



AVG Anti-Virus 2012

Руководство пользователя

Версия документа 2012.20 (4/11/2012)

© AVG Technologies CZ, s.r.o. Все права защищены.
Все другие товарные знаки являются собственностью соответствующих владельцев.

Этот продукт использует RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc., созданный в 1991.

В этом продукте используется код из библиотеки C-SaCzech, (c) Яромир Долечек (Jaromir Dolecek) (dolecek@ics.muni.cz), 1996-2001.

В этом продукте используется библиотека сжатия zlib, © Жан-Луп Гайлли (Jean-loup Gailly) и Марк Адлер (Mark Adler), 1995-2002.

В этом продукте использована библиотека компрессии libbzip2, © Джулиан Севард (Julian R. Seward), 1996-2002.



Содержимое

1. Введение	6
2. Требования для установки AVG	7
2.1 Поддерживаемые операционные системы	7
2.2 Минимальные требования и рекомендуемое оборудование	7
3. Процесс установки AVG	8
3.1 Добро пожаловать! Выбор языка	8
3.2 Добро пожаловать! Лицензионное соглашение	9
3.3 Активация лицензии	10
3.4 Выбор типа установки	12
3.5 Пользовательские параметры	14
3.6 Установка панели AVG Security Toolbar	15
3.7 Состояние процесса установки	16
3.8 Установка выполнена успешно	17
4. После установки	18
4.1 Регистрация продукта	18
4.2 Доступ к интерфейсу пользователя	18
4.3 Сканирование всего компьютера	18
4.4 Тестирование Eicar	18
4.5 Конфигурация AVG по умолчанию	19
5. Интерфейс пользователя AVG	20
5.1 Системное меню	21
5.1.1 Файл	21
5.1.2 Компоненты	21
5.1.3 История	21
5.1.4 Инструменты	21
5.1.5 Справка	21
5.1.6 Поддержка	21
5.2 Информация о состоянии безопасности	28
5.3 Быстрые ссылки	29
5.4 Обзор компонентов	30
5.5 Значок на панели задач	32
5.6 Советник AVG	34



5.7 Гаджет AVG	34
6. Компоненты AVG	37
6.1 Anti-Virus	37
6.1.1 Модуль сканирования	37
6.1.2 Постоянная защита	37
6.1.3 Защита Anti-Spyware	37
6.1.4 Интерфейс Anti-Virus	37
6.1.5 Обнаружения Resident Shield	37
6.2 LinkScanner	44
6.2.1 Интерфейс LinkScanner	44
6.2.2 Обнаружения Search-Shield	44
6.2.3 Обнаружения Surf-Shield	44
6.2.4 Обнаружения Online Shield	44
6.3 Защита электронной почты	49
6.3.1 E-mail Scanner	49
6.3.2 Anti-Spam	49
6.3.3 Интерфейс защиты электронной почты	49
6.3.4 Обнаружение E-mail Scanner	49
6.4 Anti-Rootkit	54
6.4.1 Интерфейс Anti-Rootkit	54
6.5 PC Analyzer	56
6.6 Identity Protection	58
6.6.1 Интерфейс защиты личных данных	58
6.7 Удаленное администрирование	61
7. Мои приложения	62
7.1 AVG Family Safety	62
7.2 AVG LiveKive	63
7.3 AVG Mobilation	63
7.4 AVG PC Tuneup	64
8. Панель AVG Security Toolbar	66
9. AVG Do Not Track	69
9.1 Интерфейс AVG Do Not Track	70
9.2 Информация о следящих процессах	71
9.3 Блокировка следящих процессов	72
9.4 Настройки AVG Do Not Track	72



10. Дополнительные параметры AVG	75
10.1 Внешний вид	75
10.2 Звуки	78
10.3 Временное отключение защиты AVG	79
10.4 Антивирус (Anti-Virus)	80
10.4.1 Resident Shield	80
10.4.2 Сервер кэширования	80
10.5 Защита электронной почты	86
10.5.1 E-mail Scanner	86
10.6 LinkScanner	95
10.6.1 Настройки Link Scanner	95
10.6.2 Online Shield	95
10.7 Сканирования	98
10.7.1 Сканирование всего компьютера	98
10.7.2 Сканирование расширения оболочки	98
10.7.3 Сканирование определенных файлов или папок	98
10.7.4 Сканирование съемного устройства	98
10.8 Расписания	104
10.8.1 Запланированное сканирование	104
10.8.2 Расписание обновления определений	104
10.8.3 Расписание обновления программы	104
10.9 Обновление	114
10.9.1 Прокси-сервер	114
10.9.2 Подключение по коммутируемой линии	114
10.9.3 URL-адрес	114
10.9.4 Управление	114
10.10 Anti-Rootkit	120
10.10.1 Исключения	120
10.11 Identity Protection	122
10.11.1 Параметры компонента Identity Protection	122
10.11.2 Список разрешенных объектов	122
10.12 Потенциально нежелательные программы	126
10.13 Хранилище вирусов	129
10.14 Программа улучшения продуктов	129
10.15 Игнорировать состояние ошибки	133
10.16 Advisor — известные сети	134
11. Сканирование AVG	135



11.1	Интерфейс сканирования	135
11.2	Предопределенные сканирования	136
11.2.1	Сканирование всего компьютера	136
11.2.2	Сканирование определенных файлов или папок	136
11.3	Сканирование в Проводнике Windows	146
11.4	Сканирование с помощью командной строки	146
11.4.1	Параметры сканирования с помощью командной строки	146
11.5	Расписание сканирования	149
11.5.1	Параметры расписания	149
11.5.2	Способы сканирования	149
11.5.3	Объекты сканирования	149
11.6	Обзор результатов сканирования	159
11.7	Сведения о результатах сканирования	160
11.7.1	Вкладка "Обзор результатов"	160
11.7.2	Вкладка "Заражения"	160
11.7.3	Вкладка "Шпионское ПО"	160
11.7.4	Вкладка "Предупреждения"	160
11.7.5	Вкладка Rootkits	160
11.7.6	Вкладка "Сведения"	160
11.8	Хранилище вирусов	168
12.	Обновления AVG	170
12.1	Запуск обновления	170
12.2	Ход обновления	170
12.3	Уровни обновлений	171
13.	Журнал событий	173
14.	Часто задаваемые вопросы и техническая поддержка	175



1. Введение

Руководство пользователя содержит полные сведения о системе **AVG Anti-Virus 2012**.

AVG Anti-Virus 2012 защищает от опаснейших современных угроз в режиме реального времени. Общайтесь, загружайте файлы и обменивайтесь ими, играйте и смотрите видео без проблем и прерываний.

- Отправляйте сообщения, загружайте файлы и обменивайтесь в полной безопасности благодаря AVG Online Shield™.
- Безопасно общайтесь в социальных сетях благодаря компоненту AVG защита социальных сетей.
- Просматривайте веб-сайты и ищите информацию с уверенностью благодаря LinkScanner, защите в режиме реального времени.



2. Требования для установки AVG

2.1. Поддерживаемые операционные системы

AVG Anti-Virus 2012 обеспечивает защиту рабочих станций, на которых используются следующие операционные системы.

- Windows XP Home Edition с пакетом обновления SP2
- Windows XP Professional с пакетом обновления SP2
- Windows XP Professional x64 Edition с пакетом обновления SP1
- Windows Vista (x86 и x64, все версии)
- Windows 7 (x86 и x64, все версии)

(и, возможно, более поздние пакеты обновления для некоторых операционных систем)

***Примечание.** Компонент [ID Protection](#) не поддерживается операционной системой Windows XP x64. В этой операционной системе можно установить AVG Anti-Virus 2012, но только без компонента IDP.*

2.2. Минимальные требования и рекомендуемое оборудование

Минимальные требования к оборудованию для **AVG Anti-Virus 2012**.

- Процессор Intel Pentium 1,5 ГГц
- 512 МБ памяти ОЗУ
- 950 МБ свободного места на жестком диске (для установки)

Рекомендуемые требования к оборудованию для **AVG Anti-Virus 2012**.

- Процессор Intel Pentium 1,8 ГГц
- 512 МБ памяти ОЗУ
- 1350 МБ свободного места на жестком диске (для установки)



3. Процесс установки AVG

Как получить файл установки?

Для установки **AVG Anti-Virus 2012** на компьютер требуется файл установки последней версии. Для установки самой последней версии **AVG Anti-Virus 2012** рекомендуется загрузить файл установки с веб-сайта компании AVG (<http://www.avg.com/>). В разделе **Центр поддержки/Загрузка** можно ознакомиться с подробным обзором файлов установки для каждой версии AVG.

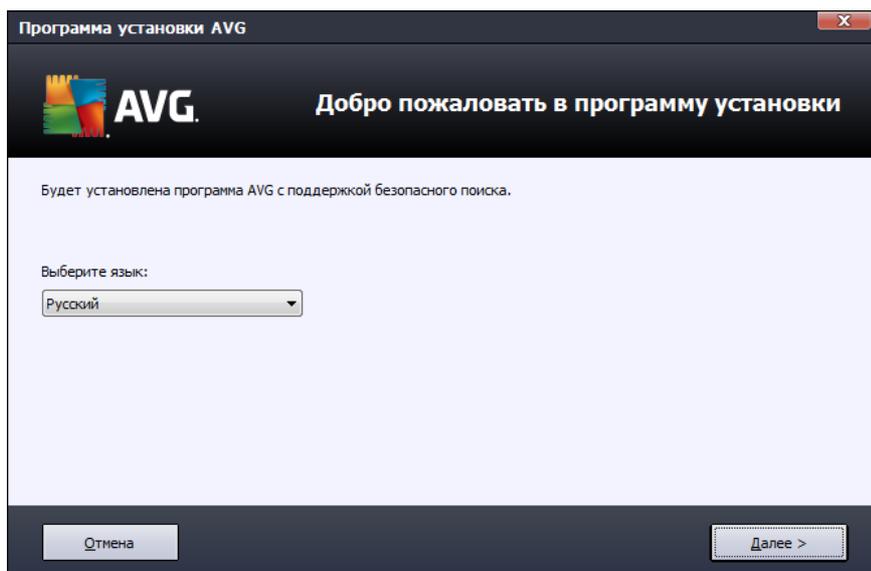
Если вы не уверены в том, какой именно файл необходимо загружать и устанавливать, воспользуйтесь службой **Выбрать продукт** в нижней части веб-страницы. Получив ответы на три простых вопроса, служба сама подберет необходимые вам файлы. Нажмите кнопку **Продолжить**, чтобы перейти к полному списку файлов для загрузки, которые соответствуют вашим потребностям.

Как выглядит процесс установки?

После загрузки и сохранения файла установки на жестком диске можно запустить процесс установки. Процесс установки представляет собой последовательность простых и понятных диалоговых окон. Каждое окно содержит краткие пошаговые инструкции по процессу установки. Далее приводится описание каждого диалогового окна.

3.1. Добро пожаловать! Выбор языка

Процесс установки начинается с диалогового окна **Добро пожаловать в установщик AVG**.



В этом диалоговом окне можно выбрать язык, который будет использоваться в процессе установки. В правом верхнем углу окна щелкните раскрывающийся список для вызова языкового меню. Выберите необходимый язык, и процесс установки продолжится на

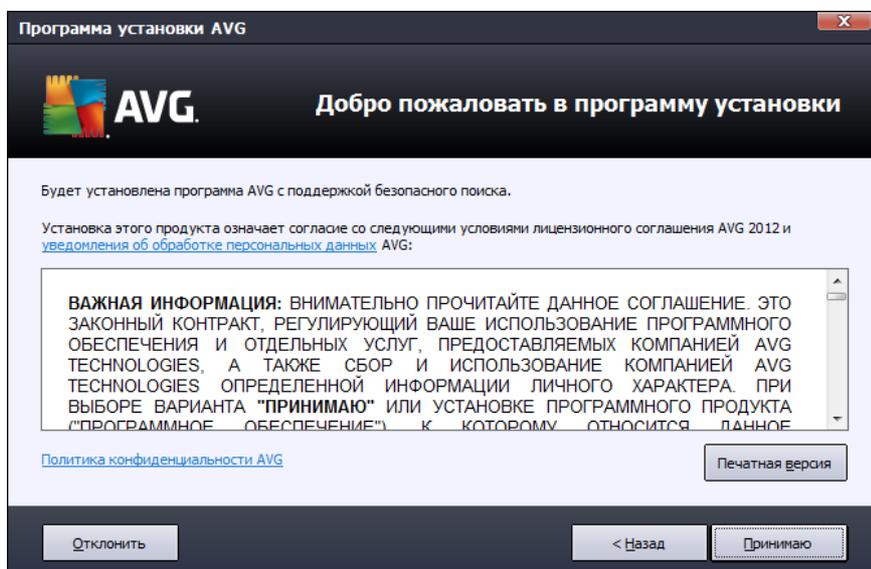


выбранном языке.

Внимание! В данном окне выбирается только язык процесса установки. Приложение AVG Anti-Virus 2012 будет установлено на выбранном языке и на английском, который устанавливается автоматически. В дальнейшем для работы с AVG Anti-Virus 2012 можно будет установить любые другие языки. Дополнить список языков можно в диалоговом окне установки [Пользовательские параметры](#).

3.2. Добро пожаловать! Лицензионное соглашение

Далее в диалоговом окне **Добро пожаловать в установщик AVG** представлен полный текст лицензионного соглашения AVG.



Внимательно прочтите весь текст. Чтобы подтвердить, чтобы вы прочитали, понимаете и принимаете условия соглашения, нажмите кнопку **Принимаю**. Если вы не согласны с лицензионным соглашением, нажмите кнопку **Не принимаю**. Процесс установки будет прерван.

Политика конфиденциальности AVG

Помимо лицензионного соглашения, данное окно также содержит дополнительные сведения о политике конфиденциальности AVG. В левом нижнем углу данного диалогового окна находится ссылка **политика конфиденциальности AVG**. Щелкните ссылку для перехода на веб-сайт компании AVG (<http://www.avg.com/>), где в полном объеме представлены принципы политики конфиденциальности AVG.

Кнопки управления

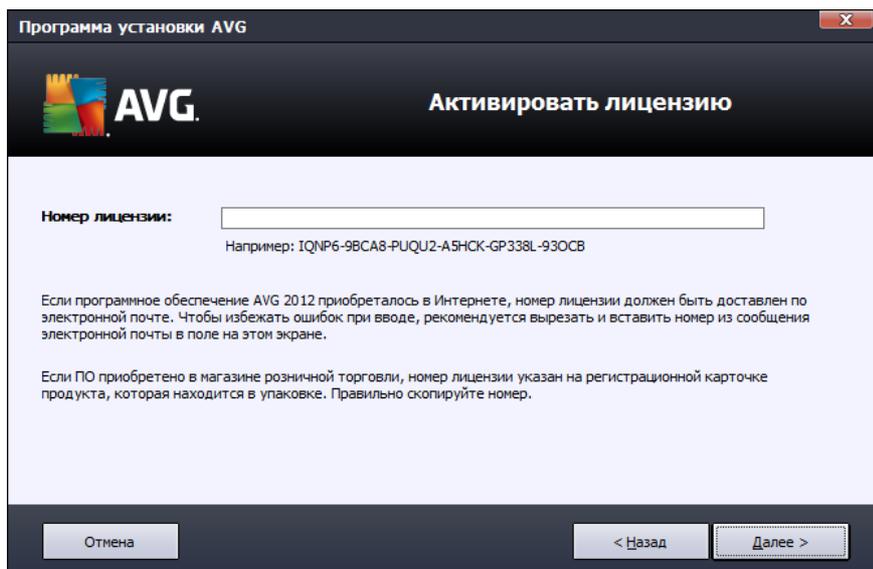
В первом диалоговом окне установки имеется всего две кнопки управления.



- **Печатная версия.** Нажмите здесь, чтобы распечатать весь текст лицензионного соглашения AVG.
- **Не принимаю.** Нажмите, чтобы отклонить условия лицензионного соглашения. Процесс установки при этом будет закрыт. **AVG Anti-Virus 2012** не будет установлена.
- **Назад.** Нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.
- **Принимаю.** Нажмите, чтобы подтвердить, что вы прочитали, понимаете и принимаете условия соглашения. Таким образом установка продолжится и вы перейдете к диалоговому окну следующего шага установки.

3.3. Активация лицензии

В диалоговом окне **Активация лицензии** отображается запрос на ввод номера лицензии в соответствующем текстовом поле:



Как определить номер лицензии

Номер продажи указан на футляре компакт-диска из коробки **AVG Anti-Virus 2012**. Номер лицензии будет указан в подтверждающем сообщении электронной почты, которое будет получено после оформления покупки **AVG Anti-Virus 2012** через Интернет. Необходимо правильно ввести номер. Номер лицензии в цифровом виде (*приведенный в сообщении электронной почты*) можно вставить с использованием стандартного метода копирования и вставки.

Как пользоваться методом копирования и вставки



Использование метода **копирования и вставки** при вводе номера лицензии **AVG Anti-Virus 2012** гарантирует правильное введение номера. Выполните данные шаги:

- Откройте сообщение электронной почты, содержащее ваш номер лицензии.
- Щелкните левой кнопкой мыши в начале номера лицензии и удерживая перетащите указатель мыши в конец номера, затем отпустите кнопку. При этом номер должен быть выделенным.
- Нажмите и удерживайте клавишу **Ctrl**, затем нажмите **C**. Это действие копирует номер.
- Поместите курсор в место, куда необходимо вставить скопированную информацию, и щелкните правой кнопкой мыши.
- Нажмите и удерживайте клавишу **Ctrl**, затем нажмите **V**. Это действие обеспечивает вставку номера в заданное место.

Кнопки управления

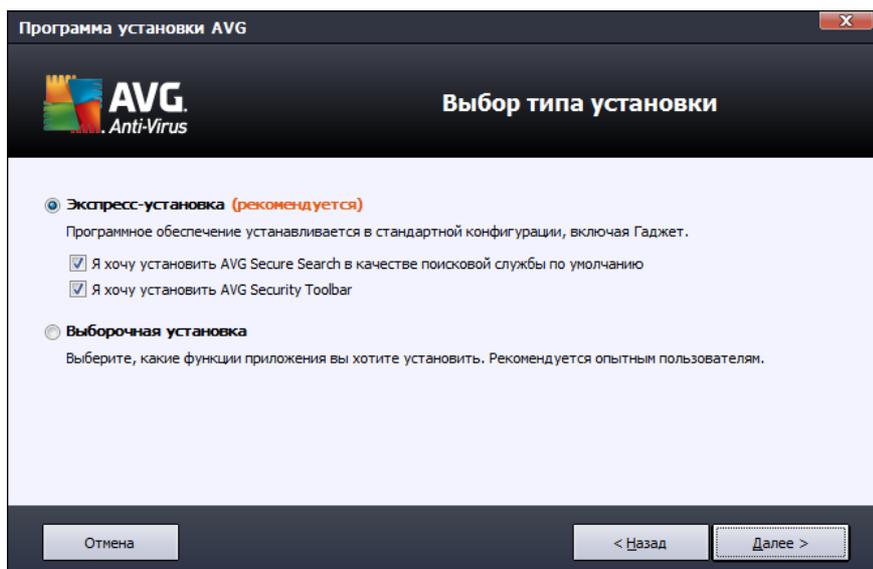
Как и в большинстве диалоговых окон установки, здесь имеется три кнопки управления.

- **Отмена**. Нажмите для немедленного выхода из процесса установки; **AVG Anti-Virus 2012** установка не будет выполнена.
- **Назад**. Нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.
- **Далее**. Нажмите для продолжения установки и перехода на один шаг вперед.



3.4. Выбор типа установки

В диалоговом окне **Выбор типа установки** можно выбрать один из двух типов установки: **Быстрая установка** и **Выборочная установка**.



Быстрая установка

Для большинства пользователей рекомендуется стандартный вариант **Быстрая установка**. В этом случае установка программы **AVG Anti-Virus 2012** выполняется в полностью автоматическом режиме с параметрами, предварительно заданными поставщиком программного обеспечения, включая [Гаджет AVG](#). Данный вариант установки обеспечивает максимальный уровень защиты наряду с оптимальным уровнем использования ресурсов. Если в дальнейшем потребуется изменить конфигурацию, это всегда можно будет сделать напрямую в приложении **AVG Anti-Virus 2012**.

Для этого параметра предварительно установлены два флажка. Снимать их настоятельно не рекомендуется.

- **Сделать безопасный поиск AVG службой поиска по умолчанию.** Не снимайте данный флажок, чтобы использовать подсистему безопасного поиска AVG, тесно взаимодействующую с компонентом [LinkScanner](#) и обеспечивающую максимальную защиту во время работы в Интернете.
- **Установить AVG Security Toolbar.** Установите данный флажок, чтобы установить компонент [AVG Security Toolbar](#), обеспечивающий максимальную защиту во время работы в Интернете.

Нажмите кнопку **Далее**, чтобы перейти к диалоговому окну [Установка AVG Security Toolbar](#).



Выборочная установка

Выборочную установку следует выбирать только опытным пользователям, у которых есть веские основания для установки программы **AVG Anti-Virus 2012** с настройками, отличными от стандартных (например, при наличии определенных системных требований).

При выборе этого параметра в диалоговом окне появляется раздел **Папка назначения**. Здесь должно быть указано местоположение, куда нужно установить **AVG Anti-Virus 2012**. По умолчанию установка **AVG Anti-Virus 2012** выполняется в папку "Program Files", которая расположена на диске С:, как указано в текстовом поле диалогового окна. Чтобы изменить это местоположение, нажмите кнопку **Обзор**, чтобы отобразить структуру дисков, и выберите соответствующую папку. Чтобы восстановить папку назначения по умолчанию, предустановленную поставщиком программного обеспечения, нажмите кнопку **По умолчанию**.

Нажмите кнопку **Далее**, чтобы перейти к диалоговому окну [Пользовательские параметры](#).

Кнопки управления

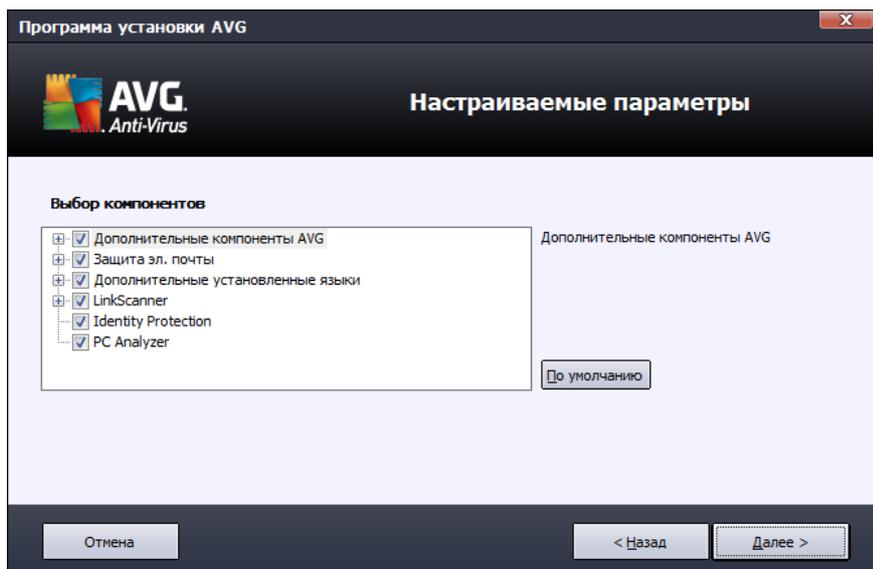
Как и в большинстве диалоговых окон установки, здесь имеется три кнопки управления.

- **Отмена**. Нажмите для немедленного выхода из процесса установки; **AVG Anti-Virus 2012** установка не будет выполнена.
- **Назад**. Нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.
- **Далее**. Нажмите для продолжения установки и перехода на один шаг вперед.



3.5. Пользовательские параметры

Диалоговое окно *Пользовательские параметры* позволяет установить детальные параметры установки.



В разделе **Выбор компонентов** содержится список всех компонентов **AVG Anti-Virus 2012**, которые можно установить. Если значения параметров по умолчанию не подходят, можно добавить или удалить определенные компоненты.

При этом можно выбирать только компоненты, включенные в купленную версию AVG!

Выделите любой элемент в списке **Выбор компонентов** и в правой части раздела отобразится описание соответствующего компонента. Подробные сведения о функциях определенных компонентов см. в главе [Обзор компонентов](#) данного документа. Чтобы восстановить конфигурацию по умолчанию, предустановленную поставщиком программного обеспечения, нажмите кнопку **По умолчанию**.

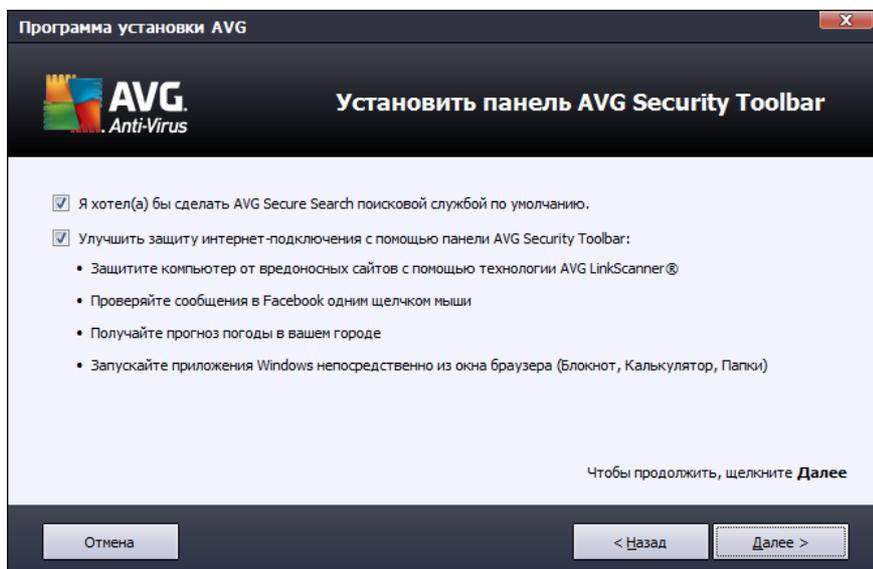
Кнопки управления

Как и в большинстве диалоговых окон установки, здесь имеется три кнопки управления.

- **Отмена.** Нажмите для немедленного выхода из процесса установки; **AVG Anti-Virus 2012** установка не будет выполнена.
- **Назад.** Нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.
- **Далее.** Нажмите для продолжения установки и перехода на один шаг вперед.



3.6. Установка панели AVG Security Toolbar



В диалоговом окне **Установка панели AVG Security Toolbar** выберите, требуется ли установка [панели AVG Security Toolbar](#). Если значения настроек по умолчанию не изменены, этот компонент будет автоматически установлен в веб-обозревателе (*в данный момент поддерживаются веб-обозреватели Microsoft Internet Explorer версии 6.0 или выше и Mozilla Firefox версии 3.0 и выше*), чтобы обеспечить комплексную защиту при работе в Интернете.

Также в данном окне можно назначить *AVG Secure Search (powered by Google)* в качестве службы поиска по умолчанию. Для этого установите соответствующий флажок.

Кнопки управления

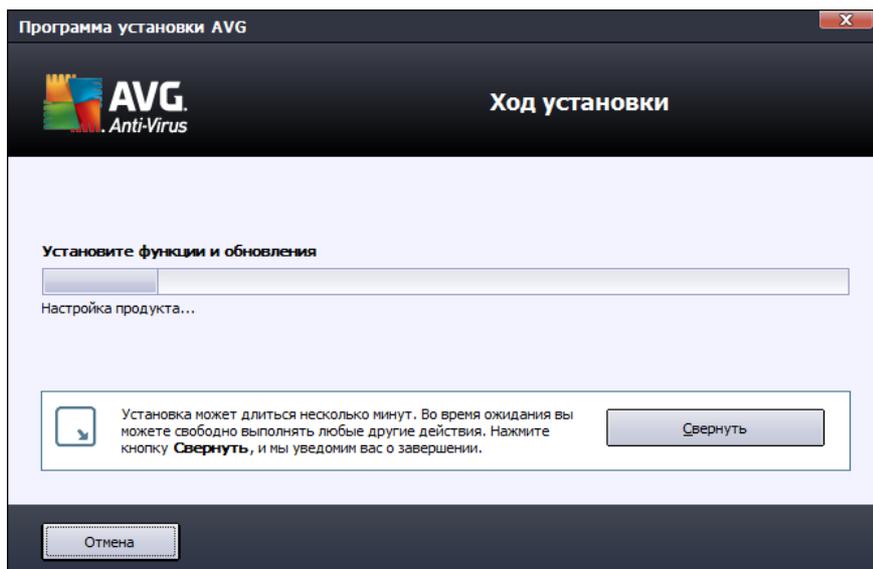
Как и в большинстве диалоговых окон установки, здесь имеется три кнопки управления.

- **Отмена.** Нажмите для немедленного выхода из процесса установки; **AVG Anti-Virus 2012** установка не будет выполнена.
- **Назад.** Нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.
- **Далее.** Нажмите для продолжения установки и перехода на один шаг вперед.



3.7. Состояние процесса установки

В диалоговом окне *Состояние процесса установки* отображается ход выполнения процесса установки. Данное окно не требует от пользователя каких-либо действий.



После завершения процесса установки автоматически будет произведен переход к следующему диалоговому окну.

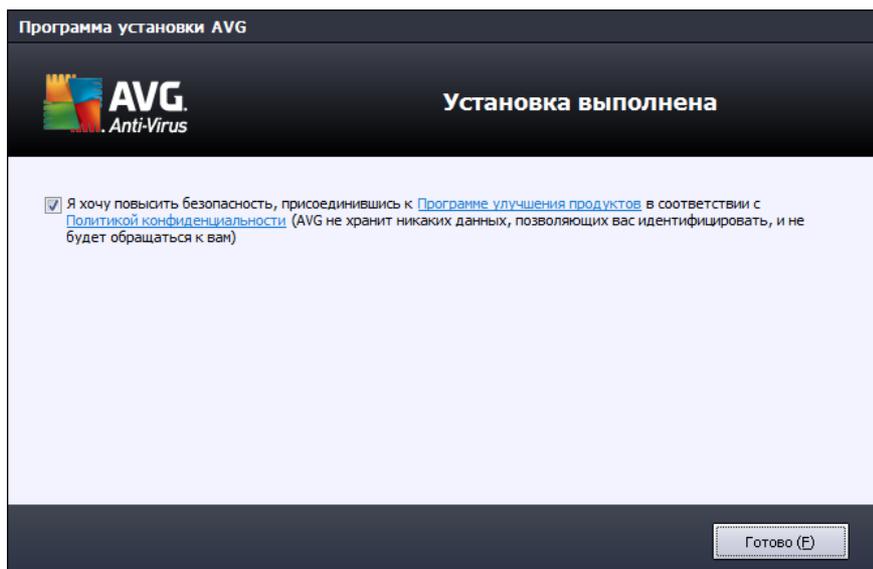
Кнопки управления

В данном диалоговом окне имеется только одна кнопка управления — **Отмена**. Эту кнопку следует использовать только при необходимости прерывания процесса установки. Обратите внимание, что в таком случае программа **AVG Anti-Virus 2012** установлена не будет.



3.8. Установка выполнена успешно

Диалоговое окно **Установка выполнена успешно** отображается для подтверждения того, что программа **AVG Anti-Virus 2012** полностью установлена и настроена:



Программа улучшения продуктов

Здесь можно дать свое согласие на участие в программе улучшения продуктов AVG (*дополнительные сведения см. в разделе [Расширенные настройки AVG / Программа улучшения продуктов](#)*), в рамках которой выполняется сбор анонимных сведений об обнаруженных угрозах с целью повышения общего уровня безопасности в Интернете. Если вы согласны с данным предложением, поставьте флажок на **Я принимаю условия участия в программе веб-безопасности и улучшения продуктов AVG 2012...** (данный параметр выбран по умолчанию).

Чтобы завершить процесс установки, нажмите кнопку **Завершить**.



4. После установки

4.1. Регистрация продукта

После завершения установки **AVG Anti-Virus 2012** выполните регистрацию продукта через Интернет на веб-сайте компании AVG (<http://www.avg.com/>). После регистрации вы получите полный доступ к учетной записи пользователя AVG, информационному бюллетеню обновлений AVG, а также к другим службам, доступ к которым имеют только зарегистрированные пользователи.

Самым простым способом является регистрация непосредственно из интерфейса пользователя **AVG Anti-Virus 2012**. В главном меню выберите элемент [Справка/Зарегистрировать сейчас](#). Будет выполнено перенаправление на страницу веб-сайта компании AVG **Регистрация** (<http://www.avg.com/>). Следуйте инструкциям, приведенным на странице.

4.2. Доступ к интерфейсу пользователя

Доступ к [главному диалоговому окну AVG](#) можно получить одним из следующих способов:

- дважды щелкните [значок AVG на панели задач](#)
- дважды щелкните значок AVG на рабочем столе
- выберите меню **Пуск / Все программы / AVG 2012**

4.3. Сканирование всего компьютера

Существует потенциальная опасность того, что до установки **AVG Anti-Virus 2012** компьютер был заражен вирусом. Поэтому необходимо запустить операцию [Сканирование всего компьютера](#), чтобы убедиться, что компьютер не заражен. Первое сканирование может занять достаточно много времени (*около часа*), но рекомендуется запустить его, чтобы компьютер не был подвержен угрозам. Инструкции по запуску операции [Сканирование всего компьютера](#) см. в главе [Сканирование AVG](#).

4.4. Тестирование Eicar

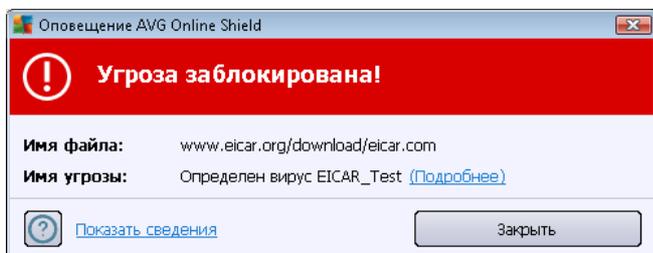
Чтобы проверить правильность установки **AVG Anti-Virus 2012**, можно выполнить тест EICAR.

Тестирование EICAR — стандартный и абсолютно безопасный метод для тестирования работы антивирусных систем. Он безопасен, так как не является настоящим вирусом и не включает в себя фрагменты вирусного кода. Большинство продуктов реагируют на него как на настоящий вирус (*хотя они обычно сообщают о нем, используя настоящее имя, например "EICAR-AV-Test"*). Загрузить вирус EICAR можно на веб-сайте EICAR www.eicar.com; также там можно получить необходимую информацию о проверке EICAR.

Загрузите файл **eicar.com** и сохраните его на локальном диске. Сразу после подтверждения загрузки тестового файла [Online Shield](#) (в составе компонента [Link Scanner](#)) отреагирует предупреждением. Данное оповещение означает, что система AVG на компьютере



установлена правильно.



На веб-сайте <http://www.eicar.com> также можно загрузить сжатую версию "вируса" EICAR (например в файле *eicar_com.zip*). [Компонент Online Shield](#) позволяет загрузить этот файл и сохранить его на локальном жестком диске, но затем компонент [Resident Shield](#) (в составе компонента [Anti-Virus](#)) обнаруживает вирус, как только вы попытаетесь распаковать его.

Если программе AVG не удалось определить тестовый файл EICAR как вирус, проверьте параметры программы еще раз.

4.5. Конфигурация AVG по умолчанию

Параметры по умолчанию (*параметры приложения после установки*) **AVG Anti-Virus 2012** настроены поставщиком ПО таким образом, чтобы все компоненты и функции обеспечивали оптимальную производительность.

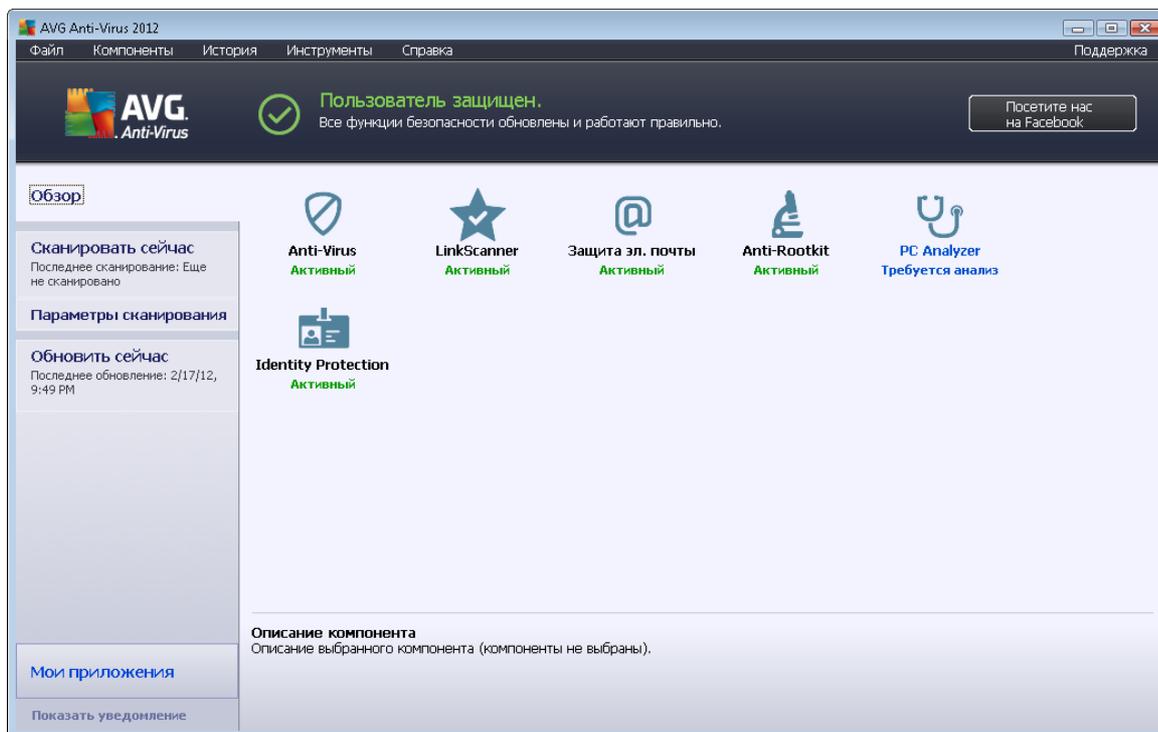
Не изменяйте настройки AVG без необходимости! Все изменения параметров должны выполняться опытным пользователем.

Допустимо незначительное изменение параметров [компонентов AVG](#) непосредственно с помощью интерфейса пользователя определенного компонента. При необходимости изменить конфигурацию AVG перейдите в раздел [Расширенные настройки AVG](#). Выберите пункт системного меню **Инструменты/Расширенные настройки** и измените конфигурацию AVG в открывшемся диалоговом окне [Расширенные настройки AVG](#).



5. Интерфейс пользователя AVG

AVG Anti-Virus 2012 открывается в главном окне.



Главное окно состоит из нескольких разделов.

- **Системное меню** (системная область сверху окна). Стандартное средство навигации, с помощью которого можно получить доступ ко всем компонентам, службам и функциям **AVG Anti-Virus 2012**. [Подробнее сведения >>](#)
- **Информация о состоянии безопасности** (верхняя часть окна). Информация о текущем состоянии программы **AVG Anti-Virus 2012**. [Подробнее сведения >>](#)
- Кнопкой **Присоединиться в Facebook** (в верхней правой части окна) можно присоединиться к [сообществу AVG в Facebook](#). Однако эта кнопка появляется только в случае, если все компоненты полностью функциональны и работают правильно (чтобы узнать о том, как определить состояние компонентов AVG, см. главу [Информация о состоянии безопасности](#))
- **Быстрые ссылки** (левая часть окна). Позволяют получить быстрый доступ к наиболее важным и часто используемым задачам **AVG Anti-Virus 2012**. [Подробнее сведения >>](#)
- **Мои приложения** (левая нижняя часть окна). Открывает обзор дополнительных приложений, доступных для следующих элементов **AVG Anti-Virus 2012**: [LiveKive](#), [Безопасность семьи](#) и [PC Tuneup](#)
- **Обзор компонентов** (центральная часть окна). Обзор всех установленных



компонентов **AVG Anti-Virus 2012** . [Подробные сведения >>](#)

- **Значок на панели задач** (правая нижняя часть экрана, панель задач). Отображение текущего состояния. **AVG Anti-Virus 2012** [Подробные сведения >>](#)
- **Гаджет AVG** (боковая панель Windows, поддерживает ОС Windows Vista/7). Позволяет получить быстрый доступ к функциям сканирования и обновления. **AVG Anti-Virus 2012** [Подробные сведения >>](#)

5.1. Системное меню

Системное меню — это стандартное средство навигации, которое используется во всех приложениях Windows. Оно расположено горизонтально в верхней части главного окна **AVG Anti-Virus 2012**. С помощью системного меню можно получить доступ к специальным компонентам, службам и функциям AVG.

Системное меню состоит из двух основных разделов.

5.1.1. Файл

- **Выход**. Закрытие интерфейса **AVG Anti-Virus 2012** пользователя. При нажатии данной кнопки приложение AVG продолжит свою работу в фоновом режиме, а компьютер будет находиться под защитой!

5.1.2. Компоненты

Элемент [Компоненты](#) системного меню содержит ссылки на все установленные компоненты AVG и позволяет открывать их стандартные диалоговые окна в интерфейсе пользователя.

- **Обзор системы**. Переключение к стандартному диалоговому окну интерфейса пользователя, которое содержит [обзор всех установленных компонентов и сведения об их состоянии](#).
- **Anti-Virus**. Выполняет обнаружение вирусов, червей, шпионских и троянских программ, нежелательных исполняемых файлов или библиотек в системе, а также защищает от вредоносного рекламного ПО — [Подробные сведения >>](#)
- **Link Scanner**. Обеспечивает защиту от интернет-атак, когда вы работаете или выполняете поиск в Интернете — [Подробные сведения >>](#)
- **Защита эл. почты**. Проверяет все входящие сообщения электронной почты на наличие спама, блокирует вирусы, фишинг-атаки и другие угрозы — [Подробные сведения >>](#)
- **Anti-Rootkit**. Выполняет сканирование на наличие опасных средств rootkit, скрытых в приложениях, драйверах или библиотеках — [Подробные сведения >>](#)
- **PC Analyzer**. Предоставляет сведения о состоянии компьютера — [Подробные сведения >>](#)
- **Identity Protection**. Обеспечивает постоянную защиту ваших цифровых данных от новых и неизвестных угроз — [Подробные сведения >>](#)



- **Удаленное администрирование.** Отображается только при использовании версий AVG Business Edition, если пользователь выбрал установку данного компонента [в процессе установки программы](#).

