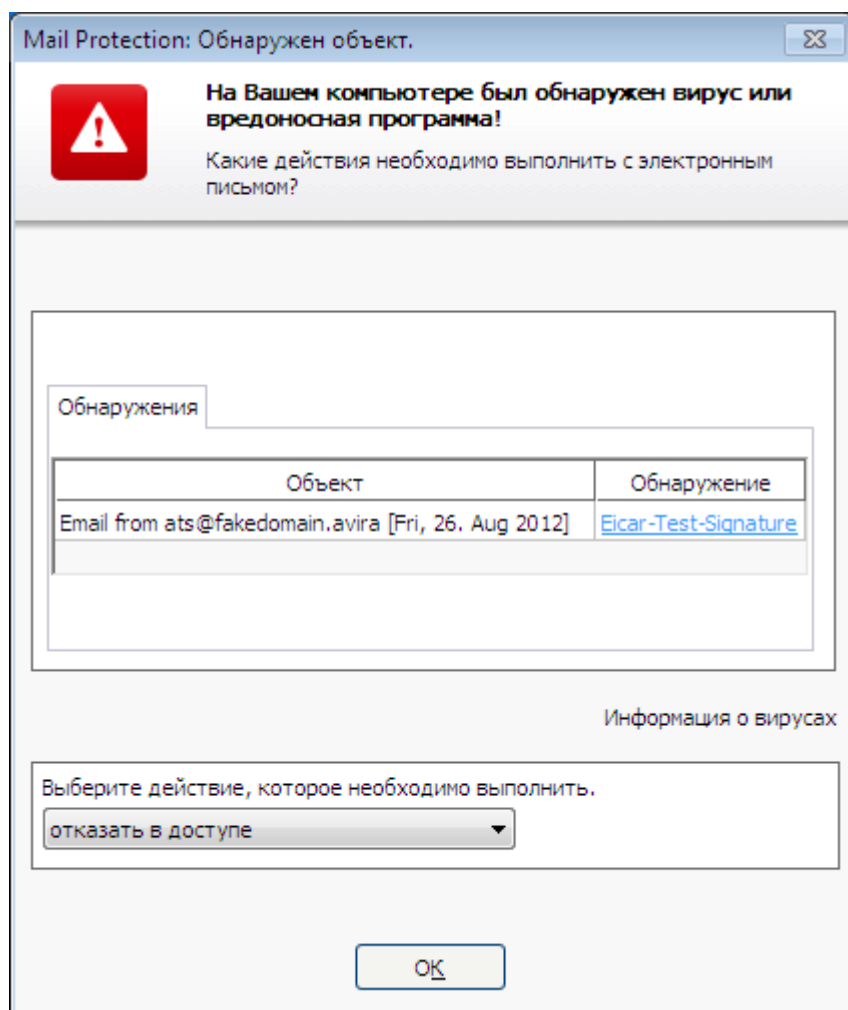
5.7.4 Кнопки и ссылки

Кнопка/ссылка	Описание
	По этой ссылке вы попадаете - при установленном Интернет-соединении - на веб-страницу, содержащую подробную информацию о вирусе или вредоносной программе.
	Эта кнопка или ссылка открывает страницу справочной онлайн-системы.

5.8 Исходящие письма

При обнаружении вируса модулем Mail Protection вы получаете предупреждение, если для обнаружения вирусов выбран режим *интерактивный* (см. вкладку настроек [Mail Protection > Поиск > Действия при обнаружении](#)). В интерактивном режиме вы можете выбрать в окне диалога, что делать с инфицированным письмом или приложением.

5.8.1 Предупреждение



5.8.2 Обнаружения, ошибки, предупреждения

Во вкладках **Обнаружения**, **Ошибки** и **Предупреждения** показываются сообщения и подробная информация о подозрительных или инфицированных письмах:

- **Обнаружения:** Объект: Соответствующее письмо с указанием отправителя и времени отправки письма
Обнаружение: Имя обнаруженного вируса или вредоносной программы
- **Ошибка:** Сообщения об ошибках, которые возникли во время проверки модулем Mail Protection
- **Предупреждения:** Предупреждения, относящиеся к поврежденным объектам

5.8.3 Возможности выбора

Поместить письмо на карантин (не отправлять)

Если эта опция включена, копия письма со всеми вложениями помещается в [Карантин](#), а письмо 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.

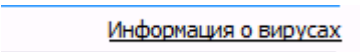

Пропустить

Если опция включена, инфицированное письмо будет отправлено даже в случае обнаружения в нем вирусов и вредоносных программ.

Предупреждение

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

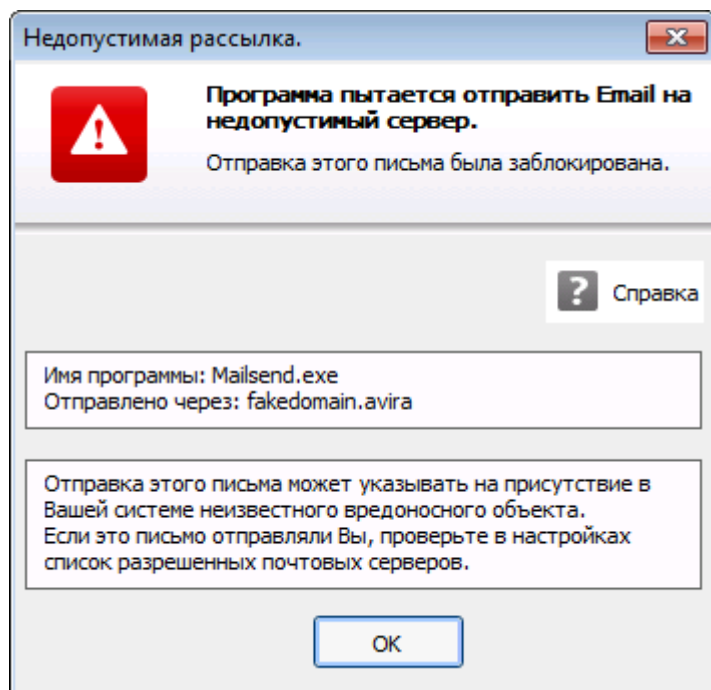
5.8.4 Кнопки и ссылки

Кнопка/ссылка	Описание
	<p>По этой ссылке вы попадаете - при установленном Интернет-соединении - на веб-страницу, содержащую подробную информацию о вирусе или вредоносной программе.</p>
	<p>Эта кнопка или ссылка открывает страницу справочной онлайн-системы.</p>

5.9 Отправитель

Если вы используете функцию AntiBot модуля Mail Protection, модуль Mail Protection блокирует письма, отправляемые с неавторизованных серверов SMTP. Проверка выполняется с помощью списка разрешенных отправителей, составленного пользователем в настройках [Mail Protection > Поиск > AntiBot](#). О заблокированном письме сообщается в диалоговом окне.

5.9.1 Предупреждение



5.9.2 Используемая программа, используемый сервер SMTP и адрес отправителя письма

В среднем окне сообщения отображается следующая информация:

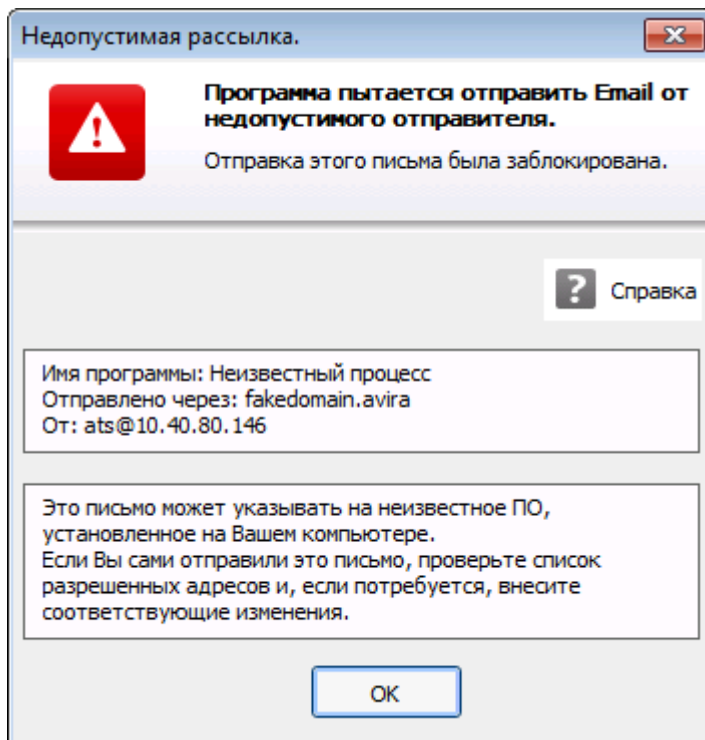
- Название программы, которая использовалась для отправки письма
- Название сервера SMTP, который использовался для отправки письма
- Адрес электронной почты отправителя

Если вы отправили письмо с помощью своей почтовой программы, сравните список разрешенных отправителей в настройках в [Mail Protection > Поиск > AntiBot](#) с адресами отправителей, которые вы используете в учетных записях своей почтовой программы. Если список разрешенных отправителей в настройках неполон, внесите дополнительные адреса отправителей в список. Заблокированное письмо будет находиться в папке исходящих писем вашей почтовой программы. Для отправки заблокированного письма снова начните процесс отправки после дополнения списка в настройках.

5.10 Сервер

Если вы используете функцию AntiBot модуля Mail Protection, модуль Mail Protection блокирует письма, отправляемые с неавторизованных серверов SMTP. Проверка выполняется с помощью списка разрешенных серверов SMTP, содержащегося в настройках [Mail Protection > Поиск > AntiBot](#). О заблокированном письме сообщается в диалоговом окне.

5.10.1 Предупреждение



5.10.2 Используемая программа, используемый сервер SMTP

В среднем окне сообщения отображается следующая информация:

- Название программы, которая использовалась для отправки письма
- Название сервера SMTP, который использовался для отправки письма

Если вы отправили письмо с помощью своей почтовой программы, сравните список разрешенных серверов в настройках в [Mail Protection > Поиск > AntiBot](#) с адресами серверов SMTP, которые вы используете для отправки писем. Используемые серверы SMTP можно посмотреть в почтовой программе в используемых учетных записях электронной почты. Если список разрешенных серверов в настройках неполон, внесите дополнительные адреса используемых вами серверов SMTP в список. Заблокированное письмо будет находиться в папке исходящих писем вашей почтовой программы. Для отправки заблокированного письма снова начните процесс отправки после дополнения списка в настройках.

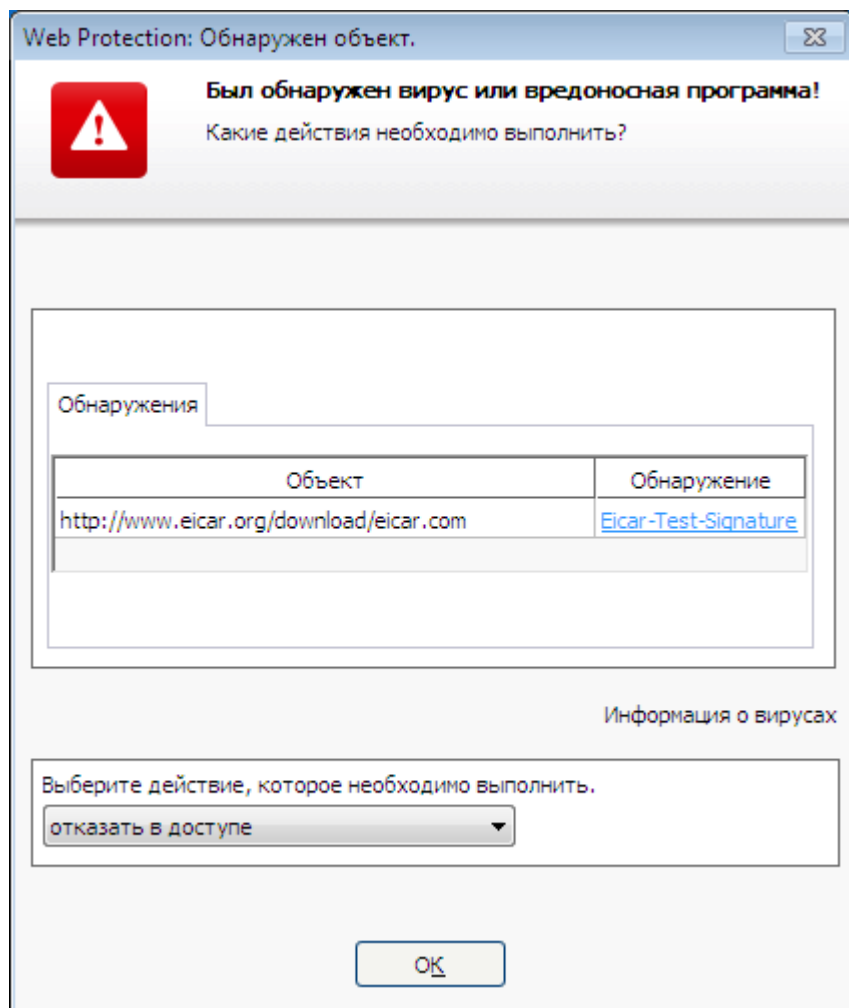
5.11 Web Protection

При обнаружении вируса модулем Web Protection вы получите, если для поиска вирусов выбран *интерактивный* режим или *автоматический* режим с опцией **отображения уведомлений** (см. раздел [Web Protection > Поиск > Действия при обнаружении](#)). В интерактивном режиме вы можете выбрать в диалоговом окне, что делать с данными, полученными от веб-сервера. В автоматическом режиме с уведомлением нет возможности выбора действий с вирусом. В сообщении вы можете подтвердить автоматически выполняемое действие или завершить работу Web Protection.

Указание

Диалог внизу экрана - это уведомление об обнаружении вируса в интерактивном режиме.

Предупреждение



Обнаружения, ошибки, предупреждения

Во вкладках **Обнаружения**, **Ошибки** и **Предупреждения** показываются сообщения и подробная информация касательно обнаруженных вирусов:

- **Обнаружение:** URL, а также имя обнаруженного вируса или вредоносной программы
- **Ошибка:** Сообщения об ошибках, которые возникли во время проверки модулем Web Protection
- **Предупреждения:** Предупреждения касательно обнаруженных вирусов

Возможные действия

Указание

Если обнаруженный объект был определен системой эвристического поиска (HEUR/), был создан необычным паковщиком (PSK/) или является файлом со скрытым расширением (HEUR-DBLEXT/), то в **интерактивном режиме** доступны только опции **Поместить в карантин** и **Пропустить**. В **автоматическом режиме** обнаруженный инфицированный или вредоносный объект автоматически помещается в **Карантин**. Это ограничение препятствует тому, чтобы обнаруженные файлы, которые, возможно, были ошибочно отнесены к вредоносным программам, сразу же удалялись из вашего компьютера. Файл может быть в любое время восстановлен с помощью **менеджера карантина**. В зависимости от настроек пользователю предлагаются различные опции.

Запретить доступ

Запрошенная веб-сервером страница или переданные данные и файлы не будут перенаправлены вашему браузеру. В окне веб-браузера отображается информация об отказе в доступе. Web Protection заносит сведения об обнаруженном объекте в файл отчета, если включена Функция отчетов.

Изолировать (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.

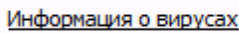

Пропустить

Запрошенная веб-сервером страница или переданные данные и файлы отправляются модулем Web Protection вашему веб-браузеру.

Предупреждение

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

Кнопки и ссылки

Кнопка/ссылка	Описание
	<p>По этой ссылке вы попадаете - при установленном Интернет-соединении - на веб-страницу, содержащую подробную информацию о вирусе или вредоносной программе.</p>
	<p>Эта кнопка или ссылка открывает страницу справочной онлайн-системы.</p>

6. System Scanner

6.1 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**

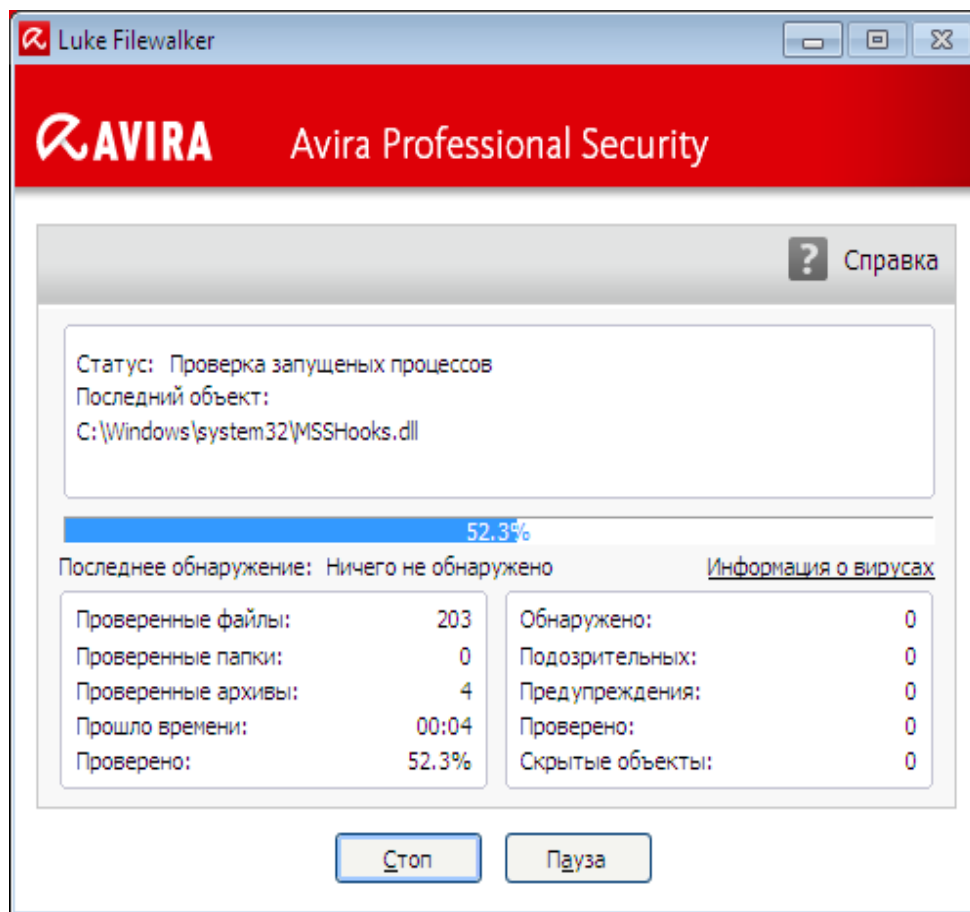
6.2 Luke Filewalker

Во время прямого поиска появляется окно состояния **Luke Filewalker**, в котором показывается точная информация о состоянии проверки.

Если в настройках модуля **System Scanner** в группе **Действие при обнаружении вируса** включена опция **Интерактивно**, то при обнаружении вируса или вредоносной программы вы получите вопрос о дальнейших действиях. Если включена опция **Автоматически**, то возможные обнаружения фиксируются в **Отчете System Scanner**.

После завершения поиска в дополнительном окне показываются результаты проверки (статистика), а также сообщения об ошибках и предупреждения.

6.2.1 Luke Filewalker: Окно состояния проверки



Отображаемая информация

Состояние: Существуют различные статусные сообщения:

- *Инициализация программы*
- *Поиск скрытых объектов!*
- *Проверка запущенных процессов*
- *Файл проверяется*
- *Инициализация архива*
- *Память разблокирована*

- *Файл распаковывается*
- *Проверяются загрузочные секторы*
- *Проверяется главный загрузочный сектор (MBR)*
- *Проверяется реестр*
- *Программа завершается!*
- *Проверка была завершена*

Последний объект: Имя и путь файла, который проверяется сейчас или был проверен недавно

Последнее обнаружение: Существуют различные сообщения, касающиеся последнего обнаружения:

- *Вирусы не обнаружены!*
- *Имя последнего обнаруженного вируса или вредоносной программы*

Проверенные файлы: Количество проверенных файлов

Проверенные папки: Количество проверенных папок

Проверенные архивы: Количество проверенных архивов

Необходимое время: Продолжительность проверки

Проверено до этого: Процент выполненной проверки

Обнаружено: Количество обнаруженных вирусов и вредоносных программ

Подозрительные файлы: Количество файлов, обнаруженных эвристическим модулем

Предупреждения: Количество предупреждений об обнаружении вирусов

Проверенные объекты: Количество объектов, которые были проверены во время поиска Rootkits

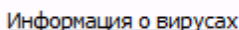

Скрытые объекты: Общее количество обнаруженных скрытых объектов

Указание

Rootkits скрывают процессы и объекты, например записи в реестре или файлы, но не каждый скрытый объект является указанием на существование Rootkits. Скрытые объекты могут указывать и на безвредные программы. Если во время проверки были обнаружены скрытые объекты, а предупредительные сообщения об обнаружении вирусов не поступали, то на основе отчета вам необходимо определить,

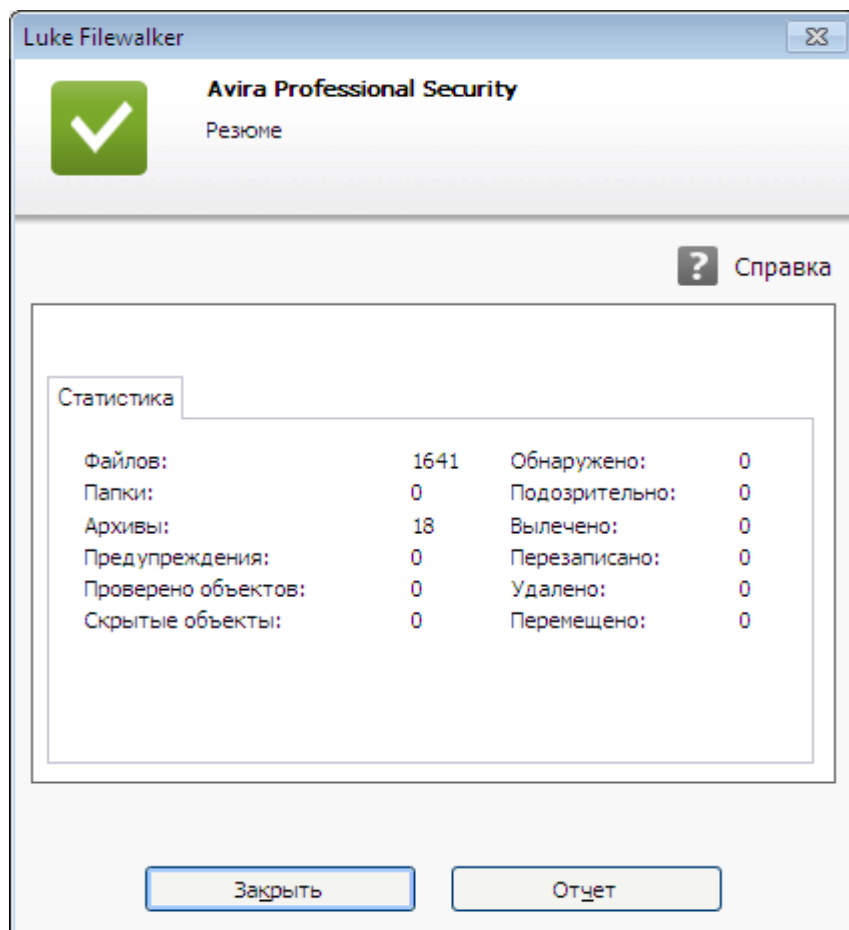
что это за объекты, и найти дополнительную информацию о найденных объектах.

Кнопки и ссылки

Кнопка/ссылка	Описание
	По этой ссылке вы попадаете - при установленном Интернет-соединении - на веб-страницу, содержащую подробную информацию о вирусе или вредоносной программе.
	Откроется страница справочной онлайн-системы.
Стоп	Процесс проверки останавливается.
Пауза	Процесс проверки прерывается и может быть продолжен с помощью кнопки Продолжить .
Продолжить	Прерванный процесс проверки продолжается.
Закреть	Компонент System Scanner закрывается.

Отчет	Отображается файл отчета о проверке.
--------------	--------------------------------------

6.2.2 Luke Filewalker: Статистика проверки



Отображаемая информация: статистика

Файлы: Количество проверенных файлов

Папки: Количество проверенных папок

Архивы: Количество проверенных архивов

Предупреждения: Количество предупреждений об обнаружении вирусов

Проверенные объекты: Количество объектов, которые были проверены во время поиска Rootkits

Скрытые объекты: Количество обнаруженных скрытых объектов (Rootkits)

Обнаружено: Количество обнаруженных вирусов и вредоносных программ

Подозрительные: Количество файлов, обнаруженных эвристическим модулем


Вылечено: Количество вылеченных файлов

Переписано: Количество переписанных файлов

Удалено: Количество удаленных файлов

Перемещено: Количество файлов, помещенных на карантин

Кнопки и ссылки

Кнопка/ссылка	Описание
	Откроется страница справочной онлайн-системы.
Закреть	Окно с результатами закроется.
Отчет	Отображается файл отчета о проверке.

7. Control Center

7.1 Обзор

Центр управления служит в качестве центра информации, настроек и управления. В дополнение к отдельным выбираемым [Вкладкам](#) центр имеет большое количество опций, доступных в [линейке меню](#).

Линейка меню

В линейке меню представлены следующие функции:

Файл

- [Выход](#) (Alt+F4)

Вид

- [Состояние](#)
- Безопасность компьютера
 - [System Scanner](#)
 - [Real-Time Protection](#)
- Интернет-безопасность
 - [FireWall](#)
 - [Web Protection](#)
 - [Mail Protection](#)
- Управление
 - [Карантин](#)
 - [Планировщик](#)
 - [Отчеты](#)
 - [События](#)
- [Обновить](#) (F5)

Сервис

- [Проверка загрузочных секторов...](#)
- [Список вирусов...](#)
- [Загрузить восстановления CD](#)
- [Настройка](#) (F8)

Обновление

- [Запустить обновление...](#)
- [Обновление вручную...](#)

Справка

- [Темы](#)
- [Помощь](#)
- [Руководство по загрузке](#)
- [Загрузить файл лицензии...](#)
- [Отправить сообщение обратной связи](#)
- [О Avira Professional Security](#)

Указание

Управление клавиатурой в меню можно включить с помощью клавиши [Alt]. Если навигация включена, Вы можете перемещаться в меню с помощью клавиш курсора. Кнопкой Enter Вы можете выбрать выделенный пункт меню.

Вкладки

На левой навигационной панели расположены следующие вкладки:

- [Состояние](#)

БЕЗОПАСНОСТЬ КОМПЬЮТЕРА

- [System Scanner](#)
- [Real-Time Protection](#)

ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

- [FireWall](#)
- [Web Protection](#)
- [Mail Protection](#)

УПРАВЛЕНИЕ

- [Карантин](#)
- [Планировщик](#)
- [Отчеты](#)
- [События](#)

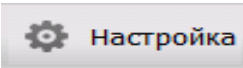
Описание вкладок

- **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".
- **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 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. Письма можно удалять из буфера модуля Mail Protection. (см. [Mail Protection](#)).
- **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](#)).

Кнопки и ссылки

Доступны следующие кнопки и ссылки.

Кнопка/ссылка	Горячие клавиши	Описание
		Открывается соответствующее диалоговое окно с настройками для вкладки.
	F1	Открывается соответствующая тема онлайн-справки.

7.2 Файл

7.2.1 Закреть

Пункт меню **Закреть** в меню **Файл** закрывает Центр управления.

7.3 Вид

7.3.1 Состояние

Стартовый экран центра управления **Состояние** показывает, защищена ли ваша система и какие модули Avira активны. В окне **Состояние** отображается информация о последнем произведенном обновлении. Дополнительно можно видеть, обладает ли пользователь действующей лицензией.

- **Безопасность компьютера:** [Real-Time Protection](#), [Последняя проверка](#), [Последнее обновление](#), [Ваш продукт активирован](#)
- **Интернет-безопасность:** [Web Protection](#), [Mail Protection](#), [FireWall](#), [Режим презентации](#),

Указание

Системе контроля учетных записей пользователей (UAC) требуется ваше разрешение на включение или отключение служб [Real-Time Protection](#), [FireWall](#), [Web Protection](#) и [Mail Protection](#) (в операционных системах, начиная с Windows Vista).

Безопасность компьютера

В этом разделе отображается информация о текущем состоянии служб и функций защиты, которые обеспечивают локальную защиту вашего компьютера от вирусов и вредоносного ПО.

Real-Time Protection


В этом разделе отображается информация о текущем состоянии модуля Real-Time Protection.

Модуль Real-Time Protection включается и выключается с помощью кнопки **Вкл./выкл.** Для дополнительных опций модуля Real-Time Protection нажмите **Real-Time Protection** на навигационной панели. Вы получите информацию о последних найденных вредоносных программах и инфицированных файлах. Нажмите кнопку **Конфигурация**, чтобы выполнить дополнительные настройки.

- **Конфигурация:** вы переходите в меню конфигурации, в котором можно установить параметры компонентов модуля Real-Time Protection.

Существуют следующие возможности:

Пиктограмма	Состояние	Опция	Описание
	<i>Включено</i>	Отключить	<p>Служба Real-Time Protection включена, то есть ваша система постоянно проверяется на наличие вирусов и вредоносных программ.</p> <div data-bbox="839 506 1399 936" style="background-color: #f0f0f0; padding: 10px;"> <p>Указание Службу Real-Time Protection можно отключить. Обратите внимание, что при отключенном модуле Real-Time Protection ваш компьютер больше не защищен от вирусов и вредоносных программ. Все файлы беспрепятственно попадают в систему и могут причинить вред.</p> </div>
	<i>Отключено</i>	Включить	<p>Служба Real-Time Protection отключена. Это означает, что служба загружена, но не активна.</p> <div data-bbox="839 1140 1399 1496" style="background-color: #f0f0f0; padding: 10px;"> <p>Предупреждение Поиск вирусов и вредоносных программ не выполняется. Любые файлы могут беспрепятственно проникнуть в систему. Ваш компьютер не защищен от вирусов и вредоносных программ.</p> </div> <div data-bbox="839 1532 1399 1888" style="background-color: #f0f0f0; padding: 10px;"> <p>Указание Чтобы возобновить защиту от вирусов и вредоносных программ, воспользуйтесь кнопкой ВКЛ./ВЫКЛ. рядом с модулем Real-Time Protection в разделе окна состояния «Безопасность компьютера».</p> </div>

	Служба остановлена	Запустить	Служба Real-Time Protection остановлена. <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Предупреждение Поиск вирусов и вредоносных программ не выполняется. Любые файлы могут беспрепятственно проникнуть в систему. Ваш компьютер не защищен от вирусов и вредоносных программ.</p> </div> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc; margin-top: 10px;"> <p>Указание Чтобы возобновить защиту от вирусов и вредоносных программ, нажмите кнопку ВКЛ./ВЫКЛ. Текущее состояние должно измениться на <i>Включено</i>.</p> </div>
	Неизвестно	Справка	Данное состояние отображается при возникновении неизвестной ошибки. В этом случае обратитесь в нашу службу поддержки .

Последняя проверка

В этом разделе отображается информация о последней проверке системы. При полной проверке все жесткие диски вашей системы проверяются в полном объеме. При этом используются все методы поиска и проверки, за исключением проверки целостности системных файлов: проверка файлов по умолчанию, проверка реестра и загрузочных секторов, поиск руткитов и активных вредоносных программ.

Отображается следующая информация:

- Дата последней полной проверки системы

Существуют следующие возможности:

Проверка системы	Опция	Описание
Не выполнялась	Проверить систему	<p>С момента установки полная проверка системы не проводилась.</p> <div style="background-color: #cccccc; padding: 10px; margin: 10px 0;"> <p>Предупреждение Система не проверена. На вашем компьютере может находиться вирус или вредоносная программа.</p> </div> <div style="background-color: #cccccc; padding: 10px; margin: 10px 0;"> <p>Указание Для проверки компьютера нажмите кнопку «Проверить систему».</p> </div>
Дата последней проверки системы, например, 18.09.2011	Проверить систему	<p>Вы выполнили полную проверку системы в указанный срок.</p> <div style="background-color: #cccccc; padding: 10px; margin: 10px 0;"> <p>Указание Рекомендуется использовать стандартную задачу проверки <i>Полная проверка системы</i>: активируйте задачу проверки «Полная проверка системы» в Планировщике.</p> </div>
Неизвестно	Справка	<p>Данное состояние отображается при возникновении неизвестной ошибки. В этом случае обратитесь в нашу службу поддержки.</p>


Последнее обновление


В этом разделе отображается информация о текущем состоянии последнего обновления.

Отображается следующая информация:

- Дата последнего обновления
 - ▶ Нажмите кнопку «Конфигурация», чтобы выполнить дополнительные настройки автоматического обновления.

Существуют следующие возможности:

Пиктограмма	Состояние	Опция	Описание
	Дата последнего обновления, например, 18.07.2011	Запустить обновление	Программа была обновлена в течение последних 24 часов. <div style="background-color: #f0f0f0; padding: 10px;"> <p>Указание С помощью кнопки «Запустить обновление» вы сможете поддерживать ваш продукт Avira в актуальном состоянии.</p> </div>
	Дата последнего обновления, например, 15.07.2011	Запустить обновление	С момента последнего обновления прошло более 24 часов, но вы все еще находитесь внутри выбранного вами цикла напоминаний об обновлениях. Он зависит от настроек в меню Конфигурация . <div style="background-color: #f0f0f0; padding: 10px;"> <p>Указание С помощью кнопки «Запустить обновление» вы сможете поддерживать ваш продукт Avira в актуальном состоянии.</p> </div>




	<i>Не выполнялось</i>	Запустить обновление	<p>С момента установки обновление еще не выполнялось или были превышены параметры выбранного вами цикла оповещений об обновлении (см. Конфигурация), а обновление не было выполнено, или файл определений вирусов старше выбранного вами цикла оповещений об обновлении (см. Конфигурация).</p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Указание С помощью кнопки Запустить обновление вы сможете поддерживать ваш продукт Avira в актуальном состоянии.</p> </div>
		<i>Невозможно</i>	<p>При истекшем сроке действия лицензии обновление невозможно.</p>

Ваш продукт активирован




В этом разделе отображается информация о текущем статусе вашей лицензии.

Существуют следующие возможности:

Полная версия

Пиктограмма	Состояние	Опция	Значение
	Срок действия текущей лицензии для полной версии, например, 31.10.2011	Обновить	Вы обладаете действующей лицензией для программы Avira. С помощью кнопки «Обновить» вы перейдете в онлайн-магазин Avira. Там вы сможете выбрать лицензию, отвечающую вашим потребностям, и обновить ваш продукт до версии Avira Premium.
	Срок действия текущей лицензии для полной версии, например, 31.10.2011	Обновить	Вы обладаете действующей лицензией на продукт Avira. Однако срок действия лицензии составляет 30 или менее дней. С помощью кнопки Обновить вы перейдете в онлайн-магазин Avira. Там вы сможете продлить свою лицензию.
	Срок действия лицензии истек, например, 31.08.2011	Купить	Срок действия лицензии на ваш продукт Avira истек. С помощью кнопки Купить вы перейдете в онлайн-магазин Avira. Там вы сможете приобрести действующую лицензию. <div style="background-color: #cccccc; padding: 10px; border: 1px solid #000;"> <p>Предупреждение Если срок действия вашей лицензии истек, то дальнейшее обновление невозможно. Защитные функции программы отключены и не могут быть активированы.</p> </div>

Тестовая лицензия

Пиктограмма	Состояние	Опция	Значение
	Тестовая лицензия действительна, например, до 31.10.2011	Купить	Вы обладаете тестовой лицензией и имеете возможность в течение определенного времени опробовать функции вашего продукта Avira в полном объеме. С помощью кнопки Купить вы перейдете в онлайн-магазин Avira. Там вы сможете приобрести действующую лицензию.
	Тестовая лицензия действительна, например, до 31.10.2011	Обновить	Вы обладаете тестовой лицензией. Однако срок действия лицензии составляет 30 или менее дней. С помощью кнопки Обновить вы перейдете в онлайн магазин Avira. Там вы сможете приобрести действующую лицензию.
	Срок действия тестовой лицензии истек 31.08.2011	Купить	Срок действия лицензии на ваш продукт Avira истек. С помощью кнопки Купить вы перейдете в онлайн-магазин Avira. Там вы сможете приобрести действующую лицензию. <div style="background-color: #cccccc; padding: 10px; border: 1px solid #999;"> <p>Предупреждение Если срок действия вашей лицензии истек, то дальнейшее обновление невозможно. Защитные функции программы отключены и не могут быть активированы.</p> </div>

Интернет-безопасность

В этом разделе отображается информация о текущем состоянии служб, которые защищают ваш компьютер от вирусов и вредоносного ПО из Интернета.


- **FireWall:** служба контролирует входящий и исходящий трафик.


- **Web Protection:** служба проверяет данные, передаваемые при работе в Интернете и загружаемые вашим веб-браузером (контроль портов 80, 8080, 3128).
- **Mail Protection:** служба проверяет электронную почту и вложения на наличие вирусов и вредоносных программ.
- **Режим презентации:** если эта опция активирована, то ваш продукт Avira автоматически переключается в режим презентации, если на вашем компьютере запущено приложение в полноэкранном режиме. См. [Режим презентации](#).

Дополнительные опции служб отображаются в контекстном меню с помощью кнопки **Конфигурация** рядом с кнопкой **ВКЛ./ВЫКЛ.:**

- **Конфигурация:** вы переходите в меню конфигурации, где можно настроить параметры компонентов службы.

Существуют следующие возможности: *Службы*

Пиктограмма	Состояние	Состояние службы	Опция	Значение
	OK	Включено	Отключить	Активны все службы Интернет-безопасности. <div style="background-color: #e0e0e0; padding: 10px; border: 1px solid #ccc;"> <p>Указание Вы можете деактивировать службу с помощью кнопки ВКЛ./ВЫКЛ. Обратите внимание, что при отключении службы не обеспечивается полная защита от вирусов и вредоносных программ.</p> </div>

	С ограничениями	Отключено	Включить	Служба отключена. Это означает, что служба запущена, но не активна. <div data-bbox="1078 376 1398 878" style="background-color: #cccccc; padding: 10px; margin-top: 10px;"> <p>Предупреждение Ваша система проверяется не полностью. Существует вероятность того, что вирусы и вредоносные программы проникнут в вашу систему.</p> </div> <div data-bbox="1078 913 1398 1301" style="background-color: #cccccc; padding: 10px; margin-top: 10px;"> <p>Указание Чтобы включить службу, нажмите кнопку ВКЛ./ВЫКЛ. рядом с названием соответствующей службы.</p> </div>
---	--------------------	-----------	----------	---

	Предупрежде ние	Служба остановлен а	Запустить	Служба была остановлена. <div style="background-color: #cccccc; padding: 5px;"> <p>Предупрежде ние Ваша система проверяется не полностью. Существует вероятность того, что вирусы и вредоносные программы проникнут в вашу систему.</p> </div> <div style="background-color: #cccccc; padding: 5px; margin-top: 10px;"> <p>Указание Чтобы запустить службу и активировать защиту, нажмите кнопку ВКЛ./ВЫКЛ. Служба запустится и активируется.</p> </div>
		Неизвестно	Справка	Данное состояние отображается при возникновении неизвестной ошибки. В этом случае обратитесь в нашу службу поддержки .