5.1.3. История

- [Результаты сканирования](#). Переход в интерфейс проверки AVG, а именно в диалоговое окно [Обзор результатов сканирования](#).
- [Обнаружение в рамках постоянной защиты](#). Открытие диалогового окна, содержащего обзор угроз, обнаруженных компонентом [Resident Shield](#)
- [Обнаружение в рамках сканера эл. почты](#). Открытие диалогового окна с обзором вложений сообщений электронной почты, признанных опасными компонентом [Защита эл. почты](#)
- [Обнаружение Online Shield](#). Открытие диалогового окна с обзором угроз, обнаруженных службой [Online Shield](#) в составе компонента [LinkScanner](#).
- [Хранилище вирусов](#). Отображение интерфейса среды карантина ([Хранилища вирусов](#)), куда программа AVG отправляет все обнаруженные зараженные файлы, которые по какой-либо причине не удалось вылечить автоматически. Внутри зоны карантина зараженные файлы изолированы и не представляют угрозы для безопасности компьютера, но в то же время они сохраняются для их возможного восстановления в будущем
- [Журнал событий](#). Отображение интерфейса журнала событий, содержащего обзор всех зарегистрированных в журнале действий **AVG Anti-Virus 2012**.

5.1.4. Инструменты

- [Сканировать компьютер](#). Запуск сканирования всего компьютера.
- [Сканировать выбранную папку...](#) Переход к [интерфейсу сканирования AVG](#), который позволяет с помощью структуры дерева определить, какие файлы и папки должны подвергаться сканированию.
- **Сканировать файл...** Позволяет запустить проверку по требованию отдельного файла. Выберите этот параметр, чтобы открыть новое окно с деревом структуры диска. Выберите нужный файл и подтвердите запуск сканирования.
- [Обновить](#). Автоматический запуск процесса обновления **AVG Anti-Virus 2012**.
- **Обновить из каталога...** Запуск процесса обновления с помощью файлов обновления, расположенных в указанной папке на локальном диске. Однако данный параметр рекомендуется использовать только в экстренном случае. Например, в случае отсутствия подключения к Интернету (*например, компьютер заражен и отключен от Интернета или подключен к сети, не имеющей доступа к Интернету и т. п.*). В открывшемся окне выберите папку, где ранее был размещен файл обновления, и запустите процесс обновления.
- [Расширенные настройки...](#) Открытие диалогового окна [Расширенные настройки AVG](#),



которое позволяет изменять AVG Anti-Virus 2012 конфигурацию программы. Обычно рекомендуется сохранить настройки приложения по умолчанию, определенные производителем.

5.1.5. Справка

- **Содержимое.** Открытие файла справки AVG.
- **Получить поддержку.** Открытие веб-сайта AVG (<http://www.avg.com/>) на странице центра поддержки пользователей.
- **AVG в Интернете.** Открытие веб-сайта компании AVG (<http://www.avg.com/>)
- **О вирусах и угрозах.** Открытие интерактивной [Энциклопедии вирусов](#), в которой можно найти подробные сведения об обнаруженных вирусах.
- **Повторно активировать.** Открытие диалогового окна **Активировать AVG** с данными, введенными в диалоговом окне [Персонализация AVG при установке](#). В этом диалоговом окне можно ввести номер лицензии, чтобы заменить им номер продажи (номер, который использовался при установке AVG) или заменить старый номер лицензии (например, при обновлении до новой версии продукта AVG).
- **Регистрация.** Переход на страницу регистрации веб-сайта компании AVG (<http://www.avg.com/>). Введите данные для регистрации. Только клиенты, зарегистрировавшие продукт AVG, могут получать бесплатную техническую поддержку.

Примечание. При использовании пробной версии **AVG Anti-Virus 2012** вместо последних двух элементов будут отображаться пункты **Купить** и **Активировать**, которые позволяют сразу приобрести полную версию программы. Для программы **AVG Anti-Virus 2012**, установленной с указанием номера продажи, будут отображаться пункты **Зарегистрировать** и **Активировать**.

- **Сведения об AVG.** Открытие диалогового окна **Сведения**, содержащего шесть вкладок с такими данными: название программы, версии программы и вирусной базы данных, системная информация, лицензионное соглашение, а также контактная информация компании **AVG Technologies CZ**.

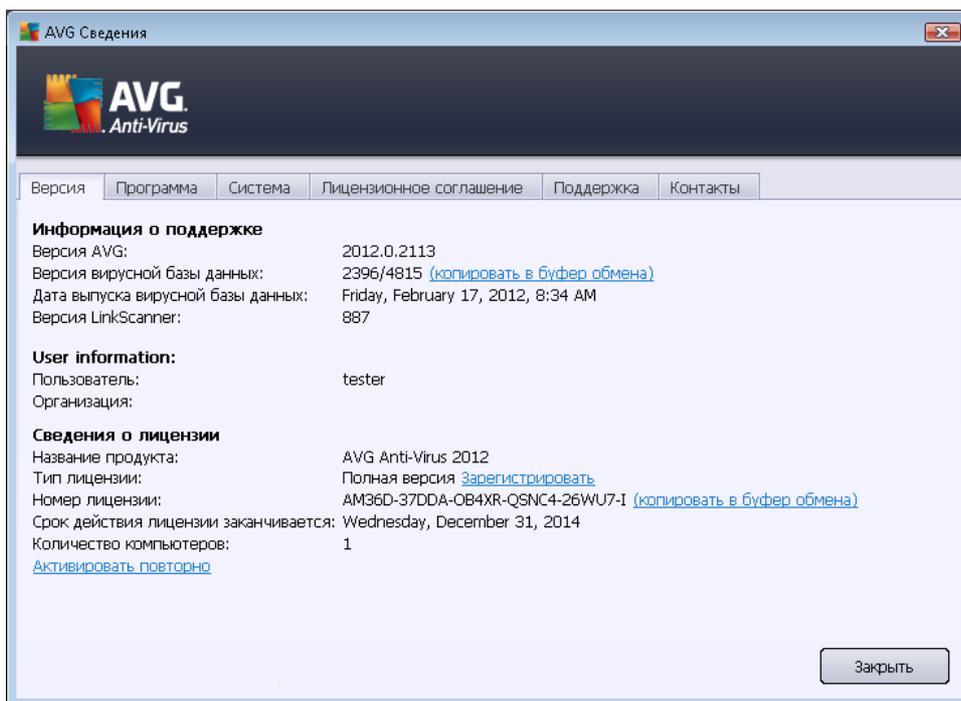
5.1.6. Поддержка

Ссылка **Поддержка** открывает новое диалоговое окно **Сведения** со всей необходимой информацией для решения проблемы. В этом окне содержится основная информация об установленной программе AVG (*программа/версия базы данных*), сведения о лицензии и список ссылок для быстрого перехода в соответствующий раздел поддержки.

В диалоговом окне **Сведения** содержится шесть вкладок:



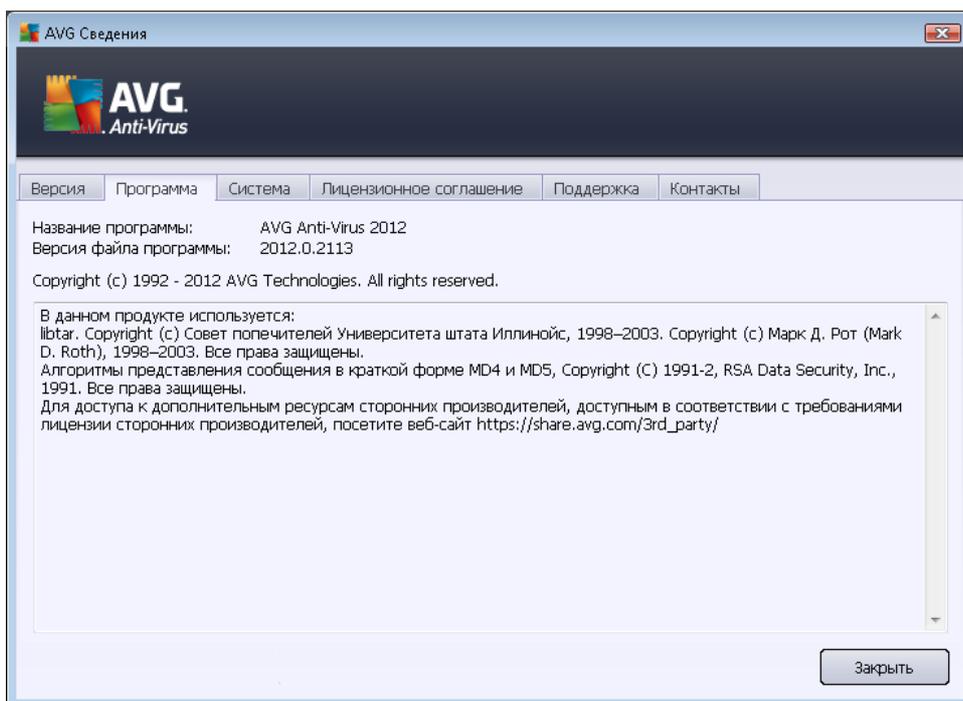
Диалоговое окно **Версия** состоит из трех разделов.



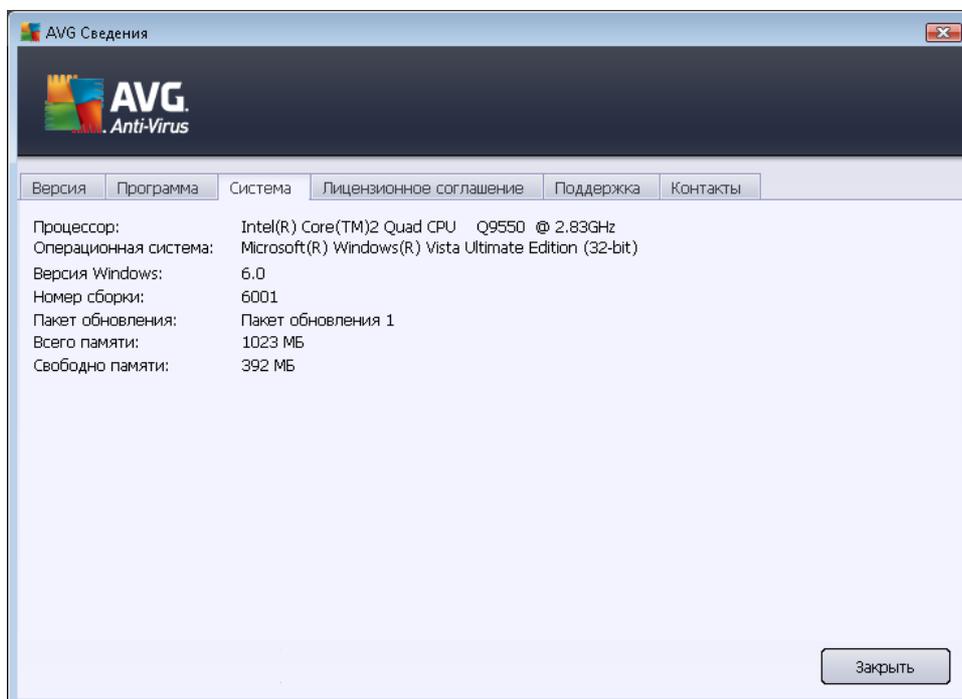
- **Информация для поддержки.** Предоставляет информацию о версии **AVG Anti-Virus 2012**, версии вирусной базы данных, версии базы данных Anti-Spam и версии [LinkScanner](#).
- **Информация о пользователе.** Предоставляет информацию о пользователе и компании, на которую была оформлена лицензия.
- **Сведения о лицензии.** Предоставляет информацию о лицензии (*название продукта, тип лицензии, номер лицензии, дата истечения, количество компьютеров*). В этом разделе можно также зарегистрировать **AVG Anti-Virus 2012** в Интернете, щелкнув ссылку **Зарегистрировать**. Это позволит в более полной мере использовать [техническую поддержку компании AVG](#). Чтобы открыть диалоговое окно **Активировать AVG**, щелкните ссылку **Активировать повторно**. В соответствующем поле введите номер лицензии, чтобы заменить им номер продажи (*номер, который использовался при AVG Anti-Virus 2012 установке*) или изменить текущий номер лицензии (*например, при обновлении до нового продукта AVG*).



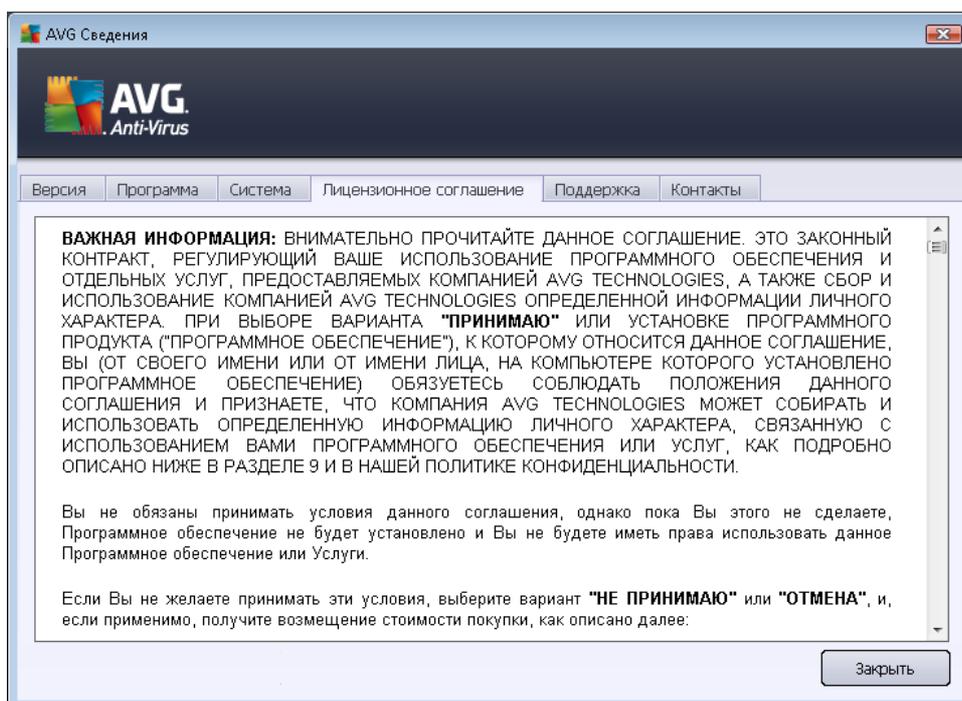
На вкладке **Программа** расположена информация о версии файла программы **AVG Anti-Virus 2012**, а также информация о кодах третьих сторон, использованных в продукте:



Вкладка **Система** предлагает список параметров вашей операционной системы (*тип процессора, операционная система и ее версия, номер сборки, установленные пакеты обновления, объем общей и свободной памяти*).

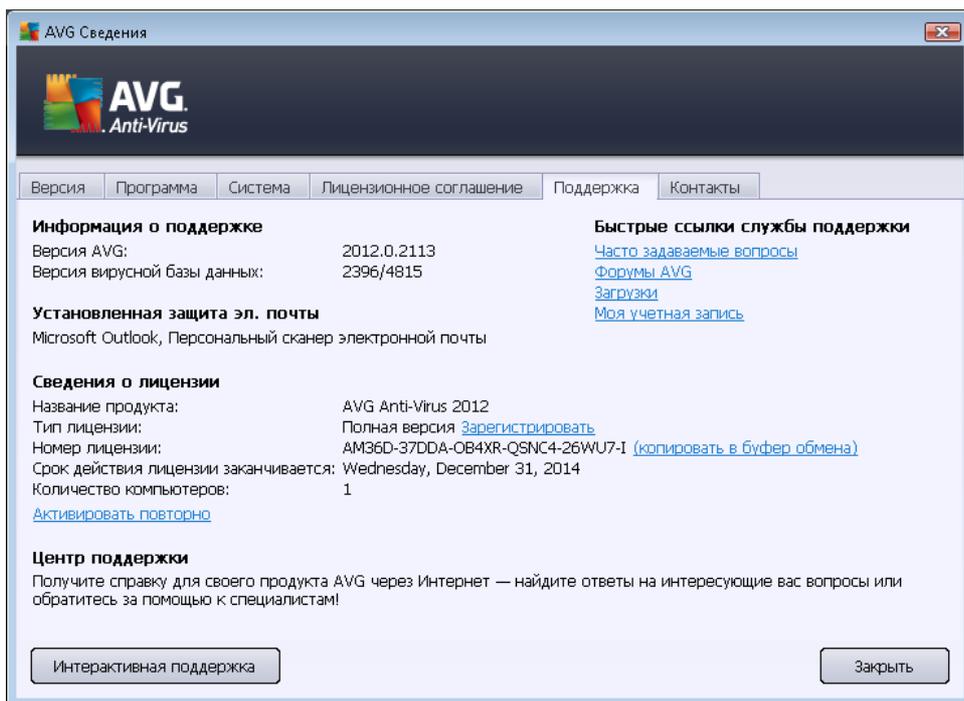


На вкладке **Лицензионное соглашение**, можно ознакомиться с полным текстом лицензионного соглашения между пользователем и компанией AVG Technologies.



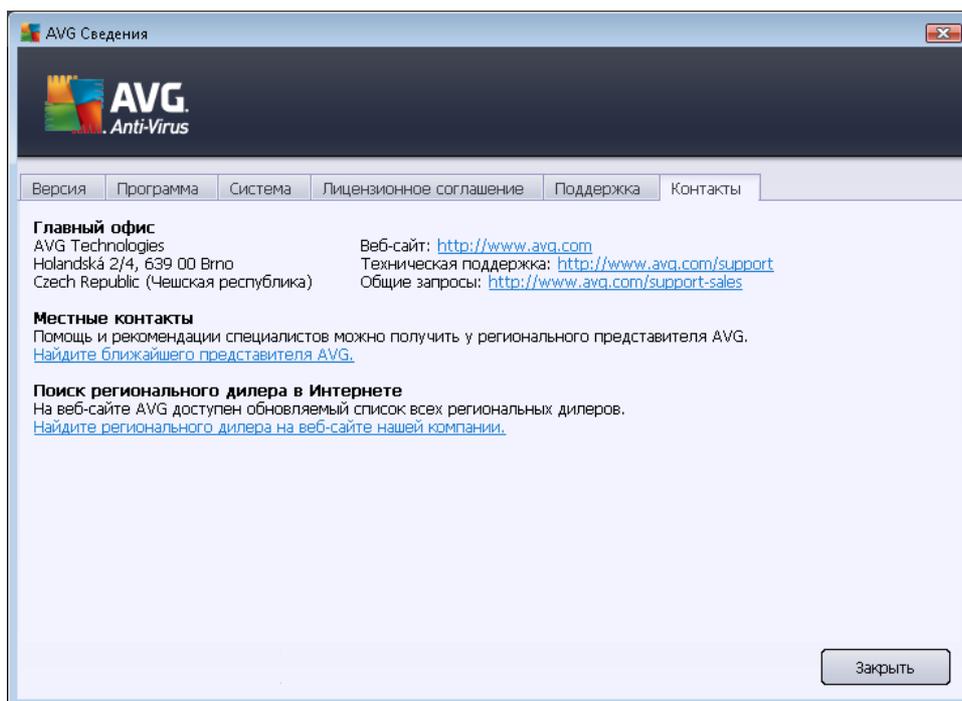


Вкладка **Поддержка** предоставляет список всех возможных вариантов для связи со службой поддержки пользователей. Также на ней имеются ссылки на веб-сайты компании AVG (<http://www.avg.com/>), форумы компании AVG, часто задаваемые вопросы, ... Далее находится информация, которая может понадобиться при обращении в службу поддержки пользователей.





Вкладка **Контакты** содержит список всех контактов компании AVG Technologies, а также контактную информацию региональных представителей и реселлеров компании AVG.



5.2. Информация о состоянии безопасности

Раздел **Информация о состоянии безопасности** расположен в верхней части главного окна **AVG Anti-Virus 2012**. Этот раздел позволяет быстро определить текущее состояние безопасности **AVG Anti-Virus 2012**. Ознакомьтесь со значками, представленными в данном разделе, и их значением.



— Зеленый значок означает, что программа **AVG Anti-Virus 2012 работает правильно**. Ваш компьютер полностью защищен, установлены все необходимые обновления. Все установленные компоненты работают правильно.



— Желтый значок означает, что **один или несколько компонентов настроены неправильно**. Необходимо обратить внимание на их свойства или настройки. Нет серьезных проблем, связанных с работой программы **AVG Anti-Virus 2012**. Скорее всего, некоторые компоненты были отключены по какой-либо причине. Компьютер находится под защитой. Однако необходимо уделить внимание настройке компонента. Его имя будет отображено в разделе **Информация о состоянии безопасности**.

Желтый значок отображается также в том случае, если по какой-либо причине было



принято решение игнорировать состояние ошибки компонента. Параметр **Игнорировать состояние компонента** доступен в контекстном меню, отображаемом при нажатии с помощью правой кнопки мыши значка соответствующего компонента в [обзоре компонентов](#) в главном окне **AVG Anti-Virus 2012**. Выберите данный параметр, если известно о состоянии ошибки компонента, но по какой-либо причине не требуется изменять состояние **AVG Anti-Virus 2012** и необходимо отключить оповещение с помощью [значка на панели задач](#). Использование данного параметра может потребоваться в определенной ситуации, при этом настоятельно рекомендуется сразу же отключать параметр **Игнорировать состояние компонента** по завершении действия.

Также желтый значок будет отображаться, если **AVG Anti-Virus 2012** требует перезагрузки компьютера (**Требуется перезагрузка**). Обратите внимание на это предупреждение и перезагрузите компьютер кнопкой **Перезагрузить сейчас**.



— Оранжевый значок указывает на критическое состояние программы **AVG Anti-Virus 2012**. Один или несколько компонентов работают неправильно, программа **AVG Anti-Virus 2012** не может защитить компьютер. Необходимо немедленно устранить указанные проблемы. Если проблему не удастся устранить самостоятельно, обратитесь в [службу технической поддержки компании AVG](#).

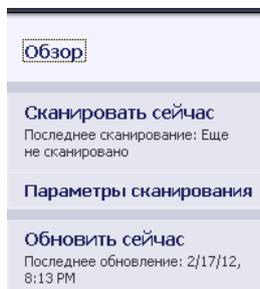
Если программа **AVG Anti-Virus 2012** не настроена для обеспечения оптимальной производительности, рядом со сведениями о состоянии безопасности отобразится новая кнопка **Исправить** (или **Исправить все** при возникновении проблемы с несколькими компонентами). Нажмите эту кнопку, чтобы запустить автоматический процесс проверки и настройки. Это наиболее простой способ настройки оптимальной производительности программы **AVG Anti-Virus 2012** и обеспечения максимального уровня безопасности.

Настоятельно рекомендуется обращать внимание на раздел **Информация о состоянии безопасности**. В случае возникновения проблемы необходимо постараться незамедлительно ее устранить. В противном случае безопасность компьютера может быть под угрозой.

Примечание. *Информация о состоянии безопасности AVG Anti-Virus 2012 может быть получена в любое время с помощью [значка на панели задач](#).*

5.3. Быстрые ссылки

Быстрые ссылки расположены в левой части [интерфейса пользователя AVG Anti-Virus 2012](#). Данные ссылки позволяют получить быстрый доступ к наиболее важным и часто используемым функциям приложения, таким как сканирование и обновление. Быстрые ссылки доступны из всех диалоговых окон интерфейса пользователя.



Быстрые ссылки визуально разделены на три секции:

- **Сканировать сейчас.** По умолчанию данная кнопка позволяет получить сведения о последнем запущенном сканировании (*тип сканирования, дата последнего запуска*). Щелкните команду **Сканировать сейчас** для запуска сканирования. Для запуска другого типа сканирования щелкните ссылку **Параметры сканирования**. В результате откроется [интерфейс сканирования AVG](#), с помощью которого можно запускать и планировать процессы сканирования или изменять их параметры. *(Для получения подробных сведений см. главу [Сканирование AVG](#))*
- **Параметры сканирования** . Используйте данную ссылку для перехода из открытого диалогового окна AVG в окно по умолчанию, содержащее [обзор всех установленных компонентов](#). *(Для получения подробных сведений см. главу [Обзор компонентов](#))*
- **Обновить сейчас.** Данная ссылка предоставляет сведения о времени последнего запуска процесса [обновления](#). Нажмите эту кнопку, чтобы немедленно запустить процесс обновления и пройти все его этапы. *(Для получения подробных сведений см. главу [Обновление AVG](#))*

Быстрые ссылки всегда доступны в [интерфейсе пользователя AVG](#). После запуска процесса сканирования или обновления при помощи ссылки приложение переключится на новое диалоговое окно, но быстрые ссылки будут по-прежнему доступны. Более того, запущенный процесс графически отображается на навигационной панели, так что можно контролировать все выполняющиеся в данный момент процессы **AVG Anti-Virus 2012** .

5.4. Обзор компонентов

Разделы обзора компонентов

Раздел **Обзор компонентов** расположен в центральной части [интерфейса пользователя AVG Anti-Virus 2012](#). Раздел состоит из двух частей.

- **Обзор всех установленных компонентов** в виде графических панелей для каждого установленного компонента. Каждая панель обозначена соответствующим значком компонента и содержит информацию о текущей активности компонента.
- **Описание компонента** находится в нижней части этого диалогового окна. Описание вкратце объясняет основные функции компонента, а также информирует о текущем состоянии выбранного компонента.



Список установленных компонентов

В **AVG Anti-Virus 2012** раздел **Обзор компонентов** содержит сведения о следующих компонентах:

- **Anti-Virus.** Выполняет обнаружение вирусов, червей, шпионских и троянских программ, нежелательных исполняемых файлов или библиотек в системе, а также защищает от вредоносного рекламного ПО — [Подробные сведения >>](#)
- **LinkScanner.** Обеспечивает защиту от интернет-атак, когда вы работаете или выполняете поиск в Интернете — [Подробные сведения >>](#)
- **Защита эл. почты.** Проверяет все входящие сообщения электронной почты на наличие спама, блокирует вирусы, фишинг-атаки и другие угрозы — [Подробные сведения >>](#)
- **Anti-Rootkit.** Выполняет сканирование на наличие опасных средств rootkit, скрытых в приложениях, драйверах или библиотеках — [Подробные сведения >>](#)
- **PC Analyzer.** Предоставляет сведения о состоянии компьютера — [Подробные сведения >>](#)
- **Identity Protection.** Обеспечивает постоянную защиту ваших цифровых данных от новых и неизвестных угроз — [Подробные сведения >>](#)
- **Удаленное администрирование.** Отображается только при использовании версий AVG Business Edition, если пользователь выбрал установку данного компонента [в процессе установки программы.](#)

Доступные действия

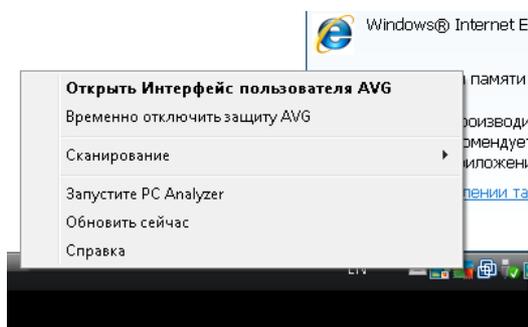
- **Для выделения любого из компонентов** в обзоре следует навести курсор мыши на значок компонента. При этом в нижней части [интерфейса пользователя](#) отобразится описание основных функций компонента.
- **Щелкните значок любого компонента, чтобы** открыть собственный интерфейс компонента со списком основных статистических данных.
- **Щелкните правой кнопкой мыши значок компонента,** чтобы открыть контекстное меню со следующими параметрами:
 - **Открыть.** Нажатие этого параметра открывает диалоговое окно компонента (аналогично щелчку значка компонента).
 - **Игнорировать состояние данного компонента.** Выберите этот параметр, если вам известно о [состоянии ошибки компонента](#), но по какой-либо причине не требуется изменять данное состояние и нет необходимости получать предупреждения с помощью [значка на панели задач.](#)



- **Открыть дополнительные параметры...** Данная настройка доступна только для компонентов, которые имеют возможность настройки [дополнительных параметров](#).

5.5. Значок на панели задач

Значок AVG на панели задач (на панели задач Windows, правая нижняя часть экрана). Отображение текущего состояния **AVG Anti-Virus 2012**. Этот значок всегда отображается на панели задач независимо от того, открыт ли [интерфейс пользователя AVG Anti-Virus 2012](#).



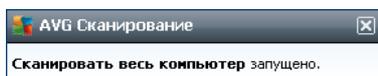
Отображение значка AVG на панели задач

-  При полноцветном отображении значок на панели задач указывает, что все **AVG Anti-Virus 2012** компоненты активны и работают правильно. Однако полноцветный значок может также отображаться в случае, если один из компонентов находится в состоянии ошибки, но был выбран параметр [Игнорировать состояние компонентов](#). (Выбрав параметр *Игнорировать состояние компонентов*, пользователь показывает, что ему известно о [состоянии ошибки компонента](#), но по какой-либо причине не требуется изменять данное состояние и нет необходимости получать предупреждения о данной ситуации.)
-  Значок с восклицательным знаком указывает на [ошибку](#) в компоненте (или в нескольких компонентах). Всегда обращайте внимание на подобные предупреждения и старайтесь должным образом настроить компонент и исправить неполадку. Чтобы изменить настройки компонента, дважды щелкните значок на панели задач и откройте [интерфейс пользователя приложения](#). Подробные сведения о том, какой именно компонент находится в [состоянии ошибки](#), см. в разделе [Сведения о состоянии безопасности](#).
-  Значок на панели задач может также отображаться в полном цвете с мигающим и крутящимся лучом света. Такое отображение означает, что запущился процесс обновления.
-  Полноцветный значок со стрелкой символизирует **AVG Anti-Virus 2012** запуск сканирования.



Информация на значке AVG на панели задач

Значок AVG на панели задач информирует о текущих действиях **AVG Anti-Virus 2012** и возможных изменениях состояния в программе (*например, об автоматическом запуске запланированного сканирования или обновления, изменении состояния компонента, возникновении ошибки и т. д.*) с помощью всплывающего окна, которое открывается из значка на панели задач.



Действия, доступные из значка AVG на панели задач

Дважды щелкнув **значок AVG на панели задач**, можно быстро получить доступ к [интерфейсу пользователя AVG Anti-Virus 2012](#). Если щелкнуть правой кнопкой мыши значок на панели задач, откроется краткое контекстное меню, содержащее следующие пункты:

- **Открыть интерфейс пользователя AVG.** Открытие [интерфейса пользователя AVG Anti-Virus 2012](#).
- **Временно отключить защиту AVG.** Данный параметр позволяет полностью выключить защиту, обеспечиваемую **AVG Anti-Virus 2012**. Используйте данный параметр только в случае крайней необходимости! В большинстве случаев программу **AVG Anti-Virus 2012** не рекомендуется выключать перед установкой нового ПО или драйверов, даже если программа или мастер установки рекомендует завершить все запущенные программы и приложения, чтобы они не препятствовали процессу установки. Если вам пришлось временно выключить защиту **AVG Anti-Virus 2012**, включите ее, как только завершите установку. Если вы подключены к Интернету или локальной сети, но антивирусная защита выключена, ваш компьютер может подвергнуться атакам.
- **Сканирования.** Щелкните, чтобы открыть контекстное меню [предварительно настроенных сеансов сканирования](#) ([Сканирование всего компьютера](#), [Сканирование отдельных файлов или папок](#)), и выберите соответствующий вариант. Сканирование будет запущено немедленно.
- **Запущенные сканирования...** — Данный элемент отображается, только если на компьютере выполняется сканирование. Для запущенного сканирования можно назначить приоритет. Кроме того, его можно приостановить или остановить полностью. Доступны следующие действия: *Установить приоритет для всех сканирований*, *Приостановить все сканирования* или *Остановить все сканирования*.
- **Запустить PC Analyzer.** Щелкните, чтобы запустить компонент [PC Analyzer](#).
- **Обновить сейчас.** Немедленный запуск [обновления](#).
- **Справка.** Открытие файла справки на начальной странице.



5.6. Советник AVG

AVG Advisor — это улучшающая производительность функция, которая контролирует все текущие процессы вашего компьютера и советует, как избежать проблем. **AVG Advisor** отображается в форме всплывающего окна над панелью задач.



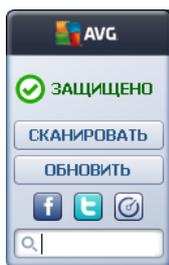
AVG Advisor может появиться в следующих ситуациях:

- Используемому вами веб-обозревателю не хватает памяти, что может замедлять работу (*AVG Advisor поддерживает только веб-обозреватели Internet Explorer, Chrome, Firefox, Opera и Safari*).
- Текущий процесс в компьютере занимает слишком много памяти и замедляет производительность компьютера.
- Компьютер будет автоматически подключен к неизвестной сети WiFi.

В каждой из этих ситуаций **AVG Advisor** предупреждает о возможной проблеме и предоставляет название и значок конфликтующего процесса или приложения. Также **AVG Advisor** предлагает меры, которые следует принять во избежание возможных проблем.

5.7. Гаджет AVG

Гаджет AVG отображается на рабочем столе Windows (на боковой панели Windows). Данное приложение поддерживает только операционные системы Windows Vista и Windows 7. **Гаджет AVG** позволяет мгновенно получить доступ к самым важным функциям **AVG Anti-Virus 2012**, например, к операциям [сканирования](#) и [обновления](#).

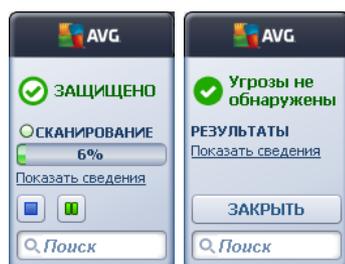




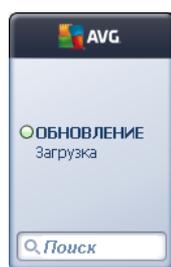
Быстрый доступ к сканированию и обновлению

При необходимости **гаджет AVG** позволяет немедленно запустить процесс сканирования или обновления.

- **Сканировать.** Щелкните ссылку **Сканировать**, чтобы запустить [сканирование всего компьютера](#). Состояние выполнения процесса сканирования будет отображаться в пользовательском интерфейсе гаджета. Краткая сводка статистики содержит сведения о количестве сканированных объектов, обнаруженных угроз и вылеченных угроз. Во время выполнения сканирования всегда можно приостановить  или остановить  данный процесс. Подробные результаты сканирования можно просмотреть в диалоговом окне [Обзор результатов сканирования](#), которое можно открыть непосредственно из гаджета с помощью параметра **Показать сведения** (соответствующие результаты сканирования отобразятся в разделе *Сканирование с помощью гаджета на боковой панели*).



- **Обновить сейчас.** Щелкните ссылку **Обновить сейчас AVG Anti-Virus 2012**, чтобы запустить процесс обновления непосредственно в гаджете.



Доступ к социальным сетям

Гаджет AVG также предоставляет быструю ссылку для подключения к основным социальным сетям. Используйте соответствующую кнопку для подключения к сообществам AVG в Twitter, Facebook или LinkedIn.

- **Ссылка Twitter** . Открытие нового интерфейса **гаджета AVG**, содержащего сводку последних веб-каналов AVG, размещенных на сайте Twitter. Щелкните ссылку **Просмотреть все веб-каналы AVG на Twitter**, чтобы открыть в новом окне браузера страницу Twitter, содержащую новости AVG



- **Ссылка Facebook**  . Открытие в веб-обозревателе страницы **сообщества AVG** на веб-сайте Facebook.
- **LinkedIn**  . Данный параметр доступен только во время сетевой установки (*т. е. предполагается, что программа AVG была установлена с использованием одной из лицензий AVG Business Edition*), он позволяет открыть веб-обозреватель на сайте **сообщества AVG SMB** в социальной сети LinkedIn.

Через гаджет можно также получить доступ к другим функциям

- **PC Analyzer**  . Открытие пользовательского интерфейса компонента [PC Analyzer](#) и мгновенный запуск анализа.
- **Поле поиска**. Отображение результатов поиска по ключевому слову в новом окне веб-обозревателя по умолчанию.



6. Компоненты AVG

6.1. Anti-Virus

Компонент **Anti-Virus** является основой **AVG Anti-Virus 2012** и включает в себя ряд ключевых функций программы обеспечения безопасности.

- [Модуль сканирования](#)
- [Постоянная защита](#)
- [Защита Anti-Spyware](#)

6.1.1. Модуль сканирования

Модуль сканирования, являющийся основой компонента **Anti-Virus**, сканирует все файлы и их активность (*открытие, закрытие файлов и т. п.*) на известные вирусы. Каждый обнаруженный вирус блокируется, удаляется или помещается в [хранилище вирусов](#).

Важной особенностью защиты AVG Anti-Virus 2012 является то, что ни один из известных вирусов не сможет запуститься на компьютере.

Способы обнаружения

Большая часть антивирусного ПО использует метод эвристического сканирования, при котором файлы сканируются на типичные признаки вирусов, так называемые "вирусные подписи". Это означает, что антивирусный сканер может обнаружить новый, неизвестный вирус, если новый вирус содержит некоторые типичные признаки уже существующих вирусов. **Компонент Anti-Virus** использует следующие способы обнаружения:

- *Сканирование.* Поиск строки символов, характерной для конкретного вируса.
- *Эвристический анализ.* Динамическая эмуляция сканированных объектов в виртуальной компьютерной среде.
- *Типовое определение.* Определение характерных команд данного вируса/группы вирусов.

Когда одна технология не может справиться с обнаружением и определением вируса, компонент **Anti-Virus** использует несколько технологий для защиты компьютера от вирусов. **AVG Anti-Virus 2012** может анализировать и обнаруживать выполнимые приложения или библиотеки DLL, использование которых в системе потенциально нежелательно. Подобные угрозы называются "Потенциально нежелательные программы" (*различные виды шпионского ПО, рекламное ПО и прочее*). Более того, **AVG Anti-Virus 2012** сканирует системный реестр на подозрительные записи, временные интернет-файлы, следящие файлы cookie и поступает с потенциально вредоносными элементами так же, как и с другими зараженными объектами.

AVG Anti-Virus 2012 обеспечивает непрерывную защиту компьютера.



6.1.2. Постоянная защита

AVG Anti-Virus 2012 обеспечивает постоянную защиту с помощью компонента Resident Shield. Компонент **Anti-Virus** сканирует каждый файл (с любым расширением или без расширения), который открывается, сохраняется или копируется. Он защищает системные области компьютера и съемные носители (съемный носитель и т. п.). Если при доступе к файлу будет обнаружен вирус, то выполняемое в данный момент действие с файлом завершается. Таким образом, вирус не сможет активировать себя. Как правило, пользователь даже не замечает этот процесс, поскольку постоянная защита работает в фоновом режиме. Уведомления отображаются только при обнаружении угроз. В то же время компонент **Anti-Virus** блокирует активизацию угрозы и удаляет ее.

Постоянная защита загружается в память компьютера при запуске системы. Крайне необходимо, чтобы данный компонент всегда включен.

6.1.3. Защита Anti-Spyware

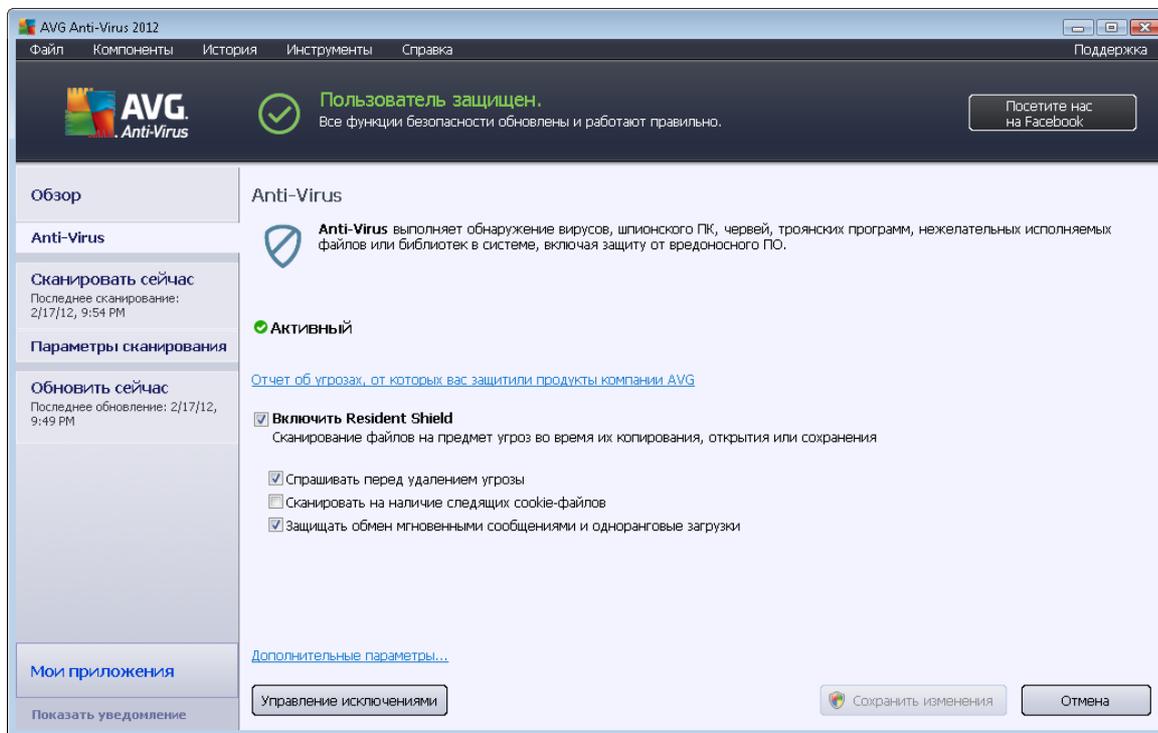
Компонент **Anti-Spyware** содержит базу данных шпионского программного обеспечения, предназначенную для распознавания известных видов определений шпионского ПО. Специалисты компании AVG в области шпионского ПО проделывают большую работу по распознаванию и описанию последних образцов шпионского ПО по мере их появления, после чего добавляют определения в базу данных шпионского программного обеспечения. В процессе обновления новые определения загружаются на компьютер, обеспечивая надежную защиту даже от самых последних типов шпионского ПО. С помощью компонента **Anti-Spyware** можно выполнить полное сканирование компьютера на наличие вредоносного или шпионского программного обеспечения. При сканировании также можно обнаружить "спящее" и неактивное вредоносное ПО, то есть вредоносное ПО, которое загружено, но еще не активировано.

Что такое шпионское ПО?

Шпионское программное обеспечение — это тип вредоносного ПО, собирающего информацию на компьютерах пользователей без их ведома или согласия. Некоторые шпионские приложения устанавливаются осознанно и часто содержат рекламу, всплывающие окна или различные типы нежелательного ПО. В настоящее время основным источником заражений являются веб-сайты с потенциально опасным содержанием. Кроме того, шпионское ПО может распространяться по электронной почте, а также в виде червей или вирусов. Самым эффективным средством защиты от перечисленных угроз является использование сканера **Anti-Spyware**, работающего постоянно в фоновом режиме аналогично компоненту Resident Shield, который сканирует приложения при их запуске.

6.1.4. Интерфейс Anti-Virus

Интерфейс компонента **Anti-Virus** предоставляет краткий обзор функций компонента, сведения о текущем состоянии компонента (*Активный*), а также основные параметры конфигурации компонента.