7.3.2 Режим презентации

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

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

- ▶ Чтобы активировать режим презентации, нажмите на кнопку слева от **ВЫКЛ**.
 - ↪ Режим презентации 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 режиме презентации вы не увидите сообщения рабочего стола и предупреждения о сетевом доступе, а также о возможных опасностях.

7.3.3 System Scanner

Раздел **System Scanner** дает возможность быстро и просто настроить и запустить сканирование системы. [Предустановленные профили](#) позволяют производить сканирование системы с оптимальными настройками по умолчанию. Можно также адаптировать сканирование системы на наличие вирусов и нежелательных программ к своим личным требованиям с помощью [выборочной проверки](#) или путем создания [пользовательских профилей](#). Требуемое действие можно выбрать с помощью значка на [панели инструментов](#), с помощью [ярлыка](#) или [контекстного меню](#). Запустите сканирование системы с помощью элемента [Проверка с выбранным профилем](#).

Внешний вид и работа с редактируемыми профилями аналогичны работе с Проводником Windows. Каждая папка в корневом каталоге соотносится с определенным профилем. Подлежащие сканированию папки или файлы можно выбрать, установив флажок перед соответствующей папкой или файлом для сканирования.

- Для смены каталогов дважды щелкните необходимый каталог.
- Для смены дисков дважды щелкните букву необходимого диска.
- Для выбора папок и дисков можно щелкнуть поле перед соответствующей папкой или диском левой кнопкой мыши или выбрать их с помощью [контекстного меню](#).
- Навигация в структуре меню осуществляется с помощью полосы прокрутки и стрелок прокрутки.

Предустановленные профили

Доступны предустановленные профили сканирования.

Примечание

Эти профили защищены от записи и не могут быть изменены или удалены. Чтобы профиль соответствовал вашим потребностям, выберите для однократного сканирования папку [Выборочная проверка](#) или [Создать новый профиль](#) для создания [пользовательского профиля](#), который может быть сохранен.

Примечание

Параметры сканирования для предустановленных профилей могут настраиваться в меню [Настройка > System Scanner > Проверка > Файлы](#). Эти параметры можно настроить в соответствии со своими потребностями.

Локальные диски

Все локальные диски вашей системы сканируются на наличие вирусов или нежелательных программ.

Локальные жесткие диски

Все локальные жесткие диски вашей системы сканируются на наличие вирусов или нежелательных программ.

Съемные диски

Все доступные съемные диски вашей системы сканируются на наличие вирусов или нежелательных программ.

Системная папка Windows

Системная папка Windows вашей системы сканируется на наличие вирусов или нежелательных программ.

Полная проверка системы

Все локальные жесткие диски вашего компьютера сканируются на наличие вирусов или нежелательных программ. При сканировании используются все процессы сканирования, за исключением проверки целостности системных файлов: стандартное сканирование файлов, сканирование реестра и загрузочных секторов, поиск руткитов и т. д. (см. [System Scanner > Обзор](#)). Процессы сканирования выполняются независимо от настроек сканера в разделе [System Scanner > Проверка: Дополнительные настройки](#).

Быстрая проверка системы

Важные папки вашей системы (папки *Windows*, *Program Files*, *Documents and Settings\Default User*, *Documents and Settings\All Users*) проверяются на наличие вирусов и нежелательных программ.

Мои документы

Место сохранения по умолчанию "*Мои документы*" вошедшего в систему пользователя сканируется на наличие вирусов или нежелательных программ.

Примечание

"*Мои документы*" в Windows является папкой в профиле пользователя, которая используется как место сохранения по умолчанию для документов. По умолчанию этот каталог находится в *C:\Documents and Settings\[имя пользователя]\Мои документы*.

Активные процессы

Все запущенные процессы сканируются на наличие вирусов и нежелательных программ.

Поиск "руткитов" и активного вредоносного ПО

Выполняется сканирование компьютера на наличие руткитов и активных (работающих) вредоносных программ. При этом проверяются все работающие процессы.

Примечание

В [интерактивном режиме](#) доступно несколько вариантов реакции на обнаруженный объект. В [автоматическом режиме](#) факт обнаружения фиксируется в файле отчета.

Примечание

Сканирование на наличие руткитов недоступно в 64-разрядных версиях Windows XP !

7.3.4 Выборочная проверка

Выберите эту папку, если хотите адаптировать сканирование к своим индивидуальным требованиям. Отметьте папки и файлы для сканирования. Если продукт Avira управляется консолью управления Avira, можно использовать поле **Выборочная проверка** в диалоговом окне **Команды** для сканирования нескольких каталогов, разделенных знаком вопроса (?) (например: `c:\temp?d:\test`).

Примечание

Профиль **Выборочная проверка** обеспечивает возможность сканирования данных без предварительного создания нового профиля.

Пользовательские профили

Создать новый профиль можно через [панель инструментов](#), [горячими клавишами](#) или через [контекстное меню](#).

Новые профили можно сохранять с выбранным именем и использовать в дополнение к [сканированию](#), [запускаемому вручную](#) для создания процессов сканирования в установленное время с помощью [планировщика](#).

Панель инструментов и ярлыки

Значок	Ярлык	Описание
	F3	Запуск сканирования с выбранным профилем Выделенный профиль сканируется на наличие вирусов и нежелательных программ.
	F6	Запуск администратором сканирования с выбранным профилем Выделенный профиль сканируется с правами администратора.
	Ins	Создать новый профиль Создается новый профиль.
	F2	Переименование выбранного профиля Присваивает выделенному профилю выбранное вами имя.
	F4	Создание ярлыка на рабочем столе для выбранного профиля Создание на рабочем столе ярлыка для выбранного профиля.
	Del	Удаление выбранного профиля Выбранный профиль удаляется навсегда.

Контекстное меню

Доступ к контекстному меню можно получить, щелкнув требуемый профиль правой кнопкой мыши.

Запустить проверку

Выделенный профиль сканируется на наличие вирусов и нежелательных программ.

Проверка (администратор)

(Эта функция доступна только в Windows Vista. Для выполнения этого действия требуются права администратора.)

Выделенный профиль сканируется на наличие вирусов и нежелательных программ.

Создать новый профиль

Создается новый профиль. Выделите папки и файлы, которые необходимо сканировать.

Переименовать профиль

Присваивает выделенному профилю выбранное вами имя.

Примечание

Этот элемент невозможно выбрать в контекстном меню, если выбран [предопределенный профиль](#).

Удалить профиль

Выбранный профиль удаляется навсегда.

Примечание

Этот элемент невозможно выбрать в контекстном меню, если выбран [предопределенный профиль](#).

Файловый фильтр

По умолчанию:

Означает, что файлы будут сканироваться в соответствии с настройкой группы [Файлы](#) меню настройки. Эту [настройку](#) можно установить в соответствии со своими потребностями. В раздел настройки можно перейти, выбрав кнопку или ссылку [Настройка](#).

Проверить все файлы:

Будут сканироваться все файлы, независимо от установок в меню [Настройка](#).

Определено пользователем:

Вызывается диалоговое окно, в котором отображаются все расширения файлов, проверяемых при сканировании. Для списка расширений определены базовые

расширения по умолчанию. Можно добавлять в список расширений новые строки или удалять их.

Примечание

Этот элемент контекстного меню можно выбрать, если курсор находится над соответствующим флажком.

При использовании [предопределенных профилей](#) выбор этого элемента невозможен.

Выбрать**С подкаталогами:**

Сканируются все файлы и папки, находящиеся в выделенном (черный флажок) каталоге.

Без подкаталогов:

Сканируются только файлы, находящиеся в указанном (зеленый флажок) каталоге.

Только подкаталоги:

В выделенном корневом каталоге проверяются только подкаталоги, но не файлы, находящиеся в корневом каталоге (серый флажок, подкаталоги выделены черными флажками).

Без выбора:

Выбор отменен (нет флажков), сканирование текущего каталога не производится.

Примечание

Этот элемент контекстного меню можно выбрать, если курсор находится над соответствующим флажком.

При использовании [предопределенных профилей](#) выбор этого элемента невозможен.

Создать ярлык

Создает на рабочем столе ярлык для выбранного профиля.

Примечание

Этот элемент недоступен в контекстном меню при выборе профиля [Выборочная проверка](#), так как настройки в профиле [Выборочная проверка](#) не подлежат постоянному хранению.



7.3.5 Real-Time Protection

Вкладка **Real-Time Protection** отображает [информацию о проверенных файлах](#) и другие [статистические данные](#), которые в любое время можно [обнулить](#), и позволяет открыть [файл отчета](#). Подробная [информация](#) о последнем обнаруженном вирусе или нежелательной программе вызывается "одним щелчком".

Указание

Если [служба Real-Time Protection](#) не запущена, то кнопка рядом с модулем отображается желтым цветом. Вы можете ознакомиться с [файлом отчета](#) модуля Real-Time Protection.

Графическое меню

Пиктограмма	Описание
	Показать файл отчета Отображается файл отчета модуля Real-Time Protection.
	Сбросить данные статистики Статистические данные этой вкладки сбрасываются до нуля.


Отображаемая информация

Последний инфицированный файл

Отображает имя и местонахождение последнего файла, найденного модулем Real-Time Protection.

Последнее найденное вредоносное ПО

Отображает имя последнего обнаруженного вируса или вредоносной программы.

Пиктограмма	Описание
 Информация о вирусах	Щелчком по пиктограмме или ссылке при установленном Интернет-соединении вы вызываете подробную информацию о вирусах и вредоносных программах.

Последний проверенный файл

Отображает имя и путь к последнему проверенному службой Real-Time Protection файлу.

Статистика

Количество файлов

Отображает количество проверенных ранее файлов.

Количество найденных вредоносных программ

Отображает число обнаруженных вирусов и вредоносных программ.

Количество подозрительных файлов

Отображает количество файлов, отмеченных модулем эвристики.

Количество удаленных файлов

Отображает количество удаленных ранее файлов.

Количество вылеченных файлов

Отображает количество вылеченных ранее файлов.

Количество перемещенных файлов

Отображает количество перемещенных ранее файлов.

Количество переименованных файлов

Отображает количество переименованных ранее файлов.


7.3.6 FireWall

Avira FireWall (Avira Professional Security)

Во вкладке FireWall также отображается скорость передачи данных и все активные приложения, использующие сетевые соединения. Во вкладке FireWall можно

изменять основные настройки брандмауэра Avira FireWall: с помощью ползункового регулятора можно настроить степень защиты. Для настройки пользовательской степени защиты необходимо перейти в раздел настроек.

Графическое меню

Пиктограмма	Описание
	<p>Сброс статистики</p> <p>Статистические данные этого раздела обнуляются.</p>

Уровень безопасности

Вы можете выбрать различные настройки безопасности:

Указание

Вы можете изменить уровень безопасности, передвинув ползунок на нужное значение шкалы безопасности. Выбранный уровень безопасности сразу активируется. Дополнительная информация по этой теме находится в настройках брандмауэра: [правила адаптера](#)

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.

Новые внешние подключения не разрешены.

Предотвращается сканирование портов и флудинг.

Пользователь

Правила, установленные пользователем

Блокировать все

Завершает все текущие сетевые соединения.

Передача данных

В этом разделе отображается информация о последних процессах отправки (*Выгрузка*) и получения (*Загрузка*) данных. Максимальное значение находится в левом верхнем углу окна.

Входящие пакеты показываются красным цветом, исходящие пакеты - зеленым. Область, в которой данные перекрываются, выделена серым цветом.

брандмауэр Windows (начиная с Windows 7)



Начиная с Windows 7, Avira FireWall больше не содержится в Avira Professional Security. Вместо этого брандмауэром брандмауэр Windows можно управлять с помощью Центра управления сетями и общим доступом.

В разделе "FireWall" можно проверить состояние брандмауэр Windows и восстановить рекомендуемые настройки, нажав на кнопку **Устранить проблему**.

7.3.7 Web Protection

Вкладка **Web Protection** показывает [информацию о проверенных URL](#) и 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".

Графическое меню

Пиктограмма	Описание
	<p>Показать файл отчета</p> <p>Отобразится файл отчета модуля Web Protection.</p>
	<p>Сброс данных статистики</p> <p>Статистические данные этого раздела обнуляются.</p>


Отображаемая информация

Последний инфицированный URL

Показывает последний обнаруженный модулем Web Protection URL.

Последний обнаруженный вирус/вредоносная программа

Отображает имя последнего обнаруженного вируса или вредоносной программы.

Пиктограмма/Ссылка	Описание
 Информация о вирусах	Щелчком на пиктограмме или ссылке при установленном Интернет-соединении вы вызываете подробную информацию о вирусах и вредоносных программах.

Последний проверенный URL

Отображает имя последнего обнаруженного модулем Web Protection URL.

Статистика

Количество проверенных URL

Отображает количество проверенных URL.

Количество сообщений

Отображает число обнаруженных вирусов и вредоносных программ.

Количество заблокированных URL

Отображает число заблокированных URL.

Количество пропущенных URL

Отображает число пропущенных URL.

7.3.8 Защита электронной почты

Вкладка **Mail Protection** показывает проверенные модулем Mail Protection письма, их свойства и данные статистики.






Указание

Если [служба Real-Time Protection](#) не запущена, то кнопка рядом с модулем отображается желтым цветом. Вы можете ознакомиться с [файлом отчета](#) модуля Mail Protection. Если в вашей программе Avira эта служба недоступна, то кнопка будет серой.

Указание



Исключение избранных Email-адресов из процедуры проверки на наличие вредоносного ПО касается только входящих писем. Для отключения проверки исходящих писем отключите ее в настройках [Mail Protection > Поиск](#).

Графическое меню

Пиктограмма	Описание
	Показать файл отчета Файл отчета модуля Mail Protection будет показан.
	Показать свойства выбранного письма Открывает окно с подробной информацией о выделенном письме.
	Не проверять это письмо на наличие вредоносных программ Выделенное письмо в дальнейшем не проверяется на наличие вирусов и вредоносных программ. Вы можете отменить эту установку здесь: Mail Protection > Общие > Исключения (см. Исключения).
	Удалить выделенное письмо (письма) Выделенное письмо будет удалено из буфера. Файл сохраняется в вашей почтовой программе.
	Сбросить данные статистики Статистические данные этой вкладки сбрасываются до нуля.

Проверено писем

Здесь отображается количество писем, проверенных службой Mail Protection.

Пиктограмма	Описание
	Не было обнаружено вирусов или вредоносных программ.
	Был обнаружен вирус или вредоносная программа.

Тип

Показывает протокол, который использовался для получения или отправки писем:

- POP3: полученные по POP3 письма
- IMAP: полученные по IMAP письма
- SMTP: отправленные по SMTP письма

Отправитель/получатель

Показывает адрес отправителя письма.

Тема

Показывает тему полученного письма.

Дата/время

Показывает, когда письмо было проверено на предмет спама.

Указание

Дополнительную информацию о письме можно получить, щелкнув по нему дважды левой кнопкой мыши.

Статистика**Действие с письмом**

Отображает действие, производимое службой Mail Protection в случае обнаружения в письме вируса или вредоносной программы. В [интерактивном режиме](#) проверки эта информация не отображается, так как необходимые действия пользователь выбирает сам.

Указание

Эту [настройку](#) вы можете установить в соответствии со своими потребностями. В настройки можно перейти нажатием кнопки или ссылки [Настройки](#).

Инфицированные вложения

Отображает действие, производимое службой Mail Protection в случае обнаружения во вложении письма вируса или вредоносной программы. В [интерактивном режиме](#) проверки эта информация не отображается, так как необходимые действия пользователь выбирает сам.

Указание

Эту [настройку](#) вы можете установить в соответствии со своими потребностями. В настройки можно перейти нажатием кнопки или ссылки [Настройки](#).

Всего писем

Отображает количество проверенных модулем Mail Protection электронных писем.

Последнее сообщение

Отображает имя последнего обнаруженного вируса или вредоносной программы.

Количество сообщений

Отображает количество обнаруженных до настоящего времени вирусов и вредоносных программ.

Подозрительные письма

Отображает число писем, отмеченных эвристикой.

Всего полученных писем

Отображает число входящих писем.

Всего отправленных писем

Отображает число исходящих писем.

7.3.9 Карантин



Менеджер карантина управляет инфицированными объектами (файлы и электронные письма). Продукт Avira помещает инфицированные объекты в специальном формате в каталог карантина. Они не могут быть выполнены или открыты.




Примечание





Для перемещения объектов в менеджер карантина выберите соответствующую функцию карантина в меню **Настройки**, разделы **System Scanner**, **Real-Time Protection** и **Mail Protection**, а также **Поиск > Действия при обнаружении**, если вы работаете в **автоматическом режиме**.



Можно также выбрать соответствующую функцию карантина в **интерактивном режиме**.

Панель инструментов, ярлыки и контекстное меню

Значок	Ярлык	Описание
	F2	<p>Повторное сканирование объекта (объектов)</p> <p>Выделенный объект повторно сканируется на наличие вирусов и нежелательных программ. Для этого используются настройки проверки.</p>
	Enter	<p>Свойства</p> <p>Открывает диалоговое окно с подробной информацией о выбранном объекте.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Примечание Подробную информацию можно также вызвать, дважды щелкнув объект.</p> </div>

  (Windows Vista)	F3	<p>Восстановление объекта (объектов)</p> <p>Восстановление выделенного объекта. После этого данный объект помещается на свое прежнее место.</p> <div data-bbox="496 414 1398 580" style="background-color: #f0f0f0; padding: 5px;"> <p>Примечание Эта функция недоступна для объектов типа электронное письмо.</p> </div> <div data-bbox="496 618 1398 898" style="background-color: #d0d0d0; padding: 5px;"> <p>Предупреждение Серьезные повреждения системы из-за вирусов и нежелательных программ! При восстановлении файлов убедитесь, что восстанавливаются только те файлы, которые удалось вылечить при повторном сканировании.</p> </div> <div data-bbox="496 936 1398 1102" style="background-color: #f0f0f0; padding: 5px;"> <p>Примечание В Windows Vista для восстановления объектов необходимы права администратора.</p> </div>
	F6	<p>Восстановление объекта (объектов) в...</p> <p>Выделенный объект может быть восстановлен и помещен в указанное вами место. При выборе данной функции отображается диалоговое окно "Сохранить как", в котором можно выбрать место для хранения.</p> <div data-bbox="496 1420 1398 1700" style="background-color: #d0d0d0; padding: 5px;"> <p>Предупреждение Серьезные повреждения системы из-за вирусов и нежелательных программ! При восстановлении файлов убедитесь, что восстанавливаются только те файлы, которые удалось вылечить при повторном сканировании.</p> </div>

	Ins	<p>Добавление файла в карантин</p> <p>Если вы считаете файл подозрительным, можно добавить его в менеджер карантина вручную с помощью этой функции. При необходимости загрузите файл на веб-сервер центра исследования вредоносного ПО Avira для его исследования, воспользовавшись функцией Отправить объект.</p>
	F4	<p>Отправка объекта (объектов)</p> <p>Объект загружается на веб-сервер центра исследования вредоносного ПО Avira для его изучения. При выборе кнопки Отправить объект открывается диалоговое окно с формой для ввода ваших контактных данных. Введите все необходимые данные. Выберите тип: Подозрительный файл или Ложное срабатывание. Щелкните ОК для загрузки подозрительного файла.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Примечание Можно загрузить неархивированный файл размером до 20 Мб или архив размером до 8 Мб.</p> <p>Примечание Можно одновременно загрузить несколько файлов, выделив их и щелкнув кнопку Отправить объект.</p> </div>
	Del	<p>Удаление объекта (объектов)</p> <p>Выделенный объект удаляется из менеджера карантина. Объект нельзя будет восстановить.</p>
		<p>Копирование объекта (объектов) в...</p> <p>Сохранение выделенного объекта карантина в указанном каталоге.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Примечание Объект карантина не будет идентичным восстановленному файлу. Объект карантина зашифрован и не может быть выполнен или считан в первоначальном формате.</p> </div>

	F7	Экспорт всех свойств Экспорт свойств выделенного объекта карантина в текстовый файл.
	F10	Открытие папки карантина Открытие папки INFECTED.




Примечание

Можно выполнять действия с несколькими выделенными объектами. Чтобы выделить несколько объектов (объекты в столбцах), удерживайте клавишу Ctrl или Shift во время выбора объектов в менеджере карантина. Нажмите **Ctrl + A**, чтобы выделить все отображаемые объекты. При выборе действия **Показать свойства** его выполнение для нескольких объектов невозможно.

Таблица

Состояние

Помещенный в Карантин объект может иметь различные состояния:

Значок	Описание
	Вирусов или нежелательных программ не обнаружено. Объект "чистый".
	Был обнаружен вирус или нежелательная программа.
	Если подозрительный файл был добавлен в менеджер карантина с помощью функции Добавить файл , он отображается с этим символом предупреждения.

Тип

Обозначение	Описание
Электронное письмо	Обнаруженный объект является электронным письмом.
Файл	Обнаруженный объект является файлом.

Обнаружение

Отображает имя обнаруженной вредоносной программы.
Объекты, обнаруженные системой эвристического поиска, помечаются сокращением HEUR/.

Источник

Отображает путь, по которому был указан объект.

Дата/время

Отображает дату и время обнаружения.

Подробная информация**Имя файла**

Полный путь и имя файла объекта

Помещенный на карантин объект

Имя помещенного на карантин объекта

Восстановлен

ДА/НЕТ

ДА: объект был восстановлен.

НЕТ: объект не был восстановлен.

Загружен в Avira

ДА/НЕТ

ДА: объект уже загружен в центр исследования вредоносного ПО Avira для изучения.

НЕТ: объект еще не был загружен на веб-сервер центра исследования вредоносного ПО Avira

для изучения.

Операционная система

Windows XP: вредоносное ПО идентифицировано настольным продуктом Avira.

Антивирусное ядро

Номер версии антивирусного ядра

Файл обновления вирусной базы

Номер версии файла обновления вирусной базы

Обнаружение

Имя обнаруженной вредоносной программы

Дата/время

Дата и время обнаружения





7.3.10 Scheduler

Scheduler позволяет создавать выполняемые в определенное время задачи по проверке и обновлению, а также согласовывать или удалять существующие задачи.

По умолчанию после установки создается следующая задача:

- Проверка **Quick system scan** (настройка по умолчанию): Еженедельно автоматически выполняется быстрая проверка системы. При быстрой проверке системы все важные файлы и папки вашего компьютера проверяются на наличие вирусов и вредоносных программ. Вы можете изменить задачу проверки; рекомендуется устанавливать задачу проверки так, чтобы она лучше отвечала вашим потребностям.



Панель инструментов, горячие клавиши и контекстное меню

Пиктограмма	Горячие клавиши	Контекстное меню
	Ins	Добавление новой задачи Создает новую задачу. Ассистент поможет вам создать необходимые настройки.
	Enter	Properties Открывает окно, содержащее более подробную информацию о выбранной задаче.
	F2	Edit job Открывает программу-ассистент для создания и изменения задач.
	Del	delete job Удаляет выбранную задачу из списка.

		Show report file Отображается файл отчета планировщика.
	F3	Запустить задачу Запускает выделенную задачу из списка.
	F4	Остановить задачу Остатавливает запущенную и выделенную задачу.

Таблица

Вид задачи

Пиктограмма	Описание
	Данная задача является задачей обновления.
	Данная задача является задачей проверки.

Имя

Имя задачи.

Действие

Показывает, идет ли речь о задаче **Scan** или об **Update**.

Частота

Показывает, как часто и когда запускается данная задача.

Визуальный режим

Доступны следующие визуальные режимы:

invisible: Задача выполняется в фоновом режиме и не имеет визуального отображения. Это имеет отношение к задачам сканирования и обновления.

minimized: В окне отображается только строка прогресса выполнения задачи.

maximized: Окно отображается полностью.

Включена

Задача активируется после установки флажка.

Указание

Если выбрана частота выполнения "Немедленно", задача будет запущена непосредственно после активации. Это позволяет Вам перезапустить задачу при необходимости.

Состояние

Отображает состояние задачи:

Ready: Задача готова к выполнению.

Running: Задача запущена и выполняется.

Создание задач с помощью планировщика

Ассистент планировщика будет вам полезен в создании новых задач, настройках и планировании

- поиска вирусов и вредоносных программ в заранее определенное время
- обновления через Интернет или интранет в заранее определенное время

Для обоих типов задач вам необходимо указать

- имя и описание задачи
- когда задача должна быть запущена
- как часто должна выполняться задача
- режим отображения задачи

Частота задачи

Опция	Описание
Немедленно	Задача запускается сразу после закрытия ассистента планировщика.
Ежедневно	Задача выполняется ежедневно в определенное время, например в 22:00.

Еженедельно	Задача запускается еженедельно в определенный день или несколько дней и заранее установленное время, например во вторник и в пятницу, в 16:26.
Интервал	Задача запускается через определенный промежуток, например каждые 24 часа.
Однократно	Задача выполняется только однократно в заранее установленное время, например 10.04.04 в 10:04.
Логин	Задача выполняется каждый раз при входе пользователя Windows в систему.

Время начала выполнения задачи

Вы можете установить день недели, дату, время или интервал в качестве времени запуска задачи. Оно не будет отображаться, если выбран пункт *Immediately*.

В зависимости от типа задачи существуют дополнительные опции:

Дополнительно запускать задачу при подключении к Интернету (через модем)

Помимо выполнения задач с установленной частотой осуществляется дополнительный запуск задач при каждом установленном Интернет-соединении. Эту опцию можно выбрать для задачи обновления, выполнение которой планируется ежедневно, еженедельно или с определенным интервалом.

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. Эту опцию можно выбрать для задач проверки, которые должны быть запущены ежедневно, еженедельно или с определенным временным интервалом.

Выключить компьютер после завершения задачи

После выполнения и завершения задачи компьютер выключается. Опция доступна для задач проверки в минимизированном и максимизированном режиме отображения.





Указание

При выполнении задачи проверки в диалоговом окне "Выбор профиля" можно выбрать как [предустановленный стандартный профиль](#), так и [определенный пользователем профиль](#). Профиль [Выборочная проверка](#) выполняется всегда с текущими настройками.

7.3.11 Отчеты



Во вкладке **Reports** можно получить информацию о результатах действий, выполненных программой.



Панель инструментов, горячие клавиши и контекстное меню

Пиктограмма	Горячие клавиши	Описание
	Enter	Display report Открывает окно, в котором отображается результат выполнения выделенного действия. Например результат Проверки .
	F3	Show report file Показывает файл выбранного отчета.
	F4	Print report file Открывает окно печати Windows для печати файла отчета.
	Del	Delete report(s) Удаляет выделенное сообщение и файл соответствующего отчета.

Таблица

Состояние

Пиктограмма	Описание
	Проверка: вирусов не обнаружено!
	Проверка: не завершена или найдены вирусы

	Обновление: обновление выполнено успешно
	Обновление: обновление не выполнено

Действие

Отображает предпринятое действие.

Результат

Отображает результат действия.

Дата/Время

Отображает дату и время создания отчета.

Содержание отчета по результатам проверки

- *Date of the scan:*
Дата проверки.
- *Start time of the scan:*
Время начала проверки.
- *Scanning time required::*
Отображает время в формате мин:сек.
- *Scan status:*
Показывает, была ли проверка проведена полностью или была прервана.
- *Last detection:*
Имя последнего обнаруженного вируса или вредоносной программы.
- *Scanned directories:*
Общее количество проверенных папок.
- *Files searched:*
Общее количество проверенных файлов.
- *Scanned archives:*
Количество проверенных архивов.
- *Hidden objects:*
Общее количество обнаруженных скрытых объектов.
- *Detections:*
Общее количество обнаруженных вирусов и вредоносных программ.
- *Suspicious:*

Количество подозрительных файлов.

- *Warnings:*

Количество предупреждений об обнаружении вирусов.

- *Information:*

Количество переданных системой сообщений, например, содержащих дополнительную информацию, появляющуюся в процессе проверки.

- *Repaired::*

Общее количество восстановленных файлов.

- *Quarantine:*

Общее количество помещенных на карантин файлов.

- *Renamed:*

Общее количество переименованных файлов

- *Deleted:*

Общее количество удаленных файлов.

- *Wiped:*

Число перезаписанных файлов.

Указание

Rootkits скрывают процессы и объекты, например записи в реестре или файлы, но не каждый скрытый объект является указанием на существование Rootkits. Скрытые объекты могут указывать и на безвредные программы. Если во время проверки были обнаружены скрытые объекты, а предупредительные сообщения об обнаружении вирусов не поступали, то на основе отчета вам необходимо определить, что это за объекты, и найти дополнительную информацию о найденных объектах.

7.3.12 События

Events показываются события, созданные компонентами программы.




События сохранены в базе данных. Вы можете ограничить размер базы данных или отключить ограничение размера базы данных (см. [Events](#)). По умолчанию сохраняются события последних 30 дней. Индикация событий обновляется автоматически при выборе вкладки **Events**.

Указание

Автоматическое обновление вкладки не выполняется, если в базе данных

событий сохранено более 20 000 событий. В этом случае для обновления списка событий нажмите клавишу F5.

Панель инструментов, горячие клавиши и контекстное меню

Пиктограмма	Горячие клавиши	Описание
	Enter	Show selected event Открывает окно, в котором отображается результат выполнения выбранного действия. Например результат проверки .
	F3	Export selected event(s) Экспортирует выбранные события.
	Del	Delete selected event(s) Удаляет выбранное событие.

Указание

Вы можете применять выбранное действие к нескольким выделенным событиям. Чтобы выделить несколько событий, удерживайте клавишу Ctrl или Shift (выбор нескольких расположенных друг под другом событий), пока выбираете события.

При выборе действия Показать выбранное событие его выполнение для нескольких объектов невозможно.

Модули

События следующих модулей (отображаются в алфавитном порядке) могут отображаться с помощью индикации событий:





Обозначение модуля
Web Protection
Real-Time Protection


Mail Protection
FireWall
Helper Service
Scheduler
System Scanner
Модуль обновления

При выделении чек-бокса **All** можно просмотреть события всех доступных модулей. Для просмотра событий определенного модуля отметьте чек-бокс перед нужным модулем.

Filter

В окне отображения событий показываются эти типы событий:

Пиктограмма	Описание
	Information
	Warning
	Error
	Detection

При выделении чек-бокса **Filter**  можно просмотреть все события. Для просмотра определенных событий отметьте чек-бокс рядом с нужным событием.

Table

В окне событий показывается следующая информация:

Пиктограмма

Пиктограмма для отображения типа события.

Тип

Классификация события: информация, предупреждение, ошибка, обнаружение.

Module

Модуль Avira, зарегистрировавший событие. Например Real-Time Protection, зафиксировавший обнаружение.

Действие

Описание событий конкретного модуля.

Date/Time

Дата и местное время наступления события.

7.3.13 Обновить

Обновляет вид открытой вкладки.

7.4 Сервис

7.4.1 Проверка загрузочных секторов

Можно также проверить загрузочные секторы дисков рабочей станции с помощью сканирования системы. Это действие рекомендуется, например, если при сканировании системы был обнаружен вирус и требуется убедиться в том, что загрузочные секторы не затронуты.

Чтобы выделить несколько загрузочных секторов, удерживайте клавишу Shift и отмечайте с помощью мыши нужные диски.

Примечание

Можно настроить автоматическую проверку загрузочных секторов при каждом запуске сканера (см. [Проверить загрузочные секторы](#)).

Примечание

В Windows Vista проверка загрузочных секторов возможна только с правами администратора.

7.4.2 Список вирусов

Здесь содержатся имена вирусов и потенциально опасных программ, распознаваемых программой Avira. Встроена удобная функция поиска по именам.

Поиск в списке вирусов

Задайте в поле *Scan for*: слово или последовательность символов.

Поиск последовательности символов внутри имени

Вы можете ввести набор символов, после чего курсор автоматически переместится на первую же позицию, где встречаются эти символы, в т.ч. и в середине имени (пример: "raха" - "Abraxas").

Поиск начинается с первого знака имени

Вы можете ввести начальные символы имени, после чего курсор будет установлен по алфавитному принципу (пример: "Ra" - "Rabbit").

Если искомое имя/последовательность присутствует в списке, позиция подсвечивается курсором.

Прямой поиск

Запускает поиск в прямом алфавитном порядке.

Обратный поиск

Запускает поиск в обратном алфавитном порядке.

Первое совпадение

Перемещается к первому совпадению с запросом.

Компоненты списка обнаружения

Здесь находится список имен вирусов или вредоносных программ, которые могут определяться. Большинство элементов списка могут быть удалены программой Avira. Элементы расположены в алфавитном порядке (сначала - спецсимволы и цифры, затем - буквы). Используйте полосу прокрутки для перемещения в списке вверх и вниз.

7.4.3 Download rescue CD

Пункт меню **Download rescue CD** позволяет загрузить пакет Avira Rescue-CD. Пакет включает в себя загрузочную Live-систему для компьютера, а также сканер Avira с актуальным VDF-файлом и поисковым движком. Вы используете Avira Rescue-CD, чтобы в случае повреждения операционной системы вашего компьютера его можно было бы запустить с CD или DVD, что позволит сохранить данные или произвести проверки.

После загрузки пакета Avira Rescue-CD возникает диалоговое окно, в котором можно выбрать CD/DVD-диск, чтобы записать на него Rescue-CD. У вас есть возможность сохранить пакет Avira Rescue-CD, чтобы записать CD позже.

Указание

Вам потребуется активное интернет-соединение для загрузки пакета Avira Rescue-CD. Вам потребуется CD-/DVD-дисковод и пишущий привод для записи диска.

7.4.4 Настройка

Пункт **Настройка** в меню **Дополнительно** открывает [Настройку](#).

7.5 Обновление

7.5.1 Запустить обновление...

Пункт меню **Запустить обновление...** в меню **Обновление** запускает немедленное обновление. Обновляется файл вирусных сигнатур и поисковый движок.

7.5.2 Ручное обновление...

Элемент меню **Ручное обновление...** в меню **Обновление** открывает диалоговое окно для выбора и загрузки пакета обновления файла VDF/поисковой системы. Пакет обновления также можно загрузить с веб-сайта разработчика, в него входит текущий файл обновления вирусной базы и антивирусное ядро:
<http://www.avira.ru>

Примечание

В Windows Vista для ручного обновления необходимы права администратора.

7.6 Справка

7.6.1 Темы

Пункт **Темы** в меню **Справка** открывает содержание онлайн справки.

7.6.2 Помощь

Пункт меню **Помощь** в меню **Справка** при активном Интернет-соединении открывает сайт поддержки для вашей программы Avira. Там вы сможете найти ответы на часто задаваемые вопросы, вызвать базу знаний или связаться со службой по работе с клиентами Avira.

7.6.3 Руководство по загрузке

Пункт меню **Руководство по загрузке** в меню **Справка** при активном Интернет-соединении открывает страницу с загрузкой вашей программы Avira. Здесь вы найдете ссылку для загрузки последней версии руководства по вашей программе Avira.

7.6.4 Загрузка файла лицензии

Элемент меню **Загрузка файла лицензии** в меню **Справка** открывает диалоговое окно для загрузки файла лицензии *.KEY*.

Примечание

В Windows Vista для загрузки файла лицензии необходимы права администратора.

7.6.5 Отправить сообщение обратной связи

Команда меню **Обратная связь** в меню **Справка** при активном Интернет-соединении открывает страницу с часто задаваемыми вопросами по продукции Avira. Там вы найдете формуляр по оценке продукции, с помощью которого вы можете выразить свое мнение о программе и отправить его компании Avira.

7.6.6 О Avira Professional Security

Общее

Адреса и информация по вашей программе Avira

Информация о версии

Информация о версии пакета программы Avira

Информация о лицензии

Данные текущей лицензии и ссылки на онлайн-магазин (приобретение или продление лицензии)

Указание

Вы можете хранить данные лицензии в буферной памяти. Нажмите правой кнопкой мыши на область информации о лицензии. Откроется контекстное меню. В контекстном меню щелкните по команде **Копировать в буферную память**. Теперь информация о вашей лицензии сохранена в

буферной памяти, она может быть добавлена в письма, формуляры или другие документы с помощью команды Windows.

8. Настройка

8.1 Конфигурация

- [Обзор опций меню конфигурации](#)
- [Профили конфигурации](#)
- [Кнопки](#)

Обзор опций меню конфигурации

Предусмотрены следующие опции меню конфигурации:

- **System Scanner:** конфигурация прямой проверки
 - Опции поиска
 - Действие при обнаружении
 - Дополнительные действия
 - Опции проверки архивов
 - Исключения из прямой проверки
 - Эвристика прямой проверки
 - Настройка функции составления отчета
- **Real-Time Protection:** конфигурация модуля Real-Time Protection
 - Опции поиска
 - Действие при обнаружении
 - Исключения из защиты в режиме реального времени
 - Эвристика защиты в режиме реального времени
 - Настройка функции составления отчета
- **Обновление:** конфигурация настроек обновления
 - Загрузка с файлового сервера
 - Загрузка с веб-сервера
 - Настройки прокси-сервера
- **FireWall:** конфигурация FireWall
 - Настройка правил адаптера
 - Пользовательская настройка правил приложения
 - Список доверенных производителей (исключения при доступе приложений к сети)
 - Расширенные настройки: превышение по времени для правил, отключение Windows FireWall, оповещения
 - Настройка всплывающих окон (уведомления при доступе приложений к сети)
- **Web Protection:** конфигурация 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 Web Protection: URL, типы файлов, типы MIME
- Эвристика службы Web Protection
- Настройка функции составления отчета
- **Mail Protection:** конфигурация модуля Mail Protection
 - Опции поиска: активация контроля учетных записей POP3 и IMAP, а также исходящей электронной почты (SMTP)
 - Действие при обнаружении
 - Дополнительные действия
 - Эвристика проверки модулем Mail Protection
 - Функция AntiBot: разрешенные серверы SMTP и отправители электронной почты
 - Исключения из проверки модулем Mail Protection
 - Настройка буфера обмена, очистка буфера
 - Настройка строки примечания в отправленных письмах
 - Настройка функции составления отчета
- **Общее:**
 - Расширенные категории угроз для прямой проверки и проверки в режиме реального времени
 - Расширенная защита: включение опций ProActiv и Protection Cloud
 - Фильтр приложений: блокировка или разрешение приложений
 - Защита паролем доступа к центру управления и конфигурации
 - Безопасность: блокировка функций автозапуска, блокировка хост-файлов Windows, защита продукта
 - WMI: активация поддержки WMI
 - Настройка протокола событий
 - Настройка функций составления отчета
 - Настройка используемых папок
 - Предупреждения:
Настройка сетевых предупреждений компонента(ов):
System Scanner
Real-Time Protection
Настройка предупреждений компонента(ов) в виде рассылки по электронной почте:
System-Scanner
Real-Time Protection
Менеджер обновлений
 - Настройка звуковых предупреждений при обнаружении вируса

Профили конфигурации

Для управления профилями конфигурации щелкните по значку в трее справа от раздела «Настройки по умолчанию» (см. [Значок в трее](#)).