Параметры конфигурации

Диалоговое окно содержит основные параметры конфигурации функций, доступных в компоненте **Anti-Virus**. Ниже приведено краткое описание этих функций.

- **Просмотреть интерактивный отчет о том, как AVG удалось обеспечить вашу защиту.** Данная ссылка перенаправляет на определенную страницу на веб-сайте AVG (<http://www.avg.com/>). На этой странице можно посмотреть подробный статистический обзор всех **AVG Anti-Virus 2012** действий, выполненных на вашем компьютере за определенный промежуток времени или за все время.
- **Включить Resident Shield** — позволяет легко включать и отключать постоянную защиту. Компонент Resident Shield сканирует копируемые, открываемые или сохраняемые файлы. При обнаружении вируса или любой другой угрозы сразу же появляется предупреждение. По умолчанию данная функция включена, рекомендуется оставить ее без изменений. Если постоянная защита включена, можно определить действия, которые будут производиться с зараженными объектами.
 - **Спрашивать перед удалением угроз.** Не снимайте данный флажок, чтобы подтвердить возникновения запроса каждый раз, когда возникает угроза, перед тем как переместить ее в [хранилище вирусов](#). Данный параметр не влияет на уровень безопасности, поэтому может быть настроен на усмотрение пользователя.
 - **Сканировать на наличие следящих файлов cookie** — вне зависимости от предыдущих параметров можно выбрать сканирование следящих файлов



cookie. (Файлы cookie — текстовые пакеты, отправляемые сервером в веб-браузер, а затем веб-браузером обратно на сервер при каждом подключении браузера к серверу. Файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзины для покупок в Интернете.) В некоторых случаях может потребоваться включение данного параметра, чтобы обеспечить максимальный уровень безопасности. Однако по умолчанию данный параметр отключен.

- **Включить защиту программ обмена мгновенными сообщениями и загрузок P2P**. Установите данный флажок, чтобы проверять на наличие вирусов вашу программу обмена мгновенными сообщениями (например, ICQ, MSN Messenger и т. п.).
- **Дополнительные параметры**. Щелкните эту ссылку, чтобы перейти в соответствующее диалоговое окно, содержащее [Дополнительные параметры AVG Anti-Virus 2012](#). Здесь можно изменить дополнительные настройки компонента. Обратите внимание, что параметры всех компонентов по умолчанию настроены на **AVG Anti-Virus 2012** обеспечение оптимальной производительности и максимального уровня безопасности. Не изменяйте установленные по умолчанию настройки без необходимости.

Кнопки управления

В данном диалоговом окне расположены следующие кнопки управления:

- **Управление исключениями**. При нажатии данной кнопки открывается новое диалоговое окно **Исключения Resident Shield**. Чтобы получить доступ к разделу Конфигурация исключений в окне "Сканирование Resident Shield", выберите [Расширенная настройка / Anti-Virus / Постоянная защита / Исключения](#) (подробное описание смотрите в соответствующей главе). В этом диалоговом окне можно указать файлы и папки, которые должны быть исключены из сканирования компонентом Resident Shield. Настоятельно рекомендуется не исключать какие-либо элементы без необходимости. В диалоговом окне содержатся следующие кнопки управления:
 - **Добавить путь**. Укажите каталоги, которые должны быть исключены из сканирования, выбрав их последовательно в дереве навигации локального диска.
 - **Добавить файл**. Укажите файлы, которые должны быть исключены из сканирования, выбрав их последовательно в дереве навигации локального диска.
 - **Редактировать элемент**. Позволяет редактировать указанный путь к выбранному файлу или папке.
 - **Удалить элемент**. Позволяет удалить путь к выбранному элементу из списка.
 - **Редактировать список**. Позволяет редактировать весь список определенных



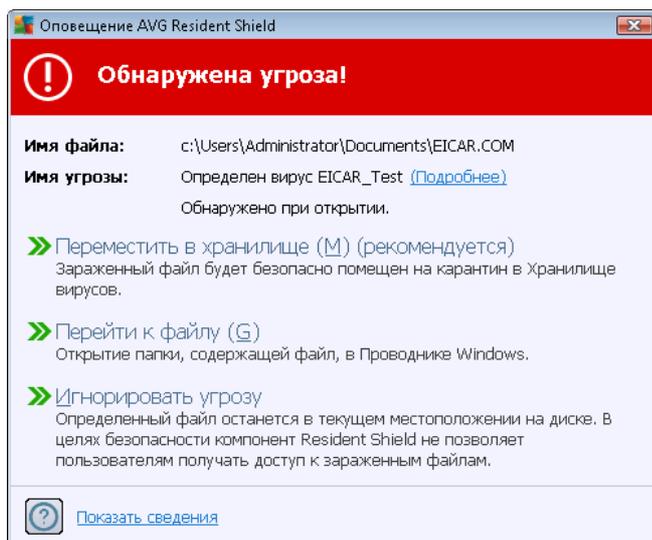
исключений в новом диалоговом окне, как в стандартном текстовом редакторе.

- **Сохранить изменения.** Позволяет сохранить все изменения параметров компонента, произведенные в данном диалоговом окне, и вернуться к основному [интерфейсу пользователя AVG Anti-Virus 2012](#) (обзор компонентов).
- **Отменить.** Нажмите данную кнопку, чтобы отменить все изменения параметров компонента, произведенные в данном диалоговом окне. Изменения не будут сохранены. Произойдет возврат к [интерфейсу пользователя](#) по умолчанию **AVG Anti-Virus 2012** (Обзор компонентов).

6.1.5. Обнаружения Resident Shield

Обнаружена угроза!

Resident Shield сканирует копируемые, открываемые или сохраняемые файлы. При обнаружении вируса или угрозы сразу же появляется предупреждение в следующем диалоговом окне:



В данном диалоговом окне с предупреждением содержатся данные, которые были обнаружены в файле и определены как "зараженные" (*Имя файла*), название распознанного заражения (*Название угрозы*) и ссылка на [Энциклопедию вирусов](#), в которой содержатся подробные сведения об обнаруженном заражении, если оно известно (*Подробная информация*).

Далее необходимо выбрать действие, которое будет применено к заражениям. Доступно несколько вариантов. **Обратите внимание, что при определенных условиях (зависит от типа зараженного файла и его месторасположения) могут быть доступны не все варианты.**

- **Вылечить.** Данная кнопка отображается только в том случае, если лечение обнаруженных объектов возможно. При ее нажатии заражение удаляется из файла, а



файл восстанавливается в исходное состояние. Если файл сам является вирусом, используйте данную функцию для его удаления (*перемещения в [хранилище вирусов](#)*).

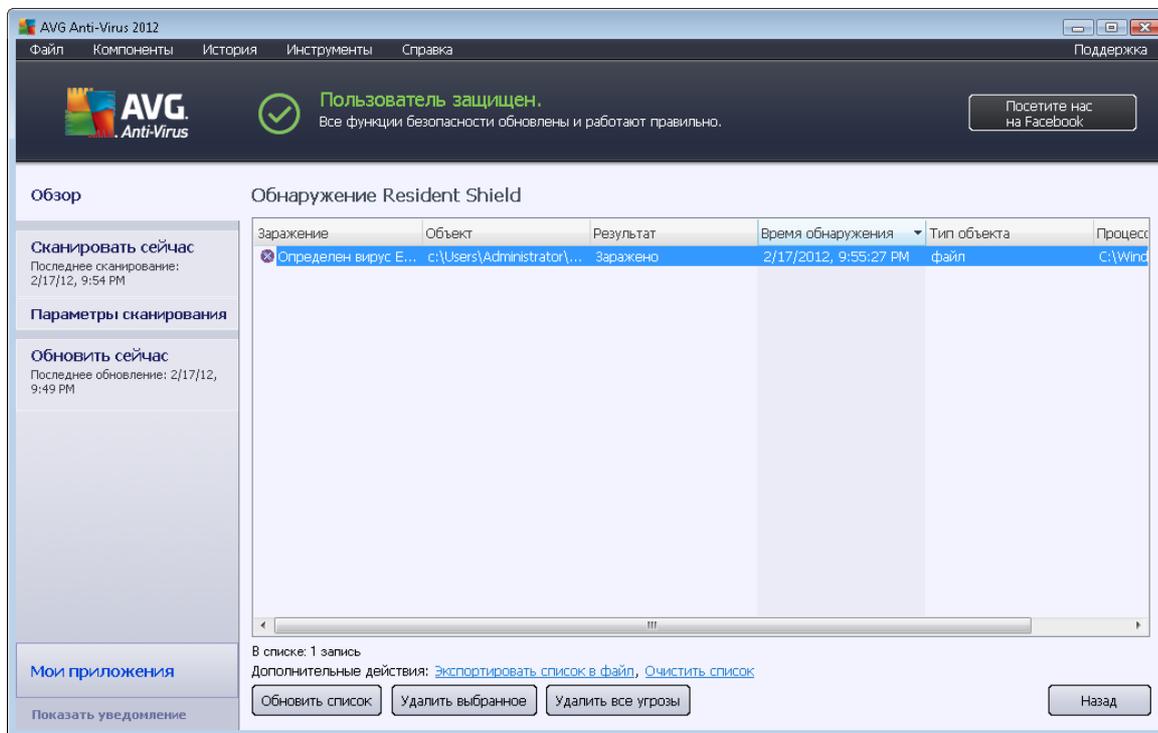
- **Поместить в хранилище (рекомендуется).** Вирус будет помещен в [хранилище вирусов](#)
- **Перейти к файлу.** Перенаправление в папку размещения подозрительного объекта (*в новом окне Проводника Windows*).
- **Игнорировать угрозу.** Категорически НЕ рекомендуется использовать данный параметр без необходимости!

Примечание. *Размер обнаруженного объекта может превышать объем свободного места в хранилище вирусов. В этом случае при попытке переместить зараженный объект в хранилище вирусов отобразится всплывающее предупреждение о проблеме. Однако объем хранилища вирусов можно изменить. Он определяется в процентном соотношении с фактическим объемом жесткого диска. Чтобы увеличить объем хранилища вирусов, откройте диалоговое окно [Хранилище вирусов](#) в меню [Дополнительные параметры AVG](#) с помощью параметра "Предельный размер хранилища вирусов".*

В нижней части диалогового окна отображается ссылка **Показать сведения**, при нажатии которой открывается всплывающее окно, содержащее подробные сведения о процессе, запущенном при обнаружении заражения, и идентификации процесса.

Обзор обнаружений Resident Shield

Полный обзор всех угроз, обнаруженных компонентом [Resident Shield](#), доступен в окне **Обнаружения Resident Shield** в системном меню [История/Обнаружения Resident Shield](#).



В диалоговом окне **Обнаружение Resident Shield** представлен обзор объектов, обнаруженных компонентом [Resident Shield](#) и определенных как опасные, которые были вылечены или помещенные в [Хранилище вирусов](#). По каждому обнаруженному объекту предоставляется следующая информация:

- **Заражение.** Описание (возможно, даже имя) обнаруженного объекта.
- **Объект.** Местоположение объекта.
- **Результат.** Действие, выполненное в отношении обнаруженного объекта.
- **Время обнаружения.** Дата и время обнаружения объекта.
- **Тип объекта.** Тип обнаруженного объекта.
- **Процесс.** Действия, предпринятые для обнаружения потенциально опасного объекта.

В нижней части диалогового окна под списком находится информация об общем количестве обнаруженных объектов, перечисленных выше. Далее возможно экспортировать весь список обнаруженных объектов в файл (**Экспортировать список в файл**) и удалить все записи об обнаруженных объектах (**Очистить список**). Кнопка **Обновить список** обновит список объектов, найденных компонентом **Resident Shield**. Кнопка **Назад** выполняет переход к установленному по умолчанию [главному диалоговому окну AVG](#) (*Обзор компонентов*).



6.2. LinkScanner

Компонент LinkScanner обеспечивает защиту системы от постоянно растущего количества однодневных угроз. Эти угрозы могут скрываться на любых веб-сайтах — от государственных или известных компаний и марок до небольших организаций. Многие из этих угроз существуют не более 24 часов. **Компонент LinkScanner** обеспечивает вашу защиту путем анализа веб-страниц, к которым ведут ссылки на просматриваемой вами странице. Данный компонент проверяет сайты тогда, когда это действительно необходимо — при переходе по ссылке.

Компонент LinkScanner не предназначен для использования на серверных платформах.

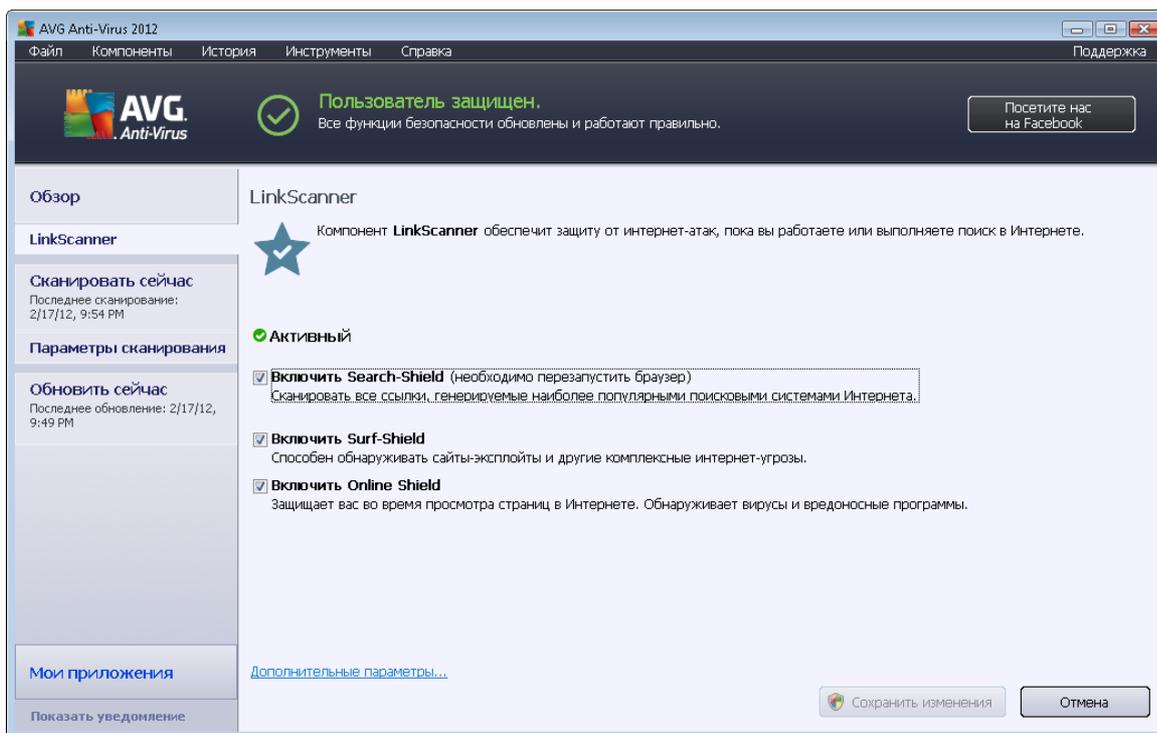
Технология **LinkScanner** включает в себя следующие основные функции:

- **Search-Shield** содержит список известных опасных веб-сайтов (*URL-адресов*). При выполнении поиска с помощью систем Google, Yahoo!, JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask и Seznam все результаты поиска проверяются в соответствии с этим списком. После этого отображается значок заключения (*для результатов поиска Yahoo! отображаются только значки заключения о наличии эксплойтов на веб-сайтах*).
- **Компонент Surf-Shield** выполняет сканирование содержимого посещаемых веб-сайтов независимо от наличия их адресов в списке. Даже если опасный веб-сайт не был обнаружен с помощью **Search-Shield** (*например, если он был создан недавно или если ранее безопасный веб-сайт теперь содержит вредоносное ПО*), он будет выявлен и заблокирован компонентом **Surf-Shield** при попытке его посещения.
- **Компонент Online Shield** предоставляет защиту в реальном времени во время работы в Интернете. Он сканирует содержимое посещаемых веб-страниц и файлов, которые могут на них содержаться, еще до того, как данное содержимое будет отображено в Интернет-браузере или загружено на компьютер. **Компонент Online Shield** обнаруживает вирусы и шпионское ПО на странице, которую вы собираетесь посетить, и мгновенно прерывает загрузку с этой страницы, чтобы данные угрозы не попали в компьютер.



6.2.1. Интерфейс LinkScanner

В главном диалоговом окне компонента [LinkScanner](#) предоставляется краткое описание функций компонента и сведения о его текущем состоянии (*Активный*):



В нижней части окна можно настроить основные функции компонента.

- **Включить [Search-Shield](#)** (по умолчанию включено). Этот флажок можно снять только при крайней необходимости отключения компонента Search Shield.
- **Включить [Surf-Shield](#)** (по умолчанию включено). Активная защита (в реальном времени) при посещении сайтов с эксплоитами. Известные вредоносные сайты и их зараженное эксплоитами содержимое блокируется при доступе к ним через веб-браузер (или любое другое приложение, использующее HTTP).
- **Включить [Online Shield](#)** (по умолчанию включено). Сканирование в реальном времени веб-страниц, которые вы собираетесь посетить, на наличие вирусов или шпионского ПО. При их обнаружении мгновенно прерывается загрузка, чтобы данные угрозы не попали в компьютер.

6.2.2. Обнаружения Search-Shield

При поиске в Интернете с включенной системой **Search-Shield** все результаты поиска, возвращаемые наиболее популярными поисковыми службами (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg u SlashDot*), оцениваются на предмет опасных или подозрительных ссылок. Проверая данные ссылки и помечая опасные, [LinkScanner](#) предотвращает переход по опасным и подозрительным ссылкам, поэтому вы можете быть уверены в том, что посещаете только безопасные веб-

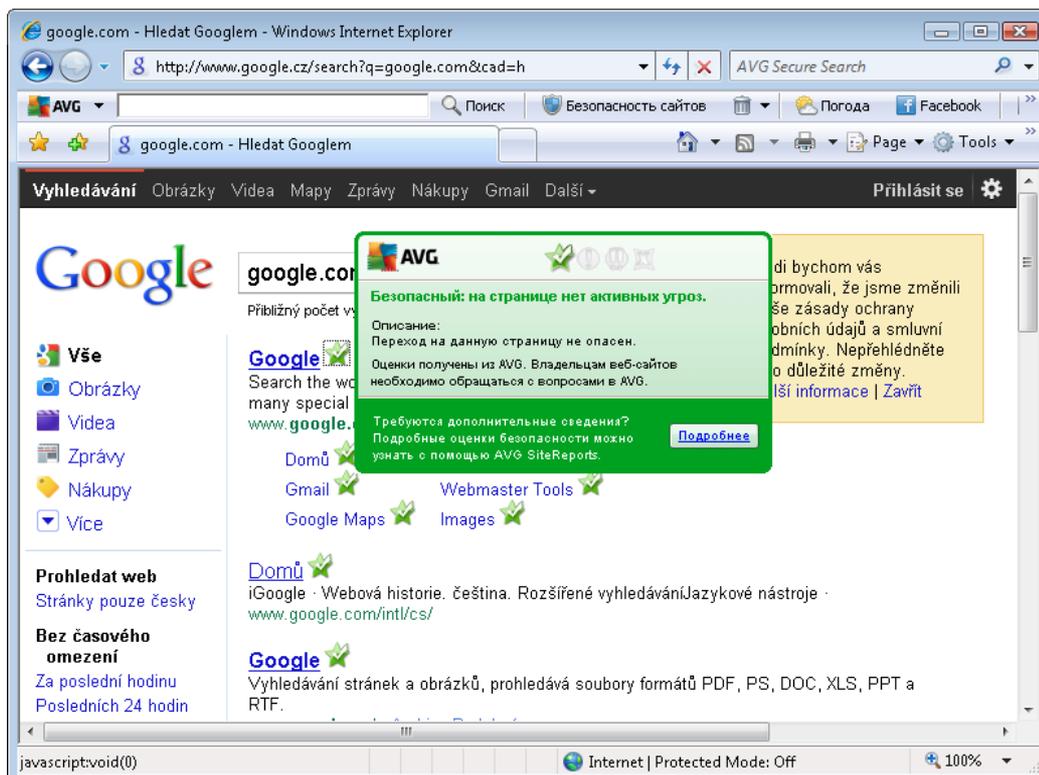


сайты.

Пока ссылка отображается на странице результатов поиска, рядом с ней находится графический значок, сообщающий о том, что проверка ссылки запущена. По завершении сканирования будет отображен соответствующий информативный значок.

-  Связанная страница безопасна.
-  Связанная страница не содержит угроз, но является подозрительной (из-за своего происхождения или особенностей работы). Поэтому не рекомендуется совершать покупки по данной ссылке и производить другие важные операции.).
-  Связанная страница может быть безопасной, но содержать дальнейшие ссылки на зараженные страницы, или иметь подозрительный код, не представляющий угроз в данный момент.
-  Связанная страница содержит активные угрозы! В целях безопасности доступ на подобные страницы будет закрыт.
-  Связанная страница недоступна, сканирование не может быть выполнено.

При наведении указателя мыши на значок отдельных рейтингов отобразятся сведения об определенной ссылке. Эти сведения содержат дополнительную информацию об угрозе (при ее наличии):

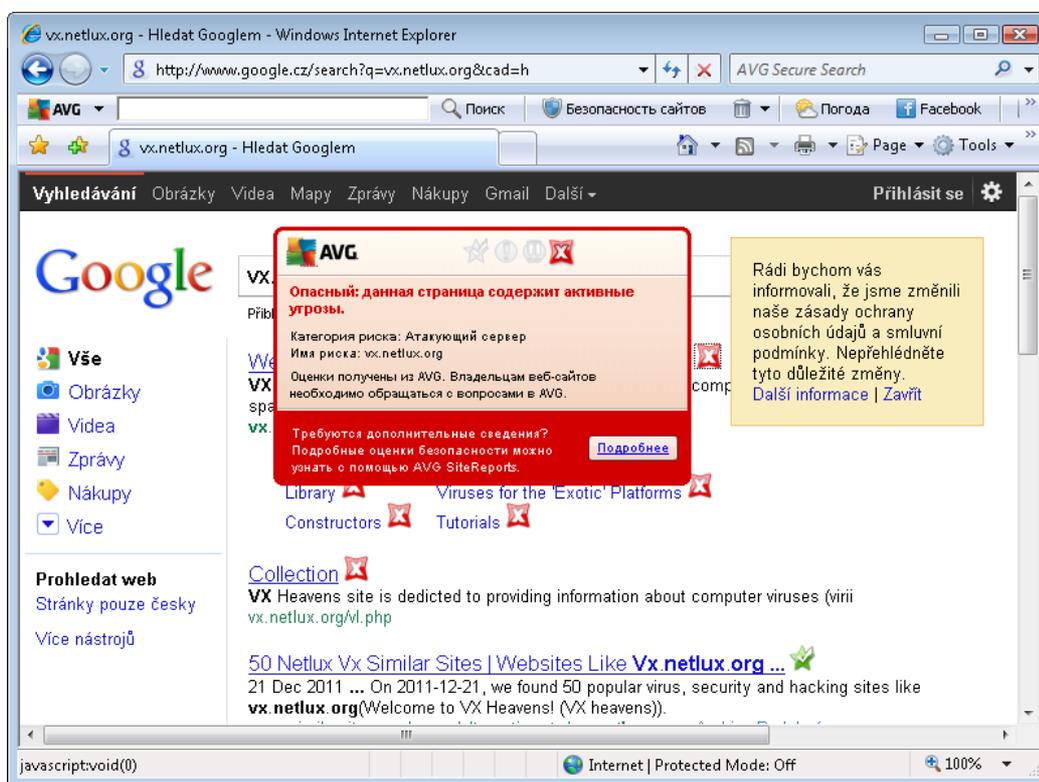




6.2.3. Обнаружения Surf-Shield

Данное мощное средство защиты предназначено для блокировки вредоносного содержимого открываемых веб-страниц от загрузки на компьютер. Если данная функция включена, то при щелчке ссылки или вводе URL-адреса опасного веб-сайта программа автоматически заблокирует открытие веб-страницы, защитив компьютер таким образом от случайного заражения. Необходимо помнить, что веб-страницы, зараженные эксплойтами, могут заразить компьютер при переходе на них. Поэтому при запросе опасной веб-страницы, содержащей эксплойты или другие серьезные угрозы, компонент [LinkScanner](#) блокирует открытие такой страницы в веб-обозревателе.

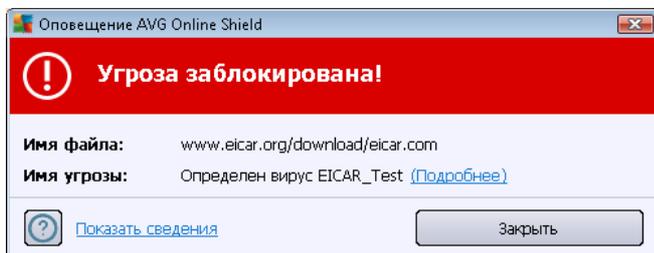
Если выполнен переход на зараженный веб-сайт, в компоненте веб-обозревателя [LinkScanner](#) отобразится предупреждение, аналогичное следующему.



Посещение подобных веб-сайтов чрезвычайно опасно и не рекомендуется.

6.2.4. Обнаружения Online Shield

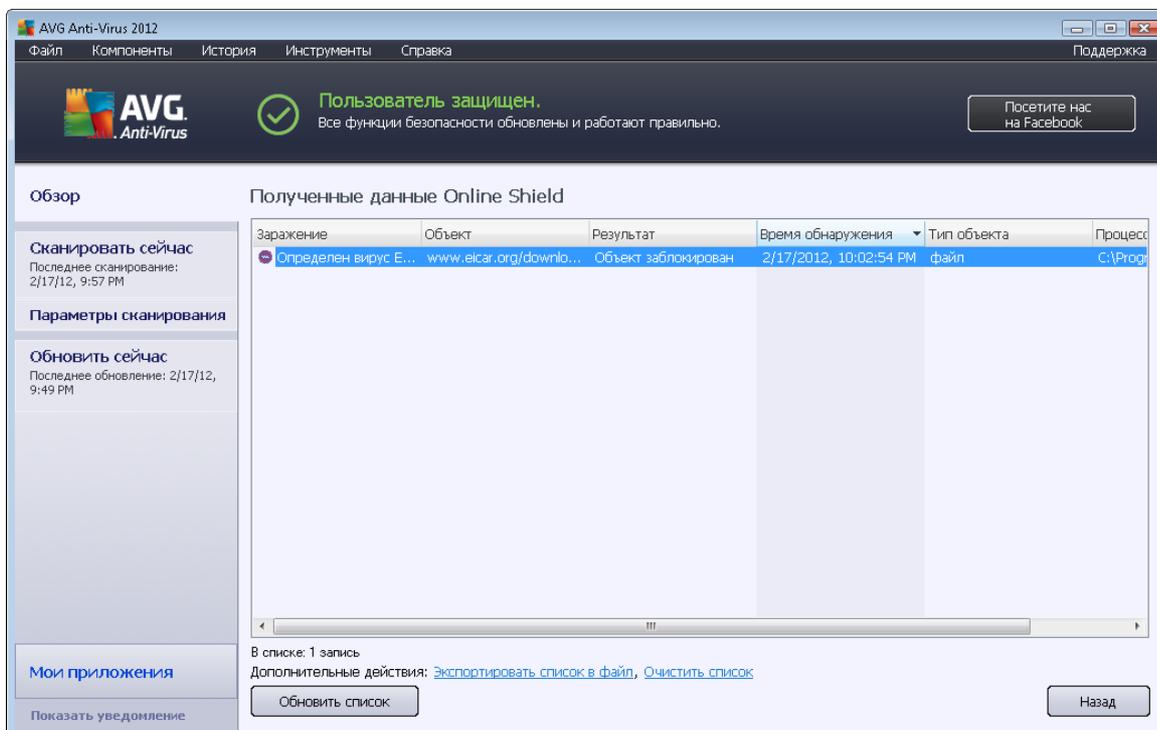
Компонент Online Shield выполняет сканирование содержимого посещаемых веб-страниц и файлов, которые могут на них содержаться, еще до того, как данное содержимое будет отображено в веб-браузере или загружено на компьютер. При обнаружении угрозы сразу же отобразится предупреждение в виде следующего диалогового окна:



В данном диалоговом окне с предупреждением содержатся данные, которые были обнаружены и определены как "зараженные" (*Имя файла*), название распознанного заражения (*Название угрозы*) и ссылка на [энциклопедию вирусов](#), в которой могут содержаться подробные сведения об обнаруженном заражении (*если оно известно*). В диалоговом окне содержатся следующие кнопки управления.

- **Показать сведения.** Нажмите кнопку **Показать сведения**, чтобы открыть новое всплывающее окно, в котором содержатся сведения о процессе, который был запущен в момент обнаружения заражения, и идентификации процесса.
- **Закрыть.** Нажмите данную кнопку, чтобы закрыть окно с предупреждением.

Подозрительная веб-страница не будет открыта, а сведения об обнаруженной угрозе будут занесены в список **Обнаружения Online Shield**. Просмотреть обнаруженные угрозы можно в системном меню [История/Обнаружения Online Shield](#).



По каждому обнаруженному объекту предоставляется следующая информация:

- **Заражение.** Описание (*возможно, даже имя*) обнаруженного объекта.



- **Объект.** источник объекта (*веб-страница*)
- **Результат.** Действие, выполненное в отношении обнаруженного объекта.
- **Время обнаружения.** дата и время обнаружения и блокировки угрозы
- **Тип объекта.** Тип обнаруженного объекта.
- **Процесс.** Действия, предпринятые для обнаружения потенциально опасного объекта.

В нижней части диалогового окна под списком находится информация об общем количестве обнаруженных объектов, перечисленных выше. Далее возможно экспортировать весь список обнаруженных объектов в файл (**Экспортировать список в файл**) и удалить все записи об обнаруженных объектах (**Очистить список**).

Кнопки управления

- **Обновить список.** Обновление списка объектов, обнаруженных с помощью **Online Shield**
- **Назад.** Переход к [главному диалоговому окну AVG по умолчанию](#) (*Обзор компонентов*).

6.3. Защита электронной почты

Электронная почта — один из основных источников вирусов и троянских программ. Фишинг и спам делают электронную почту еще более опасным источником угроз. Как правило, вредоносные сообщения электронной почты получают владельцы бесплатных учетных записей электронной почты (*так как в них редко используются технологии защиты от спама*). Несмотря на это, домашние пользователи полностью полагаются на такую электронную почту. При этом домашние пользователи, посещающие неизвестные веб-сайты и заполняющие интерактивные формы личными сведениями (*например, своими адресами электронной почты*), особенно подвержены атакам по электронной почте. Компании обычно используют корпоративные учетные записи и применяют фильтры нежелательных сообщений электронной почты.

Компонент **Защита эл. почты** предназначен для сканирования всех входящих и исходящих сообщений электронной почты; при обнаружении вируса в сообщении электронной почты он сразу же перемещается в [Хранилище вирусов](#). Данный компонент также может фильтровать определенные типы вложений электронной почты и добавлять текст сертификации в безопасные сообщения. **Защита эл. почты** состоит из двух основных функций:

- [E-mail Scanner](#)
- [Anti-Spam](#)



6.3.1. E-mail Scanner

Компонент Personal E-mail Scanner автоматически сканирует входящие и исходящие сообщения электронной почты. Его можно использовать с клиентами электронной почты, которые не имеют собственного модуля в AVG (*также его можно использовать для сканирования сообщений эл. почты при использовании клиентов, для которых доступен специальный подключаемый модуль AVG, например Microsoft Outlook, The Bat и Mozilla Thunderbird*). В первую очередь данный компонент предназначен для использования с такими приложениями, как Outlook Express, Incredimail и т. п.

При [установке](#) AVG создаются автоматические серверы для управления электронной почтой: один для проверки входящих сообщений электронной почты, второй для проверки исходящих сообщений. С помощью этих двух серверов сообщения электронной почты автоматически проверяются на портах 110 и 25 (*стандартные порты для отправки и получения сообщений электронной почты*).

E-mail Scanner работает в качестве интерфейса между клиентом электронной почты и почтовыми серверами в Интернете.

- **Входящая почта:** При получении сообщения с сервера компонент **E-mail Scanner** проверяет его на вирусы, удаляет зараженные вложения и добавляет уведомление о сертификации. При обнаружении вирусы немедленно помещаются на карантин в [Хранилище вирусов](#). Затем сообщение передается в клиент электронной почты.
- **Исходящая почта:** Сообщение отправляется из клиента электронной почты в компонент E-mail Scanner; он проверяет сообщение и его вложения на вирусы, а затем отправляет сообщение на сервер SMTP (*сканирование исходящих сообщений электронной почты по умолчанию отключено, его можно установить вручную*).

Компонент E-mail Scanner не предназначен для использования на серверных платформах.

6.3.2. Anti-Spam

Принцип работы Anti-Spam

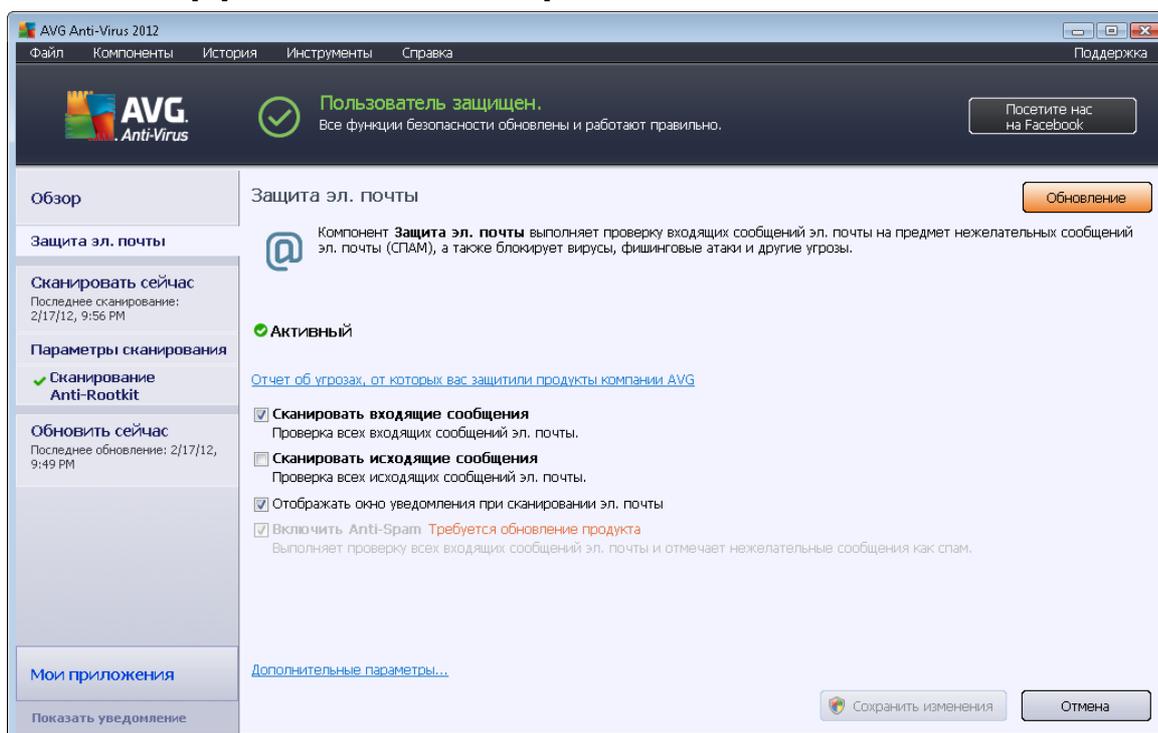
Компонент Anti-Spam проверяет все входящие сообщения электронной почты и помечает нежелательные сообщения электронной почты как спам. **Компонент Anti-Spam** может изменять тему сообщения электронной почты (*помеченного как спам*), добавляя специальную текстовую строку. Таким образом можно легко фильтровать сообщения электронной почты в почтовом клиенте. **Компонент Anti-Spam** использует несколько способов анализа для обработки каждого сообщения электронной почты, обеспечивая максимальную защиту от спама. **Компонент Anti-Spam** использует регулярно обновляемую базу данных для определения спама. Также можно использовать RBL-серверы (*общие базы данных адресов электронной почты "известных распространителей спама"*) и добавить вручную адреса электронной почты в Белый список (*никогда не помечается как спам*) и Черный список (*всегда помечается как спам*).

Что такое спам?



Спам относится к незапрашиваемым сообщениям электронной почты, в особенности к рекламным рассылкам о продуктах и услугах, которые массово рассылаются на большое количество адресов электронной почты одновременно, заполняя почтовые ящики получателей. Спам не является законной коммерческой рассылкой, на которую пользователи давали свое согласие. Спам не только досаждают, но также может содержать вирусы, сообщения оскорбительного характера или быть инструментом мошенников.

6.3.3. Интерфейс защиты электронной почты



В диалоговом окне **Защита эл. почты** можно получить краткие сведения о работе компонента и информацию о текущем состоянии (**Активный**). С помощью ссылки **Просмотреть интерактивный отчет о том, как AVG удалось обеспечить вашу защиту** можно получить подробную статистику обнаружений и действий **AVG Anti-Virus 2012** на специальной странице веб-сайта компании AVG (<http://www.avg.com/>).

Основные параметры защиты электронной почты

В диалоговом окне **Защита эл. почты** можно настроить основные функции компонента:

- **Сканировать входящие сообщения** (выбрано по умолчанию). Установите данный параметр, чтобы подтвердить проверку на вирусы всех сообщений, получаемых в используемой учетной записи.
- **Сканировать исходящие сообщения** (по умолчанию не выбрано). Установите данный параметр, чтобы подтвердить проверку на вирусы всех сообщений, отправляемых из используемой учетной записи.



- **Отображать окно уведомления при сканировании электронной почты** (по умолчанию включено). Установите этот флажок, чтобы на [значке AVG на панели задач](#) отображалось оповещение во время сканирования электронной почты.

Все компоненты AVG настроены поставщиком ПО для обеспечения оптимального качества работы. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться опытным пользователем. При необходимости изменить конфигурацию AVG выберите элемент системного меню Инструменты/Расширенные настройки и исправьте конфигурацию AVG в открывшемся диалоговом окне [Расширенные настройки AVG](#).

Элемент **Включить [Anti-Spam](#)** активирует фильтрацию нежелательных сообщений во входящей электронной почте. Однако в составе продукта **AVG Anti-Virus 2012** служба [Anti-Spam](#) не доступна. Она доступна только в более поздних версиях AVG. **Для получения информации по обновлению продуктов AVG посетите веб-сайт компании AVG (<http://www.avg.com/>).**

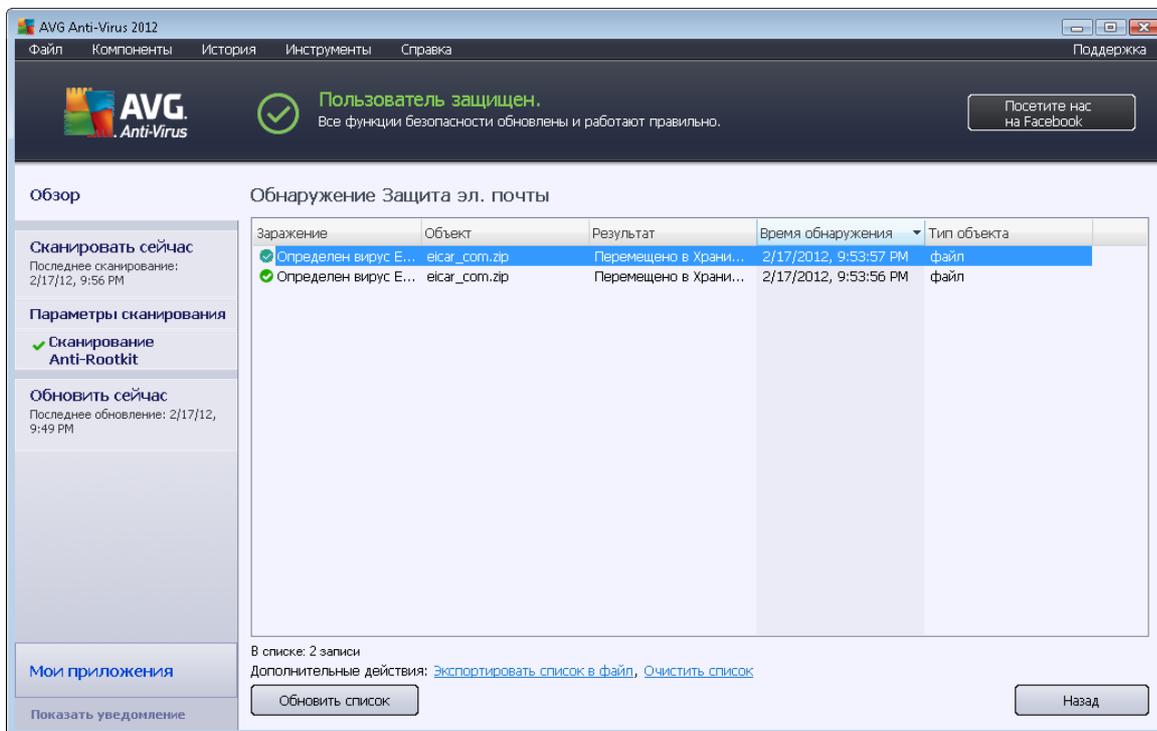
Кнопки управления

В диалоговом окне компонента **Защита эл. почты** имеются следующие кнопки управления:

- **Сохранить изменения.** Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне.
- **Отмена.** Нажмите данную кнопку для возврата к [главному диалоговому окну AVG](#) по умолчанию (*Обзор компонентов*).



6.3.4. Обнаружение E-mail Scanner



Диалоговое окно **Обнаружение E-mail Scanner** (доступное в системном меню *История/Обнаружение E-mail Scanner*) содержит список всех обнаруженных компонентом [Защита эл. почты](#) объектов. По каждому обнаруженному объекту предоставляется следующая информация:

- **Заражение.** Описание (возможно, даже имя) обнаруженного объекта.
- **Объект.** Местоположение объекта.
- **Результат.** Действие, выполненное в отношении обнаруженного объекта.
- **Время обнаружения.** Дата и время обнаружения подозрительного объекта.
- **Тип объекта.** Тип обнаруженного объекта.

В нижней части диалогового окна под списком находится информация об общем количестве обнаруженных объектов, перечисленных выше. Далее возможно экспортировать весь список обнаруженных объектов в файл (**Экспортировать список в файл**) и удалить все записи об обнаруженных объектах (**Очистить список**).

Кнопки управления

В интерфейсе компонента **E-mail Scanner** имеются следующие кнопки управления.