При этом отобразится ряд опций, с помощью которых можно будет сохранить опции конфигурации для отдельных профилей. Для этого вначале создайте новую конфигурацию и введите в нее нужные значения, т. е. необходимые правила.

Вы можете выбрать ручное или автоматическое изменение конфигурации. Вы можете выбрать или определить правило автоматического перехода к этой конфигурации. Существует несколько способов задания этих правил по умолчанию: вы можете активировать автоматическое переключение при каждом использовании непредусмотренного шлюза или определить шлюз по умолчанию через IP- или MAC-адрес (или IP-адрес и маску сети).

Если правила переключения не определены, то конфигурацию можно переключать вручную в контекстном меню значка в трее. Управление профилями конфигурации осуществляется через контекстное меню окна конфигурации:

Контекстное меню

Ввод с клавиатуры	Контекстное меню/описание
Ins	Создать новую конфигурацию Создание новой конфигурации со значениями по умолчанию для отдельных опций.
F2	Переименовать конфигурацию Изменение имени конфигурации.
Del	Удалить конфигурацию Удаление выбранной конфигурации. Вначале откроется диалоговое окно, в котором вы можете подтвердить или отменить удаление выбранной конфигурации.
F4	Копировать конфигурацию Копирование выбранной конфигурации.

F6	Сбросить конфигурацию Возвращение опций выбранной конфигурации к значениям по умолчанию.
	<p>Правила:</p> <p>Отображаются различные опции задания правил для профилей конфигурации:</p> <p>Нет Правила для переключения на выбранную конфигурацию отсутствуют. Переключение на необходимую конфигурацию должно осуществляться вручную.</p> <p>Правило по умолчанию Выбранная конфигурация используется в качестве конфигурации по умолчанию: переключение на выбранную конфигурацию происходит автоматически всякий раз, когда используется шлюз, не присвоенный ни одной другой конфигурации.</p> <p>Шлюз по умолчанию В качестве правила переключения для выбранной конфигурации можно задать IP- или MAC-адрес межсетевого шлюза, используемого по умолчанию. Если используется указанный по умолчанию межсетевой шлюз, происходит автоматическое переключение на выбранную конфигурацию.</p> <p>IP-адрес В качестве правила переключения для выбранной конфигурации можно задать IP-адрес и маску сети сетевого адаптера. Если используется указанный по умолчанию IP-адрес, происходит автоматическое переключение на выбранную конфигурацию.</p>

Указание

Вы можете сохранить не более восьми конфигураций.

Указание

Если при переключении межсетевого шлюза не было найдено подходящее правило, то активируется последняя использованная конфигурация.

Кнопки

Кнопка	Описание
Значения по умолчанию	Будет выполнен сброс всех настроек конфигурации на значения по умолчанию. При этом все изменения и пользовательские данные будут утеряны.
ОК	Все изменения будут сохранены. Меню «Конфигурация» будет закрыто. Системе контроля учетных записей пользователей (UAC) требуется ваше разрешение на внесение изменений в операционную систему, начиная с Windows Vista.
Отмена	Меню «Конфигурация» закрывается без сохранения изменений в настройках конфигурации.
Применить	Все изменения будут сохранены. Системе контроля учетных записей пользователей (UAC) требуется ваше разрешение на внесение изменений в операционную систему, начиная с Windows Vista.

8.2 System Scanner

Раздел **System Scanner** Настройки отвечает за настройку параметров прямого поиска, т.е. за проверку по требованию пользователя.

8.2.1 Поиск

Здесь вы можете задать принципиальный метод при поиске. 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. Если Вы администрируете продукт Avira под AMC, то эта опция недоступна.

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. Если Вы администрируете продукт Avira под АМС, то эта опция отображается в любом случае и может быть активирована: Если управляемый компьютер не располагает несколькими процессами, то опция System Scanner не используется.

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.

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

В диалоге System Scanner по умолчанию отображается действие **Карантин**.

Разрешенные действия

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

Лечить

System Scanner вылечит инфицированный файл, если это будет возможно.

Переименовать

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

Карантин

System Scanner помещает файлы на [Карантин](#). Файл может быть восстановлен менеджером карантина, если он имеет информативную ценность, или его можно отправить в центр исследования вирусов компании Avira. В зависимости от типа файла в менеджере карантина есть возможность выбора разных действий.

Удалить

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

Пропустить

Файл пропускается.

Переписать и удалить

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

По умолчанию

При помощи этой кнопки Вы можете определить стандартное действие System Scanner для лечения инфицированного файла. Выделите действие и нажмите кнопку "**По умолчанию**". В комбинированном режиме уведомлений для инфицированных файлов может выполняться только выбранное действие по умолчанию. В индивидуальном и экспертном режиме уведомлений выбранное действие по умолчанию для инфицированных файлов может быть выбрано предварительно.

Указание

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

Указание

Если вы выбрали действие по умолчанию **Удалить** или **Переписать и удалить**, и хотите установить комбинированный режим уведомлений, помните следующее: при обнаружении системой эвристического поиска инфицированные файлы не удаляются, а перемещаются в карантин.

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.

Показывать предупреждения

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

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.

Дополнительные действия

Запуск программы после обнаружения

После проверки System Scanner может открыть любой файл по вашему выбору (например, программу), если был обнаружен хотя бы один вирус или хотя бы одна вредоносная программа, например, почтовый клиент, чтобы уведомить других пользователей или администратора о факте обнаружения объекта.

Примечание

По соображениям безопасности после обнаружения вируса программу можно запустить только в том случае, если пользователь зарегистрирован в системе. Файл запускается с правами, действующими для активного пользователя. Если в системе не зарегистрирован ни один пользователь, эта функция не используется.

Имя программы

В этом поле ввода вы можете указать имя и местонахождение программы, которая должна запускать System Scanner после обнаружения опасного объекта.



Эта кнопка открывает окно, в котором вы можете выбрать нужную программу с помощью Проводника.

Аргументы

В этом поле ввода вы можете при необходимости указать параметры командной строки для запускаемой программы.

Протокол событий

Запись в протокол событий

Если опция включена, то при завершении проверки модулем System Scanner в журнал регистрации событий Windows будет передано сообщение о событии с результатами поиска. События можно просмотреть в списке событий Windows. Эта опция по умолчанию отключена.

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.

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*

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.

Указание

Если вы администрируете продукт Avira под AMC, при указании путей для имен процессов и файлов можно использовать переменные. Список разрешенных переменных приведен в [Переменные: Исключения Real-Time Protection и System Scanner](#).

Эвристика

Этот раздел настроек содержит параметры эвристического поиска.

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 происхождения 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.

8.2.2 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.

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.

8.3 Real-Time Protection

Раздел Real-Time Scanner в Настройке отвечает за настройку постоянной защиты в режиме реального времени.

8.3.1 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.

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.

*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.

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 "**Подробнее**". 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](#))

Показывать предупреждения

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

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.

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.

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](#).

Если вы администрируете продукт Avira под АМС, при указании путей для имен процессов и файлов можно использовать переменные. Список разрешенных переменных приведен в [Переменные: Исключения Real-Time Protection и System Scanner](#).

Примеры исключенных процессов

- приложение.exe
Процесс приложение.exe будет исключен из проверки Real-Time Protection, независимо от того, на каком жестком диске и в какой папке находится приложение.exe.
- C:\Программы1\приложение.exe
Процесс файла приложение.exe, расположенного в папке C:\Программы1, будет исключен из проверки службой Real-Time Protection.
- C:\Программы1*.exe
Все выполняемые файлы, расположенные в папке C:\Программы1, будут исключены из проверки службой Real-Time Protection.

Примеры исключенных файлов

- *.mdb
Все файлы с расширением "mdb" будут исключены из проверки службой Real-Time Protection.
- *.xls*
Все файлы, расширение которых начинается с "xls", будут исключены из проверки службой Real-Time Protection, например, файл с расширением .xls и xlsx.
- C:\папка*.log
Все файлы журнала с расширением "log", сохраненные в папке C:\папка, будут исключены из проверки службой Real-Time Protection.
- \\Имя компьютера1\разрешение1\
Из проверки службой Real-Time Protection будут исключены все файлы, обращение к которым осуществляется через "*Имя компьютера1*\разрешение1". Как правило, это подключенный сетевой диск, который обращается с именем компьютера '*Имя компьютера1*' и именем разрешения '*Разрешение1*' к другому компьютеру с разрешенной папкой.
- \\1.0.0.0\Разрешение1*.mdb
Из проверки службой Real-Time Protection будут исключены все файлы с расширением "mdb", обращение к которым осуществляется через "*1.0.0.0*\Разрешение1". Как правило, это подключенный сетевой диск, который

обращается с IP-адресом "1.0.0.0" и именем общей папки "Freigabe1" к другому компьютеру с общей папкой.

Эвристика

Этот раздел настроек содержит параметры эвристического поиска.

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 происхождения 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.

8.3.2 Отчет

Модуль Real-Time 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 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 включается 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. Место сохранения см. [Папка для отчетов](#).

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.

8.4 Переменные: Исключения для Real-Time Protection и System Scanner

Если вы администрируете свой продукт Avira под АМС, то при указании исключений для Real-Time Protection и System Scanner можно использовать переменные. При сохранении настроек на администрируемой компьютере переменные заменяются значениями, соответствующими операционной системе и языку операционной системы.

Можно использовать следующие переменные:

8.4.1 Переменные в Windows XP 32-Bit (**английский)

Переменная	Windows XP 32-Bit (**английский)
%WINDIR%	<i>C:\Windows</i>
%SYSDIR%	<i>C:\Windows\System32</i>
%ALLUSERSPROFILE%	<i>C:\Documents and Settings\All Users **</i>
%PROGRAMFILES%	<i>C:\Program Files **</i>
%PROGRAMFILES(x86)%	<i>C:\Program Files(x86) **</i>
%SYSTEMROOT%	<i>C:\Windows</i>

%INSTALLDIR%	<i>C:\Program Files\Avira\Antivir Desktop **</i>
%AVAPPDATA%	<i>C:\Documents and Settings\All Users\Avira\AntiVir Desktop **</i>

Отмеченные ** пути зависят от языка. В качестве примера здесь указаны названия, используемые в англоязычных операционных системах.

8.4.2 Переменные в Windows 7 32-Bit/ 64-Bit (**английский)

Переменная	Windows 7 32-Bit (**английский)	Windows 7 64-Bit (**английский)
%WINDIR%	<i>C:\Windows</i>	<i>C:\Windows</i>
%SYSTEMROOT%	<i>C:\Windows</i>	<i>C:\Windows</i>
%SYSDIR%	<i>C:\Windows\System32</i>	<i>C:\Windows\System32</i>
%ALLUSERSPROFILE%	<i>C:\ProgramData</i>	<i>C:\ProgramData</i>
%PROGRAMFILES%	<i>C:\Program Files **</i>	<i>C:\Program Files **</i>
%PROGRAMFILES(x86)%	<i>C:\Program Files (x86) **</i>	<i>C:\Program Files (x86) **</i>
%SYSTEMROOT%	<i>C:\Windows</i>	<i>C:\Windows</i>
%INSTALLDIR%	<i>C:\Program Files\Avira\Antivir Desktop **</i>	<i>C:\Program Files (x86)\Avira\Antivir Desktop **</i>
%AVAPPDATA%	<i>C:\ProgramData\Avira\AntiVir Desktop</i>	<i>C:\ProgramData\Avira\AntiVir Desktop</i>

Отмеченные ** пути зависят от языка. В качестве примера здесь указаны названия, используемые в англоязычных операционных системах.

8.5 Обновление

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

Примечание

Если вы настраиваете продукт Avira в Avira Management Console, настройка автоматического обновления недоступна.

Автоматическое обновление**Включить**

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

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.

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.

Загрузить**С веб-сервера**

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

Примечание

Другие настройки обновления через веб-сервер находятся здесь:

[Настройка > Безопасность компьютера > Обновление > Веб-сервер.](#)

Включив эту опцию сконфигурируйте веб-сервер и, при необходимости, прокси-сервер.

Через файловый сервер / общие папки

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

Примечание

Другие настройки обновления через файловый сервер находятся здесь: [Настройка > Безопасность компьютера > Обновление > Файловый сервер](#) . Включив эту опцию, сконфигурируйте файловый сервер, который нужно использовать.

8.5.1 Файловый сервер

Если несколько компьютеров объединены в сеть, ваш продукт Avira может загружать обновление с файлового сервера в Интранете, который, в свою очередь, загружает файлы обновления с сервера загрузки производителя в Интернете. Это позволяет поддерживать на всех компьютерах самый современный уровень продуктов Avira, экономя ресурсы. (Эти опции доступны только при включенном экспертном режиме.)

Указание

Раздел конфигурации активирован только в том случае, если в разделе [Настройка > Безопасность компьютера > Обновление](#) была выбрана опция **Через файловый сервер / Общие папки**.

Загрузка

Файловый сервер

Укажите файловый сервер, на котором находятся файлы обновления вашего продукта Avira, а также необходимые папки `'/release/update/`. Необходимо указать следующее: `file://<IP-адрес файлового сервера>/release/update/`. Каталог `'release'` должен быть папкой, доступной для всех пользователей.



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

Сервер Логин

Логин

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

Логин Пароль

Введите пароль используемой учетной записи пользователя. Вводимые символы скрываются при помощи *.

Примечание

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

8.5.2 Веб-сервер

Веб-сервер

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

*Соединение с веб-сервером***Использовать имеющееся соединение (сеть)**

Эта настройка отображается, если используется соединение через сеть.

Использовать следующее соединение

Эта настройка отображается, если вы настраиваете соединение индивидуально.

Программа обновлений автоматически определяет, какие опции соединения доступны. Несуществующие опции соединения отображаются на сером фоне, их нельзя активировать. Например, модемное соединение можно настроить вручную, внося 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.

Загрузка

Приоритетный сервер

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

Сервер по умолчанию

Укажите адреса (URL) веб-серверов, с которых необходимо загрузить обновления, а также необходимую папку обновлений 'update'. Веб-сервер должен быть указан следующим образом: `http://<адрес веб-сервера>[:Port]/update`. Если вы не укажете порт, будет использоваться порт 80. По умолчанию здесь указаны адреса доступных серверов Avira для скачивания обновлений. Однако вы можете также использовать собственные веб-серверы, например, во внутренней сети. При указании нескольких серверов, серверы разделяются запятыми.

По умолчанию

Эта кнопка позволяет восстановить предустановленные адреса.

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

8.6 Firewall

8.6.1 Конфигурация FireWall

Avira Professional Security позволяет конфигурировать брандмауэр Avira FireWall или брандмауэр Windows:

- [Avira FireWall](#)
- [Avira FireWall в AMC](#)
- [брандмауэр Windows](#)

8.6.2 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.

- [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. ICMP 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 <i>Низкий</i> .
Высокий	Блокирует входящие типы: различные типы . Блокирует исходящие типы: различные типы . Подозрение на флудинг, если задержка между пакетами составляет менее 50 миллисекунд. Фрагментированные ICMP-пакеты отклонять .

Заблокированные входящие типы: ни один тип/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 <i>Средний</i> .

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 <i>Средний</i> .

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	<ul style="list-style-type: none"> <li data-bbox="327 398 1294 734"> <p>• 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.</p> <li data-bbox="327 748 1294 1084"> <p>• Запрещать TCP-пакеты на порт 135 TCP-пакеты Отклонить, с адреса 0.0.0.0 с маской 0.0.0.0, если локальный 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.</p> <li data-bbox="327 1097 1294 1433"> <p>• 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.</p> <li data-bbox="327 1447 1294 1783"> <p>• 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.</p>

Высокий	<p>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.</p>
----------------	---

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	<ul style="list-style-type: none"> 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	<p>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.</p>
----------------	--

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	<p>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.</p>
Высокий	Те же правила, что при настройке <i>Средний</i> .

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	<p>Отображает действие, которое Avira FireWall выполнит автоматически, если приложение каким-либо образом использует сеть.</p> <p>Щелчком по этой ссылке можно сменить тип выполняемого действия.</p> <p>На выбор предлагаются следующие варианты действий: Спрашивать, Разрешить или Отклонить. Настройка по умолчанию - Спрашивать.</p>

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.

- ▶ Теперь в **Настройка > Интернет-безопасность > FireWall > Настройки** измените настройку для *Правил приложения*: включите опцию **Расширенные настройки** и сохраните настройку нажатием на **Применить** или **ОК**.
- ↪ 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	<p>Отображает действие, которое Avira FireWall выполнит автоматически, если приложение каким-либо образом использует сеть.</p> <p>При установке Фильтр - простой вы можете щелчком мыши по ссылке сменить тип выполняемого действия. На выбор предлагаются следующие варианты действий: Спрашивать, Разрешить или Отклонить.</p> <p>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.</p>
Фильтр	<p>Отображает тип фильтра. Щелчком мыши по ссылке можно сменить тип фильтра.</p> <p>Простой: При простой фильтрации указанное действие выполняется для всей типов сетевой активности приложения программы.</p> <p>Расширенный: при фильтрации выполняются правила, сохраненные в расширенной настройке.</p>

- ▶ 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 <i>Свойства</i> отображается детальная информация о приложении, выбранном вами в списке приложений.
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.

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 разработчиков, которые классифицируются как надежные.

Кнопки

Кнопка	Описание
Удалить	Отмеченная запись удаляется из списка надежных разработчиков. Чтобы окончательно удалить производителя из списка, нажмите Применить или ОК 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*Расширенные настройки***Включить FireWall**

Если выбрана эта опция, модуль Avira FireWall активен и защищает ваш компьютер от различных опасностей, исходящих со стороны Интернета и других сетей.

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

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.

8.6.3 Avira FireWall в АМС

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

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

Если ваш продукт Avira администрируется через Avira Security Management Center, отключены следующие возможности настройки FireWall в Центре управления на компьютерах-клиентах:

- Настройка уровней безопасности FireWall
- Настройка правил адаптера и приложений

Общие настройки

Расширенные настройки

Включить FireWall

Если выбрана эта опция, модуль Avira FireWall активен и защищает ваш компьютер от различных опасностей, исходящих со стороны Интернета и других сетей.

Отключать при загрузке брандмауэр Windows

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

Режим обучения

Если выбрана эта опция, активен режим обучения Avira FireWall.

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.

Общие правила адаптера

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

- **Стандартный** адаптер: локальная сеть или высокоскоростной Интернет
- **Беспроводной**
- **Вызов** Соединение

Для каждого доступного адаптера вы можете установить с помощью контекстного меню установленные по умолчанию правила (**Общие правила адаптеров**, щелчок правой кнопкой мыши на **Рабочее место** или **Стандарт, беспроводное соединение, вызов**, и т.д.):

- Установить уровень безопасности на «Низкий»
- Установить уровень безопасности на «Средний»
- Установить уровень безопасности на «Высокий»

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

Указание

Стандартная настройка Уровня безопасности для всех predetermined правил модуля Avira FireWall - **Средний**.