- **Обновить список.** Обновление списка обнаруженных угроз.
- **Назад.** Возврат к предыдущему диалоговому окну

6.4. Anti-Rootkit

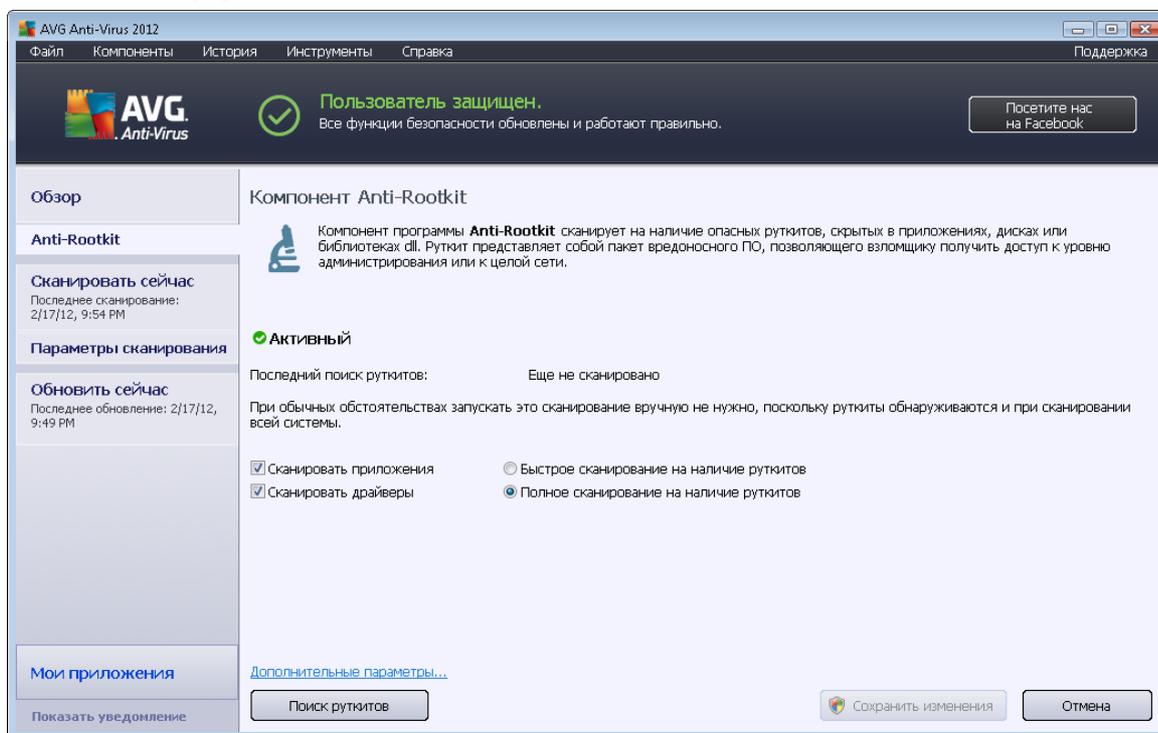
Компонент Anti-Rootkit — это специальное средство, предназначенное для обнаружения и эффективного удаления опасных пакетов программ rootkit, то есть программ и технологий, позволяющих скрывать вредоносное ПО, присутствующее на компьютере. **Компонент Anti-Rootkit** позволяет обнаруживать средства rootkit с помощью предварительно настроенного набора правил. Имейте в виду, что обнаруживаются все средства rootkit (*не только зараженные*). Если компонент **Anti-Rootkit** обнаружил средства rootkit, это еще не значит, что обнаруженный пакет программ заражен. Иногда средства rootkit используются в качестве драйверов или являются частью безопасных приложений.

Что такое средства rootkit?

Rootkit — это программа, предназначенная для полного управления системой компьютера без разрешения владельцев систем или законных управляющих. Средствам rootkit обычно не требуется доступ к оборудованию, так как они предназначены для управления операционными системами, установленными на этом оборудовании. В большинстве случаев средства rootkit скрывают свое присутствие в системе с помощью замены информации или обхода стандартных механизмов безопасности операционных систем. Кроме того, они могут попадать на компьютер в виде троянских программ, которые пользователи уверенно запускают, не подозревая об опасности. Используемые для этого технические приемы включают в себя скрытие запущенных процессов от следящих программ, а файлов и системных данных — от операционных систем.



6.4.1. Интерфейс Anti-Rootkit



Диалоговое окно **Anti-Rootkit** содержит краткое описание функций компонента, сведения о текущем состоянии компонента (*Активный*), а также о последнем запуске проверки **Anti-Rootkit** (*последний поиск пакетов программ rootkit; поиск пакетов программ rootkit — это выбранный по умолчанию процесс, запускающийся вместе со [Сканированием всего компьютера](#)*). В диалоговом окне компонента **Anti-Rootkit** также содержится ссылка [Инструменты/Дополнительные параметры](#). Щелкните данную ссылку, чтобы перейти в меню расширенной конфигурации компонента **Anti-Rootkit**.

Все компоненты AVG настроены поставщиком ПО для обеспечения оптимального качества работы. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться опытным пользователем.

Основные параметры Anti-Rootkit

В нижней части диалогового окна можно настроить некоторые из основных функций сканирования на наличие средств rootkit. Чтобы указать объекты, которые должны сканироваться, установите соответствующие флажки.

- **Сканировать приложения**
- **Сканировать драйверы**

Далее можно включить режим сканирования на наличие средств rootkit.



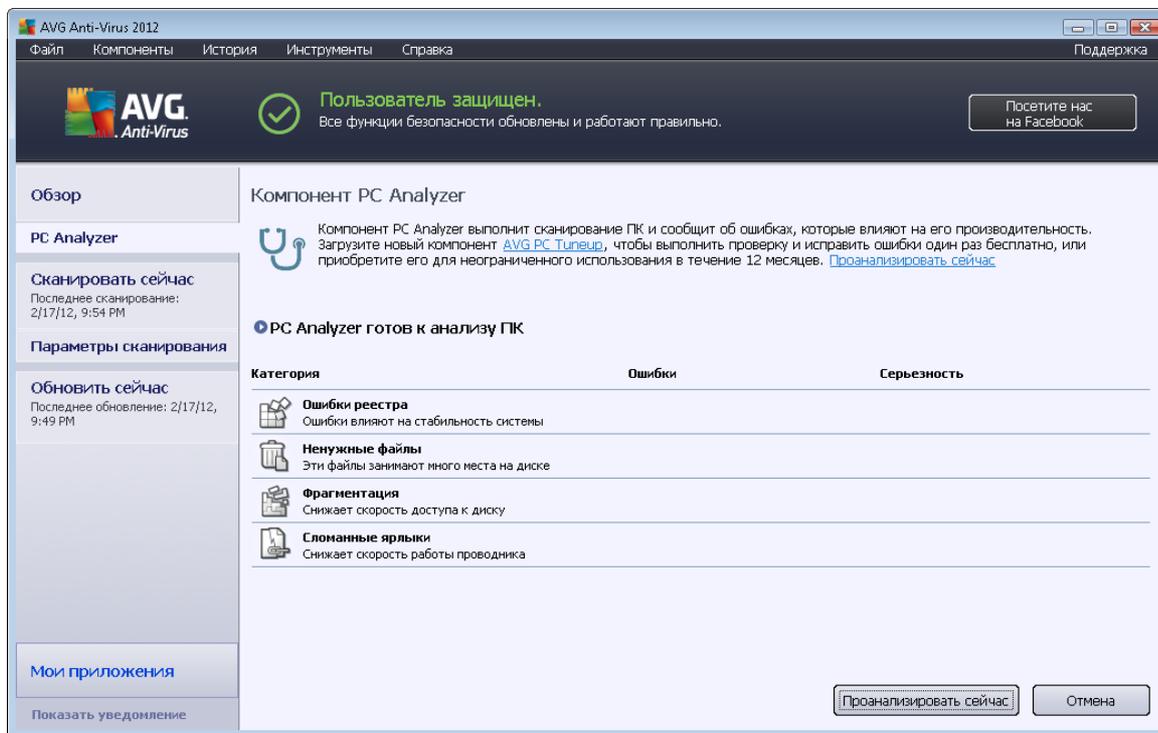
- **Быстрое сканирование rootkit.** Сканирование всех запущенных процессов, загруженных драйверов и системных папок (*обычно c:\Windows*).
- **Полное сканирование rootkit.** Сканирование всех запущенных процессов, загруженных драйверов, системных папок (*обычно c:\Windows*), а также локальных жестких дисков (*в том числе съемные накопители, кроме дисковода и привода компакт-дисков*).

Кнопки управления

- **Поиск rootkit.** Так как сканирование на наличие средств rootkit не выполняется при выборе типа сканирования [Сканирование всего компьютера](#), его можно запустить непосредственно в интерфейсе **Anti-Rootkit** с помощью данной кнопки.
- **Сохранить изменения.** Нажмите данную кнопку, чтобы сохранить все изменения, произведенные в данном интерфейсе, и вернуться к [главному диалоговому окну AVG](#) по умолчанию (*Обзор компонентов*).
- **Отмена.** Используйте данную кнопку для возврата к [главному диалоговому окну AVG](#) по умолчанию (*Обзор компонентов*) без сохранения изменений

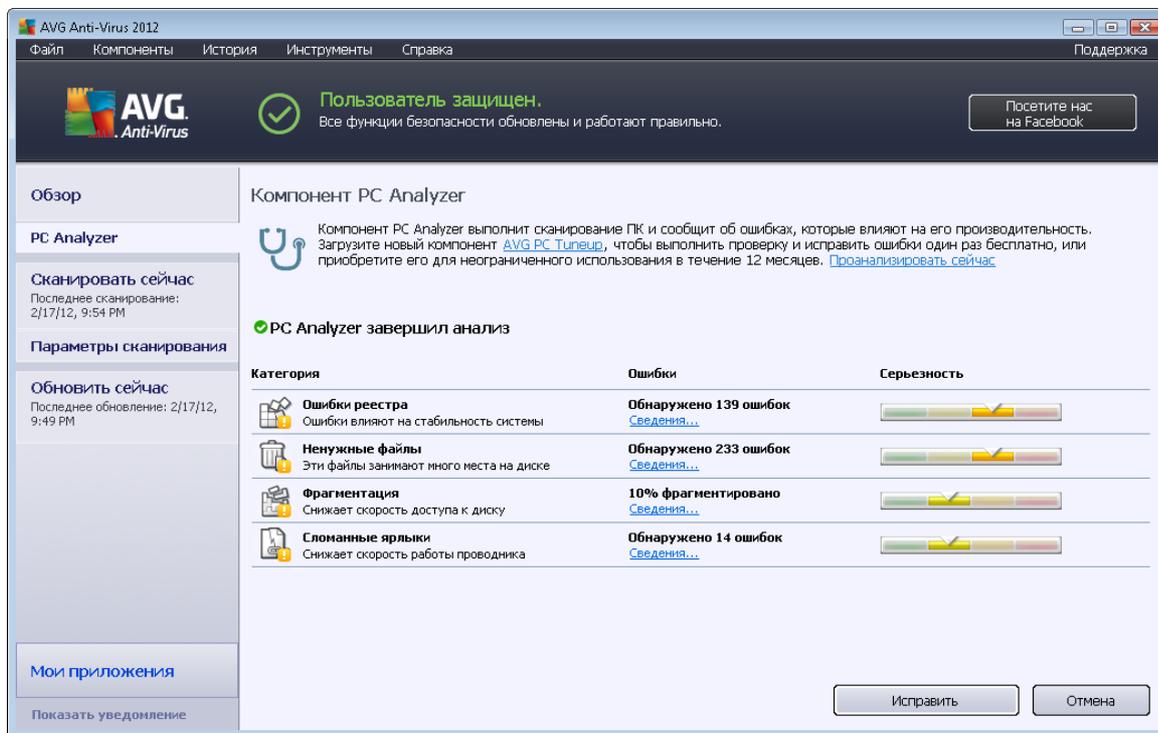
6.5. PC Analyzer

Компонент **PC Analyzer** предназначен для сканирования компьютера на наличие системных проблем и предоставления пользователю сведений о возможных причинах снижения общей производительности компьютера. В интерфейсе пользователя компонента отображается таблица, разделенная на четыре строки, относящиеся к соответствующим категориям: ошибки реестра, ненужные файлы, фрагментация и сломанные ярлыки.



- **Ошибки реестра.** Определение количества ошибок в реестре ОС Windows. В связи с тем, что для исправления ошибок реестра необходимо наличие специальных знаний, не рекомендуется пробовать исправить эти ошибки самостоятельно.
- **Ненужные файлы.** Отображение файлов, которые не требуются для работы компьютера. В большинстве случаев это временные файлы и файлы, хранящиеся в корзине.
- **Фрагментация.** Вычисление фрагментированного объема жесткого диска в процентном соотношении, т. е. места на диске, используемого в течение длительного времени, в результате чего большинство файлов теперь рассредоточены по различным частям жесткого диска. Для исправления данной проблемы воспользуйтесь специальным инструментом для дефрагментации диска.
- **Сломанные ярлыки.** Определение неработающих ярлыков, ярлыков, ведущих к несуществующим местоположениям и т. п.

Для запуска системного анализа нажмите кнопку **Проанализировать сейчас**. После этого ход выполнения анализа и соответствующие результаты будут отображаться непосредственно в таблице.



В обзоре результатов отображается количество обнаруженных системных проблем (**Ошибки**), разделенных по соответствующим категориям. Результаты анализа будут также отображены графически на оси в столбце **Серьезность**.

Кнопки управления

- **Анализировать сейчас** (отображается до запуска анализа). Нажмите данную кнопку, чтобы немедленно запустить анализ компьютера.
- **Исправить** (отображается по завершении анализа). Нажмите данную кнопку, чтобы перейти на страницу веб-сайта компании AVG (<http://www.avg.com/>), на которой подробно представлены последние сведения о компоненте **PC Analyzer**.
- **Отмена**. Нажмите данную кнопку, чтобы остановить выполнение анализа или вернуться к [главному диалоговому окну AVG](#) по умолчанию (**Обзор компонентов**) по завершении анализа.

6.6. Identity Protection

Компонент **Identity Protection** — это компонент, предназначенный для защиты компьютера от всех видов вредоносного ПО (*шпионского ПО, программ-роботов, программ для кражи личных данных и т. п.*) с помощью технологий определения моделей поведения. Этот компонент также обеспечивает защиту "нулевого дня" от новых вирусов. Главной задачей компонента **Identity Protection** является предотвращение кражи паролей, сведений о банковских счетах, номеров кредитных карт и другой важной личной информации с помощью вредоносных программ (*вредоносное ПО*), нацеленных на ваш ПК. Данный компонент

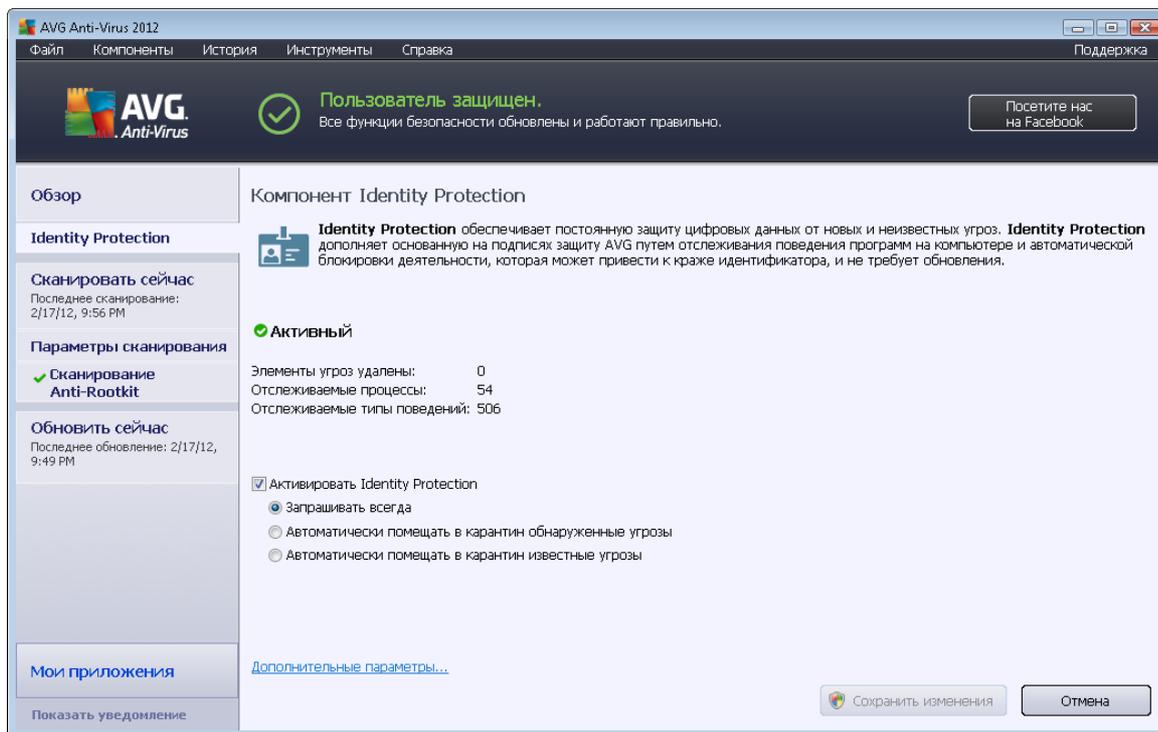


обеспечивает правильную работу всех программ на компьютере или в общей сети. **Компонент Identity Protection** непрерывно ищет и блокирует подозрительные объекты, защищая таким образом компьютер от всех новых разновидностей вредоносного ПО.

Компонент Identity Protection обеспечивает защиту компьютеров в режиме реального времени от новых и даже неизвестных угроз. Он отслеживает все процессы (*включая скрытые*) и более 285 моделей поведения с целью выявления возможной опасности для системы. По этой причине возможно обнаружение угроз, еще не описанных в вирусной базе данных. Когда на компьютер попадает незнакомый код, он немедленно проверяется на предмет вредоносного поведения и отслеживается. Если файл определяется как вредоносный, компонент **Identity Protection** переместит код в [Хранилище вирусов](#) и отменит все внесенные им в систему изменения (*вставки кодов, изменения реестра, открытие портов и т. д.*). Не требуется запускать сканирование для обеспечения защиты. Данная технология является упреждающей, редко нуждается в обновлении и постоянно обеспечивает защиту.

Компонент Identity Protection является бесплатным дополнением к компоненту [Anti-Virus](#). В целях обеспечения полной безопасности вашего ПК мы рекомендуем устанавливать оба компонента.

6.6.1. Интерфейс защиты личных данных



Диалоговое окно **Identity Protection** содержит краткое описание основных функций компонента, его состояние (*Активный*) и некоторые статистические данные.

- **Удаленные вредоносные объекты.** Количество обнаруженных вредоносных приложений, которые были удалены.
- **Отслеживаемые процессы.** Количество работающих в настоящее время



приложений, отслеживаемых с помощью IDP.

- **Отслеживаемые типы поведения.** Количество определенных действий, выполняемых отслеживаемыми приложениями.

Основные параметры защиты личных данных

В нижней части диалогового окна можно настроить основные функции компонента.

- **Включить Identity Protection** (выбрано по умолчанию). Установите данный флажок, чтобы активировать компонент IDP и открыть другие параметры редактирования.

В некоторых случаях **Identity Protection** может сообщать о том, что какой-либо легальный файл является подозрительным или опасным. **Компонент Identity Protection** обнаруживает угрозы на основе их поведения, поэтому такое обычно случается, если какая-то программа пытается отследить нажатия клавиш, установить другие программы или если на компьютере установлен новый драйвер. В связи с этим выберите один из следующих параметров, определяющих поведение компонента **Identity Protection** в случае обнаружения подозрительной активности.

- **Запрашивать всегда.** Если приложение определено как вредоносное, будет отображаться запрос на его блокировку (по умолчанию этот флажок установлен и рекомендуется снимать его только в том случае, если это действительно необходимо).
- **Автоматически помещать в карантин обнаруженные угрозы.** Все приложения, определенные как вредоносные, будут автоматически заблокированы
- **Автоматически помещать в карантин известные угрозы.** Будут заблокированы только те приложения, которые точно являются вредоносными.
- **Расширенные настройки...** — Щелкните данную ссылку, чтобы перейти в соответствующее диалоговое окно, содержащее [Дополнительные настройки AVG Anti-Virus 2012](#). Там же можно изменить дополнительные настройки компонента. Обратите внимание, что конфигурация всех компонентов по умолчанию настроена для **AVG Anti-Virus 2012** обеспечение оптимальной производительности и максимального уровня безопасности. Не изменяйте конфигурацию по умолчанию без необходимости.

Кнопки управления

В интерфейсе компонента **Identity Protection** доступны следующие кнопки управления.

- **Сохранить изменения.** Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне.
- **Отмена.** Нажмите данную кнопку для возврата к главному диалоговому [окну AVG](#) (*Обзор компонентов*).



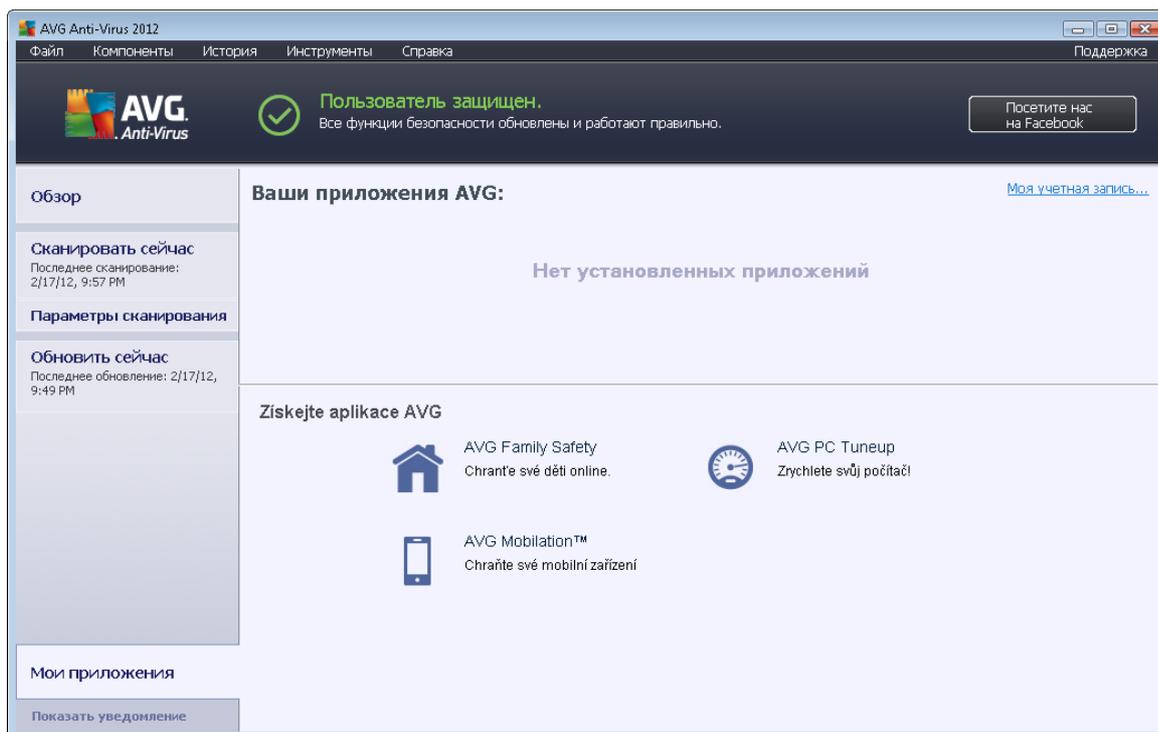
6.7. Удаленное администрирование

Компонент **Удаленное администрирование** отображается в интерфейсе пользователя **AVG Anti-Virus 2012** только в случае установки версии продукта Business Edition (*информацию о лицензии, использованной в процессе установки, см. на вкладке [Версия](#) диалогового окна [Сведения](#), которое доступно через элемент системного меню [Поддержка](#)*). Подробное описание параметров компонента и функций системы "Удаленное администрирование AVG" см. в специальной документации, посвященной данной теме. Данный документ можно загрузить с веб-сайта компании AVG (<http://www.avg.com/>) в разделе **Центр поддержки/Загрузка/Документация**.



7. Мои приложения

Диалоговое окно **Мои приложения** (доступ к нему можно получить, нажав кнопку "Мои приложения" в главном диалоговом окне AVG) представляет обзор автономных приложений AVG, которые установлены или готовы к установке на компьютер.



Диалоговое окно состоит из двух разделов:

- **Ваши приложения AVG.** Представляет обзор всех установленных на компьютере автономных приложений.
- **Получить приложения AVG.** Представляет обзор доступных автономных приложений AVG. Эти приложения готовы к установке. Предложения меняются в зависимости от лицензии, местоположения пользователя и других критериев. Чтобы получить дополнительные сведения об этих приложениях, посетите веб-сайт компании AVG (<http://www.avg.com/>).

Ниже приведен краткий обзор всех доступных приложений и краткое описание их функций.

7.1. AVG Family Safety

AVG Family Safety позволяет защитить детей от веб-сайтов, мультимедийного контента и результатов поиска, которые им не рекомендуется просматривать, а также предоставляет отчеты о деятельности детей в Интернете. **AVG Family Safety** использует технологию слежения за нажатием клавиш, чтобы контролировать деятельность ребенка в тематических чатах и на сайтах социальных сетей. При обнаружении слов, выражений или языка, используемых в Интернете для обмана детей, вы будете немедленно уведомлены об этом



SMS-сообщением или по электронной почте. Можно назначить необходимый уровень защиты для каждого ребенка, а затем отслеживать их по отдельности с помощью уникальных имен пользователей.

Дополнительные сведения см. на соответствующей веб-странице компании AVG, на которой можно быстро загрузить необходимый компонент. Для этого необходимо в окне [Мои приложения](#) щелкнуть ссылку [AVG Family Safety](#).

7.2. AVG LiveKive

Компонент **LiveKive** предназначен для резервного копирования данных через Интернет на защищенные серверы. **AVG LiveKive** позволяет автоматически выполнять резервное копирование файлов, фотографий и музыки в одно общее безопасное расположение. При этом к этим файлам можно затем предоставлять общий доступ для членов семьи или друзей, а также получать доступ с любого устройства, подключаемого к Интернету, например iPhone или Android. **AVG LiveKive** предлагает такие функции:

- Обеспечение безопасности в случае повреждения компьютера и/или жесткого диска
- Доступ к данным с любого устройства, подключенного к Интернету
- Удобная организация
- Предоставление общего доступа с вашего согласия

Дополнительные сведения см. на соответствующей веб-странице компании AVG, там же можно быстро загрузить необходимый компонент. Для этого необходимо в окне [Мои приложения](#) щелкнуть ссылку [AVG LiveKive](#).

7.3. AVG Mobilation

Приложение **AVG Mobilation** защищает мобильные телефоны от вирусов и вредоносного ПО, а также дает возможность следить за смартфоном удаленно, если он не находится рядом. Приложение **AVG Mobilation** включает такие функции:

- **File Scanner** позволяет проверять на безопасность файлы в разных местах хранения;
- **Task Killer** позволяет остановить приложение в случае, если устройство работает медленно или зависает;
- **App Locker** позволяет блокировать и защищать одно или больше приложений паролем от ненадлежащего использования;
- **Tuneup** собирает различные параметры системы (*индикатор батареи, использование дискового пространства, размер и место размещения установленных программ и т. п.*) в одном централизованном представлении, контролируя производительность системы;
- **App Backup** позволяет создавать резервные копии приложений на SD-карте и позже их восстанавливать;



- *Spam and Scam* позволяет отмечать SMS-сообщения как нежелательные и сообщать о мошеннических веб-сайтах;
- *Wipe personal data* позволяет уничтожать личные данные удаленно в случае кражи телефона;
- *Safe Web Surfing* предлагает наблюдение за посещаемыми веб-страницами в режиме реального времени.

Дополнительные сведения см. на соответствующей веб-странице компании AVG, там же можно быстро загрузить необходимый компонент. Для этого необходимо в диалоговом окне [Мои приложения](#) щелкнуть ссылку *AVG Mobilation*.

7.4. AVG PC Tuneup

Приложение **AVG PC Tuneup** представляет собой расширенное средство для выполнения подробного системного анализа и внесения исправлений для увеличения скорости работы и улучшения общей производительности компьютера. **AVG PC Tuneup** включает в себя указанные ниже функции.

- *Disk Cleaner*. Безопасное удаление нежелательных файлов, замедляющих работу компьютера.
- *Disk Defrag*. Дефрагментация жестких дисков и оптимизация расположения системных файлов.
- *Registry Cleaner*. Исправление ошибок в реестре для обеспечения стабильной работы ПК.
- *Registry Defrag*. Уменьшение объема реестра за счет удаления пустых элементов, использующих память.
- *Disk Doctor*. Определение и исправление поврежденных секторов, потерянных кластеров и ошибок каталогов.
- *Internet Optimizer*. Определение оптимальных настроек для конкретного типа подключения к Интернету.
- *Track Erase*. Удаление истории использования компьютера и Интернета.
- *Disk Wiper*. Освобождение свободного места на жестких дисках для обеспечения сохранности конфиденциальных данных.
- *File Shredder*. Полное удаление выбранных файлов на жестком диске или USB-накопителе.
- *File Recovery*. Восстановление случайно удаленных файлов на жестком диске, USB-накопителе или фотокамере.



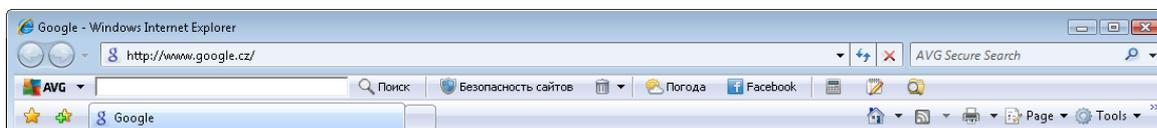
- *Duplicate File Finder*. Поиск и удаление дубликатов файлов, занимающих место на диске.
- *Services Manager*. Позволяет отключить ненужные службы, замедляющие работу компьютера.
- *Startup Manager*. Позволяет выбрать программы, которые автоматически запускаются при загрузке Windows.
- *Uninstall Manager*. Полностью удаляет неиспользуемые программы.
- *Tweak Manager*. Настройка множества скрытых параметров Windows.
- *Task Manager*. Предоставление списка всех запущенных процессов, служб и защищенных файлов.
- *Disk Explorer*. Определение файлов, которые занимают больше всего места на компьютере.
- *System Information*. Предоставление подробной информации об установленном программном и аппаратном обеспечении.

Дополнительные сведения см. на соответствующей веб-странице компании AVG, на которой можно быстро загрузить необходимый компонент. Для этого необходимо в окне [Мои приложения](#) щелкнуть ссылку *AVG PC Tuneup*.



8. Панель AVG Security Toolbar

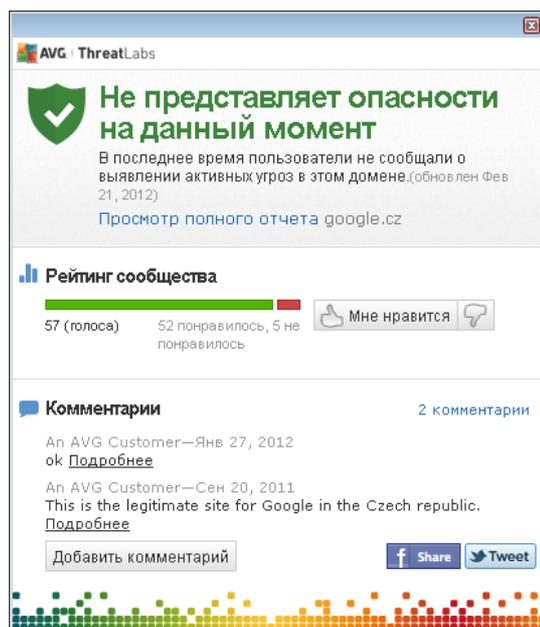
Панель AVG Security Toolbar. Инструмент, тесно взаимодействующий с компонентом [LinkScanner](#) и обеспечивающий максимальную защиту во время работы в Интернете. В программе **AVG Anti-Virus 2012** установка **панели AVG Security Toolbar** является дополнительным параметром. В [процессе установки](#) предлагается принять решение о необходимости установки данного компонента. **панель AVG Security Toolbar** встраивается непосредственно в Интернет-браузер. В настоящее время поддерживаются такие Интернет-браузеры: Internet Explorer (6.0 и более поздних версий) и/или Mozilla Firefox (3.0 и более поздних версий). Другие браузеры не поддерживаются. При использовании другого Интернет-браузера, например Avant, могут произойти неожиданные ошибки.



Панель AVG Security Toolbar включает в себя следующие элементы:

- **Логотип AVG** с раскрывающимся меню.
 - **Использовать безопасный поиск AVG.** Позволяет пользоваться поиском непосредственно в **панели AVG Security Toolbar** с помощью поисковой системы **Безопасный поиск AVG**. Все поисковые результаты проверяются службой [Search-Shield](#), так что вы можете быть абсолютно уверены в безопасной работе в Интернете.
 - **Текущий уровень угрозы.** Открытие веб-страницы лаборатории вирусов с графическим отображением текущего уровня угрозы в Интернете.
 - **Лаборатория угроз AVG.** Предоставляется доступ к специальному веб-сайту **лаборатории угроз AVG** (по адресу <http://www.avgthreatlabs.com>), который содержит информацию о безопасности различных веб-сайтов и текущем уровне угроз в Интернете.
 - **Справка по панели инструментов.** Открытие интерактивной справки, охватывающей все функции **панели AVG Security Toolbar**.
 - **Отправить отзыв о продукте.** Открытие веб-страницы с формой, заполнив которую можно поделиться мнением по поводу использования **панели AVG Security Toolbar**.
 - **О программе...** Открытие нового окна с информацией о текущей версии установленной **панели AVG Security Toolbar**.
- **Поле поиска.** Позволяет производить поиск в Интернете с помощью панели **AVG Security Toolbar** и иметь абсолютную уверенность в максимальной безопасности результатов поиска. Введите слово или фразу в поле поиска и нажмите кнопку **Поиск** (или клавишу **Enter**). Все результаты поиска проверяются службой [Search-Shield](#) (в составе компонента [LinkScanner](#)).
- **Безопасность сайта.** Эта кнопка открывает новое диалоговое окно с информацией о

текущем уровне угроз (*Не представляет опасности в данный момент*) посещаемой страницы. Этот краткий обзор можно развернуть и отобразить подробные сведения обо всех защитных действиях, связанных со страницей в окне обозревателя (*Просмотреть полный отчет*):



- **Удалить.** Кнопка «корзина» открывает меню, где можно выбрать элементы для удаления: сведения о просмотре веб-страниц, загрузках, онлайн-формах или весь архив поиска.
- **Погода.** Нажатие этой кнопки открывает новое диалоговое окно с информацией о текущей погоде в вашем регионе и прогнозом на следующие два дня. Эта информация обновляется регулярно каждые 3—6 часов. В данном диалоговом окне можно вручную изменить регион и выбрать отображение температуры по Цельсию или по Фаренгейту.



- **Facebook.** Эта кнопка позволяют подключиться к социальной сети [Facebook](#) непосредственно из **панели AVG Security Toolbar**.



- Кнопки быстрого запуска приложений: *Калькулятор*, *Блокнот*, *Проводник Windows*.



9. AVG Do Not Track

AVG Do Not Track помогает распознавать веб-сайты, которые собирают сведения о ваших действиях в Интернете. С помощью значка в браузере можно узнать, какие веб-сайты и рекламодатели пытаются собирать сведения о ваших действиях и соответственно, разрешить или запретить подобные действия.

- **AVG Do Not Track** предоставляет дополнительную информацию о политике конфиденциальности конкретной службы, а также возможность отказаться от использования этой службы.
- Кроме того, **AVG Do Not Track** поддерживает [протокол W3C DNT](#), чтобы автоматически уведомлять сайты о запрете на сбор сведений. Такое уведомление по умолчанию включено, но эту настройку можно в любое время изменить.
- **AVG Do Not Track** предоставляется на следующих [условиях](#).
- **По умолчанию служба AVG Do Not Track** включена, но ее можно в любой момент отключить. Соответствующие инструкции можно найти в статье [Отключение функции AVG Do Not Track](#) в разделе «Вопросы и ответы».
- Дополнительную информацию о **AVG Do Not Track** можно найти на нашем [веб-сайте](#).

В данный момент функцию **AVG Do Not Track** поддерживают только браузеры Mozilla Firefox, Chrome и Internet Explorer. (В Internet Explorer значок AVG Do Not Track размещен справа от командной строки. Если значок AVG Do Not Track не отображается, когда настройки обозревателя выбраны по умолчанию, убедитесь, что командная строка активирована. Если значок все равно не отображается, перетяните командную строку влево, чтобы открыть все значки и кнопки на этой панели инструментов.)

9.1. Интерфейс AVG Do Not Track

В режиме онлайн **AVG Do Not Track** мгновенно сообщает об угрозе сбора каких-либо данных. Вы увидите следующее диалоговое окно.



Все доступные службы сбора данных перечислены в обзоре **Трекеры на этой странице**. **AVG Do Not Track** поддерживает три метода сбора данных.

- **Веб-аналитика** (*разрешен по умолчанию*): службы, используемые для улучшения производительности и удобства работы соответствующего веб-сайта. К этой категории относятся такие службы, как Google Analytics, Omniture и Yahoo Analytics. Мы не рекомендуем блокировать службы веб-аналитики, так как это может привести к неправильной работе веб-сайта.
- **Кнопки социальных сетей** (*разрешен по умолчанию*): элементы, разработанные для улучшенной работы в социальных сетях. Кнопки социальных сетей служат для выхода в социальные сети с сайта, на котором вы находитесь. Они позволяют собирать сведения о ваших действиях, если вы в сети. Примеры кнопок социальных сетей: социальные плагины Facebook, кнопки Twitter, Google +1.
- **Рекламные сети** (*некоторые из них по умолчанию заблокированы*): службы, которые прямо или косвенно собирают или сообщают данные о ваших действиях в сети и размещают персонализированную рекламную информацию (в отличие от тематического размещения рекламы). Это определяется политиками конфиденциальности конкретных рекламных сетей, с которыми можно ознакомиться на их сайтах. Некоторые рекламные сети по умолчанию заблокированы.



Примечание. Некоторые из трех описанных выше разделов могут не отображаться в диалоговом окне *AVG Do Not Track* — это зависит от служб, работающих на веб-сайте в фоновом режиме.

В диалоговом окне также есть две гиперссылки:

- **Что такое отслеживание?** — нажмите на ссылку в верхней части диалогового окна, чтобы перейти на веб-страницу, где детально описаны принципы отслеживания и его конкретные типы.
- **Настройка** — нажмите ссылку в нижней части диалогового окна, чтобы перейти на веб-страницу, где можно выбрать конкретную конфигурацию параметров **AVG Do Not Track** (подробную информацию можно найти в разделе [Настройку AVG Do Not Track](#))

9.2. Информация о следящих процессах

Список обнаруженных служб сбора данных содержит только имена определенных служб. Для принятия правильного решения о том, следует ли блокировать какую-либо службу, может понадобиться дополнительная информация. Наведите указатель мыши на соответствующий элемент списка. Появится информационное сообщение с подробными данными о службе. Вы узнаете, собирает ли данная служба личные или другие доступные данные, передает ли она их третьим лицам и сохраняет ли собранные данные для возможного использования в будущем.

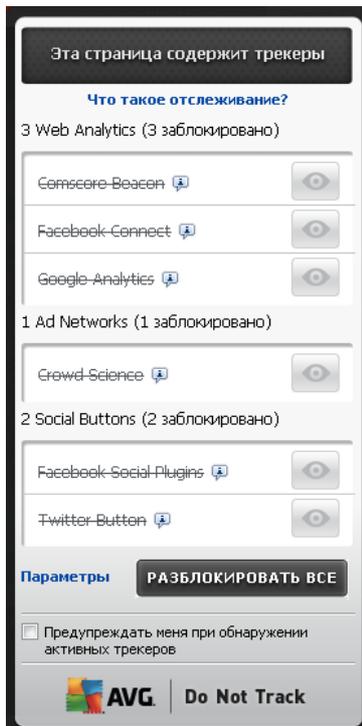
В нижней части информационного сообщения отображается гиперссылка **Политика конфиденциальности**, которая перенаправит вас на веб-сайт с описанием политики конфиденциальности соответствующей обнаруженной службы.



9.3. Блокировка следящих процессов

Имея перед собой списки всех рекламных сетей, кнопок социальных сетей и средств веб-аналитики, можно назначить блокировку определенных служб. Существует два способа.

- **Заблокировать все** — нажмите эту кнопку, расположенную в нижней области диалогового окна: любые попытки сбора данных будут блокироваться. *(Однако, следует помнить, что это действие может вызвать сбой в работе соответствующей страницы, если служба запущена.)*
-  — если блокировать все обнаруженные службы не требуется, можно для каждой службы указать, следует ли ее разрешить или заблокировать. Можно разрешить функционирование некоторых обнаруженных систем *(например, средств веб-аналитики)*: эти системы используют собранные данные для оптимизации своих веб-сайтов, совершенствуя тем самым интернет-среду для всех пользователей. В то же время можно заблокировать попытки сбора данных со стороны процессов, которые относятся к рекламным сетям. Просто щелкните значок  рядом с соответствующим процессом, чтобы заблокировать сбор данных *(имя процесса отобразится перечеркнутым)* или снова разрешить их сбор.



9.4. Настройки AVG Do Not Track

Непосредственно в диалоговом окне **AVG Do Not Track** есть только один параметр конфигурации: в нижней области можно увидеть флажок **Предупреждать меня при обнаружении активных трекеров**. По умолчанию этот параметр выключен. Установите флажок, чтобы подтвердить, что необходимо отображать уведомление каждый раз при



посещении веб-страницы, содержащей новый процесс отслеживания, который еще не блокировался. Если флажок установлен, в случае обнаружения функцией **AVG Do Not Track** новой системы отслеживания на веб-странице, посещаемой в данный момент, на экране отобразится диалоговое окно уведомления. Если флажок не установлен, вы сможете узнать о недавно обнаруженной службе только с помощью значка **AVG Do Not Track** (размещенного в командной строке обозревателя), который изменит цвет с зеленого на желтый.

Однако в нижней области диалогового окна **AVG Do Not Track** можно найти ссылку **Настройки**. Щелкните ссылку для перехода на специальную веб-страницу, где можно указать дополнительные **Параметры AVG Do Not Track**:

Параметры AVG Do Not Track

Уведомлять

Отображать уведомление для секунды

Положение уведомления

- Предупреждать меня при обнаружении активных трекеров
- Уведомлять о веб-сайтах, для которых не требуется отслеживание (с помощью [HTTP-заголовка Do Not Track](#))

Заблокировать следующее

<input checked="" type="checkbox"/>	24/7 Real Media	Ad Networks
<input checked="" type="checkbox"/>	33Across	Ad Networks
<input checked="" type="checkbox"/>	[x+1]	Ad Networks
<input checked="" type="checkbox"/>	Accelerator Media	Ad Networks
<input checked="" type="checkbox"/>	AddtoAny	Ad Networks
<input checked="" type="checkbox"/>	Adition	Ad Networks
<input checked="" type="checkbox"/>	AdReady	Ad Networks
<input checked="" type="checkbox"/>	Aggregate Knowledge	Ad Networks
<input checked="" type="checkbox"/>	Baynote Observer	Ad Networks
<input checked="" type="checkbox"/>	Bizo	Ad Networks

- **Положение уведомления** (по умолчанию в правой верхней области). Откройте раскрывающееся меню, чтобы указать, в каком положении нужно отображать на мониторе диалоговое окно **AVG Do Not Track**.
- **Отображать уведомление** (по умолчанию — 10). В этом поле нужно выбрать период (в секундах) отображения на экране уведомления **AVG Do Not Track**. Можно указать от 0 до 60 секунд (если указать 0, то уведомление на экране не отобразится).



- **Предупреждать меня при обнаружении активных трекеров** (по умолчанию выключено). Установите флажок, чтобы подтвердить, что необходимо отображать уведомление при каждом посещении веб-страницы, содержащей новую службу сбора данных, которая еще не блокировалась. Если флажок установлен, в случае обнаружения функцией **AVG Do Not Track** новой системы отслеживания на веб-странице, посещаемой в данный момент, на экране отобразится диалоговое окно уведомления. Если флажок не установлен, вы сможете узнать о недавно обнаруженной службе только с помощью значка **AVG Do Not Track** (размещенного в командной строке обозревателя), который изменит цвет с зеленого на желтый.
- **Уведомлять веб-сайты, что отслеживание нежелательно** (по умолчанию включено). Не выключайте этот параметр, чтобы подтвердить, что функция **AVG Do Not Track** должна информировать провайдера обнаруженной службы сбора данных о том, что отслеживание нежелательно.
- **Блокировать перечисленное** (все перечисленные службы сбора данных по умолчанию разрешены). В этом разделе отображается поле со списком известных служб сбора данных, которые можно отнести к рекламным сетям. По умолчанию **AVG Do Not Track** автоматически блокирует некоторые рекламные сети, а решение о том, нужно ли блокировать остальные, принимаете вы сами. Для этого просто нажмите кнопку **Заблокировать все** под списком.

На странице **Параметры AVG Do Not Track** доступны такие кнопки управления:

- **Заблокировать все** — блокирует все службы, перечисленные в указанном выше поле, которые классифицируются как рекламные сети;
- **Разрешить все** — отменяет блокировку всех заблокированных ранее служб, перечисленных в указанном выше поле, которые классифицируются как рекламные сети;
- **По умолчанию** — сброс всех пользовательских настроек и возврат к параметрам по умолчанию;
- **Сохранить** — нажмите, чтобы применить и сохранить все указанные настройки;
- **Отмена** — отмена всех ранее указанных настроек.

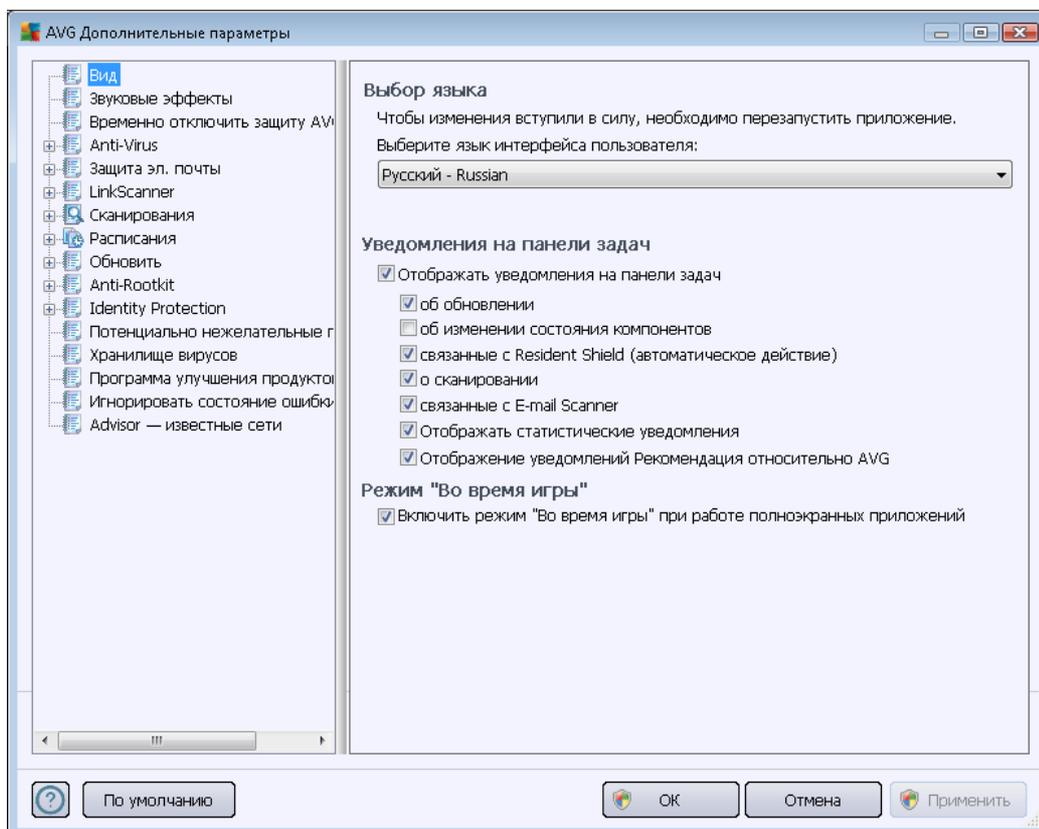


10. Дополнительные параметры AVG

Параметры дополнительной настройки **AVG Anti-Virus 2012** откроются в новом диалоговом окне **Дополнительные параметры AVG**. Окно разделено на две части. В левой части расположено навигационное дерево параметров программы. Выберите компонент, параметры которого необходимо изменить (*или часть компонента*), чтобы открыть диалоговое окно редактирования в правой части окна.

10.1. Внешний вид

Параметр **Вид**, первый элемент дерева навигации, относится к общим параметрам [интерфейса пользователя AVG Anti-Virus 2012](#) и нескольким начальным параметрам поведения приложения.

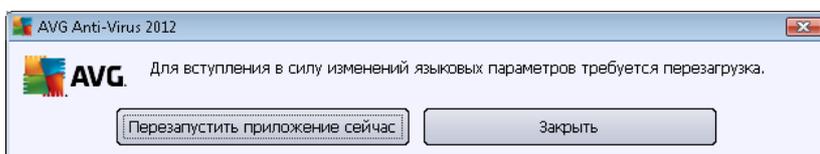


Выбор языка

В раскрывающемся меню раздела **Выбор языка** можно выбрать необходимый язык. После этого [интерфейс пользователя AVG Anti-Virus 2012](#) будет отображаться на выбранном языке. В раскрывающемся меню отображаются только языки, выбранные ранее [в процессе установки программы](#) (см. раздел [Пользовательские параметры](#)), и английский (*устанавливается по умолчанию*). Чтобы завершить процесс изменения языка **AVG Anti-Virus 2012**, необходимо перезапустить приложение. Выполните данные шаги:



- В раскрывающемся меню выберите язык установки.
- Подтвердите свой выбор, нажав кнопку **Применить** (в правом нижнем углу диалогового окна).
- Для подтверждения нажмите кнопку **OK**
- Откроется новое диалоговое окно, информирующее о том, что для изменения языка приложения требуется перезагрузка. **AVG Anti-Virus 2012**
- Нажмите кнопку **Перезапустить приложение сейчас**, чтобы подтвердить перезапуск программы, и подождите несколько секунд для вступления в силу изменений языковых параметров.



Уведомления на панели задач

В данном разделе можно отключить уведомления в виде всплывающих окон на панели задач о состоянии приложения **AVG Anti-Virus 2012**. По умолчанию включено отображение системных уведомлений. Настоятельно рекомендуется не изменять данный параметр. Системные уведомления информируют о таких событиях, как запуск процесса обновления, сканирования или изменение состояния компонента **AVG Anti-Virus 2012**. Необходимо обращать внимание на эти сообщения.

Однако, если по какой-либо причине необходимо отключить данные уведомления или настроить отображение только определенных уведомлений (*связанных с определенным компонентом AVG Anti-Virus 2012*), то это можно сделать, установив или сняв флажки с соответствующих параметров.

- **Отображать уведомления на панели задач** (по умолчанию включено). По умолчанию отображаются все уведомления. Снимите флажок с данного параметра, чтобы отключить отображение всех системных уведомлений. Если данный параметр включен, можно настроить отображение отдельных уведомлений.
 - **Отображать уведомления об [обновлении](#)** (по умолчанию включено). Позволяет определить, должна ли отображаться информация о **AVG Anti-Virus 2012** запуске процесса обновления, его состоянии и завершении.
 - **Отображать уведомления об изменении состояния компонентов** (по умолчанию выключено). Позволяет определить, должна ли отображаться информация об активности/бездействии компонента или о его возможных проблемах. Уведомляя пользователя о состоянии ошибки компонента, данный параметр соответствует информативной функции [значка на панели задач](#), информирующего о проблеме, связанной с определенным **AVG Anti-Virus 2012** компонентом.



- **Отображать уведомления Resident Shield на панели задач** (выполняется автоматически, по умолчанию включено). Определяет, должна ли отображаться информация о сохранении, копировании и открытии файлов (такая конфигурация доступна только в том случае, если функция Автоматическое лечение компонента Resident Shield включена).
- **Отображать уведомления о сканировании** на панели задач (по умолчанию включено). Определяет, должны ли отображаться сведения об автоматическом запуске запланированного сканирования, его состоянии и результатах.
- **Отображать уведомления E-mail Scanner на панели задач** (по умолчанию включено). Позволяет определить, должна ли отображаться информация о сканировании всех входящих и исходящих сообщений электронной почты.
- **Отображать статистические уведомления** (по умолчанию включено). Не снимайте данный флажок, чтобы на панели задач отображались уведомления о регулярных статистических обзорах.
- **Отображать уведомления о производительности советника AVG** (по умолчанию включено). Советник AVG отслеживает производительность поддерживаемых Интернет-браузеров (*Internet Explorer, Chrome, Firefox, Opera и Safari*) и информирует пользователя в том случае, если браузер чрезмерно использует рекомендуемый объем памяти. В этой ситуации производительность компьютера может значительно снизиться. Для ускорения процессов рекомендуется перезапустить Интернет-браузер. Не снимайте флажок **Отображать уведомления о производительности советника AVG** для получения данных сообщений.

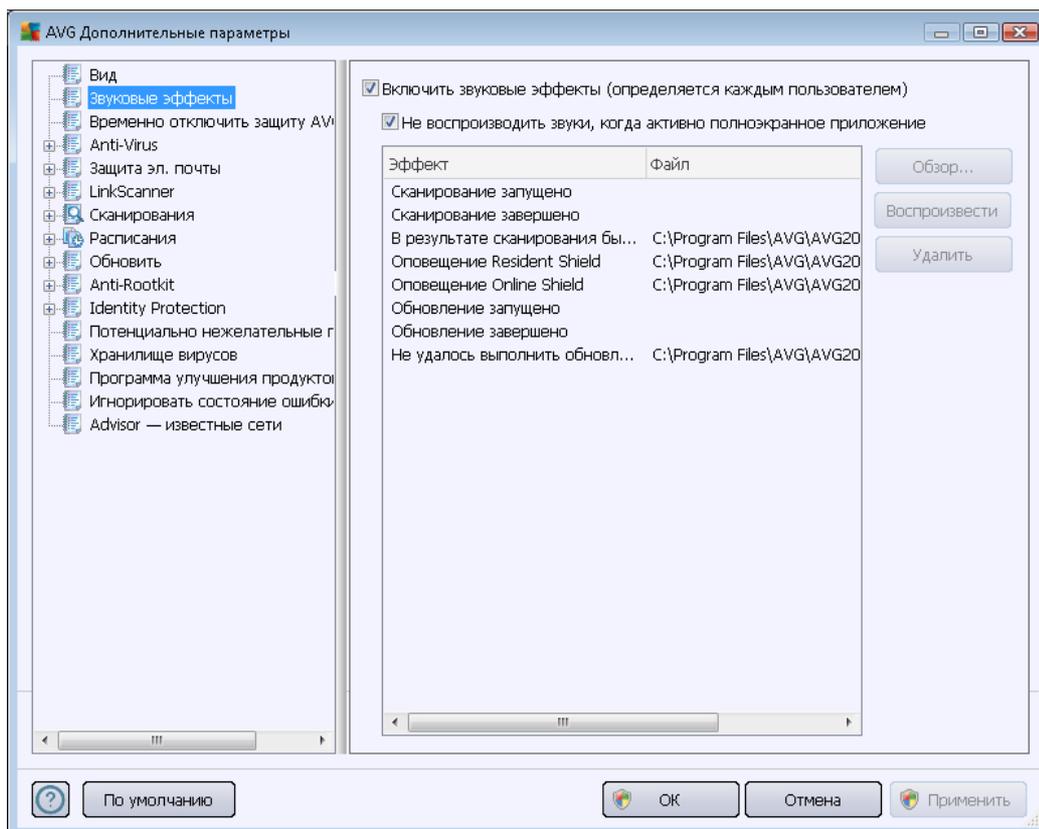


Режим "Во время игры"

Эта функция системы AVG предназначена для полноэкранных приложений, где всплывающие окна AVG (которые могут отображаться, например, при запуске запланированного сканирования) способны помешать пользователю (в результате возможно сворачивание приложения или нарушение графических параметров). Во избежание подобных ситуаций отметьте флажком параметр **Включить режим "Во время игры" при работе полноэкранных приложений** (параметр по умолчанию).

10.2. Звуки

В диалоговом окне **Звуки** можно выбрать звуковое уведомление для определенных действий программы **AVG Anti-Virus 2012**.



Данные параметры доступны только для текущей учетной записи пользователя. Это означает, что каждый пользователь может устанавливать свои собственные параметры звука. Для получения звуковых уведомлений установите флажок на параметре **Включить звуковые эффекты** (по умолчанию включено). В результате появится список соответствующих действий. Также можно выбрать параметр **Не воспроизводить звуки, когда активно полноэкранное приложение** для выключения звуковых уведомлений в случаях, когда они могут быть неуместными (см. также раздел ["Во время игры"](#) главы [Дополнительные параметры/Внешний вид](#) этого документа).

Кнопки управления

- **Обзор.** Выбрав из списка соответствующее событие, нажмите кнопку **Обзор** и укажите на диске аудиофайл, который необходимо назначить для этого события. (Обратите внимание, что поддерживаются только файлы в формате WAV).
- **Воспроизвести.** Чтобы прослушать выбранный аудиофайл, выделите событие в списке и нажмите кнопку **Воспроизвести**.

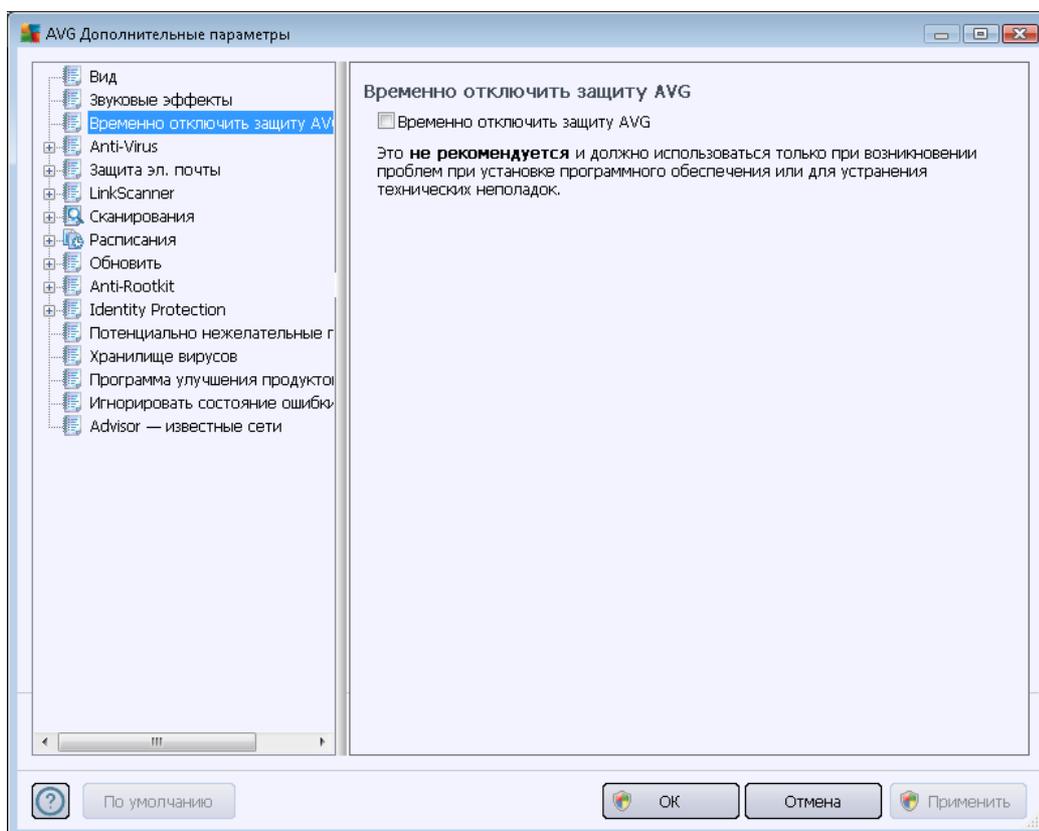


- **Удалить.** Чтобы удалить звук, назначенный определенному событию, нажмите кнопку **Удалить**.

10.3. Временное отключение защиты AVG

В диалоговом окне **Временное отключение защиты AVG** можно полностью выключить защиту, обеспечиваемую программой **AVG Anti-Virus 2012**.

Используйте данный параметр только в случае крайней необходимости!

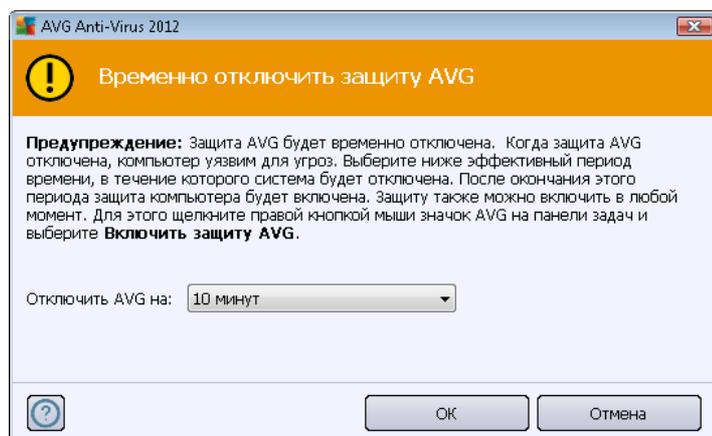


В большинстве случаев программу **AVG Anti-Virus 2012** **не рекомендуется** отключать перед установкой нового ПО или драйверов, даже если программа или мастер установки рекомендует завершить все запущенные программы и приложения, чтобы они не препятствовали процессу установки. Если во время установки возникла проблема, попробуйте сначала [отключить постоянную защиту](#) (*Включить Resident Shield*). Если вам пришлось временно отключить защиту **AVG Anti-Virus 2012**, включите ее, как только завершите установку. Если вы подключены к Интернету или локальной сети, но антивирусная защита выключена, ваш компьютер может подвергнуться атакам.

Отключение защиты AVG

- Установите флажок **Временное отключение защиты AVG** и подтвердите свой выбор нажатием кнопки **Принять**.

- В только что открытом окне **Временное отключение защиты AVG** укажите, на какой период времени вы собираетесь отключить **AVG Anti-Virus 2012**. По умолчанию защита будет отключена в течение 10 минут, чего должно хватить для выполнения наиболее распространенных задач, например установки нового ПО. Обратите внимание, что максимально допустимое значение времени составляет 15 минут. Это значение не может быть изменено на пользовательское из соображений безопасности. По истечении указанного периода все отключенные компоненты автоматически включатся.

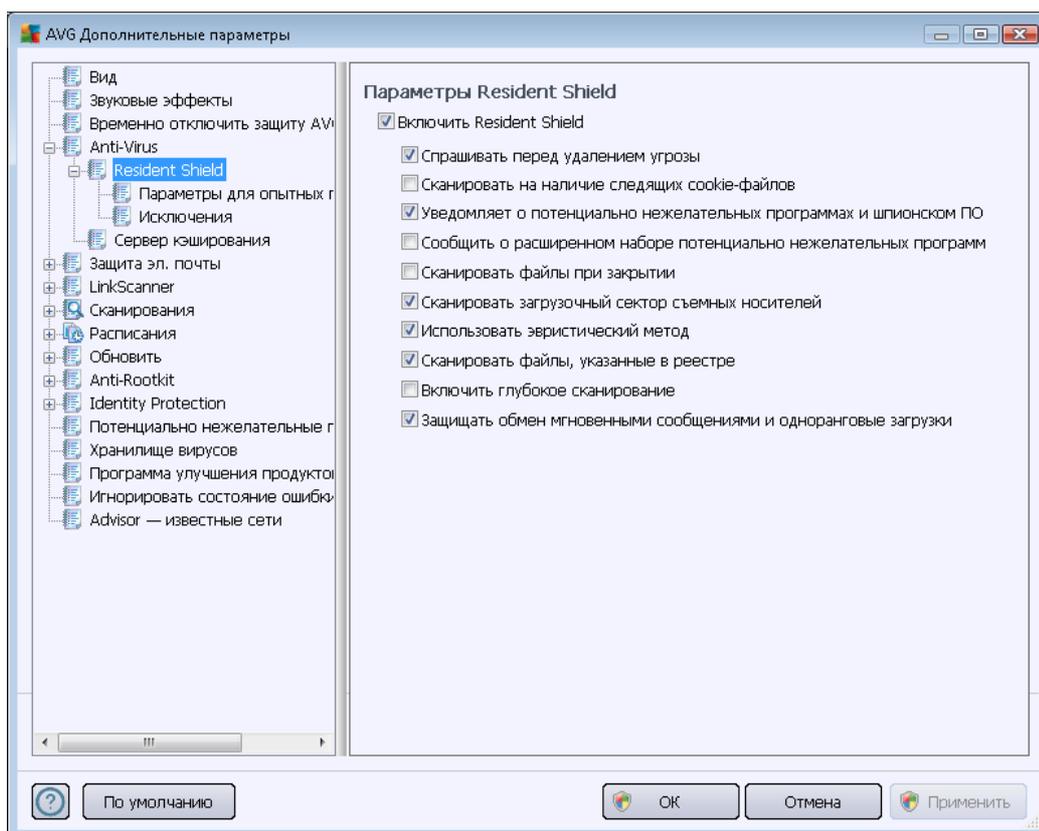


10.4. Антивирус (Anti-Virus)

Компонент **Anti-Virus** обеспечивает непрерывную защиту компьютера от всех известных разновидностей вирусов и шпионского ПО (включая так называемое "спящее" или неактивное вредоносное ПО, т. е. вредоносное ПО, которое загружено, но еще не активировано).

10.4.1. Resident Shield

Компонент Resident Shield обеспечивает защиту в реальном времени файлов и папок от вирусов, шпионского ПО и других разновидностей вредоносного ПО.



В диалоговом окне **Параметры Resident Shield** можно включить или отключить постоянную защиту, установив или сняв флажок с параметра **Включить Resident Shield** (по умолчанию включено). Также можно активировать отдельные функции постоянной защиты.

- **Спрашивать перед удалением угроз** (выбрано по умолчанию). Установите флажок, чтобы запретить Resident Shield автоматически выполнять какие-либо действия. Вместо этого будет отображаться диалоговое окно с описанием обнаруженной угрозы, позволяя пользователю выбрать действие самому. Если не установить флажок, **AVG Anti-Virus 2012** лечение зараженного объекта обеспечивается автоматически, а когда это невозможно — переносится в [хранилище вирусов](#).
- **Сканировать на наличие следящих файлов cookie** (по умолчанию выключено). Данный параметр включает обнаружение файлов cookie при сканировании. (Файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзины для покупок в Интернете.)
- **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО** (по умолчанию включено). Установите данный флажок для активации модуля [Anti-Spyware](#) и сканирования компьютера на наличие

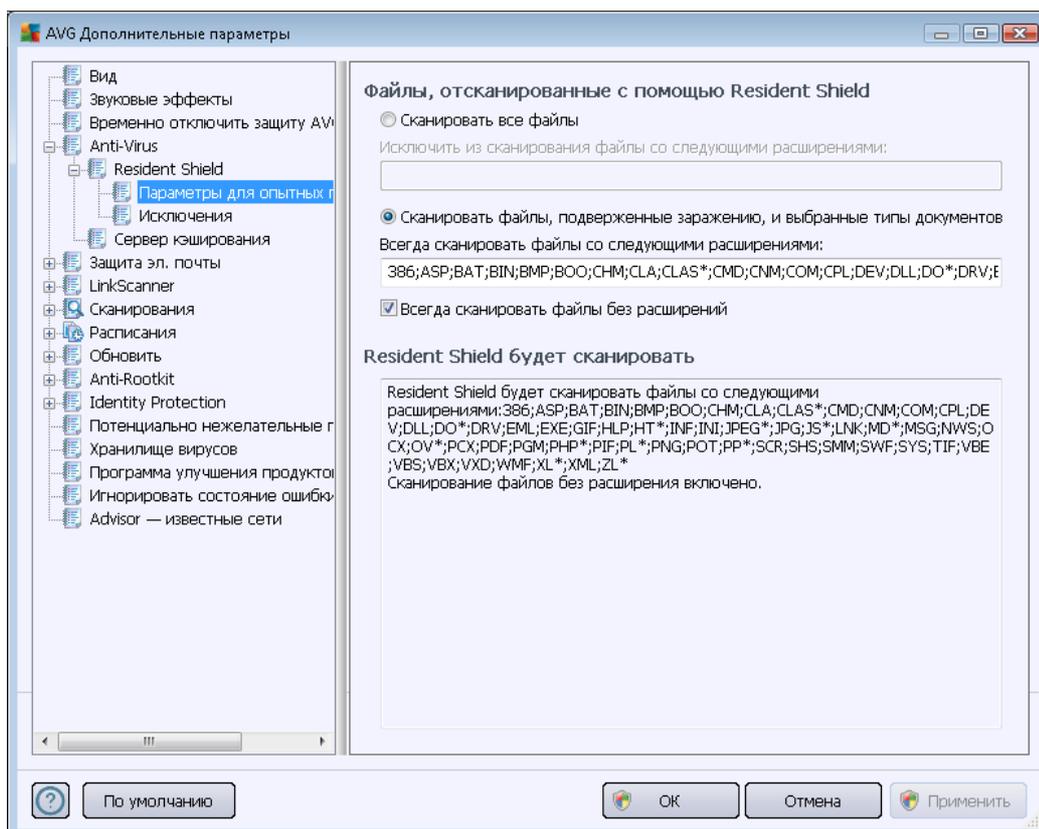


шпионского ПО и вирусов. [Шпионские программы](#) относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- **Уведомлять о расширенном наборе потенциально нежелательных программ** (по умолчанию выключено). Установите данный флажок для обнаружения расширенного пакета [шпионского ПО](#): программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.
- **Сканировать файлы при закрытии** (по умолчанию выключено). Сканирование программой AVG активных объектов (например, приложений, документов и др.) при открытии, а также при закрытии. Данная функция помогает защитить компьютер от некоторых разновидностей самых опасных вирусов.
- **Сканировать загрузочный сектор съемных носителей** (по умолчанию включено)
- **Использовать эвристический анализ** (по умолчанию включено). Для обнаружения будет использован [Эвристический анализ](#) (динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде).
- **Сканировать файлы, указанные в реестре** (по умолчанию включено). Данный параметр определяет, что программа AVG будет выполнять сканирование всех исполняемых файлов, добавляемых в реестр запуска, во избежание активации известных заражений при следующем запуске компьютера.
- **Включить глубокое сканирование** (по умолчанию выключено). В определенных случаях (в случае крайней необходимости) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые будут максимально глубоко сканировать систему на наличие потенциальных угроз. Обратите внимание, что для выполнения такого сканирования потребуется много времени.
- **Включить защиту обмена мгновенными сообщениями и защиту загрузок P2P** (по умолчанию включено). Установите данный флажок для проверки на вирусы вашей программы обмена мгновенными сообщениями (например, ICQ, MSN Messenger, ...) и загрузок P2P.



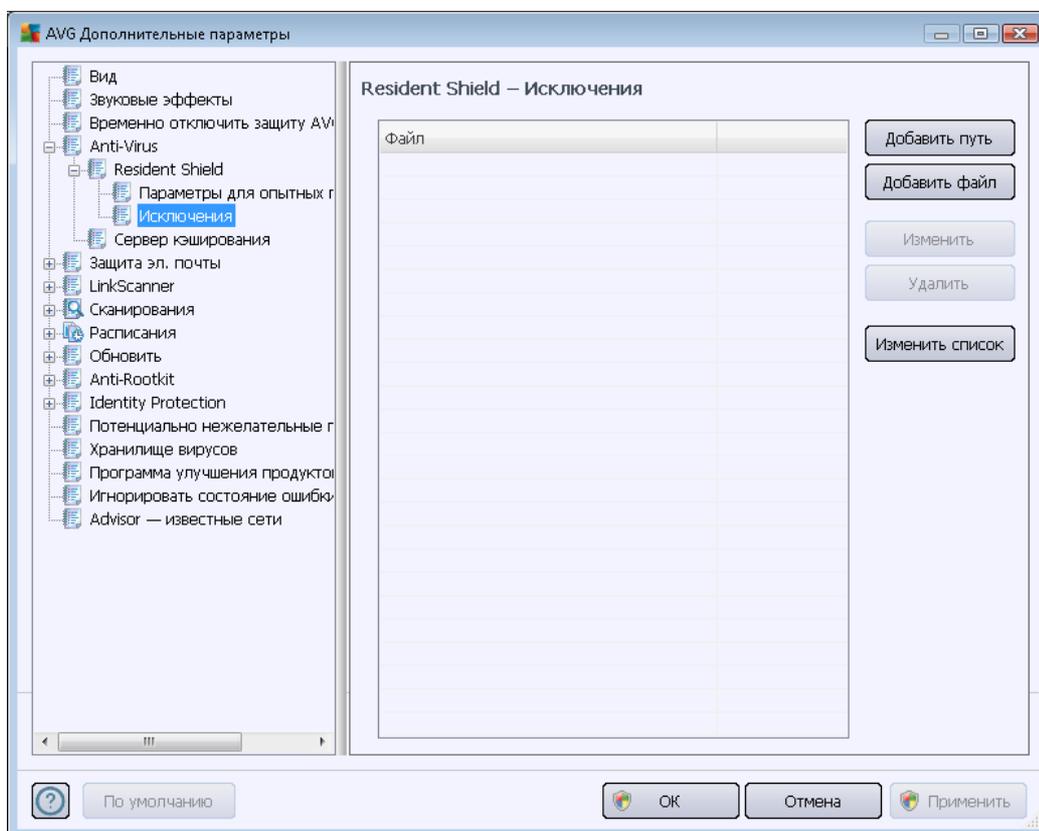
В диалоговом окне **Файлы, сканируемые с помощью компонента Resident Shield**, можно указать файлы, которые необходимо сканировать (*по определенным расширениям*).



Установите соответствующий флажок для выбора режима сканирования: **Сканировать все файлы** или **Сканировать файлы, подверженные заражению, и выбранные типы документов**. При выборе второго режима можно также указать список расширений, определяющих файлы, которые сканировать не нужно, а также список расширений файлов, которые необходимо сканировать в любом случае.

Установите флажок **Всегда сканировать файлы без расширений** (*выбрано по умолчанию*), чтобы компонент Resident Shield сканировал даже файлы без расширений и неизвестного формата. Рекомендуется включить эту функцию, поскольку файлы без расширений являются подозрительными.

В разделе **Компонент Resident Shield просканирует** приводится сводка по текущим настройкам и отображаются подробные сведения об объектах, которые будут подвержены сканированию компонентом **Resident Shield**.



В окне **Исключения Resident Shield** можно определить файлы и/или папки, которые необходимо исключить из сканирования компонентом **Resident Shield**.

Настоятельно рекомендуется не исключать какие-либо элементы без необходимости.

Кнопки управления

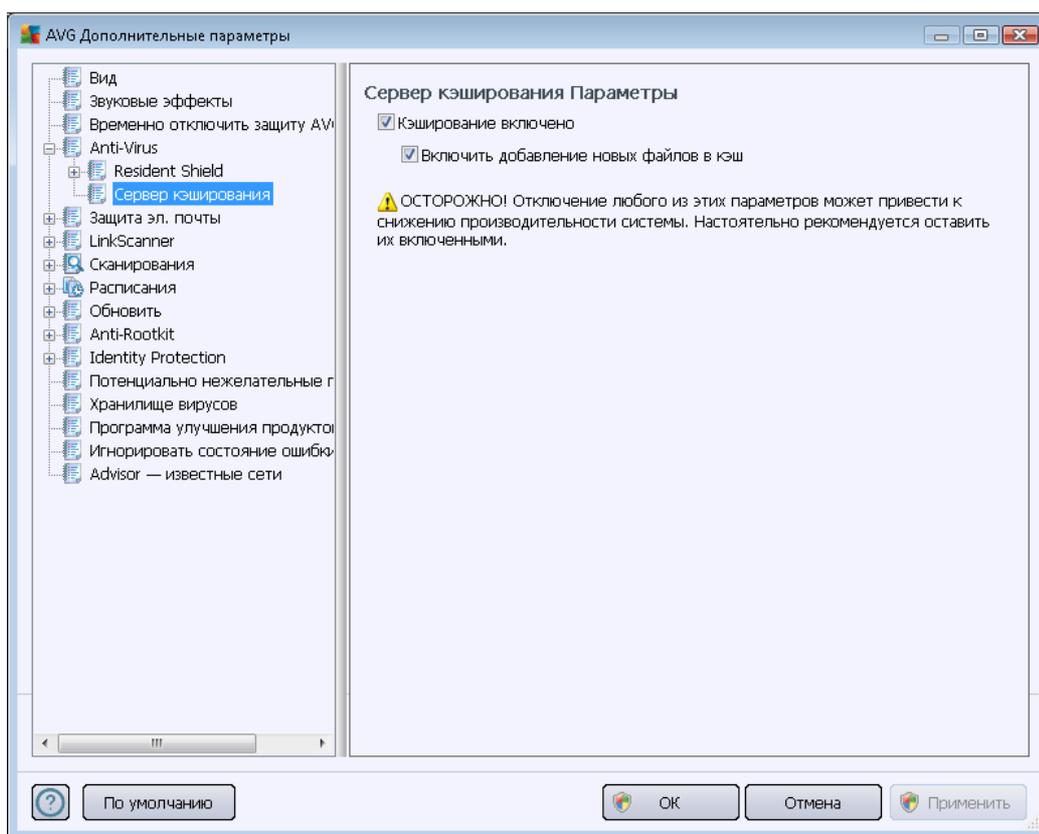
В диалоговом окне содержатся следующие кнопки управления:

- **Добавить путь.** Укажите каталоги, которые должны быть исключены из сканирования, выбрав их последовательно в навигационном дереве локального диска
- **Добавить файл.** Укажите файлы, которые должны быть исключены из сканирования, выбрав их последовательно в дереве навигации локального диска.
- **Редактировать элемент.** Позволяет редактировать указанный путь к выбранному файлу или папке.
- **Удалить элемент.** Позволяет удалить путь к выбранному элементу из списка.
- **Редактировать список.** Позволяет редактировать весь список определенных

исключений в новом диалоговом окне, как в стандартном текстовом редакторе.

10.4.2. Сервер кэширования

Диалоговое окно *Параметры сервера кэширования* относится к процессу сервера кэширования, позволяющему ускорить любые операции сканирования **AVG Anti-Virus 2012**.



Сервер кэширования собирает и хранит информацию о надежных файлах (*надежными считаются файлы, заверенные цифровой подписью надежного источника*). Эти файлы в дальнейшем считаются безопасными и пропускаются при повторном сканировании.

Диалоговое окно *Параметры сервера кэширования* содержит следующие параметры:

- **Кэширование включено** (по умолчанию флажок установлен). Снимите данный флажок, чтобы выключить **сервер кэширования** и очистить кэш-память. Примите к сведению, что сканирование может замедлять работу системы и влиять на общую производительность компьютера, так как каждый используемый файл будет проверяться на предмет вирусов и шпионского ПО.
- **Включить добавление новых файлов в кэш** (по умолчанию флажок установлен). Снимите данный флажок, чтобы остановить добавление новых файлов в кэш-память. Все добавленные в кэш-память файлы будут храниться и использоваться, пока не будет выключено кэширование или не будет обновлена вирусная база.



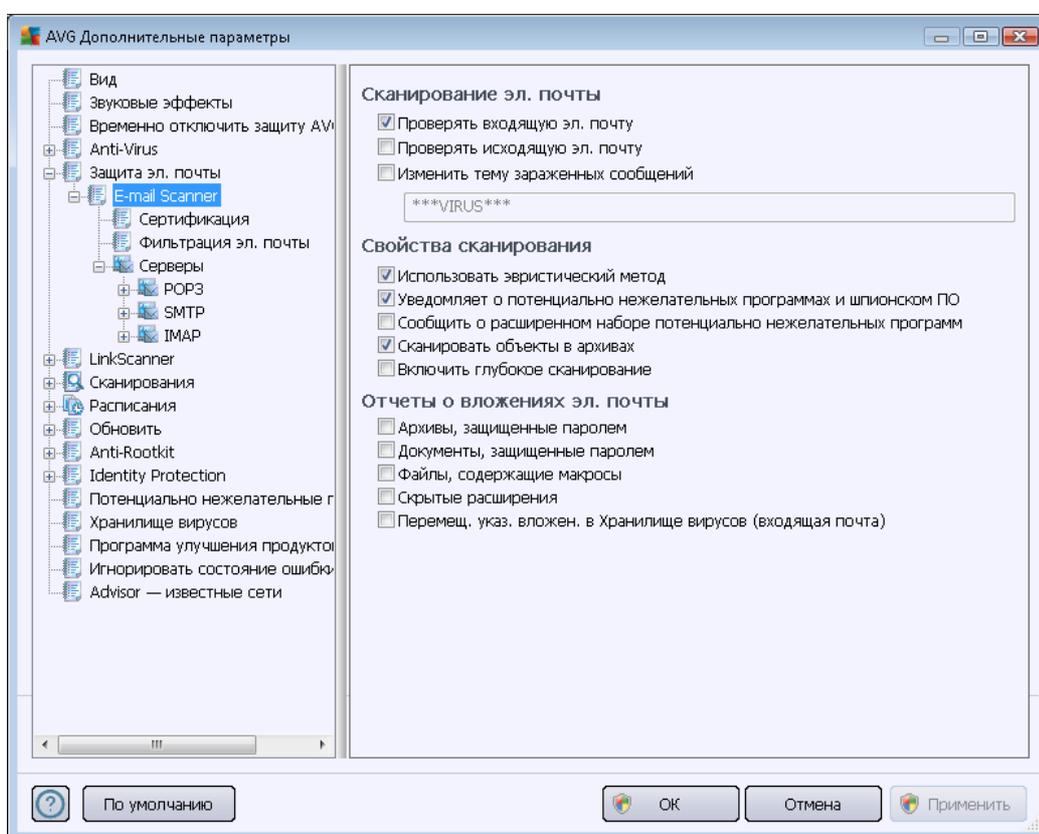
Если нет веских оснований для отключения сервера кэширования, настоятельно рекомендуется не изменять настройки по умолчанию и оставить оба параметра включенными. В противном случае, отключение этих параметров может привести к снижению скорости и производительности системы.

10.5. Защита электронной почты

В разделе **Защита эл. почты** можно изменить дополнительные настройки компонентов [E-mail Scanner](#) и Anti-Spam.

10.5.1. E-mail Scanner

Диалоговое окно **E-mail Scanner** состоит из трех разделов.



Сканирование эл. почты

В данном разделе можно указать следующие основные требования для входящих и/или исходящих сообщений электронной почты.

- **Проверять входящие сообщения электронной почты (выбрано по умолчанию).**
Включение/выключение функции сканирования всех сообщений электронной почты, доставляемых в почтовый клиент.
- **Проверять исходящие сообщения электронной почты (выбрано по умолчанию).**
Включение/выключение функции сканирования всех сообщений электронной почты,



отправляемых из учетной записи пользователя.

- **Изменить тему зараженных вирусом сообщений** (не выбрано по умолчанию). Для получения предупреждения при определении сканированного сообщения электронной почты как зараженного установите данный флажок и введите необходимый текст в соответствующем поле. В дальнейшем он будет добавляться в поле "Тема" каждого зараженного сообщения электронной почты, что упростит процесс идентификации и фильтрации. По умолчанию установлено значение *****VIRUS*****, его не рекомендуется менять.

Свойства сканирования

В данном разделе можно указать способ сканирования сообщений электронной почты.

- **Использовать эвристический анализ** (по умолчанию включено). Установите данный флажок, чтобы использовать эвристический метод обнаружения при сканировании сообщений электронной почты. Включение данного параметра позволяет выполнить фильтрацию вложений сообщений электронной почты не только по их расширению, но также с учетом фактического содержимого вложений. Параметры фильтрации можно указать в диалоговом окне [Фильтрация электронной почты](#).
- **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО** (выбрано по умолчанию). Установите данный флажок для активации модуля [Anti-Spyware](#) и сканирования компьютера на наличие шпионского ПО и вирусов. [Шпионские программы](#) относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.
- **Уведомлять о расширенном наборе потенциально нежелательных программ** (по умолчанию выключено). Установите данный флажок для обнаружения расширенного пакета [шпионского ПО](#): программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.
- **Сканировать объекты в архивах** (выбрано по умолчанию). Установите данный флажок, чтобы выполнять сканирование архивов, вложенных в сообщения электронной почты.
- **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (например, при подозрении, что компьютер заражен вирусом или эксплойтом) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

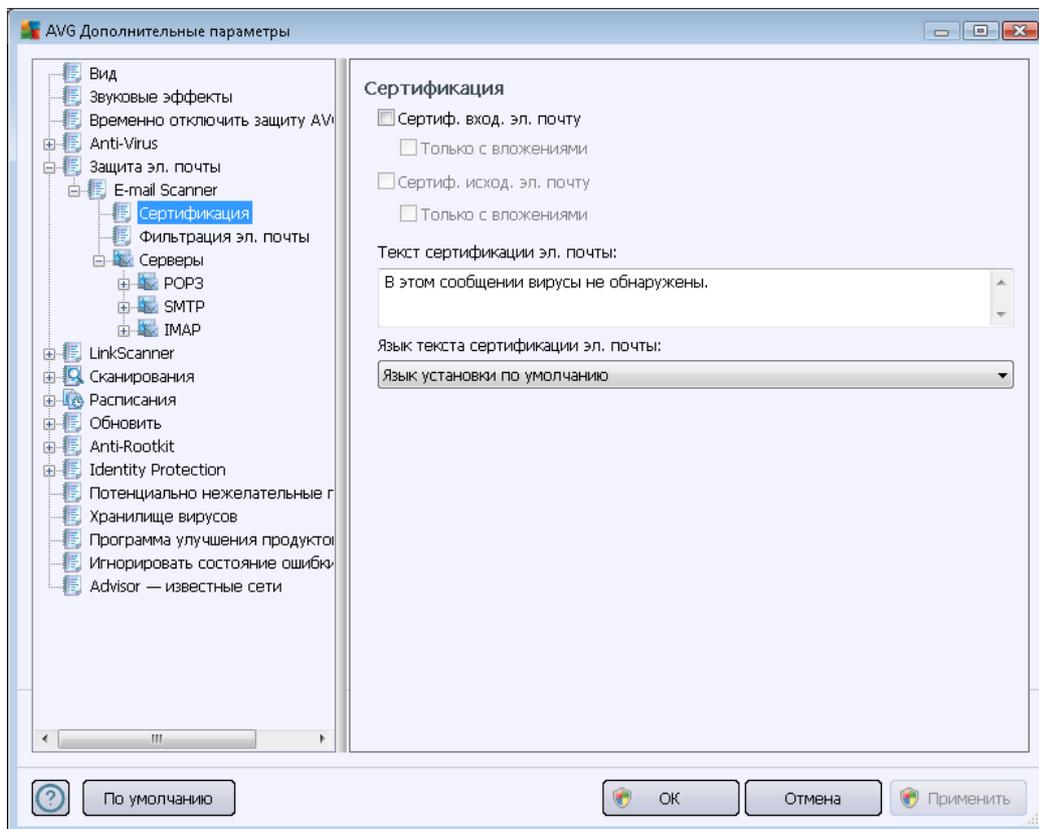


Отчеты о вложениях электронной почты

В этом разделе можно настроить функцию предоставления дополнительных отчетов о потенциально опасных или подозрительных файлах. Обратите внимание, что диалоговое окно с предупреждением отображено не будет. Только текст сертификации будет добавлен в конце сообщения электронной почты и все подобные отчеты будут перечислены в списке диалогового окна [Обнаружение E-mail Scanner](#).