- [ICMP-протокол](#)
- [Сканирование порта TCP](#)
- [Сканирование порта UDP](#)
- [Входящее правило](#)
- [Правило IP-протокола](#)
- [Исходящее правило](#)
- [Кнопка](#)

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. ICMP 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	То же правило, что и для настройки "Низкий".
Высокий	Блокирует входящие типы: различные типы . Блокирует исходящие типы: различные типы . Подозрение на флудинг, если задержка между пакетами составляет менее 50 миллисекунд. Фрагментированные ICMP-пакеты отклонять .

Заблокированные входящие типы: ни один тип/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.

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, принимаются ли или отклоняются 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 блокирования атаки.
Высокий	Те же правила, что при настройке <i>Средний</i> .

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 порта TCP.

Файл отчета

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

Правило

Здесь Вы можете определить правила, по которым принимается решение о необходимости блокирования атаки сканирования порта 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 блокирования атаки.
Высокий	Те же правила, что при настройке <i>Средний</i> .

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.

Файл отчета

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

Правило

Здесь Вы можете определить правила, по которым принимается решение о необходимости блокирования атаки сканирования порта 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	<ul style="list-style-type: none"> <p>• 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: отклонять пакеты со следующими байтами <пустой> с маской <пустой> при оффсете 0.</p> <p>• Запрещать TCP-пакеты на порт 135 TCP-пакеты Отклонить, с адреса 0.0.0.0 с маской 0.0.0.0, если локальный порт находится в {135}, а удаленный порт в {0-65535}. Применять ко всем пакетам. Не записывать в банк событий, если пакет соответствует правилу. Дополнительно: отбирать пакеты, содержащие байты <пусто> с маской <пусто> при оффсете 0.</p> <p>• 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.</p> <p>• 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.</p>

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 .
----------------	---

TCP-пакеты разрешать / запрещать

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

IPv4 / IPv6

Щелчком по ссылке выберите IPv4 или IPv6.

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемый IPv4- или IPv6-адрес.

IP-маска

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемую IPv4- или IPv6-маску.

Локальные порты

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

Удаленные порты

Щелчком по этой ссылке открывается диалоговое окно, в котором можно указать один или несколько удаленных портов или 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.

Файл отчета

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

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

Фильтрация по содержимому: данные

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	<ul style="list-style-type: none"> 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	<p>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, 123}.</p> <p>Применять правило к открытым портам для всех потоков данных.</p> <p>Не записывать в банк событий, , если пакет соответствует правилу.</p> <p>Дополнительно: отбирать пакеты, содержащие байты <пусто> с маской <пусто> при оффсете 0.</p>
----------------	--

Разрешать / запрещать UDP-пакеты

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

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемый IPv4- или IPv6-адрес.

IP-маска

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемую IPv4- или IPv6-маску.

Локальные порты

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

Удаленные порты

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

Метод применения

Щелчком по этой ссылке можно определить необходимость применения правила ко всем портам или только ко всем открытым портам.

Файл отчета

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

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

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

Фильтрация по содержимому: данные

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 <i>Средний</i> .

Разрешать / запрещать ICMP-пакеты

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

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемый IPv4- или IPv6-адрес.

IP-маска

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемую IPv4- или IPv6-маску.

Файл отчета

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

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

Фильтрация по содержимому: данные

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	Отклонять все IP-пакеты Отклонять IPv4-пакеты с адреса 0.0.0.0 с маской 0.0.0.0. Не записывать в банк событий , если пакет соответствует правилу.

Разрешать / запрещать IP-пакеты

Щелчком по этой ссылке можно установить необходимость разрешения или запрета определенных IP-пакетов.

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемый IPv4- или IPv6-адрес.

IP-маска

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемую IPv4- или IPv6-маску.

Файл отчета

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

Правила мониторинга IP-пакетов на основании IP-протоколов:

IP-пакеты

Щелчком по этой ссылке можно установить необходимость разрешения или запрета определенных IP-пакетов.

IP-адрес

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемый IPv4- или IPv6-адрес.

IP-маска

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете указать желаемую IPv4- или IPv6-маску.

Протокол

Щелчком по этой ссылке открывается диалоговое окно, в котором вы можете выбрать нужный IP-протокол.

Файл отчета

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

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.

Список приложений

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

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

При добавлении приложений устанавливается правило **Разрешить**.

Список приложений

В этой таблице приведен список приложений, для которых определены правила. Символы показывают, разрешается или блокируется сетевой доступ для приложений. Вы можете изменять правила для приложений с помощью контекстного меню.

Кнопки

Кнопка	Описание
Добавить на основании пути	При помощи кнопки открывается диалоговое окно, в котором можно выбрать приложения. Приложение добавляется к списку приложений с правилом " Разрешить ". При использовании опции " Добавить на основании пути " добавленное приложение идентифицируется модулем FireWall, исходя из пути и имени файла.
Добавить на основании md5	Нажатием на эту кнопку открывается диалоговое окно, в котором можно выбирать приложения. Приложение добавляется к списку приложений с правилом " Разрешить ". При использовании опции " Добавить на основании md5 ", все добавленные приложения однозначно идентифицируются на основании контрольной суммы MD5. Это позволяет модулю FireWall обнаруживать изменения в содержимом файлов. Если приложение изменяется, например, в связи с обновлением, то приложение с установленным правилом автоматически удаляется из списка. После изменения приложение необходимо снова добавить к списку и заново задать необходимое правило.
Добавить группу	При помощи этой кнопки открывается диалоговое окно, в котором можно выбрать нужную папку. Все приложения для выбранного пути добавляются к списку приложений с правилом " Разрешить ".
Удалить	Выбранное правило приложения удаляется.

Удалить все	Удаление всех правил приложения.
--------------------	----------------------------------

Надежные разработчики

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

Поставщики

Список содержит всех разработчиков, которые классифицируются как надежные.

Кнопки

Кнопка	Описание
Добавить	При помощи кнопки открывается диалоговое окно, в котором можно выбрать приложения. Определяется разработчик приложения и добавляется к списку надежных разработчиков.
Добавить группу	При помощи этой кнопки открывается диалоговое окно, в котором можно выбрать нужную папку. Производители всех приложений для выбранного пути устанавливаются и добавляются к списку надежных разработчиков.
Удалить	Отмеченная запись удаляется из списка надежных разработчиков. Чтобы окончательно удалить производителя из списка, нажмите " Применить " или " ОК " в окне настройки.
Удалить все	Все записи удаляются из списка надежных разработчиков.

Обновить	Внесенные изменения отменяются: загружается последний сохраненный список.
-----------------	---

Примечание

Если вы удалите разработчиков из списка, а затем нажмете кнопку **Применить**, разработчики будут окончательно удалены из списка. Изменение не может быть отменено командой **Обновить**.

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.

Дополнительные настройки

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.

Настройки всплывающего окна

Проверить стартовый блок процесса

Если эта опция включена, происходит более тщательная проверка списка процессов. FireWall исходит из того, что каждый процесс из списка, не классифицированный как надежный, запускает 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 эта 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.

Настройки отображения

Сохранить действие для этого приложения

Всегда вкл.

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

Всегда откл.

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

Разрешать подписанные приложения

Если эта опция включена, то при доступе подписанных приложений определенных разработчиков к сети автоматически включается опция **"Сохранять действие для приложения"** диалогового окна **"Сетевое событие"**. Таким разработчиками являются: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlett Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Запомнить последнее состояние

Если выбрана эта опция, то опция **"Сохранить действие для этого приложения"** диалогового окна **"Сетевое событие"** находится в том же состоянии, что и 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 можно 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 эта опция включена, в окне "**Сетевое событие**" всегда будут отображаться подробности.

Запомнить последнее состояние

Если эта опция включена, сохраняется статус отображения подробностей, выбранный 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.

8.6.4 брандмауэр Windows

Раздел **FireWall** в меню **Конфигурация > Интернет-безопасность** отвечает за настройку брандмауэр Windows в операционных системах, начиная с Windows 7.

брандмауэр Windows

Включить брандмауэр Windows под управлением Avira

При активированной опции Avira управляет брандмауэр Windows.

Профили сети

Профили сети

С помощью сетевых профилей брандмауэр Windows блокирует доступ неразрешенных программ и приложений к вашему компьютеру:

- **Частная сеть**: для домашних или офисных сетей
- **Общая сеть**: для публичных сетей
- **Сеть домена**: для сетей с контроллером домена

Вы можете управлять этими профилями через конфигурацию вашего продукта Avira в меню **Интернет-безопасность > брандмауэр Windows > Профили сети**.

Дополнительную информацию об этих сетевых профилях можно найти на официальном сайте Microsoft.

Предупреждение

брандмауэр Windows применяет одинаковые правила для всех сетей, относящихся к одному профилю. Это значит, если вы даете разрешение на доступ для какой-либо программы или приложения, то у них также будет доступ ко всем сетям, которые используют этот же профиль.

Частная сеть*Настройки частной сети*

Настройки частной сети регулируют доступ к вашему компьютеру других компьютеров или устройств в вашей домашней или офисной сети. Эти настройки по умолчанию допускают, чтобы пользователи частной сети видели ваш компьютер и могли получить к нему доступ.

Включить

При активированной опции включается Windows FireWall под управлением Avira.

Блокировать все входящие подключения

При активированной опции Windows FireWall отклоняет все нежелательные попытки соединения с вашим компьютером, включая входящие соединения от разрешенных приложений.

Уведомлять при блокировке нового приложения

При активированной опции будет появляться соответствующее оповещение при каждой блокировке программы или приложения.

Отключить (не рекомендуется)

Если данная опция активирована, Windows FireWall отключается. Активация данной опции нежелательна, поскольку компьютер при этом подвержен повышенной опасности.

Общая сеть*Настройки публичной сети*

Настройки публичной сети регулируют доступ других компьютеров или устройств к вашему компьютеру в публичных сетях. Эти настройки по умолчанию не допускают, чтобы пользователи в публичной сети видели ваш компьютер и могли получить к нему доступ.

Включить

При активированной опции включается Windows FireWall под управлением Avira.

Блокировать все входящие подключения

При активированной опции Windows FireWall отклоняет все нежелательные попытки соединения с вашим компьютером, включая входящие соединения от разрешенных приложений.

Уведомлять при блокировке нового приложения

При активированной опции будет появляться соответствующее оповещение при каждой блокировке программы или приложения.

Отключить (не рекомендуется)

Если данная опция активирована, Windows FireWall отключается. Активация данной опции нежелательна, поскольку компьютер при этом подвержен повышенной опасности.

Сеть домена

Настройки доменной сети

Настройки доменной сети регулируют доступ к вашему компьютеру других компьютеров или устройств, если ваш компьютер соединен с сетью, аутентифицированной через контроллер домена. Эти настройки по умолчанию допускают, чтобы аутентифицированные пользователи домена видели ваш компьютер и могли получить к нему доступ.

Включить

При активированной опции включается Windows FireWall под управлением Avira.

Блокировать все входящие подключения

При активированной опции Windows FireWall отклоняет все нежелательные попытки соединения с вашим компьютером, включая входящие соединения от разрешенных приложений.

Уведомлять при блокировке нового приложения

При активированной опции будет появляться соответствующее оповещение при каждой блокировке программы или приложения.

Отключить (не рекомендуется)

Если данная опция активирована, брандмауэр Windows отключается. Активация данной опции нежелательна, поскольку компьютер при этом подвержен повышенной опасности.

Указание

Эта опция доступна лишь в том случае, если ваш компьютер соединен с сетью, оборудованной контроллером домена.

Правила приложения

Если щелкнуть по ссылке в меню **брандмауэр Windows > Правила приложения**, то будет выполнен переход к меню **Разрешенные программы и компоненты** конфигурации брандмауэр Windows.

Дополнительные параметры

Если щелкнуть по ссылке в меню **брандмауэр Windows > Дополнительные параметры**, то будет выполнен переход к меню **брандмауэр Windows в режиме повышенной безопасности** конфигурации брандмауэр Windows.

8.7 Web Protection

Раздел **Web Protection** в **Настройка > Интернет-безопасность** отвечает за настройку функции Web Protection.

8.7.1 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.

Поиск

Включить Web Protection

Если эта опция включена, функция Web Protection активна.

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.

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.

Разрешенные действия

В этом окне вы можете выбрать действия, которые отображаются в диалоговом окне при обнаружении вируса или вредоносной программы. Для этого должны быть активированы соответствующие опции.

Запретить доступ

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

По умолчанию

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

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.

Показывать предупреждения

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

Первичное действие

Первичное действие - это действие, выполняемое в случае, когда 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.

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.

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.

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 происхождения 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.

8.7.2 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.

8.8 Mail Protection

Раздел Mail Protection в Настройке отвечает за настройку защиты модуля.

8.8.1 Поиск

Модуль Mail Protection используется для проверки входящей почты на наличие вирусов, вредоносного ПО. 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.

Включить Mail Protection

Если выбрана эта опция, то обмен электронными сообщениями контролируется модулем Mail Protection. Mail Protection - это прокси-сервер, который проверяет обмен данными между почтовым сервером, который вы используете, и почтовой программой, установленной на компьютере: по умолчанию входящие письма проверяются на наличие вредоносного ПО. Если эта опция отключена, служба Mail Protection запускается, но не контролирует почту.

Проверять входящую почту

Если эта опция активирована, то входящие письма проверяются на вирусы, вредоносные программы. 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.

По умолчанию

Кнопка возвращает заданные порты к стандартному порту для POP3.

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.

По умолчанию

Кнопка возвращает настройки по умолчанию для порта IMAP.

Проверять исходящую почту (SMTP)

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

Контролируемые порты

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

По умолчанию

Кнопка возвращает заданные порты к стандартному порты для SMTP.

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 не доступна 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.

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**.

Разрешенные действия

В этом окне вы можете выбрать действия, которые отображаются в диалоговом окне при обнаружении вируса или вредоносной программы. Для этого должны быть активированы соответствующие опции.

Поместить на карантин

Если эта опция включена, электронное сообщение с вложениями помещается в карантин. Оно может быть позже доставлено через [Менеджер карантина](#). Инфицированное письмо удаляется. Тело письма и приложения к нему, если они есть, заменяются Стандартным текстовым шаблоном.

Удалить письмо

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

Удалить приложение

Если эта опция включена, инфицированное приложение заменяется текстовым шаблоном. Если поврежден текст письма, то оно удаляется и заменяется текстовым шаблоном. Письмо доставляется адресату.

Поместить приложение на карантин

Если выбрана эта опция, инфицированное вложение помещается в Карантин, а затем удаляется (заменяется текстовым шаблоном). Текст письма доставляется адресату. Инфицированное приложение может быть позже доставлено адресату из [Менеджера карантина](#).

Пропустить

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

По умолчанию

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

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.

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.

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 происхождения 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.

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.

8.8.2 Общее

Исключения

Адреса, не подвергающиеся проверке

В этой таблице содержится список адресов, исключенных из сканирования модулем Avira Mail Protection (белый список).

Примечание

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 сканированию. В дальнейшем, в зависимости от настроек, адрес не будет проверяться модулем Mail Protection.

Добавить

С помощью этой кнопки можно добавить адрес, указанный в поле ввода, к списку не подвергающихся сканированию адресов.

Удалить

Эта кнопка удаляет выделенный адрес электронной почты из списка.

Адрес электронной почты

Адрес электронной почты, который больше не должен подвергаться сканированию.

Вредоносное ПО

Если эта функция включена, адрес электронной почты больше не сканируется на наличие вредоносного ПО.

Наверх

Кнопка перемещает выделенный адрес электронной почты на одну позицию вверх. Эта кнопка неактивна, если не выделена ни одна строка или если курсор стоит на верхней строке списка.

Вниз

Кнопка перемещает выделенный адрес электронной почты на одну позицию вниз. Эта кнопка неактивна, если не выделена ни одна строка или если курсор стоит на нижней строке списка.

Буфер

Буферная память модуля Mail Protection содержит данные о проверенных письмах, которые отображаются в статистике в Центре управления в разделе **Mail Protection**.

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.

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.

8.8.3 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. Место сохранения см. [Настройка > Общие > Папки > Папка файла отчета](#).

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.

8.9 Общее

8.9.1 Категории угроз

Выбор расширенных категорий угроз

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.

8.9.2 Расширенная защита

Расширенная защита

ProActiv

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 заблокировать 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***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.

Сканирование файлов в реальном времени

Если данная функция включена, то неизвестные файлы, по мере доступа к ним, отправляются в Protection Cloud для анализа.

Показать статус загрузки в Avira Protection Cloud

В окне в виде индикатора выполнения отображается следующая информация о загружаемых файлах:

- местоположение файла;
- имя файла;
- состояние (загрузка/анализ);
- результат (безопасен/заражен).

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.

8.9.3 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

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	Если 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.
Карантин	Если эта опция включена
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.
Загрузить восстановление CD из Интернета	Если эта опция включена, требуется установленный пароль для запуска загрузки восстановления CD Avira.
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.

8.9.4 Безопасность

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 !

8.9.5 WMI

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

Активировать WMI-поддержку

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

Разрешить включение / выключение служб

Если эта функция включена, вы можете включать или выключать через WMI службы программы.

8.9.6 События

Ограничить размер банка событий

Установить максимальный размер не более n записей

Если эта функция включена, можно ограничить максимальное количество записей в банке событий 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.

8.9.7 Отчеты

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.

8.9.8 Папки

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.

Папка для отчетов

Поле ввода

Это поле содержит абсолютный путь к папке отчетов.



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

По умолчанию

Нажатием на эту кнопку восстанавливается предустановленный путь к папке отчетов.

Папка карантина

Поле ввода

Это поле содержит путь к папке карантина.



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

По умолчанию

Нажатием на эту кнопку восстанавливается предустановленный путь для папки карантина.

8.9.9 Акустический сигнал предупреждения

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.

8.9.10 Предупреждения

Сеть

Вы можете отправить любые сконфигурированные вами сообщения от [System Scanner](#) или от [Real-Time Scanner](#) на любой компьютер вашей сети.

Примечание

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

Предупреждение

Предупреждение всегда отправляется на компьютер, а не определенному пользователю.

Предупреждение

Эта функция **больше не поддерживается** следующими операционными системами:

- Windows Server 2008 и выше
- Windows Vista и выше

Сообщение отправлять

Список в данном окне содержит имена компьютеров, которые получают сообщение в случае обнаружения.

Примечание

Компьютер можно внести в список только один раз.

Добавить

С помощью этой кнопки вы можете добавлять компьютеры. Открывается окно, в которое можно добавить имя нового компьютера. Длина имени компьютера не может превышать 15 знаков.



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

Удалить

С помощью этой кнопки вы можете удалить из списка отмеченную в данный момент запись.

Real-Time Scanner - Сетевые уведомления

Сетевые уведомления

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

Примечание

Чтобы было возможно активировать эту опцию, в разделе [Настройки > Общее > Предупреждения > Сеть](#) должны быть указаны хотя бы один получатель.

Сообщение для отправки

Окно показывает сообщение, отправляемое на выбранный компьютер при обнаружении вируса. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующие комбинации клавиш используются для форматирования сообщения:

Горячие клавиши	Описание
Ctrl + Tab	Вставляет табулятор Текущая строка сдвигается на несколько символов вправо.
Ctrl + Ввод	Вставляет разрыв строки.

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

Применяются следующие символы-заполнители:

Символ-заполнитель	Описание
%VIRUS%	Содержит имя обнаруженного вируса или нежелательной программы
%FILE%	Содержит путь и имя инфицированного файла
%COMPUTER%	Содержит имя компьютера, на котором запущен Real-Time Scanner
%NAME%	Содержит имя пользователя, обращавшегося к инфицированному файлу
%ACTION%	Содержит действие, выполненное после обнаружения вируса
%MACADDR%	Содержит MAC-адрес компьютера, на котором запущен Real-Time Scanner

По умолчанию

Кнопка восстанавливает предустановленный стандартный текст для предупреждающего сообщения.

System Scanner - Сетевые уведомления

Сетевые уведомления

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

Примечание

Чтобы было возможно активировать эту опцию, в разделе [Настройки > Общее > Предупреждения > Сеть](#) должен быть указан хотя бы один получатель.

Сообщение для отправки

Окно показывает сообщение, отправляемое на выбранный компьютер при обнаружении вируса. Вы можете редактировать это сообщение. Размер текста не должен превышать 500 символов.

Следующие комбинации клавиш используются для форматирования сообщения:

Горячие клавиши	Описание
Ctrl + Tab	Вставляет табулятор Текущая строка сдвигается на несколько символов вправо.
Ctrl + Ввод	Вставляет разрыв строки.

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

Применяются следующие символы-заполнители:

Символ-заполнитель	Описание
%VIRUS%	Содержит имя обнаруженного вируса или нежелательной программы
%NAME%	Содержит имя зарегистрированного пользователя, запустившего System Scanner
%FILE%	Содержит путь и имя инфицированного файла
%COMPUTER%	Содержит имя компьютера, на котором запущен System Scanner
%ACTION%	Содержит действие, выполненное после обнаружения вируса
%MACADDR%	Содержит MAC-адрес компьютера, на котором запущен System Scanner

По умолчанию

Кнопка восстанавливает предустановленный стандартный текст для предупреждающего сообщения.

Электронная почта

Продукт Avira может при наступлении определенных событий отправлять по электронной почте сообщения одному или нескольким получателям. Для этого используется Simple Message Transfer Protocol (SMTP).

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

- [Real-Time Scanner - Уведомления по электронной почте](#)
- [System Scanner - Уведомления по электронной почте](#)
- [Программа обновлений - Уведомления по электронной почте](#)

Примечание

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

Сообщения электронной почты

SMTP-сервер

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

Например:

192.168.1.100 или mail.firma.ru.

Порт

Укажите здесь нужный порт.

Адрес отправителя

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

Аутентификация

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

Использовать аутентификацию

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

Имя пользователя

Укажите здесь ваше имя пользователя.

Пароль

Укажите здесь соответствующий пароль. Пароль сохраняется в закодированном виде. Для безопасности вводимые в это поле знаки заменяются звездочками (*).

Отправить тестовое письмо

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

Real-Time Protection - Уведомления по электронной почте

Avira Real-Time Protection может при наступлении определенных событий высылать по электронной почте уведомление одному или нескольким пользователям.

Предупреждения по электронной почте

Если эта опция включена, Avira Real-Time Protection при наступлении определенных событий отправляет по электронной почте сообщения с основными данными о них. По умолчанию эта опция отключена.

Уведомление по электронной почте при наступлении следующих событий

При проверке системы сканером в режиме реального времени обнаружен вирус или вредоносная программа

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

Редактировать

При помощи кнопки "**Редактировать**" открывается окно "**Шаблон письма**", в котором Вы можете редактировать сообщение для события "Обнаружение вируса системой постоянной защиты". Вы можете ввести тексты для темы и содержания электронного письма. При этом можно использовать переменные. (См. [Шаблон письма](#))

В модуле Real-Time Protection возникла критическая ошибка

Если эта опция включена, вы получите электронное сообщение в случае обнаружения внутренней критической ошибки.

Указание

В этом случае свяжитесь с нашей службой [Технической поддержки](#) и отправьте ей данные, содержащиеся в электронном уведомлении. Указанный файл также необходимо выслать для проверки.

Редактировать

При помощи кнопки "**Редактировать**" открывается окно "**Шаблон письма**", в котором вы можете редактировать сообщение для события "критическая ошибка в модуле Real-Time Protection". Вы можете ввести тексты для темы и содержания электронного письма. При этом можно использовать переменные. (См. [Шаблон письма](#))

Получатель

В этом поле укажите адрес(а) электронной почты получателя(ей). Адреса разделяются между собой запятыми, общая длина не должна превышать 260 знаков (общая длина цепочки символов).

System Scanner - Уведомления по электронной почте

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

Предупреждения по электронной почте

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

Уведомление по электронной почте при наступлении следующих событий

В результате проверки был обнаружен вирус или вредоносная программа

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

Редактировать

При помощи кнопки "**Редактировать**" открывается окно "**Шаблон письма**", в котором Вы можете редактировать сообщение для события "Обнаружение вируса в процессе поиска". Вы можете ввести тексты для темы и содержания электронного письма. При этом можно использовать переменные. (См. [Шаблон письма](#))

Окончание плановой проверки

Если эта опция включена, отправляется электронное письмо, уведомляющее о выполнении проверки. Электронное письмо содержит данные о времени и продолжительности проверки, именах папок и файлов, а также об обнаруженных вирусах и предупреждениях.

Редактировать

При помощи кнопки "**Редактировать**" открывается окно "**Шаблон письма**", в котором Вы можете редактировать сообщение для события "Завершение

проверки". Вы можете ввести тексты для темы и содержания электронного письма. При этом можно использовать переменные. (См. [Шаблон письма](#))

Прикрепить файл отчета как приложение

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

Получатель

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

Программа обновлений - Уведомления по электронной почте

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

Предупреждения по электронной почте

Если эта опция включена, компонент «Программа обновлений» при наступлении определенных событий отправляет по электронной почте сообщения с основными данными. По умолчанию эта опция отключена.

Уведомления по электронной почте при наступлении следующих событий

Обновление не требуется. Программа имеет самую современную версию

Если эта опция включена, сообщение электронной почты отправляется, если Программа обновлений успешно установила соединение с сервером, но на сервере не оказалось новых файлов для загрузки. Это означает, что ваш продукт Avira обновлен до последней версии.

Редактировать

При помощи кнопки "**Редактировать**" открывается окно "**Шаблон письма**", в котором Вы можете редактировать сообщение для события "Обновление не требуется". Вы можете ввести тексты для темы и содержания электронного письма. При этом можно использовать переменные. (См. [Шаблон письма](#))

Обновление успешно завершено. Установлены новые файлы

Если эта опция включена, при выполнении каждого обновления отправляется электронное сообщение: это может быть обновлением продукта или файла вирусных сигнатур или поискового движка.

Редактировать

При помощи кнопки "**Редактировать**" открывается окно "**Шаблон письма**", в котором Вы можете редактировать сообщение для события "Обновление успешно завершено - Установка новых файлов". Вы можете ввести тексты для

темы и содержания электронного письма. При этом можно использовать переменные. (См. [Шаблон письма](#))

Не удалось выполнить обновление

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

Редактировать

При помощи кнопки "**Редактировать**" открывается окно "**Шаблон письма**", в котором Вы можете редактировать сообщение для события "Не удалось выполнить обновление". Вы можете ввести тексты для темы и содержания электронного письма. При этом можно использовать переменные. (См. [Шаблон письма](#))

Прикрепить файл отчета как приложение

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

Получатель

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

Шаблон письма

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

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

Общепринятые переменные

Переменная	Значение
Переменные окружения Windows	Компонент уведомлений по электронной почте поддерживает все переменные окружения Windows.
%SYSTEM_IP%	IP-адрес компьютера

%FQDN%	Полное имя домена (fully qualified domain name)
%TIMESTAMP%	Штемпель времени наступления события: Форматы даты и времени в соответствии с языковыми настройками операционной системы
%COMPUTERNAME%	Имя компьютера NetBIOS
%USERNAME%	Имя пользователя, имеющего доступ к компоненту
%PRODUCTVER%	Версия продукта
%PRODUCTNAME%	Название продукта
%MODULENAME%	Название компонента, отправляющего сообщение электронной почты
%MODULEVER%	Версия компонента, отправляющего сообщение электронной почты

Специфические переменные компонентов

Переменная	Значение	Электронные сообщения компонентов
%ENGINEVER%	Версия используемого поискового движка	Real-Time Protection System Scanner
%VDFVER%	Версия используемого файла вирусных сигнатур	Real-Time Protection System Scanner

%SOURCE%	Полное имя файла	Real-Time Protection
%VIRUSNAME%	Имя вируса или вредоносной программы	Real-Time Protection
%ACTION%	Действие, выполненное после обнаружения вируса	Real-Time Protection
%MACADDR%	MAC-адрес первой зарегистрированной сетевой карты	Real-Time Protection
%UPDFILESLIST%	Список обновленных файлов	Модуль обновления
%UPDATETYPE%	Тип обновления: Обновление поискового движка и файла вирусных сигнатур или обновление продукта с обновлением поискового движка и файла вирусных сигнатур	Модуль обновления
%UPDATEURL%	URL сервера, использованного для обновления	Модуль обновления
%UPDATE_ERROR%	Ошибка обновления в словах	Модуль обновления
%DIRCOUNT%	Количество проверенных папок	System Scanner
%FILECOUNT%	Количество проверенных файлов	System Scanner
%MALWARECOUNT%	Количество обнаруженных вирусов или вредоносных программ	System Scanner
%REPAIREDCOUNT%	Вылечено инфицированных файлов	System Scanner

%RENAMEDCOUNT%	Переименовано инфицированных файлов	System Scanner
%DELETEDCOUNT%	Удалено инфицированных файлов	System Scanner
%WIPECOUNT%	Количество инфицированных файлов, которые были перезаписаны и удалены	System Scanner
%MOVEDCOUNT%	Количество инфицированных файлов, помещенных в карантин	System Scanner
%WARNINGCOUNT%	Число предупреждений	System Scanner
%ENDTYPE%	Статус завершения проверки: Прервана Успешно завершена	System Scanner
%START_TIME%	Время начала проверки Время начала обновления	System Scanner, Программа обновлений
%END_TIME%	Время окончания проверки Время окончания обновления	System Scanner, Программа обновлений
%TIME_TAKEN%	Время выполнения проверки в минутах Время выполнения обновления в минутах	System Scanner, Программа обновлений
%LOGFILEPATH%	Путь и имя файла отчета	System Scanner, Программа обновления

Акустический сигнал предупреждения

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.

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.

9. Tray Icon

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

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

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
 - **Активировать брандмауэр Windows:** активирует или деактивирует брандмауэр Windows (эта функция доступна только, начиная с Windows 8).
 - **Блокировать весь трафик:** Включен: блокирует всю передачу данных за исключением передачи в собственной компьютерной системе (Local Host/IP 127.0.0.1).
- **Запустить Avira Professional Security:** Открывает [Центр управления](#).
- **Настройка Avira Professional Security :** открывает [Настройку](#).
- **Запустить обновление:** Запускает [Обновление](#).
- **Выбор настроек:** Открывает подменю с доступными профилями настроек. Нажмите на настройку, чтобы активировать ее. Команда меню деактивируется, если вы уже определили правила для автоматического переключения на настройку.
- **Справка:** Открывает справочную онлайн-систему.
- **Avira Professional Security:** Открывает диалоговое окно с информацией о вашей программе Avira: информация о продукте, номер версии, лицензия.

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

10. FireWall

Avira Professional 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 Professional Security.

- [Avira FireWall в АМС](#)

В системах, управляемых через Avira Management Console, брандмауэр Avira FireWall также содержится в Avira Professional Security.

- [брандмауэр Windows](#)

Начиная с Windows 7, брандмауэр Avira FireWall больше не содержится в Avira Professional Security. Вместо этого брандмауэром брандмауэр Windows можно управлять с помощью Центра управления сетями и общим доступом.

10.1 Avira FireWall

10.1.1 FireWall

Avira FireWall отслеживает и управляет входящим и исходящим трафиком в вашей системе и защищает ее от множества атак и угроз, исходящих из Интернета: На основании директив безопасности допускается или запрещается входящий и исходящий трафик прослушивания портов. Вы получите уведомление, если брандмауэр Avira FireWall отклоняет сетевую активность и блокирует таким образом сетевые соединения. Существует несколько вариантов настройки Avira FireWall:

с помощью настройки уровня безопасности в центре управления

В Центре управления можно задать уровень безопасности. Уровни безопасности *Низкий*, *Средний* и *Высокий* содержат несколько дополняющих друг друга правил безопасности, основанных на фильтрах пакетов. Эти правила безопасности заданы по умолчанию в настройках: [FireWall > Правила адаптера](#).

с помощью сохранения действия в окне Сетевых событий

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

Примечание

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

путем создания правил адаптера и приложений в настройках

В меню настроек можно изменять или создавать новые правила адаптера. При добавлении или изменении правил адаптера уровень безопасности брандмауэра автоматически устанавливается на значение *Пользователь*.

С помощью правил приложений можно задать правила контроля, зависящие от приложения:

С помощью простых правил приложений вы можете запретить или разрешить всю сетевую активность приложения или управлять ею интерактивно при помощи всплывающего окна *Сетевое событие*.

В расширенной настройке раздела *Правила приложения* вы можете определить различные фильтры пакетов для приложения, которые должны выполняться как специальные правила приложения.

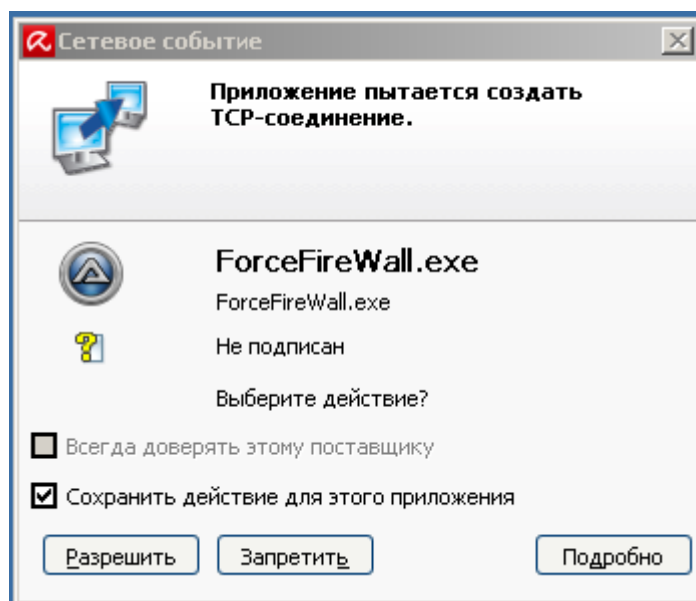
10.1.2 Сетевое событие

В окне Сетевое событие компонента Avira FireWall программе можно разрешить или запретить сетевой доступ, отправку данных или прочую сетевую активность: можно запретить или разрешить трафик или прослушивание портов. Запрет сетевой активности может привести к разрыву соединения.

Окно Сетевое событие открывается при доступе приложений к сети в следующих случаях:

- Для приложения еще не создано правил приложения. Это происходит в том случае, когда приложение впервые после установки Avira FireWall пытается установить сетевое соединение. Исключение составляют приложения, производители которых признаны надежными, поэтому для них доступ в сеть автоматически разрешен (см. гл. [Надежные разработчики](#)).
- Для приложения было создано простое правило с типом действия **Запрашивать**.
- Для приложения были созданы специальные правила, основанные на фильтрах пакетов, с расширенными настройками, но для возникшего сетевого события правил не найдено. В этом случае у вас есть возможность, используя кнопку *Дополнительно*, вызывать имеющиеся правила для приложения и установить сетевой доступ в качестве нового правила.

Сетевое событие



Отображаемая информация

Имя приложения

Имя приложения

Имя файла

Имя исполняемого файла

Проверка сигнатур и рекомендации

Результат проверки сигнатур и рекомендуемое действие
. Если приложение отмечено сертификатом надежного производителя,
рекомендуется разрешить обмен данными.

Подробная информация

Локальный адрес

Исходный адрес и исходный порт

Удаленный адрес

Конечный адрес и конечный порт

Пользователь

Зарегистрированный пользователь, под именем которого работает приложение

ID процесса

Идентификатор процесса, который занимает приложение

Путь

Путь к исполняемому файлу приложения

Предприниматель

Разработчик приложения (информация о версии)

Версия

Версия приложения

Подписано

Производитель приложения (сигнатура)

Действия и кнопки**Всегда доверять этому разработчику**

Если опция включена, то разработчик программы при выполнении запроса *Сетевое событие* добавляется в список надежных разработчиков. Кнопка *Запрещать* выключается при включении опции.

Примечание

Действие доступно только для подписанных приложений.

Сохранить действие для этого приложения

Если эта опция включена, то выполненное действие будет сохранено как правило для приложения. Правило для приложения можно вызвать в настройках как [FireWall > Настройки всплывающего окна](#).

Если опция *Сохранять действие для приложения* включена и для приложения имеются специальные правила, основанные на фильтрах пакетов, при нажатии кнопок **Разрешить** или **Запретить** открывается окно для расширенной настройки правил для приложения. Трафик автоматически добавляется на первую позицию в качестве правила приложения. В окне *FireWall > Правила приложения* вы можете изменить положение добавленного правила приложения или удалить добавленное правило приложения.

Кнопки	Значение
Дополнительно	Откроется окно для расширенной настройки правил для приложения. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Примечание Эта кнопка доступна лишь в том случае, когда для правил для приложений активированы расширенные настройки (см. Настройка > FireWall > Настройки).</p> </div>
Разрешить	Данная сетевая активность разрешается.
Запретить	Данная сетевая активность запрещается.
Показать /скрыть подробности	Отображается или скрывается подробная информация о приложении.

10.2 брандмауэр Windows

Начиная с Windows 8, брандмауэр Avira FireWall больше не содержится в Avira Professional Security. Вместо этого брандмауэром брандмауэр Windows можно управлять с помощью Центра управления сетями и общим доступом. Существует несколько возможностей настройки брандмауэр Windows:

Активация брандмауэр Windows в Центре управления

Брандмауэр брандмауэр Windows можно активировать или деактивировать, нажав на кнопку **ВКЛ./ВЫКЛ.** опции *FireWall* в разделе **Состояние > Безопасность**.

Проверка состояния брандмауэр Windows в Центре управления

В разделе **БЕЗОПАСНОСТЬ > FireWall** можно проверить состояние брандмауэр Windows и восстановить рекомендуемые настройки, нажав на кнопку **Устранить проблему**.

11. Обновления

11.1 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 60 минут. Автоматическую настройку можно изменить или отключить ([Настройки > Обновление](#)).

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

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

Обновления вы получаете из Интернета по веб-серверу изготовителя или по веб-серверу или серверу файлов в сети Intranet, который загружает файлы обновления из Интернета и предоставляет их другим компьютерам в сети. Это имеет смысл, если вы хотите обновить программу Avira на нескольких компьютерах в сети. Благодаря наличию сервера загрузки в сети интранет обеспечивается актуальность Avira на защищаемых компьютерах, при этом обеспечивается небольшое потребление ресурсов. Для создания работоспособного сервера загрузки в сети интранет необходим сервер, обеспечивающий структуру обновления Avira.