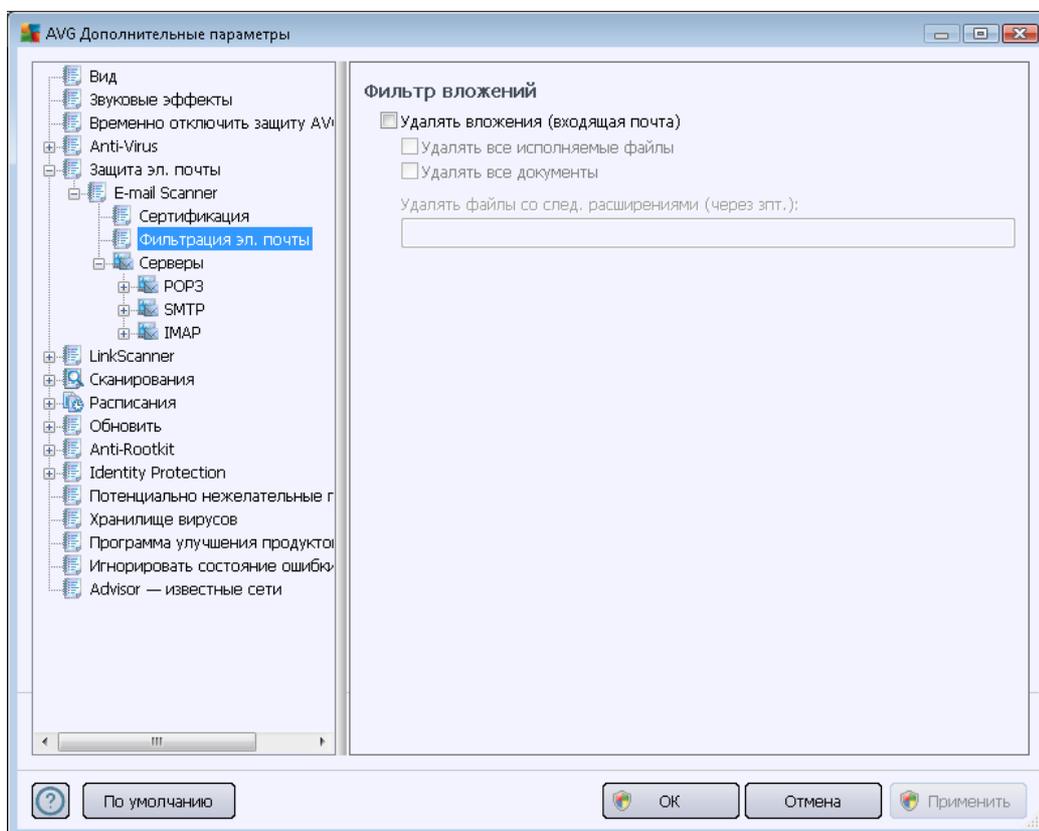
- **Сообщать об архивах, защищенных паролем.** Сканирование на наличие вирусов в архивах (*ZIP, RAR и т. п.*), защищенных паролем, недоступно; установите флажок, чтобы в отчетах они были отмечены как потенциально опасные.
- **Сообщать о документах, защищенных паролем.** Сканирование на наличие вирусов в документах, защищенных паролем, недоступно; установите флажок, чтобы в отчетах они были отмечены как потенциально опасные.
- **Сообщать о файлах, содержащих макросы.** Макрос — предустановленная последовательность действий, предназначенная для упрощения выполнения пользователем определенных задач (*широко известны макросы MS Word*). По этой причине макросы могут содержать потенциально опасные инструкции, и пользователю, возможно, потребуется установить флажок, чтобы файлы с макросами были отмечены в отчетах как подозрительные.
- **«Сообщать о скрытых расширениях».** При использовании скрытых расширений подозрительный выполнимый файл *something.txt.exe* может отображаться как безопасный обычный текстовый файл *something.txt*. Установите флажок, чтобы в отчетах данные файлы были отмечены как потенциально опасные.
- **Перемещать указанные вложения в хранилище вирусов.** Необходимо указать, следует ли уведомлять пользователя по электронной почте о защищенных паролями архивах, защищенных паролями документах, содержащих макросы файлах и/или файлах со скрытыми расширениями, обнаруженных во вложениях сканируемых сообщений электронной почты. Если подобное сообщение будет обнаружено при сканировании, необходимо определить, следует ли перемещать зараженные объекты в [хранилище вирусов](#).

В диалоговом окне **Сертификация** можно назначить сертификацию входящей почты (**Сертификация входящих сообщений эл. почты**) и/или исходящей почты (**Сертификация исходящих сообщений эл. почты**), установив соответствующие флажки. Для каждого из этих действий можно также выбрать параметр **Только с вложениями**, при котором сертификация будет добавляться только к сообщениям электронной почты с вложениями.



По умолчанию текст сертификации содержит основную информацию: *В данном сообщении вирусов не обнаружено*. Однако при необходимости эту информацию можно расширить или изменить. Введите необходимый текст сертификации в поле **Текст сертификации эл. почты**. В разделе **Язык текста сертификации эл. почты** можно также указать язык, на котором будет отображаться автоматически созданная часть текста (*В данном сообщении вирусов не обнаружено*).

Примечание. Обратите внимание, что на выбранном языке будет отображен только текст по умолчанию, пользовательский текст не будет переведен автоматически.



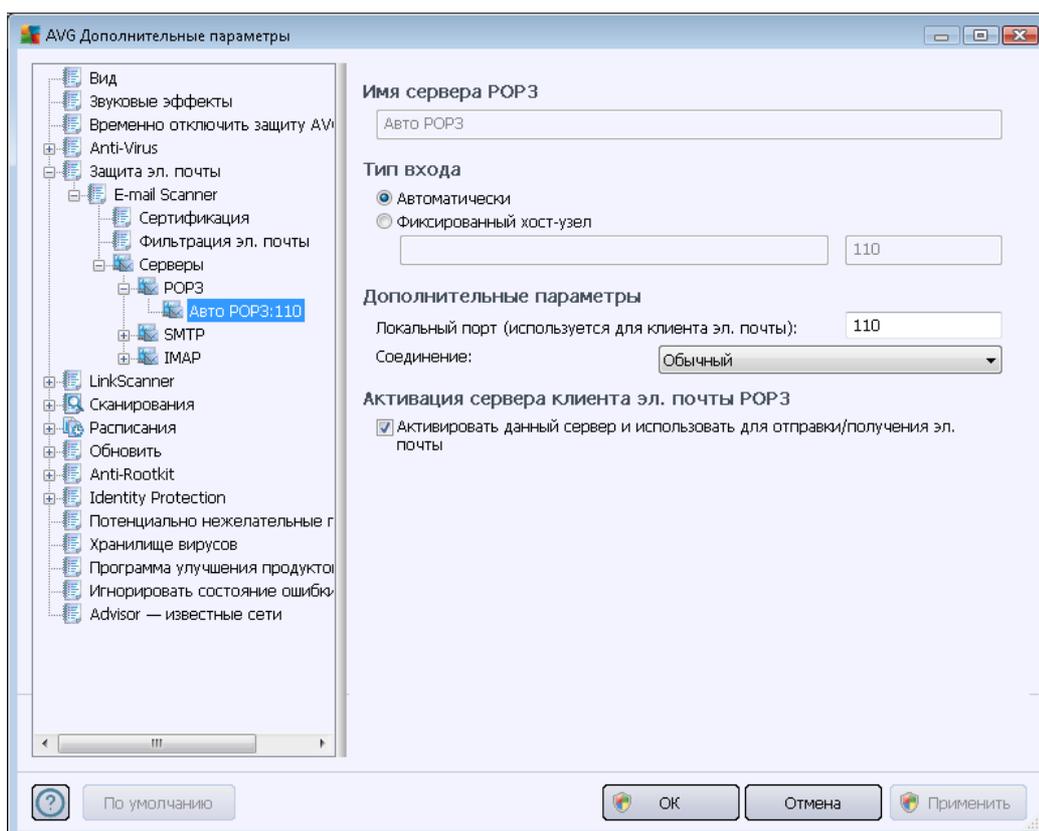
Диалоговое окно **Фильтр вложений** позволяет настроить параметры сканирования вложений в сообщениях электронной почты. По умолчанию параметр **Удалять вложения** выключен. При его установке все обнаруженные зараженные вложения в сообщениях электронной почты или потенциально опасные вложения будут автоматически удалены. Если необходимо определить специальные типы вложений, которые должны быть удалены, выберите соответствующий параметр.

- **Удалять все исполняемые файлы.** Все файлы *.exe будут удалены.
- **Удалять все документы.** Все файлы *.doc, *.docx, *.xls, *.xlsx будут удалены.
- **Удалять файлы со след. расширениями (через зпт.).** Все файлы с указанными расширениями будут удалены.

В разделе **Серверы** можно изменить настройки серверов компонента [E-mail Scanner](#).

- [Сервер POP3](#)
- [Сервер SMTP](#)
- [Сервер IMAP](#)

В этом диалоговом окне можно также определить новый сервер для исходящих или входящих сообщений электронной почты при помощи кнопки **Добавить новый сервер**.

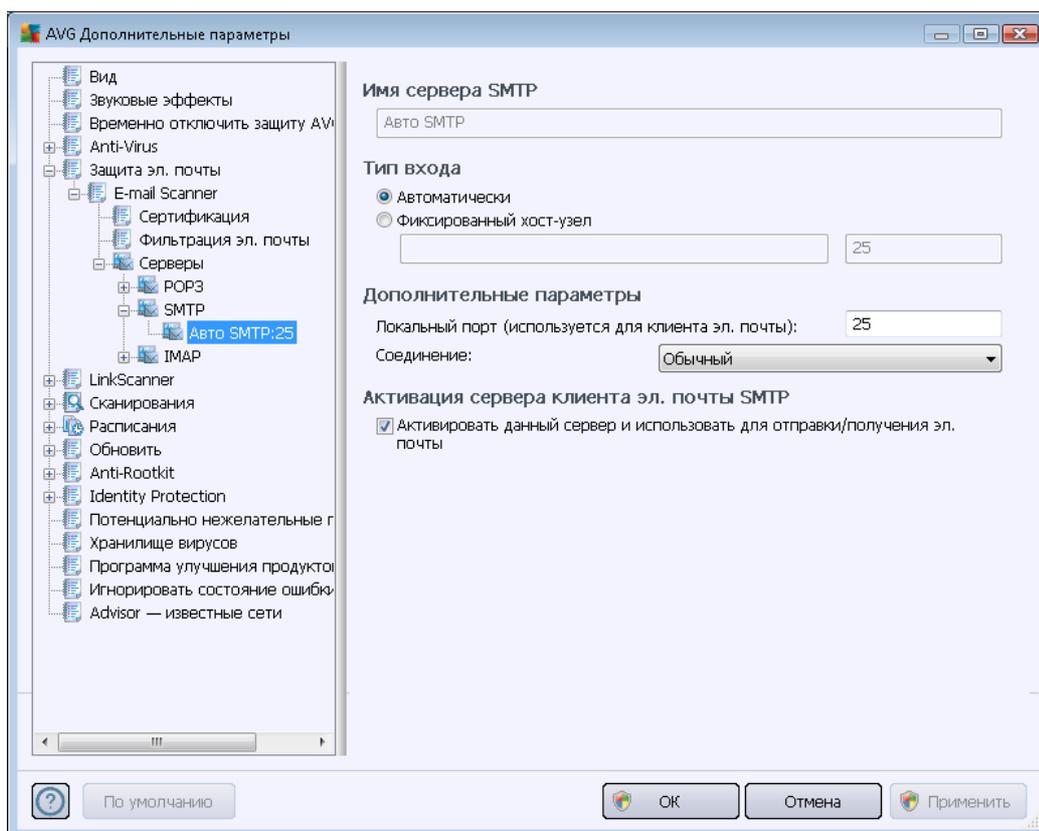


В данном диалоговом окне (открытом при выборе **Серверы/POP3**) можно установить новый сервер для компонента **E-mail Scanner** с помощью протокола POP3 для входящей почты.

- **Имя сервера POP3.** В данном поле можно указать имя добавленного сервера (чтобы добавить сервер POP3, щелкните правой кнопкой мыши элемент POP3 в меню навигации слева). При использовании созданного автоматически сервера "AutoPOP3" данное поле будет неактивным.
- **Тип входа.** Метод определения почтового сервера, используемого для входящей почты.
 - **Автоматически.** Автоматическое выполнение входа в соответствии с параметрами клиента электронной почты.
 - **Фиксированный хост-узел.** В данном случае программой всегда используется указанный в этом поле сервер. Укажите адрес или имя используемого почтового сервера. Имя пользователя не изменяется. В качестве имени можно использовать имя домена (например, *pop.acme.com*) или IP-адрес (например, *123.45.67.89*). Если почтовый сервер использует нестандартный порт, данный порт можно указать после имени сервера, используя двоеточие в

качестве разделителя (например, *pop.ascom.com:8200*). Стандартным портом соединения POP3 является порт 110.

- **Дополнительные параметры.** Определение более подробных параметров.
 - **Локальный порт.** Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом приложении необходимо указать данный порт в качестве порта соединения POP3.
 - **Подключение.** В раскрывающемся меню можно определить необходимый тип подключения (*обычное/SSL/SSL по умолчанию*). При выборе соединения SSL данные отправляются в зашифрованном виде и вероятность их отслеживания или просмотра третьей стороной отсутствует. Данная функция также доступна, только если она поддерживается почтовым сервером назначения.
- **Активация сервера POP3 клиента электронной почты.** Установите или снимите флажок напротив этого элемента, чтобы активировать или деактивировать указанный сервер POP3.

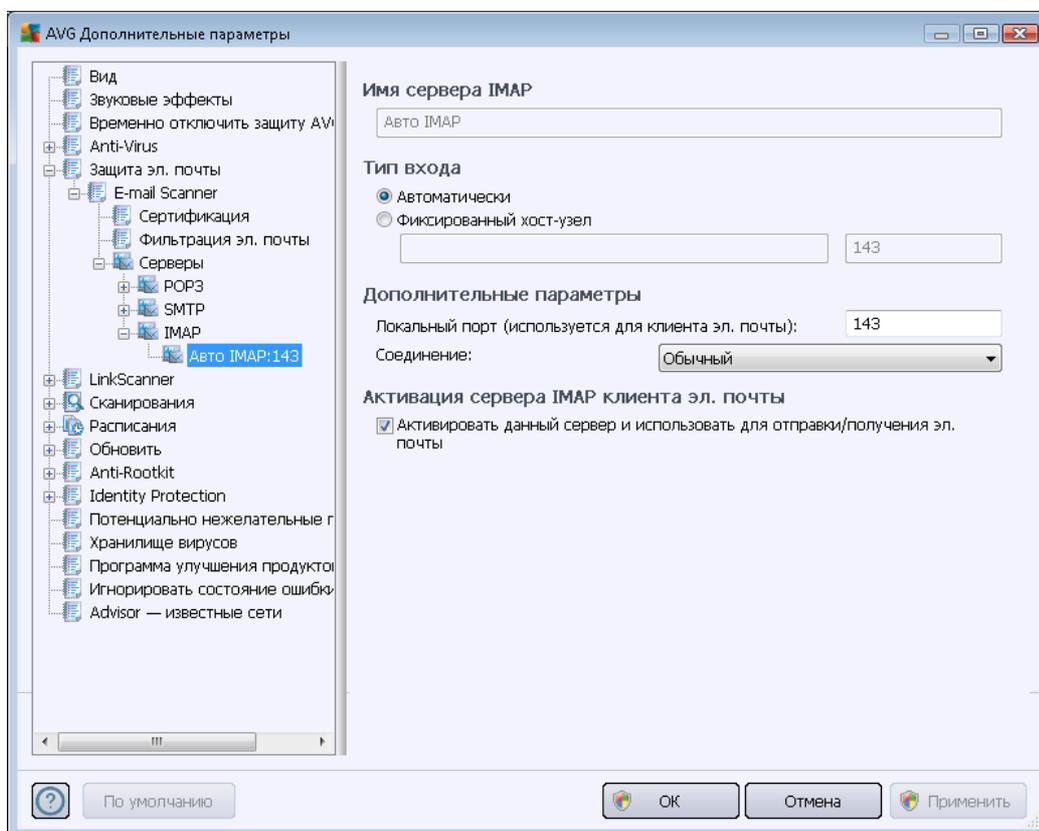


В данном диалоговом окне (*открытом через Серверы/SMTP*) можно настроить новый сервер [E-mail Scanner](#), используя протокол SMTP для исходящей почты.

- **Имя сервера SMTP.** В данном поле можно указать имя добавленного сервера (

чтобы добавить сервер SMTP, щелкните правой кнопкой мыши элемент SMTP в меню навигации слева). При использовании созданного автоматически сервера "AutoSMTP" данное поле будет неактивным.

- **Тип входа.** Метод определения почтового сервера, используемого для исходящей почты.
 - **Автоматически.** Автоматическое выполнение входа в соответствии с параметрами клиента электронной почты.
 - **Фиксированный хост-узел.** Постоянное использование программой указанного сервера. Укажите адрес или имя используемого почтового сервера. В качестве имени можно указать имя домена (*например, smtp.acme.com*) или IP-адрес (*например, 123.45.67.89*). Если почтовый сервер использует нестандартный порт, данный порт можно указать после имени сервера, используя двоеточие в качестве разделителя (*например, smtp.acme.com:8200*). Номер стандартного порта соединения SMTP — 25.
- **Дополнительные параметры.** Определение более подробных параметров.
 - **Локальный порт.** Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом клиенте необходимо указать данный порт в качестве порта соединения SMTP.
 - **Подключение.** Раскрывающееся меню, в котором можно указать необходимый тип подключения (*обычное/SSL/SSL по умолчанию*). При выборе соединения SSL данные отправляются в зашифрованном виде и вероятность их отслеживания или просмотра третьей стороной отсутствует. Данная функция доступна, только если она поддерживается конечным почтовым сервером.
- **Активация сервера SMTP клиента электронной почты.** Установите или снимите этот флажок, чтобы активировать или деактивировать указанный выше сервер SMTP.



В данном диалоговом окне (открытом через **Серверы/SMTP**) можно настроить новый сервер для компонента **E-mail Scanner**, используя протокол IMAP для исходящей почты.

- **Имя сервера IMAP.** В данном поле можно указать имя добавленного сервера (чтобы добавить сервер IMAP, щелкните правой кнопкой мыши элемент IMAP в меню навигации слева). При использовании созданного автоматически сервера "AutoIMAP" данное поле будет неактивным.
- **Тип входа.** Метод определения почтового сервера, используемого для исходящей почты.
 - **Автоматически.** Автоматическое выполнение входа в соответствии с параметрами клиента электронной почты.
 - **Фиксированный хост-узел.** Постоянное использование программой указанного сервера. Укажите адрес или имя используемого почтового сервера. В качестве имени можно указать имя домена (например, *smtp.acme.com*) или IP-адрес (например, *123.45.67.89*). Если почтовый сервер использует нестандартный порт, данный порт можно указать после имени сервера, используя двоеточие в качестве разделителя (например, *imap.acme.com:8200*). Стандартным портом соединения IMAP является порт 143.
- **Дополнительные параметры.** Определение более подробных параметров.

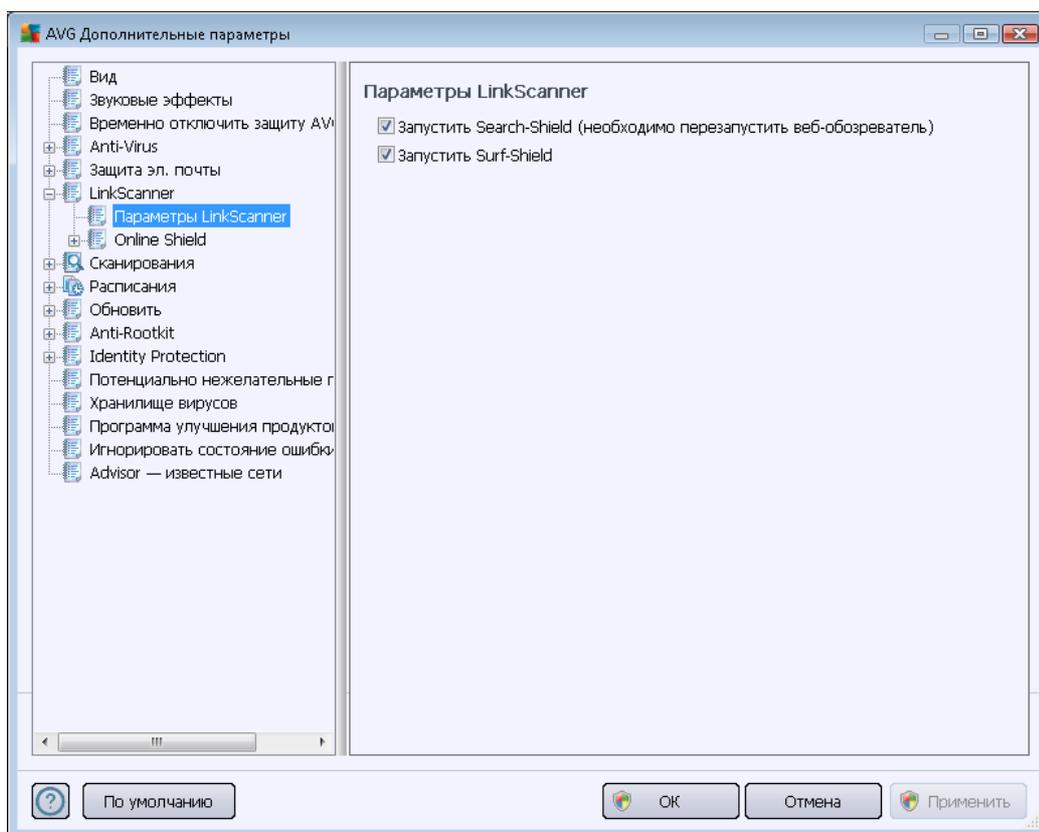


- **Локальный порт.** Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом клиенте необходимо указать данный порт в качестве порта соединения IMAP.
- **Подключение.** Раскрывающееся меню, в котором можно указать необходимый тип подключения (*обычное/SSL/SSL по умолчанию*). При выборе соединения SSL данные отправляются в зашифрованном виде и вероятность их отслеживания или просмотра третьей стороной отсутствует. Данная функция доступна, только если она поддерживается конечным почтовым сервером.
- **Активация сервера IMAP клиента электронной почты.** Установите или снимите этот флажок, чтобы активировать или деактивировать указанный выше сервер SMTP.

10.6. LinkScanner

10.6.1. Настройки Link Scanner

Диалоговое окно [Параметры LinkScanner](#) позволяет включать или отключать основные функции компонента [LinkScanner](#).

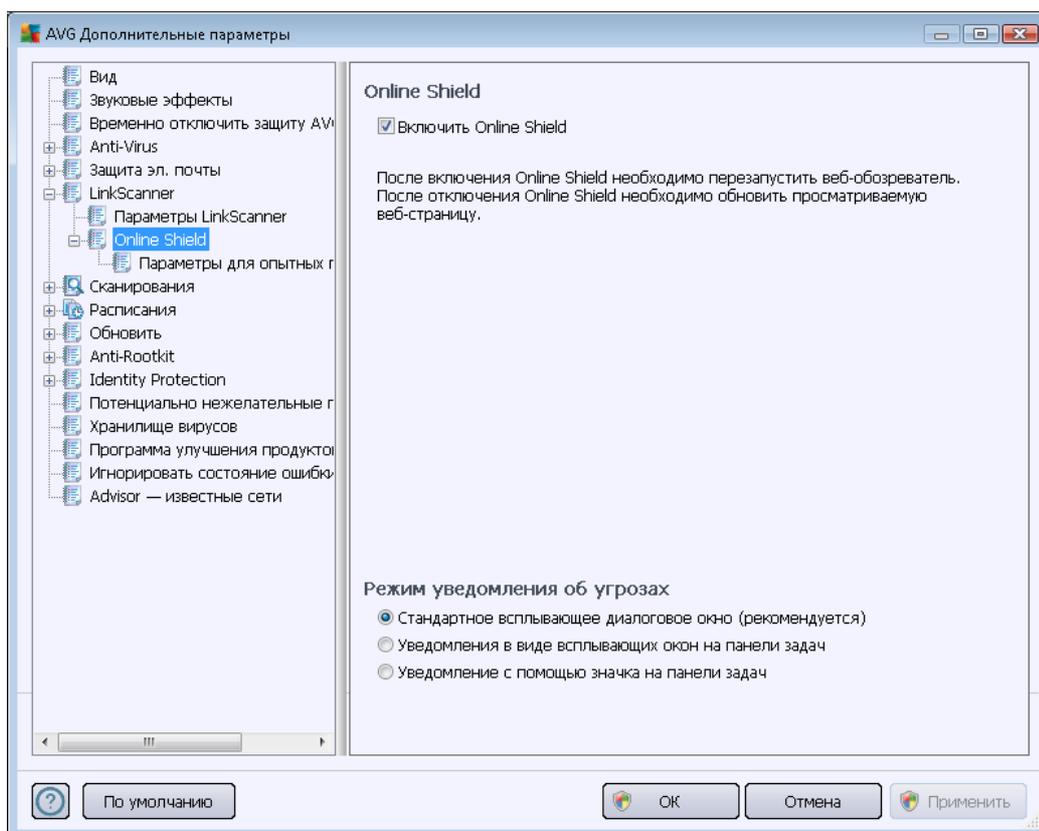


- **Включить Search-Shield (выбрано по умолчанию).** При выполнении поиска в Google, Yahoo!, JP, WebHledani, Яндекс, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg или SlashDot будут отображаться информационные значки,

сообщающие о безопасности найденных веб-сайтов.

- **Включить Surf-Shield** (выбрано по умолчанию). Активная (в реальном времени) защита от доступа к зараженным эксплойтами веб-сайтам. Известные вредоносные сайты и их зараженное эксплойтами содержимое блокируется при доступе к ним через веб-браузер (или любое другое приложение, использующее HTTP).

10.6.2. Online Shield



Диалоговое окно **Online Shield** содержит следующие параметры:

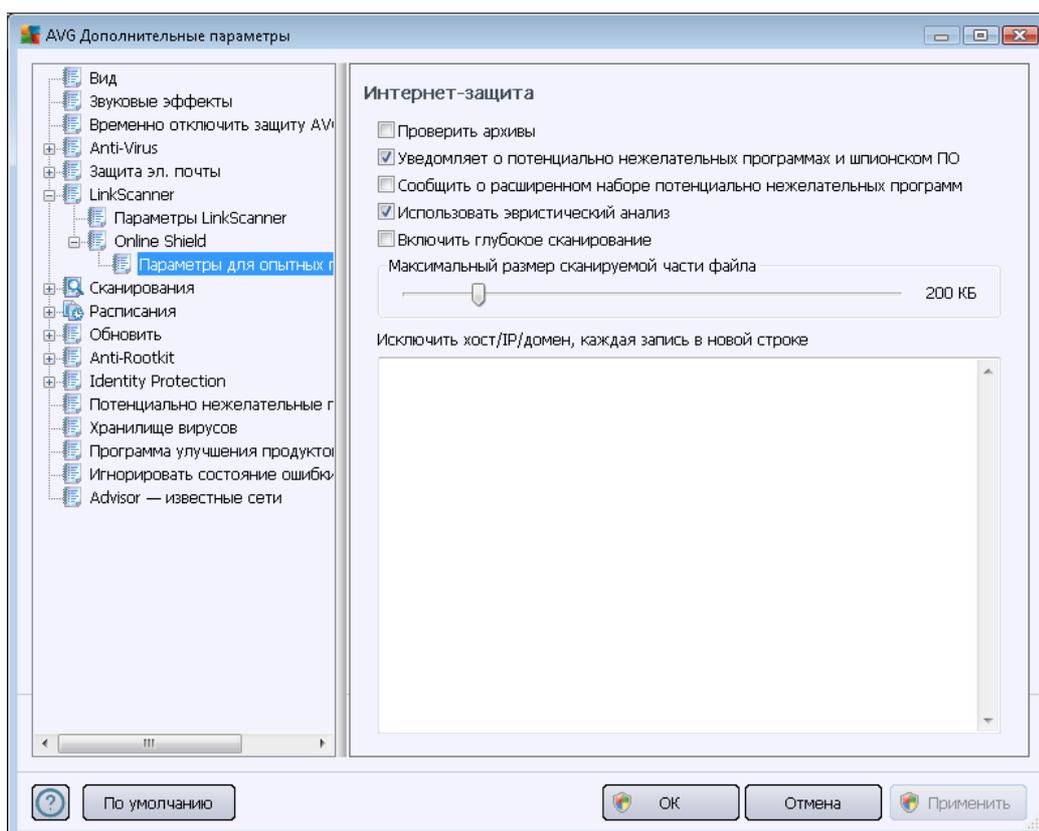
- **Включить Online Shield** (по умолчанию включено). Включение или выключение службы **Online Shield**. Для доступа к другим дополнительным параметрам компонента **Online Shield** перейдите к следующему диалоговому окну [Интернет-защита](#).
- **Включить ускоритель AVG** (по умолчанию включено). Включение или выключение службы **ускорителя AVG**, обеспечивающей более стабильное воспроизведение видеороликов в Интернете, а также ускоряющей процессы загрузки.

Режим уведомления об угрозах

В нижней части диалогового окна выберите способ оповещения о возможной обнаруженной



угрозе: с помощью стандартного всплывающего диалогового окна, уведомления в виде всплывающего окна или уведомления с помощью значка на панели задач.



Диалоговое окно **Интернет-защита** позволяет изменять настройки компонента, относящиеся к сканированию содержимого веб-сайта. Интерфейс редактирования позволяет настроить следующие начальные параметры.

- **Включить интернет-защиту.** Данный параметр подтверждает, что компонент **Online Shield** должен выполнять сканирование содержимого интернет-страниц. Данный параметр (*включен по умолчанию*) позволяет включать/отключать следующие элементы.
 - **Проверка архивов** (*не выбрано по умолчанию*). Сканирование содержимого архивов, которые могут содержаться на отображаемых интернет-страницах.
 - **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО** (*по умолчанию включено*). Установите флажок для активации модуля **Anti-Spyware** и сканирования на наличие шпионского ПО и вирусов. **Шпионские программы** относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- **Уведомлять о расширенном наборе потенциально нежелательных программ** (не выбрано по умолчанию). Установите данный флажок для обнаружения расширенного пакета [шпионского ПО](#). Программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.
- **Использовать эвристический анализ** (выбрано по умолчанию). Сканирование содержимого отображаемой страницы с использованием метода [эвристического анализа](#) (динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде).
- **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (например, при подозрении, что компьютер заражен) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.
- **Максимальный размер файла для сканирования**. Если на отображенной странице имеются файлы, можно выполнить сканирование их содержимого даже до момента их загрузки на компьютер. Однако сканирование больших файлов занимает определенное количество времени и может значительно замедлить загрузку страницы. Используйте полосу прокрутки для определения максимального размера файла, сканирование которого все же необходимо выполнить с помощью компонента **Online Shield**. Даже если размер загруженного файла превышает указанный и файл не будет отсканирован компонентом Online Shield, компьютер все равно будет защищен. Если файл заражен, компонент **Resident Shield** сразу же это обнаружит.
- **Исключить хост/IP-адрес/домен**. В данное текстовое поле можно ввести точное имя сервера (хост, IP-адрес, IP-адрес с маской, URL) или домен, который не должен сканироваться компонентом **Online Shield**. Поэтому следует исключить только тот хост, который точно не содержит вредоносного веб-содержимого.

10.7. Сканирования

Дополнительные параметры сканирования разделены на четыре категории, которые относятся к особым типам сканирования, определенным поставщиком программного обеспечения.

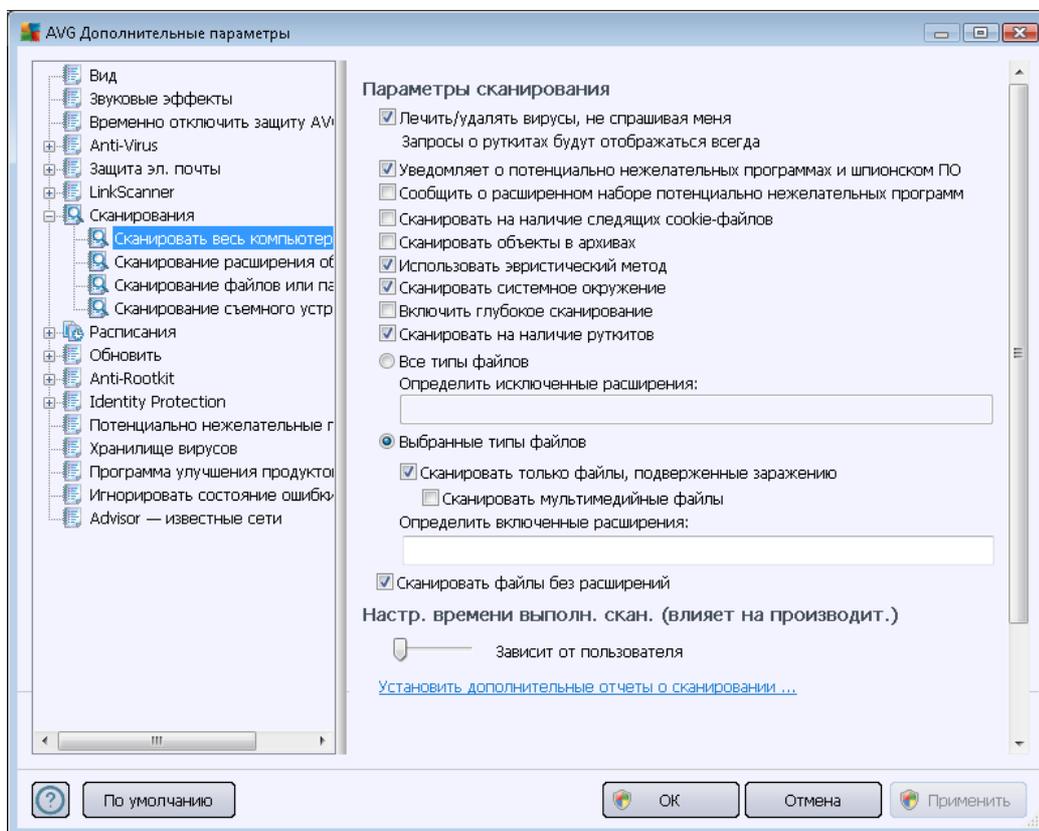
- **Сканирование всего компьютера**. Стандартное предварительно настроенное сканирование всего компьютера.
- **Сканирование расширения оболочки**. Особое сканирование выбранного объекта непосредственно в среде проводника Windows.



- **Сканирование файлов или папок.** Стандартное предварительно настроенное сканирование выбранных областей компьютера.
- **Сканирование съемного устройства.** Специальное сканирование съемных устройств, подключенных к компьютеру.

10.7.1. Сканирование всего компьютера

Параметр **Сканирование всего компьютера** позволяет редактировать параметры одного из сканирований, предварительно определенных производителем — [Сканирование всего компьютера](#).



Параметры сканирования

В разделе **Параметры сканирования** содержатся параметры сканирования, которые можно включить или выключить при необходимости.

- **Автоматически лечить или удалять зараженные вирусами объекты (выбрано по умолчанию).** Обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если не удалось автоматически вылечить зараженный файл, зараженный объект будет перемещен в [хранилище вирусов](#).
- **Уведомлять о потенциально нежелательных программах и угрозах**



появления шпионского ПО (по умолчанию включено). Установите данный флажок для активации модуля [Anti-Spyware](#) и сканирования компьютера на наличие шпионского ПО и вирусов. Шпионские программы относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- **Уведомлять о расширенном наборе потенциально нежелательных программ** (по умолчанию выключено). Установите данный флажок для обнаружения расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.
- **Сканировать на наличие следящих файлов cookie** (не выбрано по умолчанию): благодаря данному параметру компонента [Anti-Spyware](#) осуществляется поиск файлов cookie; (файлы cookie протокола HTTP используются для аутентификации, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзины для покупок через Интернет).
- **Сканировать объекты в архивах** (не выбрано по умолчанию). Благодаря данному параметру при сканировании проверяются все файлы, хранящиеся в архивах, например ZIP, RAR и т. п.
- **Использовать эвристический анализ** (выбрано по умолчанию). Эвристический анализ (динамическая эмуляция команд сканированных объектов в среде виртуального компьютера) является одним из способов, используемых для обнаружения вирусов при сканировании.
- **Сканировать системную среду** (не выбрано по умолчанию). При сканировании также будут проверены системные области компьютера.
- **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (например, при подозрении, что компьютер заражен) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.
- **Сканировать на наличие пакетов программ rootkit** (выбрано по умолчанию). Компонент [Anti-Rootkit](#) сканирует компьютер на возможное наличие пакетов программ rootkit (программы и технологии, позволяющие скрыть вредоносную активность на компьютере). Если программа rootkit обнаружена, это еще не значит, что компьютер заражен. В некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за средства rootkit.

Далее необходимо выбрать файлы для сканирования



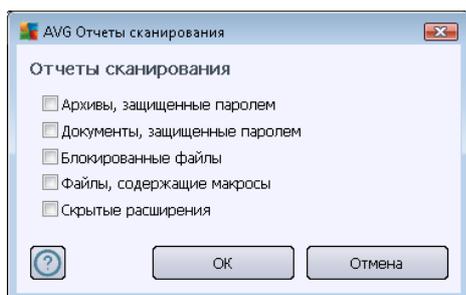
- **Все типы файлов** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми (*после сохранения запятые изменяются на точки с запятой*), сканирование которых проводиться не будет;
- **Выбранные типы файлов.** Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.
- Дополнительно можно установить флажок **Сканировать файлы без расширений.** Он установлен по умолчанию. Рекомендуется не снимать его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

Настройка времени выполнения сканирования

В разделе **Настройка времени выполнения сканирования** можно выбрать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Если необходимо, чтобы сканирование выполнялось быстрее, это займет меньше времени, но во время этого процесса будет значительно увеличено использование системных ресурсов, что снизит производительность других процессов, выполняемых на компьютере (*этот параметр можно включить, если компьютер включен, но не используется*). И наоборот, можно снизить уровень использования системных ресурсов с помощью увеличения продолжительности сканирования.

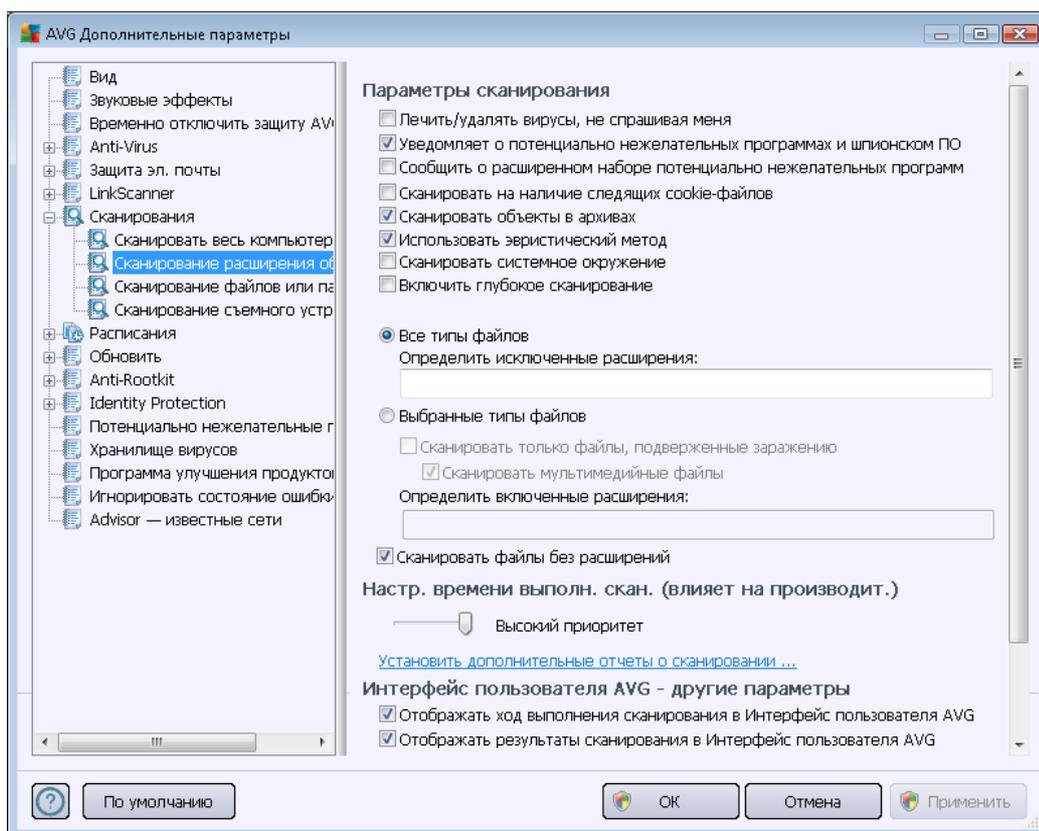
Установить дополнительные отчеты о сканировании ...

Щелкните ссылку **Установить дополнительные отчеты о сканировании**, чтобы открыть диалоговое окно **Отчеты сканирования**, в котором можно выбрать типы объектов, о которых будут выводиться отчеты при сканировании.