Указание

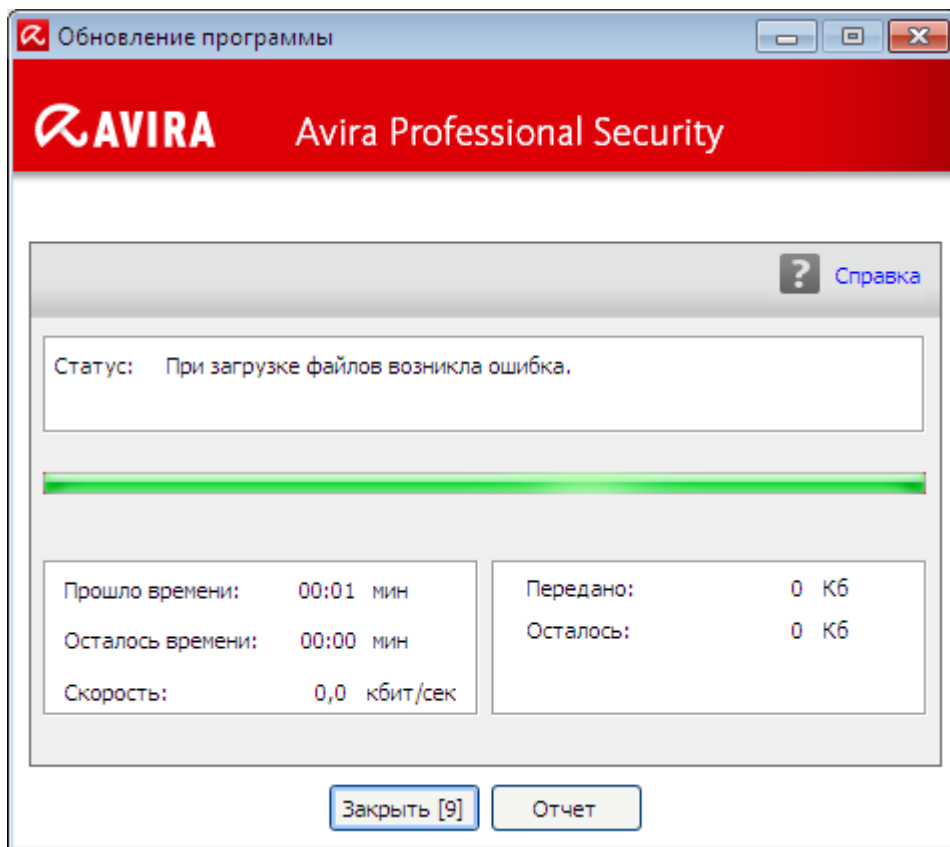
В качестве веб-сервера или сервера файлов в сети интранет можно использовать менеджер обновлений Avira (сервер файлов или веб-сервер в ОС Windows). Менеджер обновлений Avira создает зеркало сервера загрузки для программ Avira, он доступен на сайте:

<http://www.avira.ru>

При использовании веб-сервера применяется HTTP-протокол. При использовании сервера файлов доступ к файлам обновления осуществляется по сети. Параметры соединения с веб-сервером или сервером данных можно изменить в меню [Настройка > Обновление](#). В стандартной конфигурации используется существующее Интернет-соединение с веб-сервером Avira.

11.2 Модуль обновления

После запуска обновления открывается окно модуля обновления.



Указание

В заданиях обновления, которые вы устанавливаете в планировщике, можно настроить **режим отображения** для окна обновления: доступно три режима - **невидимый**, **минимизированный** или **максимальный**.

Указание

Если вы работаете с программой в полноэкранном режиме (например, компьютерные игры), а **режим отображения** окна программы - максимальный или минимизированный, происходит кратковременное переключение на рабочий стол. Для предотвращения этого вы можете запустить программу обновления в скрытом режиме. В этом режиме вы не получите уведомления от программы обновления.

Состояние: Показывает текущий статус обновления.

Прошло времени: Время, прошедшее с момента запуска процедуры обновления.


Осталось времени: Время, требуемое для завершения процедуры обновления.

Скорость: Скорость, с которой загружаются файлы обновления.

Передача: Загруженный объем в байтах.

Осталось: Объем в байтах, который еще должен быть загружен.

Кнопки и ссылки

Кнопка/ссылка	Описание
	Эта кнопка или ссылка открывает страницу справочной онлайн-системы.
Уменьшить	Окно программы обновлений отображается в уменьшенном виде.
Увеличить	Окно программы обновлений отображается в первоначальном размере.
Прервать	Процедура обновления прекращается. Программа обновлений закрывается.
Закреть	Процедура обновления завершена. Окно будет закрыто.
Отчет	Отображается файл отчета программы обновлений.

12. Устранение проблемы, рекомендации

Эта глава содержит важную информацию об устранении проблем и другие советы по использованию продукта Avira.

- см. главу [Помощь в сложных случаях](#)
- см. главу [Ярлыки](#)
- см. главу [Центр обеспечения безопасности Windows \(Windows XP\)](#) или [Центр поддержки Windows \(Windows 7\)](#)

12.1 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. См. также [Менеджер лицензий](#).

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 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.
- ▶ Выберите **System Scanner > Поиск**, активируйте в поле *Файлы* опцию **Все файлы** и подтвердите изменения нажатием на **ОК**.
- ▶ 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 **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, сделайте 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 **ОК**.
- ▶ 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](#)).

12.2 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.

12.2.1 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.

← ↑ → ↓	<p>Навигация по вкладкам настроек Сначала установите курсор мыши на раздел настроек.</p> <p>Переключение между опциями в выделенном выпадающем списке или в одной группе опций.</p>
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.

12.2.2 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.

12.2.3 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)

12.3 Центр обеспечения безопасности Windows

- от Windows XP Service Pack 2 -

12.3.1 Общие сведения

Центр обеспечения безопасности Windows проверяет состояние 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.

12.3.2 Центр обеспечения безопасности Windows и ваш продукт Avira

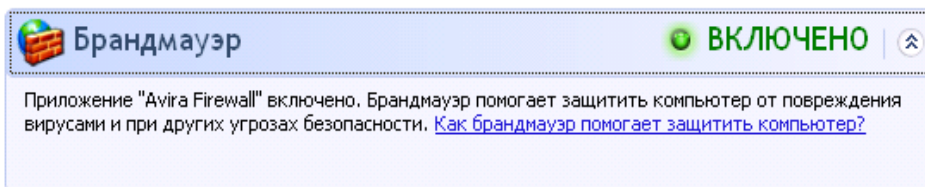
Брандмауэр

Вы можете получить следующую информацию от Центра обеспечения безопасности в отношении брандмауэра:

- [Брандмауэр АКТИВИРОВАН / Брандмауэр включен](#)
- [Брандмауэр ДЕАКТИВИРОВАН / Брандмауэр выключен](#)

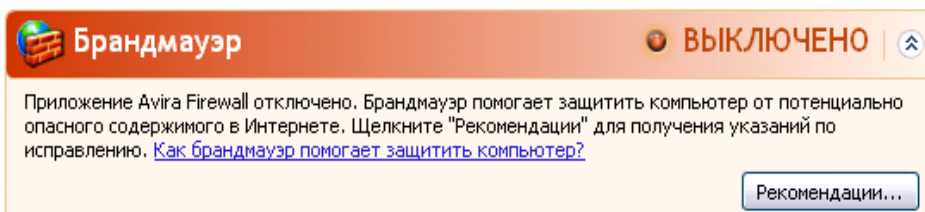
Брандмауэр АКТИВИРОВАН / Брандмауэр включен

После установки продукта Avira и включения брандмауэра Windows отображается следующее сообщение:



Брандмауэр ДЕАКТИВИРОВАН / Брандмауэр выключен

После выключения FireWall Avira отображается следующее сообщение:



Примечание

Можно включить или выключить FireWall Avira с помощью вкладки [Состояние в центре управления](#).

Предупреждение

Если выключить FireWall Avira, неавторизованные пользователи смогут получать доступ к компьютеру через сеть или Интернет.

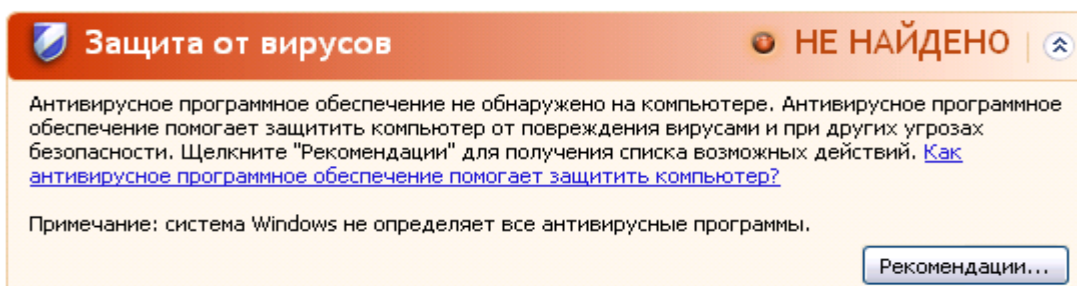
Антивирусное ПО / Защита от вредоносных программ


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.



Защита от вирусов | **НЕ НАЙДЕНО** | 

Антивирусное программное обеспечение не обнаружено на компьютере. Антивирусное программное обеспечение помогает защитить компьютер от повреждения вирусами и при других угрозах безопасности. Щелкните "Рекомендации" для получения списка возможных действий. [Как антивирусное программное обеспечение помогает защитить компьютер?](#)

Примечание: система Windows не определяет все антивирусные программы.

[Рекомендации...](#)

Примечание

Установите 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, а теперь устанавливаете продукт Avira или же устанавливаете Windows XP Service Pack 2 в систему, в которой уже установлен продукт Avira, будет выдано следующее сообщение:

Защита от вирусов
 СРОК ИСТЕК |

Приложение "AntiVir Desktop" могло устареть. Щелкните "Рекомендации" для получения списка возможных действий. [Как антивирусное программное обеспечение помогает защитить компьютер?](#)

Примечание: система Windows не определяет все антивирусные программы.

Рекомендации...

Примечание

Чтобы Центр обеспечения безопасности Windows считал 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 отображается следующее уведомление:

Защита от вирусов
 ВКЛЮЧЕНО |

AntiVir Desktop имеет последнюю версию, и сканирование на наличие вирусов включено. Антивирусное программное обеспечение помогает защитить компьютер от повреждения вирусами и при других угрозах безопасности. [Как антивирусное программное обеспечение помогает защитить компьютер?](#)

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

Защита от вирусов ВЫКЛЮЧЕНА

Следующее сообщение отображается при выключенном модуле Avira Real-Time Protection или при остановке его работы.

Защита от вирусов
 ВЫКЛЮЧЕНО |

Приложение "AntiVir Desktop" отключено. Антивирусное программное обеспечение помогает защитить компьютер от повреждения вирусами и при других угрозах безопасности. Щелкните "Рекомендации" для получения списка возможных действий. [Как антивирусное программное обеспечение помогает защитить компьютер?](#)

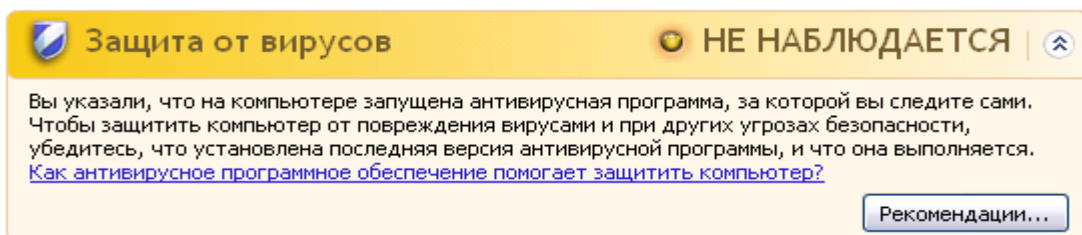
Примечание: система Windows не определяет все антивирусные программы.

Примечание

Модуль Avira Real-Time Protection можно включить или выключить в разделе [Состояние центра управления](#). Если модуль Avira Real-Time Protection включен, на [панели задач](#) отображается красный зонтик.

Защита от вирусов НЕ КОНТРОЛИРУЕТСЯ

Если вы получили следующее сообщение от Центра обеспечения безопасности Windows, значит вы решили самостоятельно контролировать ваше антивирусное ПО.



Примечание

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

Примечание

Даже если вы установили Windows XP Service Pack 2, вам требуется решение для защиты от вирусов. Несмотря на то, что Windows контролирует ваше антивирусное ПО, сама ОС не обладает функциями антивирусной защиты. Таким образом, без дополнительных средств антивирусной защиты ваша система не защищена от вирусов и вредоносного ПО!

12.4 Центр поддержки Windows

- Windows 7 и Windows 8 -

12.4.1 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*).

12.4.2 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.

Обновить параметры брандмауэра

В брандмауэре Windows не используются рекомендуемые параметры для защиты компьютера.

[Каковы рекомендуемые параметры?](#)

[Использовать рекомен. параметры](#)

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

При деактивации Avira FireWall выдается следующее сообщение:

Сетевой брандмауэр (Внимание!)

Брандмауэр Windows и "Avira FireWall" сообщают, что они выключены.

[Не получать больше сообщения на тему: "о сетевом брандмауэре"](#)

[Просмотр параметров брандмауэр...](#)

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.

Сетевой брандмауэр (Внимание!)

Брандмауэр Windows отключен или неправильно настроен.

[Не получать больше сообщения на тему: "о сетевом брандмауэре"](#)

[Включить сейчас](#)

[Поиск в Интернете приложения для защиты моего ПК](#)

Это означает, что ни **брандмауэр Windows**, ни **Avira FireWall** не активированы. Данное сообщение появляется в двух различных ситуациях:

- **Avira FireWall**

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

- **брандмауэр Windows**

Начиная с Windows 7, Avira FireWall больше не содержится в Avira Professional Security. Вместо этого брандмауэром брандмауэр Windows можно управлять с помощью Центра управления сетями и общим доступом.

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 устарело](#)
- [На компьютере не обнаружено ни одной антивирусной программы](#)
- [Ваш компьютер больше не защищен приложением Avira Desktop](#)

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.

Защита от вирусов (Внимание!)

Приложение "Avira Desktop" сообщает, что оно отключено.

Не получать больше сообщения на тему: "об антивирусной защите"

[Получение другой антивирусной программы в сети](#)

[Включить сейчас](#)

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:

Защита от вирусов (Внимание!) Обновить сейчас

Приложение "Avira Desktop" сообщает, что оно нуждается в обновлении.

Не получать больше сообщения на тему: "об антивирусной защите" Получение другой антивирусной программы в сети

Примечание

Чтобы Центр поддержки Windows считал 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.

Защита от вирусов (Внимание!) Найти программу в сети

Windows не обнаружила антивирусного программного обеспечения на этом компьютере.

Не получать больше сообщения на тему: "об антивирусной защите"

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 приобрести новую лицензию.

Защита от вирусов (Внимание!)

Приложение "Avira Desktop" больше не защищает ваш ПК.

Не получать больше сообщения на тему: "об антивирусной защите"

[Просмотреть установленные антивирусные приложения](#)

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.

Защита от программ-шпионов и нежелательных программ (Внимание!)

Защитник Windows и приложение "Avira Desktop" сообщают, что они выключены.

Не получать больше сообщения на тему: "о защите от шпионских программ и прочего вредоносного кода"

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:

Защита от программ-шпионов и нежелательных программ (Внимание!) Обновить

Приложение "Avira Desktop" сообщает, что оно нуждается в обновлении.

[Не получать больше сообщения на тему: "о защите от шпионских программ и прочего вредоносного кода"](#)
[Получение другой антишпионской программы в сети](#)


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.

Защита от программ-шпионов и нежелательных программ (Внимание!) Обновить

 Защитник Windows нуждается в обновлении.

[Не получать больше сообщения на тему: "о защите от шпионских программ и прочего вредоносного кода"](#)
[Получение другой антишпионской программы в сети](#)

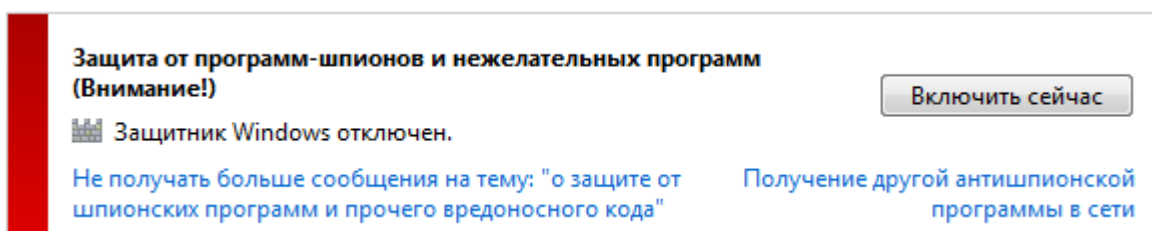
Примечание

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 найдено другое антишпионское 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.



13. Вирусы и другое

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

Соответствующие темы:

- [Категории угроз](#)
- [Вирусы и вредоносные программы](#)

13.1 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 частную сферу, могут быть опасными и являются нежелательными.

Программа Avira распознает программы, несущие риск вторжения в частную 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-шутки 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 попала 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 определенным 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 (РСК)**,

пользователь получает предупреждение в случае, если Avira обнаружит подобные объекты.

13.2 Вирусы и вредоносные программы

Рекламные программы

Под рекламными программами понимаются такие программы, которые, выполняя свою основную функцию, еще и демонстрируют пользователю рекламные баннеры и всплывающие рекламные окна. Эти рекламные сообщения иногда бывает очень сложно отключить или скрыть. Программы 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.

Ноах (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 попала 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 определенным 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.

14. Информация и сервис

В этом разделе собраны сведения, касающиеся информации и сервисов Avira.

- [Контакты](#)
- [Техническая поддержка](#)
- [Подозрительный файл](#)
- [Сообщение о ложном срабатывании](#)
- [Обратная связь для вашей безопасности](#)

14.1 Контакты

Мы с удовольствием поможем вам, если у вас есть вопросы или пожелания, касающиеся продукции Avira. Наши контактные данные можно получить в центре управления Центр контроля, в пункте меню **Справка > Об Avira Professional Security**.

14.2 Техническая поддержка

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

Всю необходимую информацию по нашим комплексным услугам поддержки можно найти на сайте:

<http://www.avira.ru/professional-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 Professional Security > Информация о лицензии**. См. [Информация о лицензии](#).
- **Информация о версии.** Информацию о версии вы найдете в меню программы, в пункте **Справка > Об Avira Professional 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.

14.3 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.

- Найдите нужный файл в менеджере карантина центра управления Центр контроля консоли Avira Server Security и выберите пункт **Отправить файл** в контекстном меню или нажмите соответствующую кнопку.
- Отправьте необходимый файл в заархивированном виде (WinZIP, PKZip, Arj, и т. д.) во вложении письма по следующему адресу:
virus-professional@avira.ru
Так как некоторые почтовые шлюзы работают с антивирусным ПО, защитите файл(ы) паролем (пожалуйста, не забудьте сообщить его нам).
- У вас есть также возможность отправить подозрительные файлы через наш сайт:
<http://www.avira.ru/sample-upload>

14.4 Сообщение о ложном срабатывании

Если вы полагаете, что пакет Avira Professional Security считает подозрительным гарантированно «чистый» файл, отправьте этот файл в архивированном виде (WinZIP, PKZip, Arj...) в качестве вложения электронного письма на следующий адрес:

virus-professional@avira.ru

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

14.5 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@avira.ru



Avira

Все названия марок и продуктов являются торговыми марками или зарегистрированными торговыми марками их владельцев. Защищенные торговые марки не обозначены в этом руководстве соответствующим образом. Тем не менее, это не означает, что их можно использовать без разрешения.

Это руководство было разработано очень тщательно. Размножение этого документа или его частей в любой форме без получения предварительного письменного разрешения Avira Operations GmbH & Co. KG запрещено.

Техническая информация по состоянию на 4-й квартал 2013 г.

© 2013 Avira Operations GmbH & Co. Все права защищены.
Ошибки и пропуски не исключены.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Germany | Телефон: +49 7542-500 0
Интернет: <http://www.avira.ru>