10.7.2. Сканирование расширения оболочки

Как и предыдущий элемент [Сканирование всего компьютера](#), элемент **Сканирование расширения оболочки** содержит несколько предварительно установленных поставщиком ПО параметров для настройки сканирования. Данные параметры предназначены для настройки [сканирования определенных объектов, запускаемых непосредственно из проводника Windows \(расширение оболочки\)](#), см. главу [Сканирование в проводнике Windows](#).



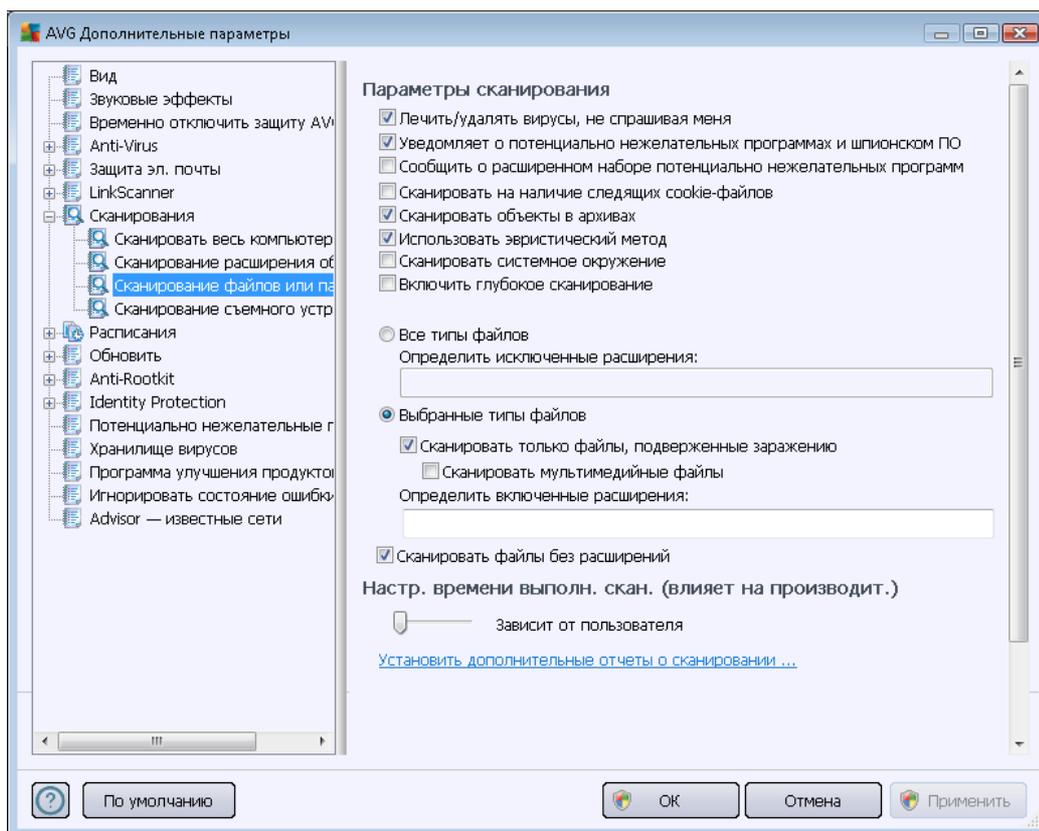
Список параметров соответствует параметрам элемента [Сканирование всего компьютера](#). Однако параметры по умолчанию отличаются (например, при сканировании всего компьютера по умолчанию не выполняется проверка архивов, однако выполняется сканирование системной среды, в то время как при сканировании расширения оболочки дела обстоят по другому).

Примечание. Описание определенных параметров приведено в главе [Расширенные настройки AVG/Сканирования/Сканирование всего компьютера](#).

В отличие от окна [Сканирование всего компьютера](#) диалоговое окно **Сканирование расширения оболочки** содержит раздел **Другие параметры, связанные с интерфейсом пользователя AVG**, в котором можно указать, будет ли отображаться процесс выполнения сканирования и результаты сканирования в интерфейсе пользователя AVG. Также можно настроить, чтобы результаты сканирования отображались только в случае обнаружения заражения при сканировании.

10.7.3. Сканирование определенных файлов или папок

Интерфейс редактирования *Сканирование файлов или папок* выглядит идентично диалоговому окну редактирования [Сканирование всего компьютера](#). Все параметры конфигурации также не отличаются; однако параметры по умолчанию являются более строгими при [сканировании всего компьютера](#):

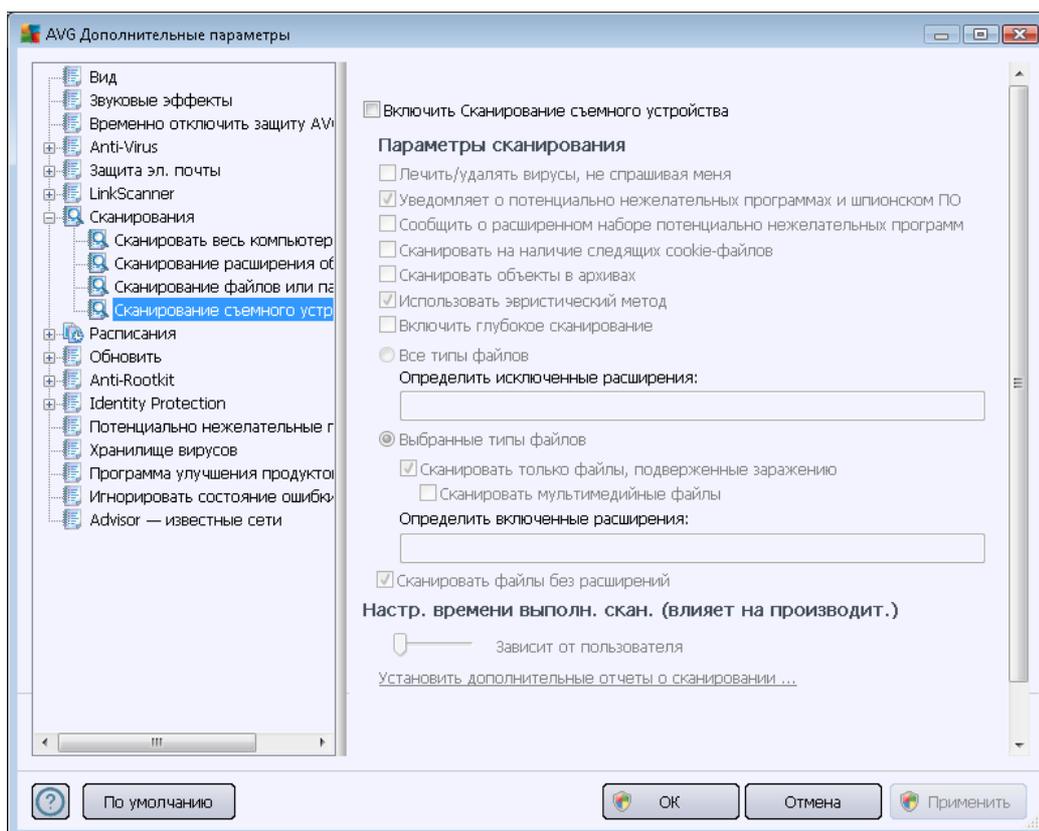


Все параметры, настроенные в этом диалоговом окне конфигурации, применяются только в выбранным для сканирования областям с помощью [Сканирование определенных файлов или папок](#)!

Примечание. Описание определенных параметров приведено в главе [Расширенные настройки AVG/Сканирования/Сканирование всего компьютера](#).

10.7.4. Сканирование съемного устройства

Интерфейс редактирования *Сканирование съемного устройства* выглядит аналогично диалоговому окну редактирования [Сканирование всего компьютера](#).



Диалоговое окно *Сканирование съемного устройства* открывается автоматически после подключения съемного устройства к компьютеру. По умолчанию сканирование отключено. Однако очень важно сканировать съемные устройства на наличие потенциальных угроз, так как они являются основным источником заражений. Чтобы данное сканирование запускалось автоматически, установите флажок **Включить сканирование съемного устройства**.

Примечание. Описание определенных параметров приведено в главе [Расширенные настройки AVG/Сканирования/Сканирование всего компьютера](#).

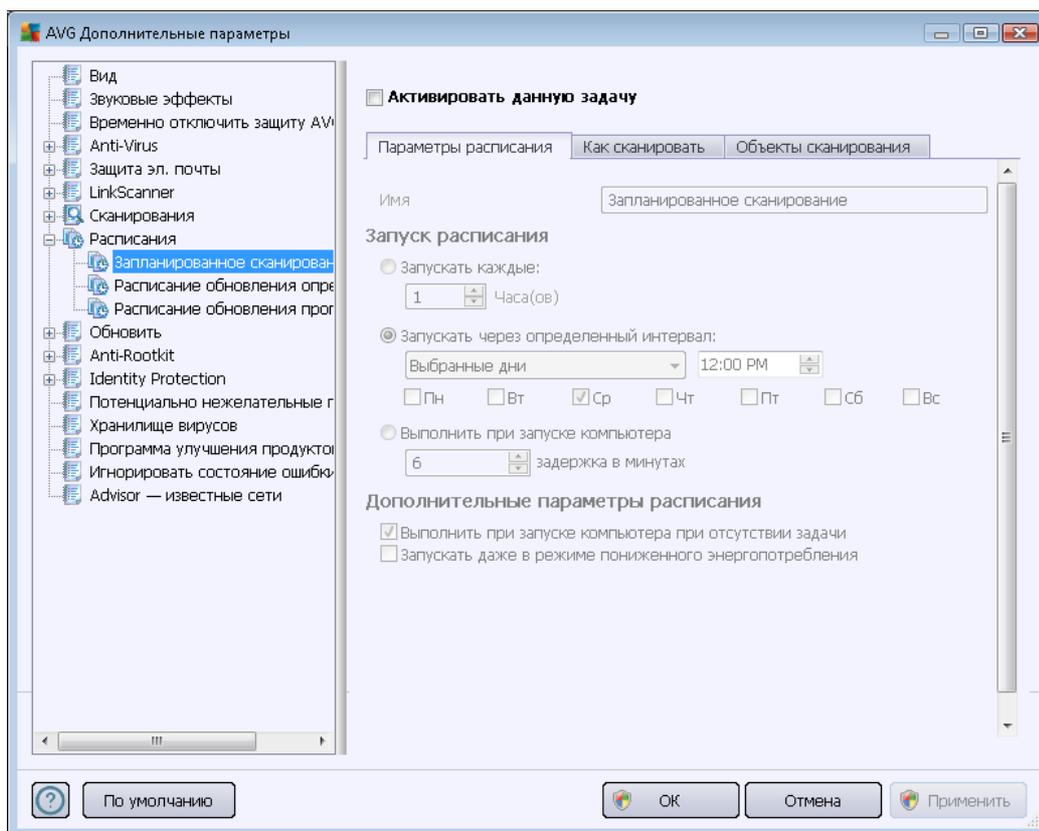
10.8. Расписания

Раздел *Расписания* позволяет изменить стандартные настройки расписания.

- [Запланированное сканирование](#)
- [Расписание обновления определений](#)
- [Расписание обновления программы](#)

10.8.1. Запланированное сканирование

Параметры запланированного сканирования можно изменить (или создать новое расписание) с помощью трех вкладок. На каждой вкладке можно установить/снять флажок **Активировать данную задачу**, чтобы временно отключить запланированную проверку, а затем включить ее при необходимости.



В текстовом поле **Имя** (неактивном для всех расписаний по умолчанию) отображается имя, назначенное данному расписанию поставщиком программы. Для новых расписаний (чтобы добавить новое расписание, щелкните правой кнопкой мыши элемент **Запланированное сканирование** в левом дереве навигации) можно указать собственное имя. При этом текстовое поле будет доступно для редактирования. Старайтесь использовать краткие, содержательные и понятные названия сканирований, так как позже это облегчит их поиск среди остальных сканирований.

Пример. Названия "Новое сканирование" или "Мое сканирование" не являются содержательными, так как не связаны с объектами, которые будут проверяться. И наоборот, название "Сканирование системных областей" является хорошим содержательным названием. Хотя и не обязательно указывать в названии сканирования, является ли оно сканированием всего компьютера или только сканированием выбранных файлов или папок, созданные сканирования будут определяться как разновидности [сканирования выбранных файлов и папок](#).



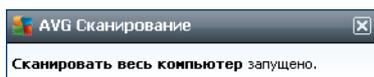
В данном диалоговом окне можно определить следующие параметры сканирования.

Выполняемое расписание

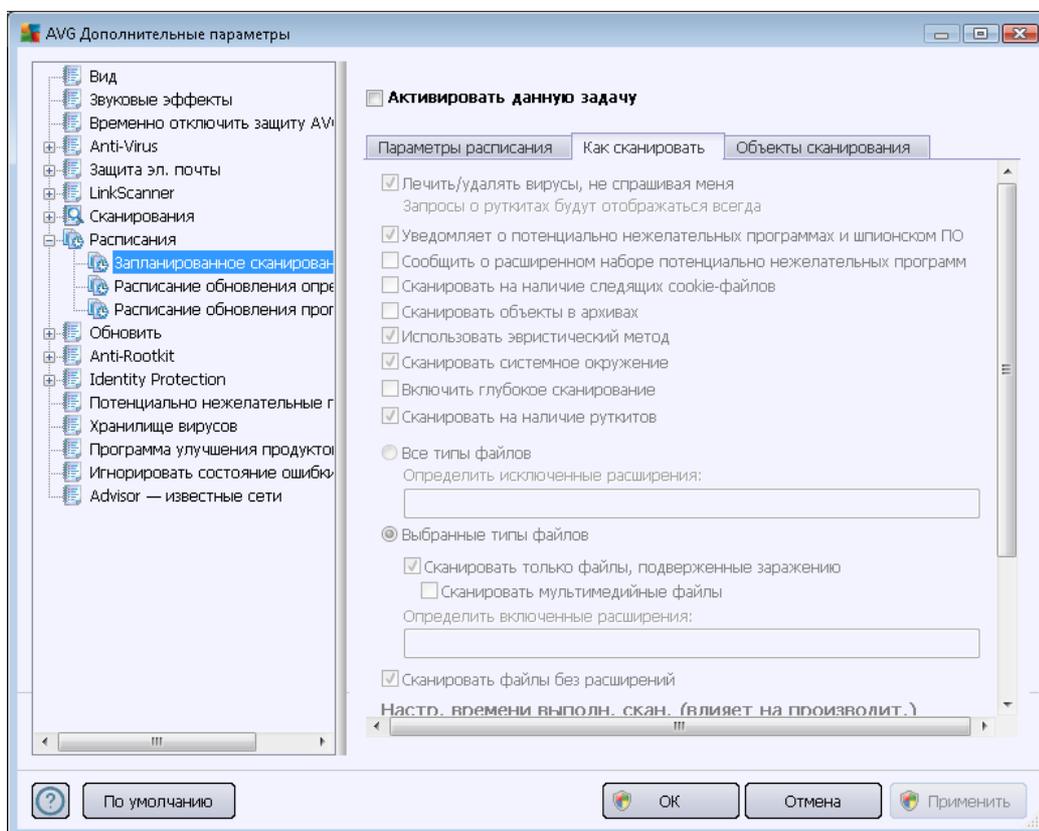
Здесь можно указать временные интервалы запуска нового запланированного сканирования. Запуск процесса сканирования можно назначить через определенные промежутки времени (**Запустить каждые ...**), указав точные дату и время запуска сканирования (**Запустить в определенное время ...**), или определить событие, с которым должен быть связан запуск сканирования (**Запустить при включении компьютера**).

Дополнительные параметры расписания

Данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск сканирования, если компьютер находится в ждущем режиме или полностью выключен. После запуска обновления в указанное время появится всплывающее окно с уведомлением о данном событии над [значком AVG на панели задач](#).



Затем появится новый [значок AVG на панели задач](#) (*цветной мигающий значок*), сообщающий о том, что запланированное сканирование запущено. Щелкните правой кнопкой мыши значок запущенного сканирования AVG, чтобы открыть контекстное меню, с помощью которого можно приостановить, завершить, а также изменить приоритет запущенного сканирования.



На вкладке **Способ сканирования** приведен список параметров сканирования, которые при необходимости можно включить или отключить. По умолчанию большинство параметров включены и используются при сканировании. **Если нет веских оснований для изменения данных параметров, рекомендуется не изменять стандартную конфигурацию.**

- **Автоматически лечить или удалять зараженные вирусами объекты (выбрано по умолчанию):** обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если зараженный файл не удалось вылечить автоматически, зараженный объект будет перемещен в [хранилище вирусов](#).
- **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО (выбрано по умолчанию).** Установите флажок для активации модуля [Anti-Spyware](#) и сканирования на наличие шпионского ПО и вирусов. Шпионские программы относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.
- **Уведомлять о расширенном наборе потенциально нежелательных программ (по умолчанию выключено).** Установите данный флажок для обнаружения расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является



дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- **Сканировать на наличие следящих файлов cookie** (по умолчанию выключено). Данный параметр компонента [Anti-Spyware](#) включает поиск файлов cookie при сканировании; (файлы cookie протокола HTTP используются для аутентификации, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержанием корзины для покупок через Интернет).
- **Сканировать объекты в архивах** (не выбрано по умолчанию). Данный параметр определяет, что при сканировании должны быть проверены все файлы, даже те, которые находятся в архивах некоторых типов, например ZIP, RAR и других.
- **Использовать эвристический анализ** (выбрано по умолчанию). Эвристический анализ (динамичная эмуляция команд сканированных объектов в виртуальной компьютерной среде) является одним из способов, используемых для выявления вирусов при сканировании.
- **Сканировать системную среду** (выбрано по умолчанию). В результате сканирования также будут проверены участки системы компьютера.
- **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (например, при подозрении заражения компьютера) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.
- **Сканировать на наличие пакетов программ rootkit** (выбрано по умолчанию). Компонент [Anti-Rootkit](#) сканирует компьютер на возможное наличие пакетов программ rootkit (программы и технологии, позволяющие скрыть вредоносную активность на компьютере). Если программа rootkit обнаружена, это еще не значит, что компьютер заражен. В некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за средства rootkit.

Далее необходимо выбрать файлы для сканирования

- **Все типы файлов** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми (после сохранения запятые изменяются на точки с запятой), сканирование которых проводиться не будет;
- **Выбранные типы файлов.** Можно указать сканирование только тех файлов, которые подвержены заражению (файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы), включая мультимедийные файлы (видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.

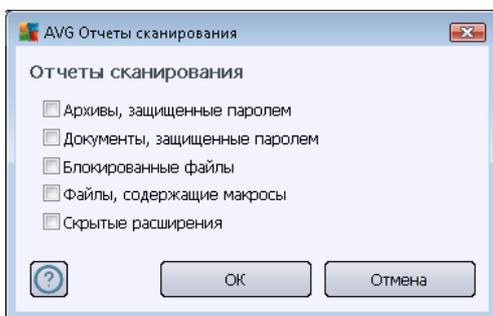
- Дополнительно можно установить флажок **Сканировать файлы без расширений**. Он установлен по умолчанию. Рекомендуется не снимать его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

Настройка времени выполнения сканирования

В разделе **Настройка времени выполнения сканирования** можно выбрать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Если необходимо, чтобы сканирование выполнялось быстрее, это займет меньше времени, но во время этого процесса будет значительно увеличено использование системных ресурсов, что снизит производительность других процессов, выполняемых на компьютере (*этот параметр можно включить, если компьютер включен и не используется*). И наоборот, можно снизить уровень использования системных ресурсов с помощью увеличения продолжительности сканирования.

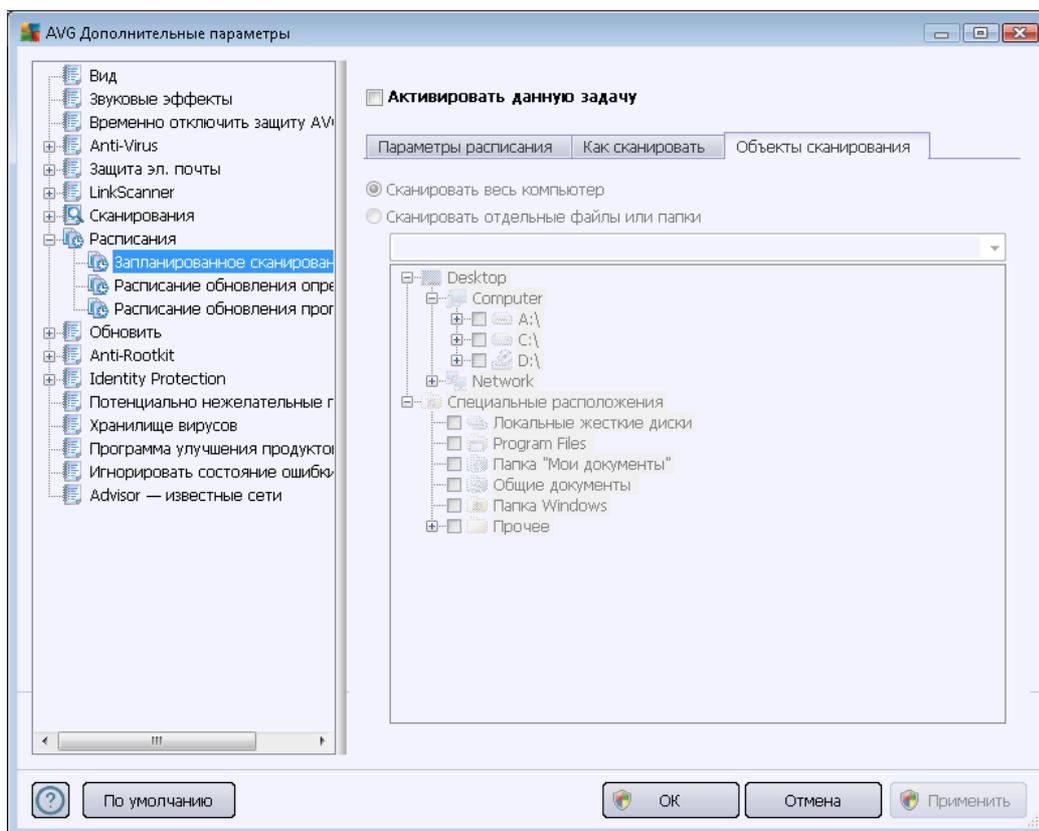
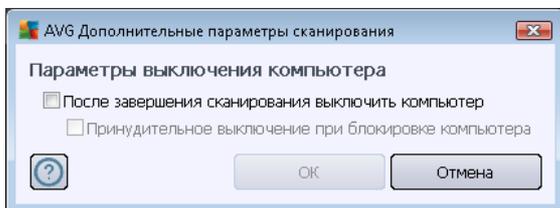
Установить дополнительные отчеты о сканировании

Щелкните ссылку **Установить дополнительные отчеты о сканировании**, чтобы открыть диалоговое окно **Отчеты сканирования**, в котором можно выбрать типы объектов, о которых будут выводиться отчеты при сканировании.



Дополнительные параметры сканирования

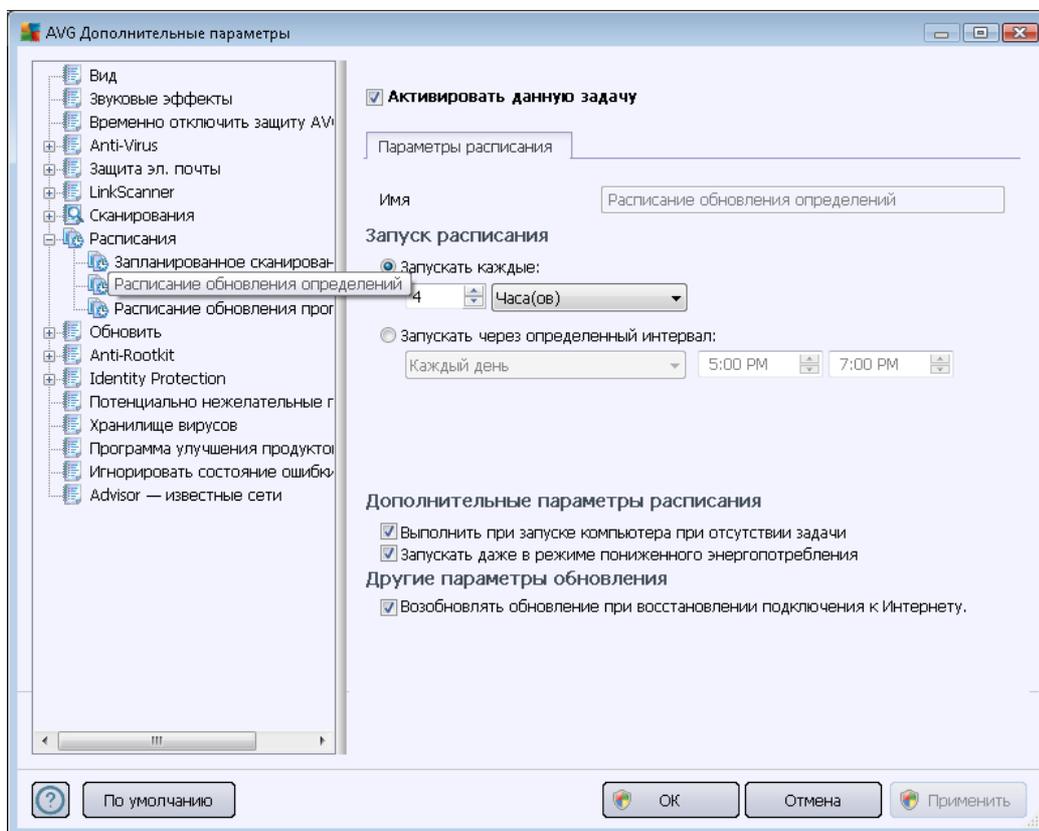
Щелкните ссылку **Дополнительные параметры сканирования ...**, чтобы открыть новое диалоговое окно **Параметры выключения компьютера**, с помощью которого можно настроить автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (**Выключить компьютер после завершения сканирования**) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (**Принудительное выключение при блокировке компьютера**).



На вкладке **Объекты сканирования** можно запланировать [сканирование всего компьютера](#) или [сканирование отдельных файлов и папок](#). Если выбрать сканирование определенных файлов и папок, в нижней части этого диалогового окна станет активной отображаемая древовидная структура, в которой можно указать сканируемые папки.

10.8.2. Расписание обновления определений

В случае **крайней необходимости** можно снять флажок **Активировать данную задачу**, чтобы временно отключить запланированное обновление программы, и включить его в любое время позже.



В данном диалоговом окне можно настроить более подробные параметры расписания обновления. В текстовом поле **Имя** (неактивном для всех расписаний по умолчанию) отображается имя, назначенное данному расписанию поставщиком программы.

Выполняемое расписание

В этом разделе необходимо указать временные интервалы для нового запланированного запуска обновления. Можно определить время запуска обновления через определенные промежутки времени (**Запускать каждые...**) или указать точные дату и время запуска (**Запускать в определенное время...**).

Дополнительные параметры расписания

Данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск обновления компонента, если компьютер работает в ждущем режиме или выключен.

Другие параметры обновления

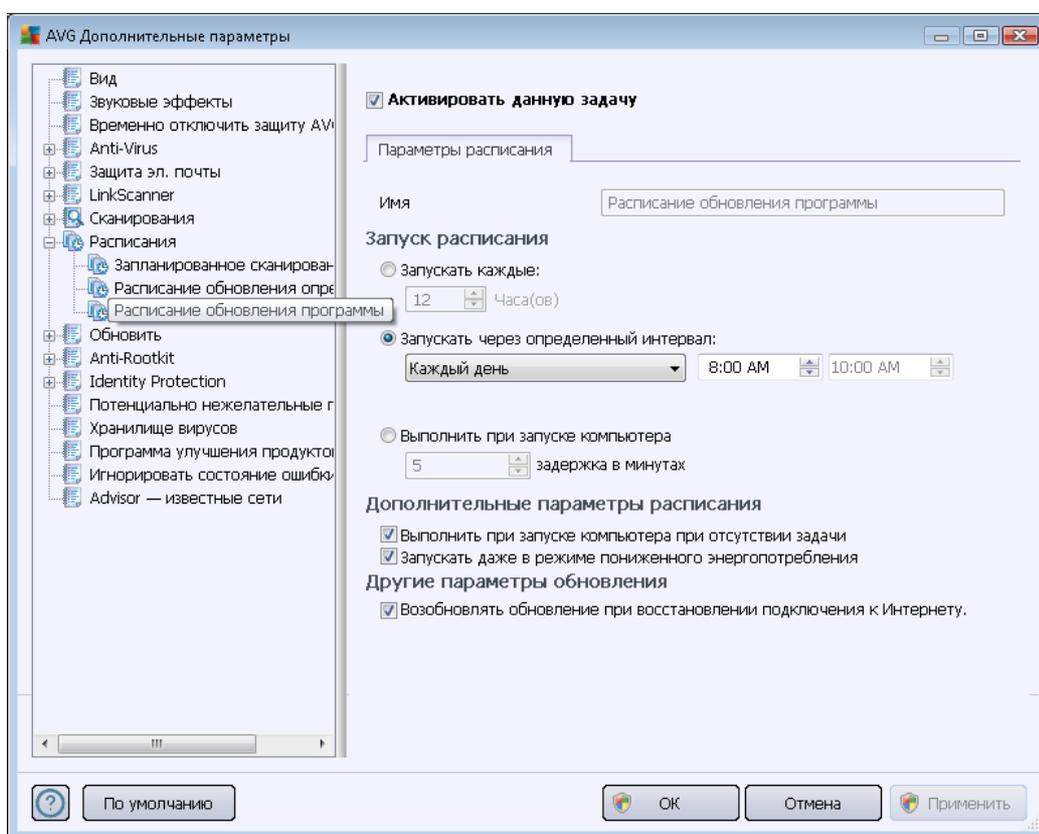
Установите флажок **Возобновлять обновление при восстановлении подключения к**



Интернету, чтобы в случае разрыва соединения с Интернетом и сбоя процесса обновления обновление было выполнено сразу после восстановления подключения к Интернету. После запуска запланированного обновления отображается всплывающее окно с уведомлением о данном событии над [значком AVG на панели задач](#) (если параметры по умолчанию диалогового окна [Дополнительные параметры/Внешний вид](#) не были изменены).

10.8.3. Расписание обновления программы

В случае **крайней необходимости** можно снять флажок **Активировать данную задачу**, чтобы временно деактивировать запланированное обновление программы, и включить его позже в любое время.



В текстовом поле **Имя** (неактивном для всех расписаний по умолчанию) отображается имя, назначенное данному расписанию поставщиком программы.

Выполняемое расписание

Укажите временные интервалы для запуска нового запланированного обновления программы. Можно определить время запуска обновления через определенные промежутки времени (**Запускать каждые...**), указать точные дату и время запуска (**Запускать в определенное время...**) или определить событие, с которым должен быть связан запуск обновления (**Действие связано с включением компьютера**).



Дополнительные параметры расписания

Данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск обновления программы, если компьютер работает в энергосберегающем режиме или выключен.

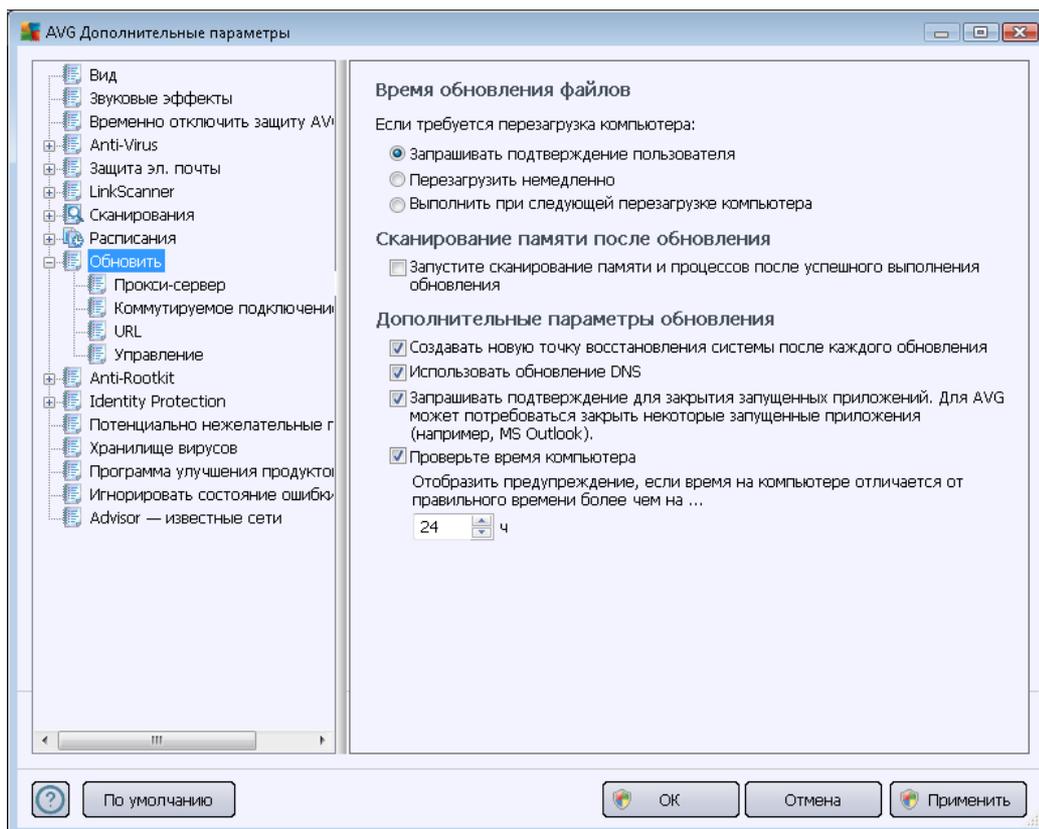
Другие параметры обновления

Установите флажок **Возобновлять обновление при восстановлении подключения к Интернету**, чтобы в случае разрыва соединения с Интернетом и сбое процесса обновления компонента обновление выполнялось сразу же после восстановления подключения к Интернету. После запуска запланированного обновления отображается всплывающее окно с уведомлением о данном событии над [значком AVG на панели задач](#) (если параметры по умолчанию диалогового окна [Дополнительные параметры/Внешний вид](#) не были изменены).

Примечание. Если запланированное обновление программы и сканирование пересекутся по времени, сканирование будет прервано, так как процесс обновления имеет более высокий приоритет.

10.9. Обновление

Элемент навигации **Обновление** открывает новое диалоговое окно, в котором можно указать общие параметры обновления продукта [AVG](#):



Время обновления файлов

В данном разделе можно выбрать один из трех альтернативных параметров, которые будут использоваться, если в процессе обновления потребуется перезагрузка ПК. Завершение обновления можно запланировать на следующую перезагрузку ПК, или можно выполнить перезагрузку сразу же.

- **Запрашивать подтверждение пользователя (по умолчанию).** Отобразится запрос на подтверждение перезагрузки ПК, необходимой для завершения [процесса](#) обновления
- **Мгновенная перезагрузка.** Перезагрузка будет выполнена автоматически сразу после завершения процесса [обновления](#). Запрос на подтверждение отображаться не будет.
- **Завершить при следующей перезагрузке компьютера.** Завершение процесса [обновления](#) будет отложено до следующей перезагрузки. Помните, что данный параметр рекомендуется выбирать, только если компьютер включается регулярно, как



минимум раз в день!

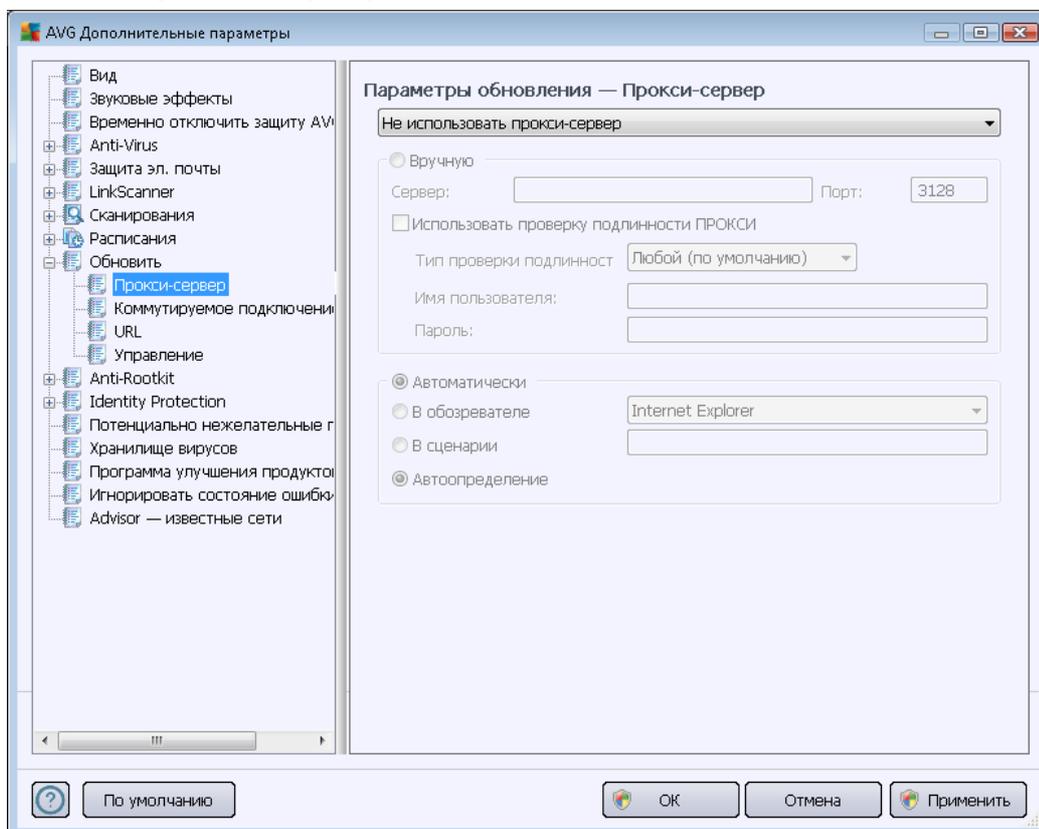
Сканирование памяти после обновления

Установите этот флажок, если требуется запускать сканирование памяти после каждого успешно завершеного обновления. Последнее загруженное обновление может содержать новые определения вирусов, которые сразу должны быть применены при сканировании.

Дополнительные параметры обновления

- **Создавать новую точку восстановления системы после каждого обновления программы.** Перед каждым запуском обновления программы AVG будет создаваться точка восстановления системы. Если не удастся выполнить обновление или произойдет сбой в работе ОС, всегда можно будет восстановить начальную конфигурацию ОС с этой точки. Данный параметр доступен в меню Пуск/Все программы/Стандартные/Служебные/Восстановление системы. Однако любые изменения следует вносить только опытным пользователям. Не снимайте этот флажок, если данный параметр будет использоваться.
- **Использовать обновление DNS (включено по умолчанию).** Если данный флажок установлен, после запуска обновления программа **AVG Anti-Virus 2012** запросит на сервере DNS сведения о последней версии вирусной базы данных и программы. После этого будут загружены и установлены только самые маленькие обязательные файлы обновления. Таким образом, удастся уменьшить количество загружаемых данных и выполнить процесс быстрее.
- **Запрашивать подтверждение на закрытие запущенных приложений (по умолчанию включено).** Благодаря этой функции пользователи могут быть уверены, что ни одно из запущенных приложений не будет закрыто без соответствующего разрешения (если это необходимо для завершения процесса обновления).
- **Проверять время компьютера.** Установите данный флажок для отображения уведомления в случаях, когда время компьютера отличается от правильного на указанное количество часов.

10.9.1. Прокси-сервер



Прокси-сервер — это автономный сервер или служба, запущенная на ПК и гарантирующая безопасное подключение к Интернету. В соответствии с определенными правилами сетей доступ к Интернету можно получить напрямую или через прокси-сервер; оба способа могут использоваться одновременно. В раскрывающемся списке первой части диалогового окна **Параметры обновления — Прокси-сервер** выберите необходимые действия.

- **Использовать прокси-сервер**
- **Не использовать прокси-сервер** (выбрано по умолчанию)
- **Подключиться через прокси-сервер, если не удастся, подключиться напрямую**

При выборе параметров, использующих прокси-сервер, необходимо указать некоторые дополнительные данные. Параметры сервера можно настроить автоматически или вручную.

Настройка вручную

При выборе настройки вручную (выберите параметр **Вручную**, чтобы активировать соответствующий раздел диалогового окна) необходимо указать следующие данные.



- **Сервер.** Укажите IP-адрес или имя сервера.
- **Порт.** укажите номер порта, через который осуществляется подключение к Интернету (номер по умолчанию — 3128, но можно задать и другой номер — если вы не уверены в правильности номера порта, обратитесь к системному администратору)

На прокси-сервере также могут быть заданы определенные правила для каждого пользователя. В этом случае установите флажок **Использовать проверку подлинности ПРОКСИ**, чтобы программа выполняла проверку подлинности имени пользователя и пароля перед подключением к Интернету через прокси-сервер.

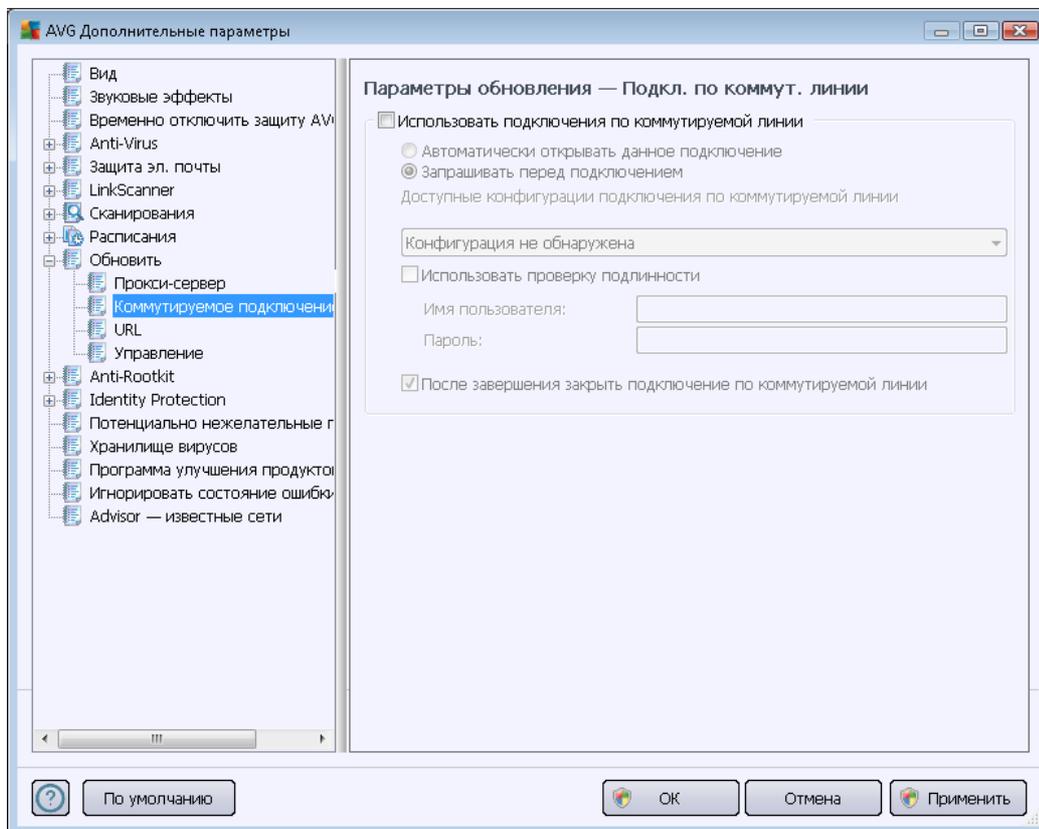
Автоматическая настройка

В случае выбора автоматической настройки (установите флажок **Автоматически**, чтобы активировать соответствующий раздел диалогового окна), а затем выберите необходимый источник конфигурации прокси-сервера.

- **Из браузера.** конфигурация будет считана с интернет-браузера по умолчанию
- **Из сценария.** конфигурация будет считана с загруженного сценария с функцией возврата адреса прокси-сервера
- **Автоопределение.** конфигурация будет определена автоматически непосредственно на прокси-сервере

10.9.2. Подключение по коммутируемой линии

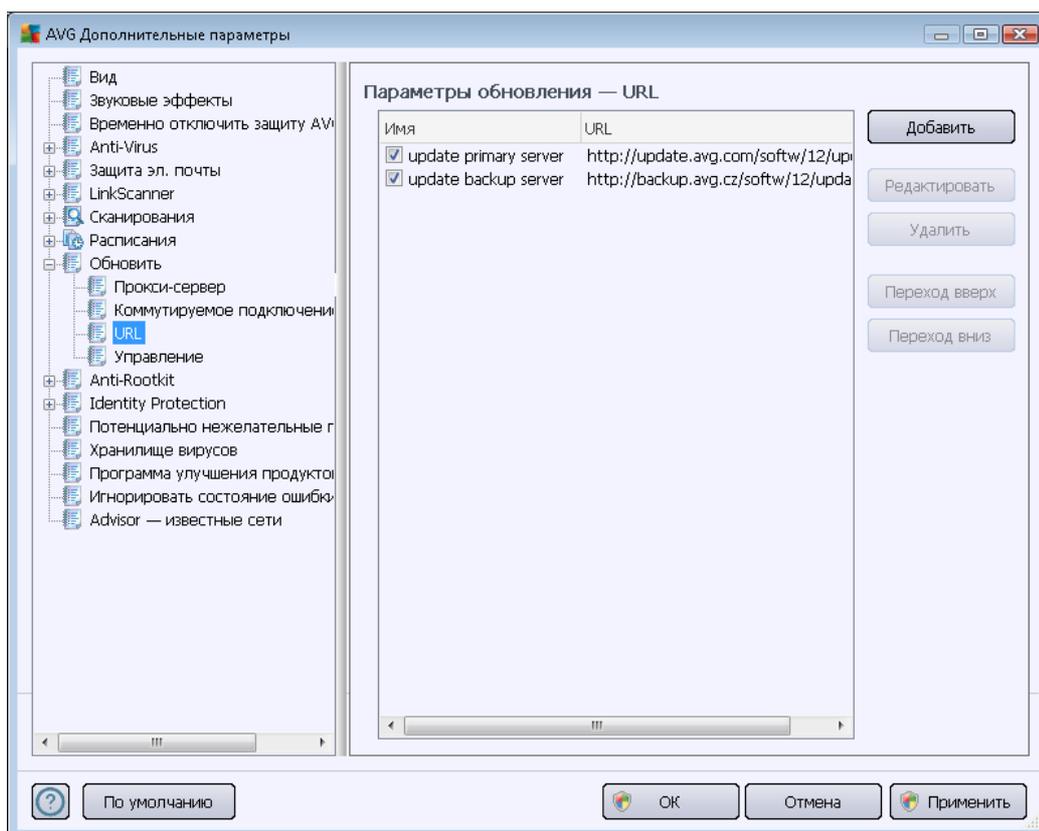
Все параметры, дополнительно заданные в диалоговом окне **Параметры обновления** — **подключение по коммутируемой линии**, относятся к подключению к Интернету по коммутируемой линии. Чтобы активировать поля диалогового окна, выберите параметр **Использовать подключения по коммутируемой линии**:



Укажите способ подключения к Интернету: автоматически (**Автоматическое открытие подключения**), подтверждение каждого подключения вручную (**Спрашивать перед подключением**). Для автоматического подключения также можно определить автоматическое закрытие подключения после обновления (**Автоматически закрыть подключение по коммутируемой линии по завершении**).

10.9.3. URL-адрес

В диалоговом окне **URL-адрес** приведен список интернет-адресов, по которым можно загрузить файлы обновлений.



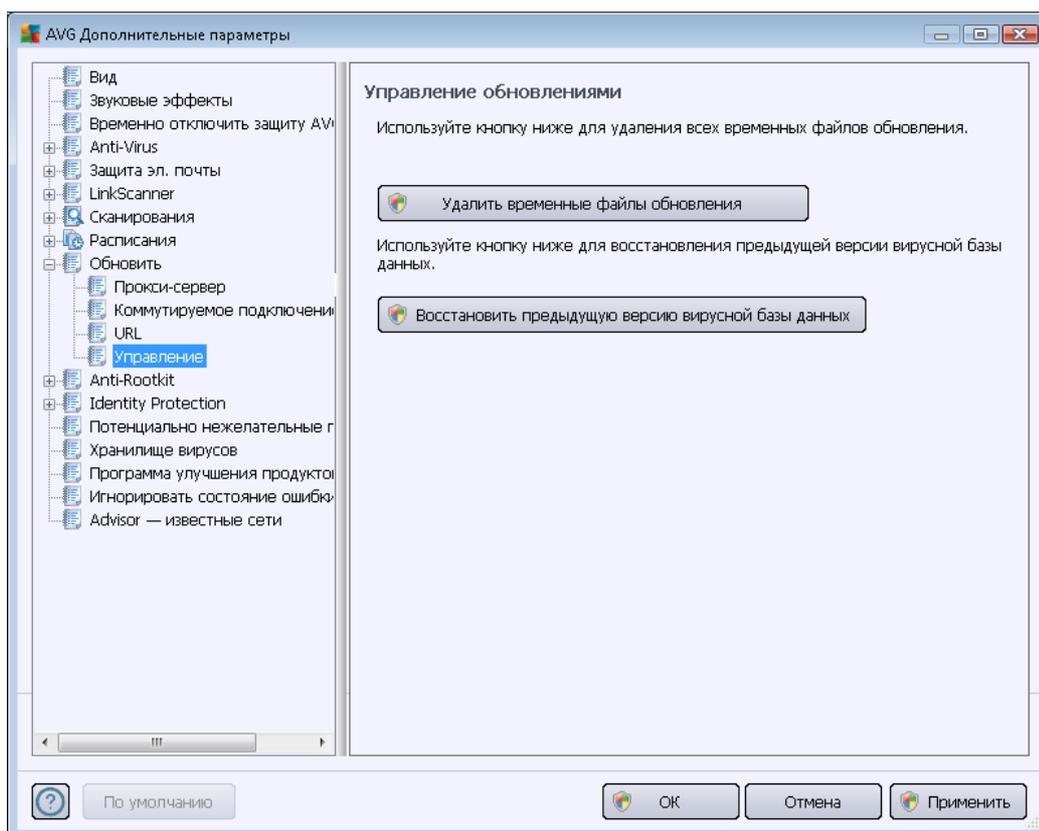
Кнопки управления

Данный список и его элементы можно изменить с помощью следующих кнопок управления:

- **Добавить.** Открывает диалоговое окно, в котором можно указать новый URL-адрес для добавления в список.
- **Редактировать.** Открывает диалоговое окно, в котором можно изменить параметры выбранного URL-адреса.
- **Удалить.** позволяет удалить выбранный URL-адрес из списка.
- **Вверх.** позволяет переместить выбранный URL-адрес на строку выше.
- **Вниз.** позволяет переместить выбранный URL-адрес на строку ниже.

10.9.4. Управление

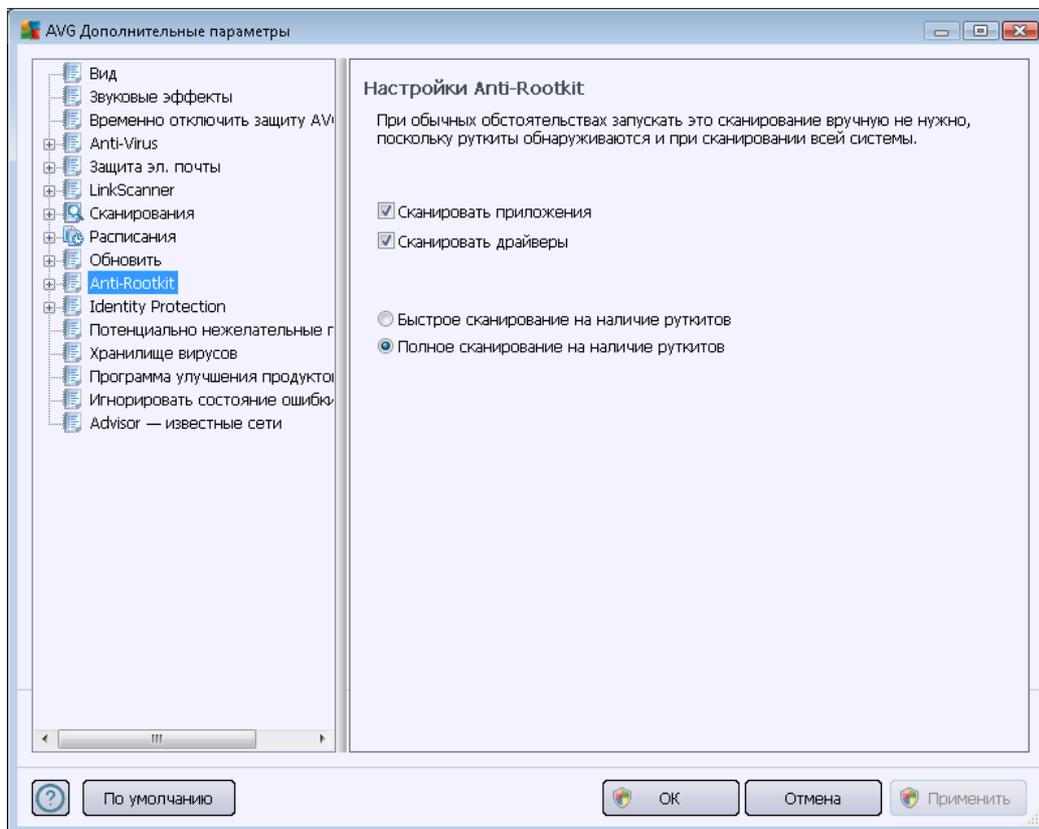
В диалоговом окне **Управление обновлениями** предлагаются два параметра, доступ к которым можно получить с помощью двух кнопок.



- **Удалить временные файлы обновлений.** Нажмите данную кнопку, чтобы удалить все резервные файлы обновлений с жесткого диска (*по умолчанию эти файлы сохраняются в течение 30 дней*)
- **Восстановить предыдущую версию вирусной базы данных.** Нажмите эту кнопку, чтобы удалить последнюю версию вирусной базы данных с компьютера и восстановить версию, сохраненную ранее (*новая версия базы данных будет входить в следующий пакет обновления*).

10.10. Anti-Rootkit

Диалоговое окно **Настройка Anti-Rootkit** позволяет изменять настройки конфигурации компонента [Anti-Rootkit](#) и определенные настройки сканирования Anti-Rootkit. Сканирование Anti-Rootkit — это выбранный по умолчанию процесс, запускающийся вместе с функцией [Сканирование всего компьютера](#).



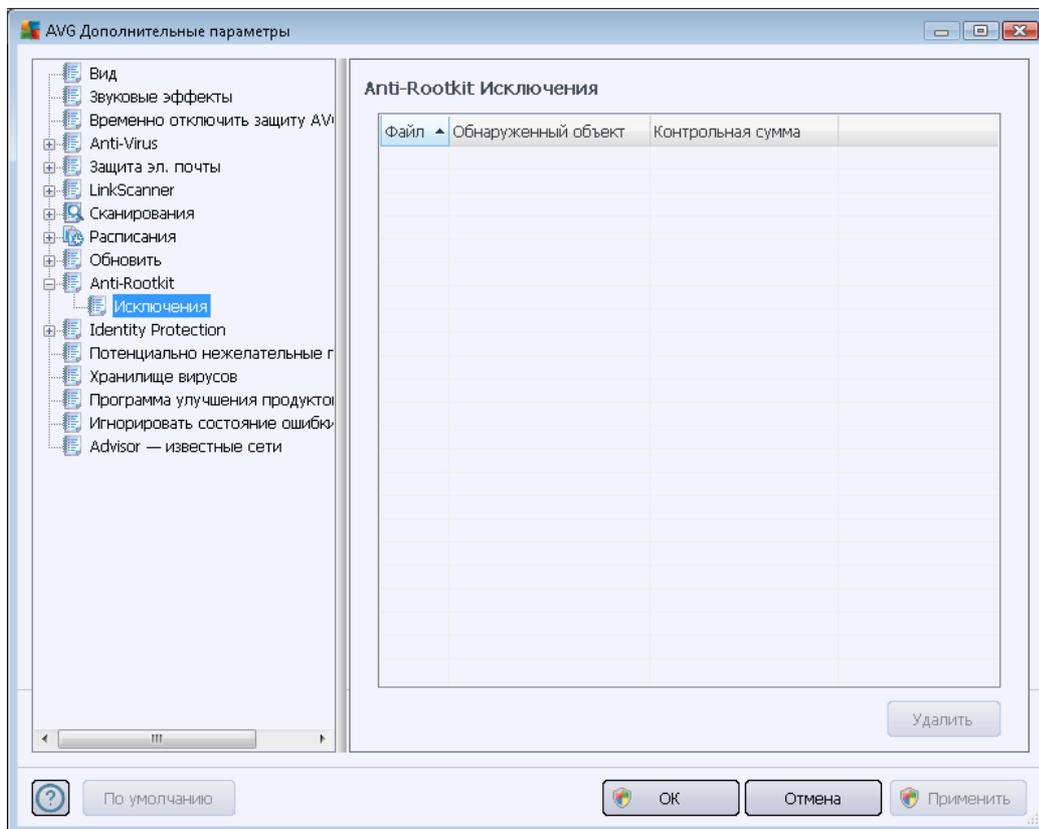
Возможность изменения всех функций компонента [Anti-Rootkit](#), доступная в данном диалоговом окне, также доступна непосредственно в [интерфейсе компонента Anti-Rootkit](#).

Функции **Сканирование приложений** и **Сканирование драйверов** позволяют четко определить, что должно быть включено в сканирование Anti-Rootkit. Данные настройки предназначены для опытных пользователей. Рекомендуется, чтобы все параметры были включены. Далее можно выбрать режим сканирования на наличие пакетов программ rootkit:

- **Быстрое сканирование rootkit.** Сканирование всех запущенных процессов, загруженных драйверов и системных папок (*обычно c:\Windows*).
- **Полное сканирование rootkit.** Сканирование всех запущенных процессов, загруженных драйверов, системных папок (*обычно c:\Windows*), а также локальных жестких дисков (*в том числе съемные накопители, кроме дисководов и привода компакт-дисков*).

10.10.1. Исключения

В окне **Исключения Anti-Rootkit** можно определить файлы (*например, некоторые драйверы, которые могут быть ошибочно приняты за средства rootkit*), которые следует исключить из процесса сканирования.

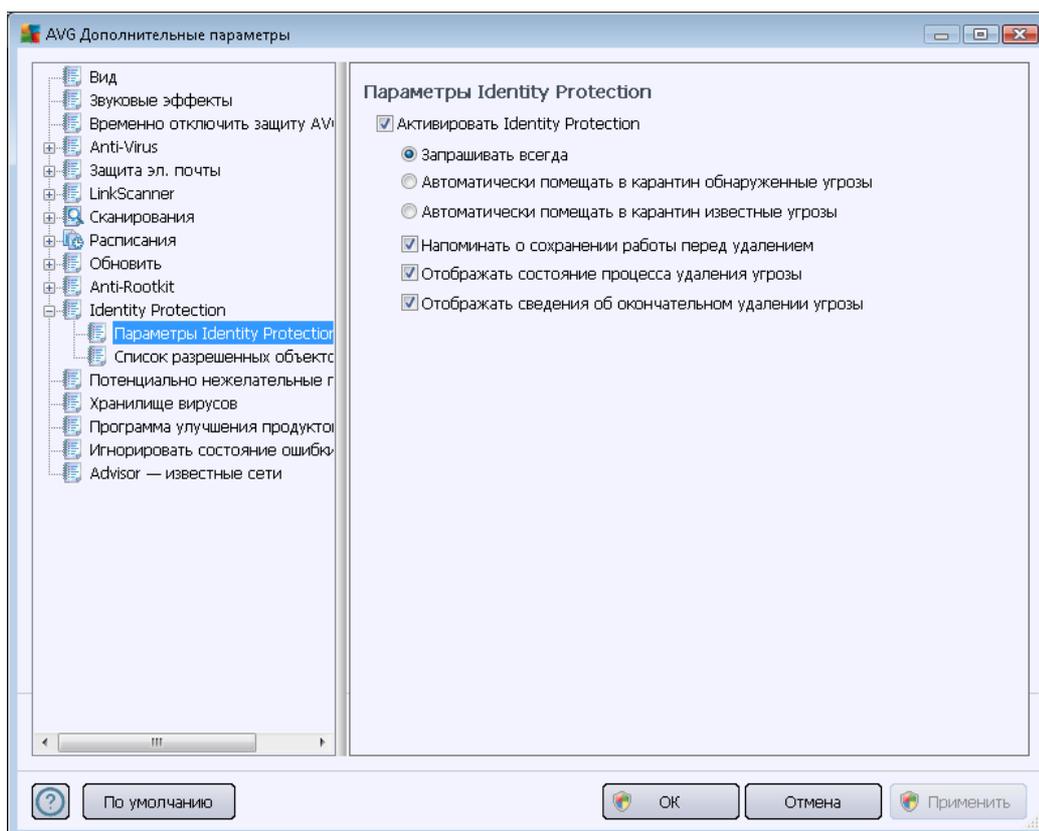


10.11. Identity Protection

Identity Protection — это компонент, предназначенный для защиты компьютера от всех видов вредоносного ПО (*шпионского ПО, программ-роботов, программ для кражи личных данных и т. п.*) с помощью технологий определения моделей поведения. Это приложение также обеспечивает защиту "нулевого дня" от новых вирусов (*более подробное описание функций компонента можно получить в разделе [Identity Protection](#)*).

10.11.1. Параметры компонента Identity Protection

В окне *Параметры Identity Protection* можно включить или отключить основные функции компонента [Identity Protection](#).



Включить Identity Protection (выбрано по умолчанию). Снимите флажок, чтобы отключить компонент [Identity Protection](#).

Настоятельно рекомендуется не выполнять данное действие без необходимости.

Если компонент [Identity Protection](#) активирован, можно определить его действия при обнаружении угрозы.

- **Запрашивать всегда** (выбрано по умолчанию). При обнаружении угрозы отобразится запрос на перемещение опасного объекта в карантин, чтобы избежать случайного удаления запускаемых приложений.
- **Автоматически помещать в карантин обнаруженные угрозы.** Установите флажок, чтобы все обнаруженные угрозы сразу же помещались в безопасное место — [хранилище вирусов](#). В случае сохранения параметров по умолчанию при обнаружении угрозы отобразится запрос на перемещение опасного объекта в карантин, чтобы избежать случайного удаления запускаемых приложений.
- **Автоматически помещать в карантин известные угрозы.** Установите этот флажок, чтобы все приложения, определенные в качестве возможного вредоносного



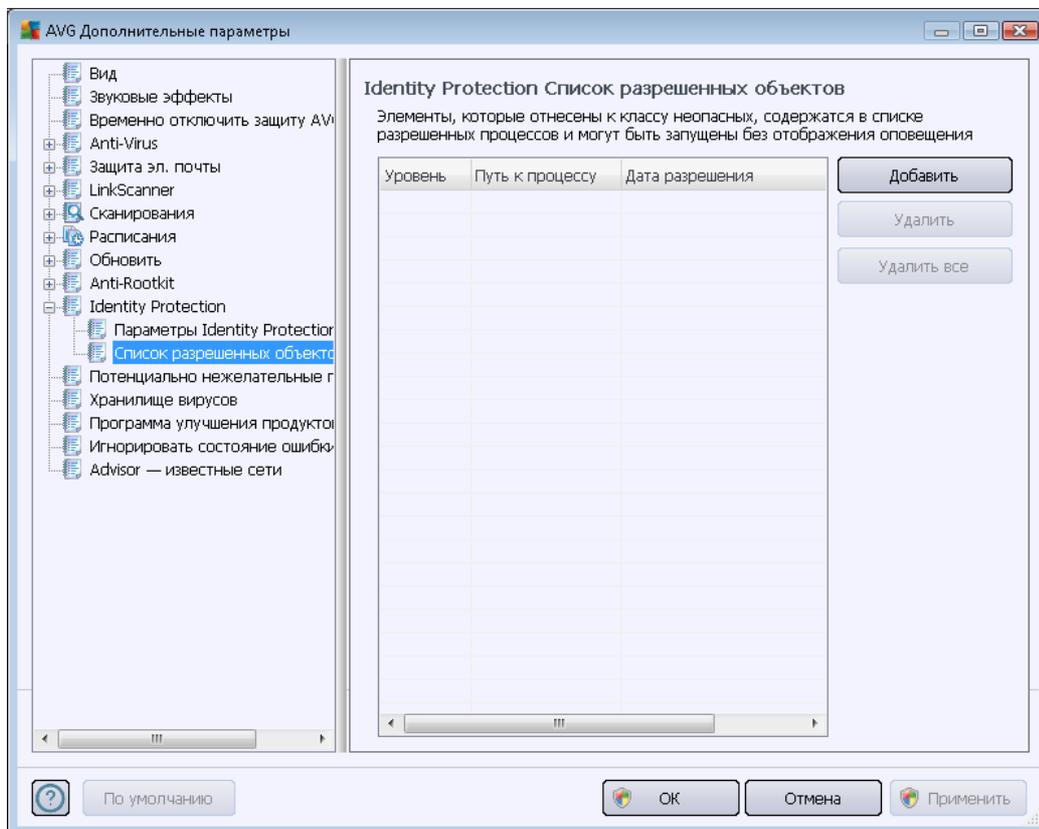
ПО, автоматически перемещались в [хранилище вирусов](#).

Также можно назначить определенные элементы для запуска других функций [Identity Protection](#).

- **Отображать запрос на сохранение текущей работы перед удалением** (выбрано по умолчанию). Установите этот флажок, чтобы получать предупреждение перед удалением или помещением в карантин приложений, определенных как возможное вредоносное ПО. В случае, если вы работаете с приложением, необходимо сохранить текущий проект, чтобы избежать потери несохраненных данных. По умолчанию данный параметр включен, рекомендуется не изменять значение для этого параметра.
- **Отображать состояние процесса удаления угроз** (выбрано по умолчанию). Если данный параметр включен, при обнаружении потенциально вредоносного ПО откроется новое диалоговое окно, отображающее состояние процесса перемещения вредоносного ПО в карантин.
- **Отображать сведения об окончательном удалении угрозы** (выбрано по умолчанию). Если выбран данный параметр, в окне **Защита личной информации** отображается детальная информация о каждом перемещенном в карантин объекте (уровень опасности, местоположение и т. п.).

10.11.2. Список разрешенных объектов

Если в диалоговом окне **Параметры Identity Protection** не выбран параметр **Автоматически помещать в карантин обнаруженные угрозы**, каждый раз при обнаружении возможного вредоносного ПО будет отображаться запрос на удаление. Если затем назначить подозрительному приложению статус (*определено по типу поведения*) безопасного и подтвердить, что оно должно оставаться на компьютере, это приложение будет добавлено в так называемый **Список разрешенных процессов Identity Protection** и не будет определяться в дальнейшем как потенциально опасное.



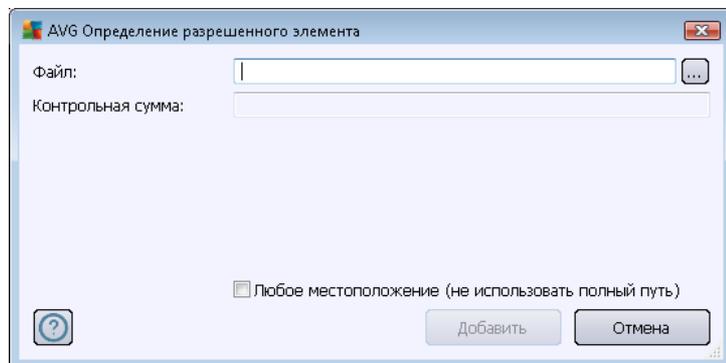
Список разрешенных процессов Identity Protection предоставляет следующие сведения по каждому элементу:

- **Уровень.** Графическое определение уровня опасности соответствующих процессов по 4-уровневой шкале от наименее важной (■□□□) до критической (■□■□).
- **Путь к процессу.** Путь к местоположению исполняемого файла приложения (процесса).
- **Дата разрешения.** Дата, когда приложение вручную было отмечено как безопасное.

Кнопки управления

В диалоговом окне **Список разрешенных элементов Identity Protection** имеются следующие кнопки управления.

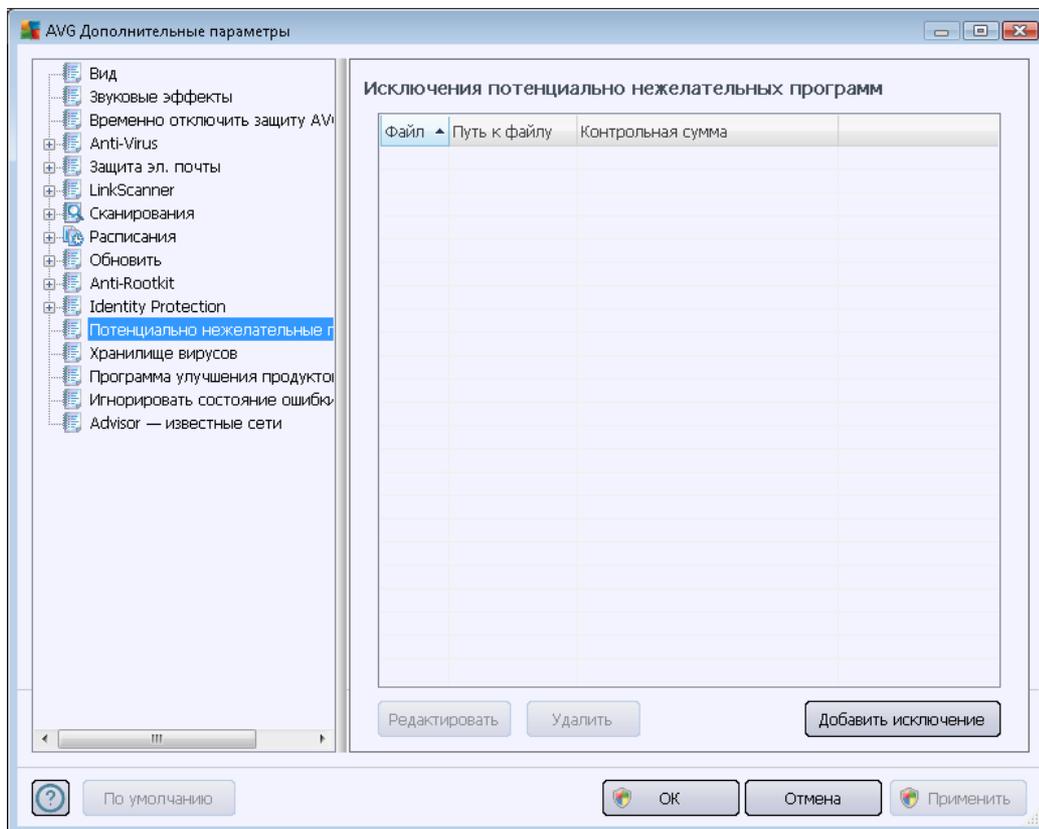
- **Добавить.** Нажмите эту кнопку, чтобы добавить приложение в список разрешенных элементов. Всплывающие диалоговые окна.



- **Файл.** Введите полный путь к файлу (*приложению*), который необходимо отметить как исключение.
 - **Контрольная сумма.** Отображение уникальной "подписи" выбранного файла. Контрольная сумма представляет собой автоматически создаваемую строку символов, позволяющих приложению AVG безошибочно отличать выбранный файл от других. Контрольная сумма создается и отображается после успешного добавления файла.
 - **Любое местоположение (не использовать полный путь).** Не устанавливайте флажок, если необходимо определить этот файл в качестве исключения только для определенного местоположения.
- **Удалить.** Нажмите для удаления выбранного приложения из списка.
 - **Удалить все.** Нажмите для удаления всех приложений в списке.

10.12. Потенциально нежелательные программы

Программа **AVG Anti-Virus 2012** может анализировать и обнаруживать исполняемые приложения или библиотеки DLL, использование которых в системе потенциально нежелательно. В некоторых случаях пользователю может потребоваться сохранить на компьютере некоторые нежелательные программы (программы, которые были установлены специально). Некоторые программы, особенно бесплатные, содержат рекламное ПО. **AVG Anti-Virus 2012** может обнаружить подобное рекламное ПО и сообщить о нем, как о *потенциально нежелательной программе*. Если необходимо сохранить подобную программу на компьютере, можно определить ее в качестве исключения потенциально нежелательной программы:



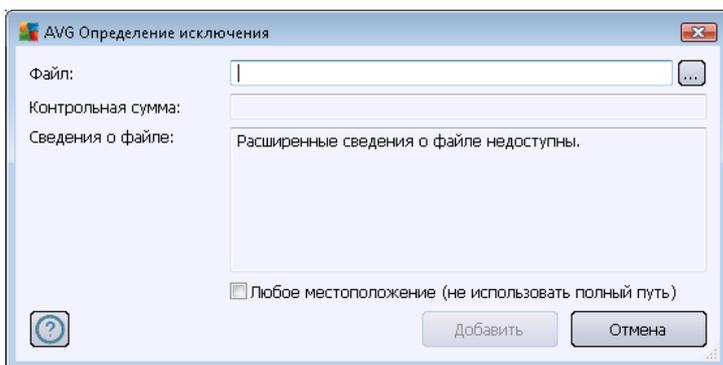
В диалоговом окне **Исключения потенциально нежелательных программ** отобразится список уже определенных исключений из числа потенциально нежелательных программ, которые на данный момент являются допустимыми исключениями. Список можно изменить, удалить из него существующие элементы или добавить новые исключения. О каждом исключении в списке предоставляется следующая информация:

- **Файл.** Указание точного имени соответствующего приложения
- **Путь к файлу.** Указание пути к папке приложения
- **Контрольная сумма.** Отображение уникальной "подписи" выбранного файла. Контрольная сумма представляет собой автоматически создаваемую строку символов, позволяющих приложению AVG безошибочно отличать выбранный файл от других. Контрольная сумма создается и отображается после успешного добавления файла.

Кнопки управления

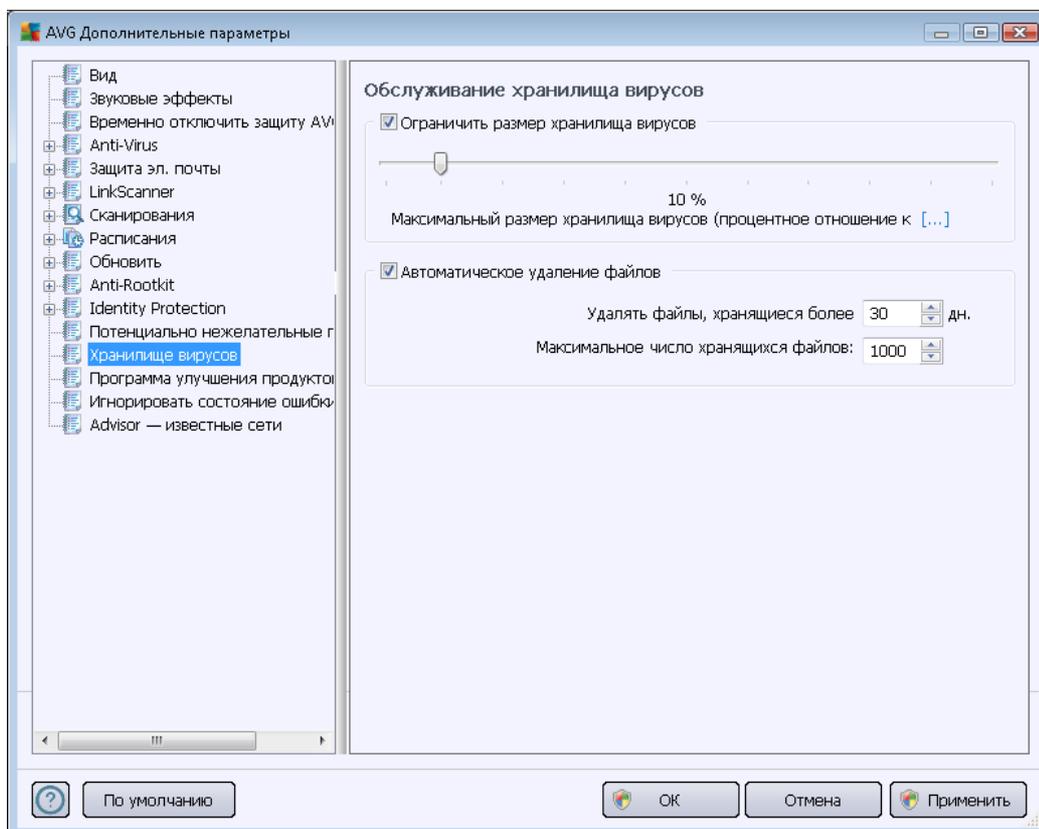
- **Редактировать.** Открытие диалогового окна редактирования (*соответствующего окну определения новых исключений, см. ниже*) определенного исключения, с помощью которого можно изменять параметры исключения.
- **Удалить.** Удаление выбранного элемента из списка исключений.

- **Добавить исключение.** Открытие диалогового окна редактирования, с помощью которого можно определить параметры нового создаваемого исключения.



- **Файл.** Введите полный путь к файлу, который необходимо отметить как исключение.
- **Контрольная сумма.** Отображение уникальной "подписи" выбранного файла. Контрольная сумма представляет собой автоматически создаваемую строку символов, позволяющих приложению AVG безошибочно отличать выбранный файл от других. Контрольная сумма создается и отображается после успешного добавления файла.
- **Сведения о файле.** Отображение другой дополнительной информации о файле (*информация о лицензии или версии и т. п.*).
- **Любое местоположение (не использовать полный путь).** Не устанавливайте флажок, если необходимо определить этот файл в качестве исключения только для определенного местоположения. Если флажок установлен, указанный файл будет определен в качестве исключения независимо от местонахождения (*однако необходимо указать полный путь к файлу; таким образом файл будет использоваться в качестве уникального примера возможности существования в системе двух файлов с одинаковым именем*).

10.13. Хранилище вирусов



Диалоговое окно **Обслуживание хранилища вирусов** позволяет определить несколько параметров администрирования объектов, находящихся в [хранилище вирусов](#):

- **Предельный размер хранилища вирусов.** С помощью ползунка установите максимальный размер [хранилища вирусов](#). Размер хранилища указывается пропорционально размеру локального диска.
- **Автоматическое удаление файлов.** В данном разделе можно указать максимальное время хранения объектов в [хранилище вирусов](#) (**Удалять файлы, хранящиеся более ... дней**), а также максимальное количество файлов, хранящихся в [хранилище вирусов](#) (**Максимальное число хранящихся файлов**).

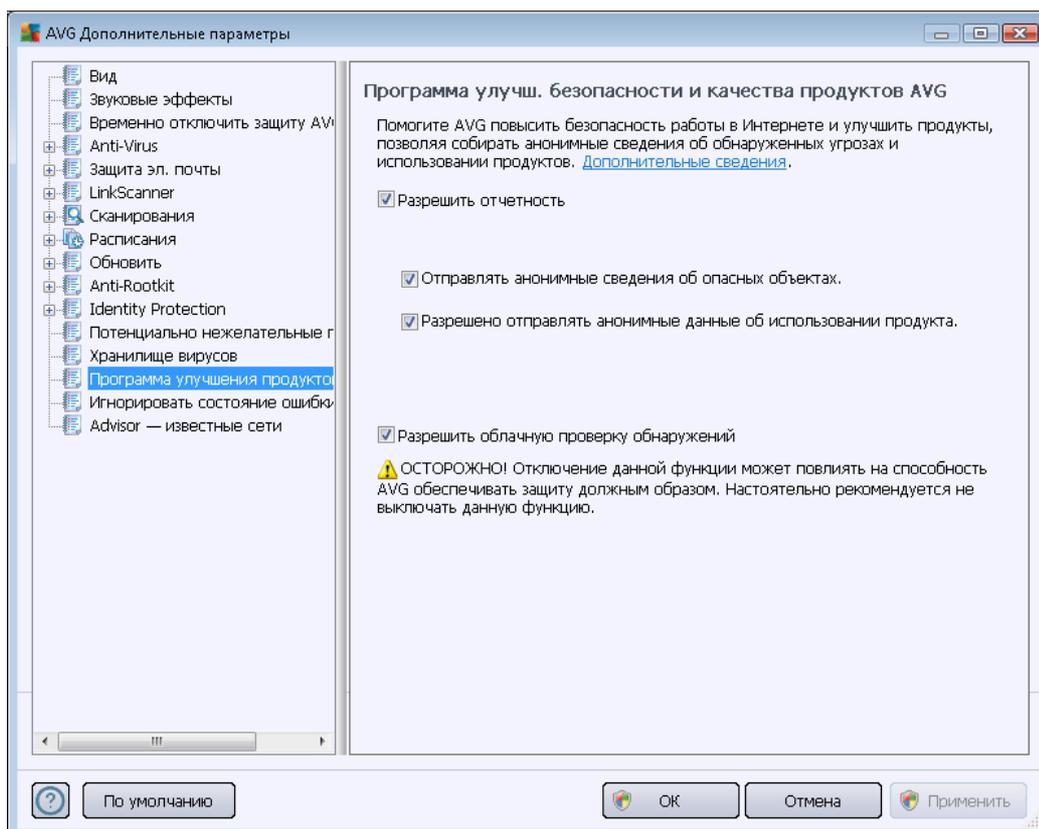
10.14. Программа улучшения продуктов

В диалоговом окне **Программа улучшения продуктов и интернет-безопасности AVG** отображается предложение на участие в программе улучшения продуктов AVG, которая направлена на увеличение общего уровня безопасности в Интернете. Установите флажок **Разрешить отчетность**, чтобы включить отправку отчетов об обнаруженных угрозах в лабораторию компании AVG. Это поможет нам собирать актуальные сведения о последних угрозах от пользователей по всему миру и улучшить защиту.

Передача отчетов осуществляется автоматически и не доставляет неудобств.



Персональные данные не включаются в отчеты. Передача отчетов об обнаруженных угрозах является необязательным параметром, однако мы рекомендуем оставить его включенным. Это поможет нам улучшать вашу защиту, а также защиту других пользователей AVG.



В этом диалоговом окне доступны приведенные ниже настройки параметров.

- **Разрешить отчетность** (выбрано по умолчанию). Если вы хотите помочь нам усовершенствовать продукты **AVG Anti-Virus 2012**, установите данный флажок. В этом случае в компанию AVG будут отправляться отчеты обо всех обнаруженных угрозах, что позволит нам собирать актуальные сведения о вредоносном ПО от пользователей по всему миру и улучшить общую защиту всех пользователей в Интернете. Передача отчетов осуществляется автоматически и не доставляет неудобств. Личные данные не включаются в отчеты.
 - **Разрешить отправлять данные о неправильно определенной электронной почте после подтверждения пользователя** (выбрано по умолчанию). Отправка сведений о сообщениях электронной почты, которые были по ошибке определены как спам, или о нежелательных сообщениях, которые не удалось обнаружить компоненту **Anti-Spam**. При отправке таких сведений отображается запрос на подтверждение.
 - **Разрешить отправлять анонимные данные об обнаруженных или подозрительных угрозах** (выбрано по умолчанию). Отправлять сведения обо



всех подозрительных или опасных кодах, а также обнаруженных на компьютере моделях поведения (*это может быть вирус, шпионское ПО или вредоносная веб-страница, на которую вы собираетесь перейти*) .

- **Разрешить отправлять анонимные данные об использовании продукта** (*выбрано по умолчанию*) . Отправка основных статистических данных об использовании приложения: количество обнаружений, запущенные сканирования, успешные или неуспешные обновления и т. п.
- **Разрешить проверку обнаружений в облаке** (*выбрано по умолчанию*) . Проверка обнаруженных угроз на предмет ложных срабатываний.

Наиболее распространенные угрозы

Сегодня существует гораздо больше угроз, чем простые вирусы. Создатели вредоносных кодов и опасных веб-сайтов всегда придумывают что-нибудь новое, в результате чего очень часто появляются новые угрозы, большинство из которых распространяется через Интернет. Далее приведены наиболее распространенные угрозы.

- **Вирус.** Это вредоносный код, способный к самостоятельному копированию и распространению, который трудно заметить, пока он не повредит систему. Некоторые вирусы представляют собой серьезную угрозу, удаляя или намеренно изменяя файлы, в то время как другие вирусы могут оказаться вполне безобидными, например они могут просто воспроизводить отрывок какой-то мелодии. Тем не менее все вирусы являются опасными из-за способности к саморазмножению, и даже самый простой вирус может очень быстро занять всю память компьютера и привести к сбою системы.
- **Червь.** Подкатегория вирусов, для которых, в отличие от обычных вирусов, не требуется объект-носитель; он самостоятельно распространяется на другие компьютеры, обычно по электронной почте, и приводит к перегрузке почтовых серверов и сетей.
- **Шпионское ПО.** Обычно относится к категории вредоносных (*вредоносное ПО = любое вредоносное программное обеспечение, включая вирусы*) исполняемых программ. Обычно это троянские кони, нацеленные на кражу личной информации, паролей, номеров кредитных карт либо на проникновения в компьютер, чтобы дать злоумышленнику возможность управлять им удаленно. Разумеется, все это происходит без ведома или согласия владельца компьютера.
- **Потенциально нежелательные программы.** Разновидность шпионского ПО, которая не обязательно представляет опасность для компьютера. В качестве конкретного примера PUP можно привести рекламное ПО. Это специальное программное обеспечение, предназначенное для распространения рекламы, как правило, посредством отображения всплывающих окон, что вызывает раздражение, но не представляет опасности.
- **Кроме того, следящие файлы cookie** могут также рассматриваться как разновидность шпионского ПО, так как эти небольшие файлы, хранящиеся в веб-браузере и автоматически отправляющиеся к "родительскому" веб-сайту при повторном его посещении, могут содержать сведения о просмотренных страницах в



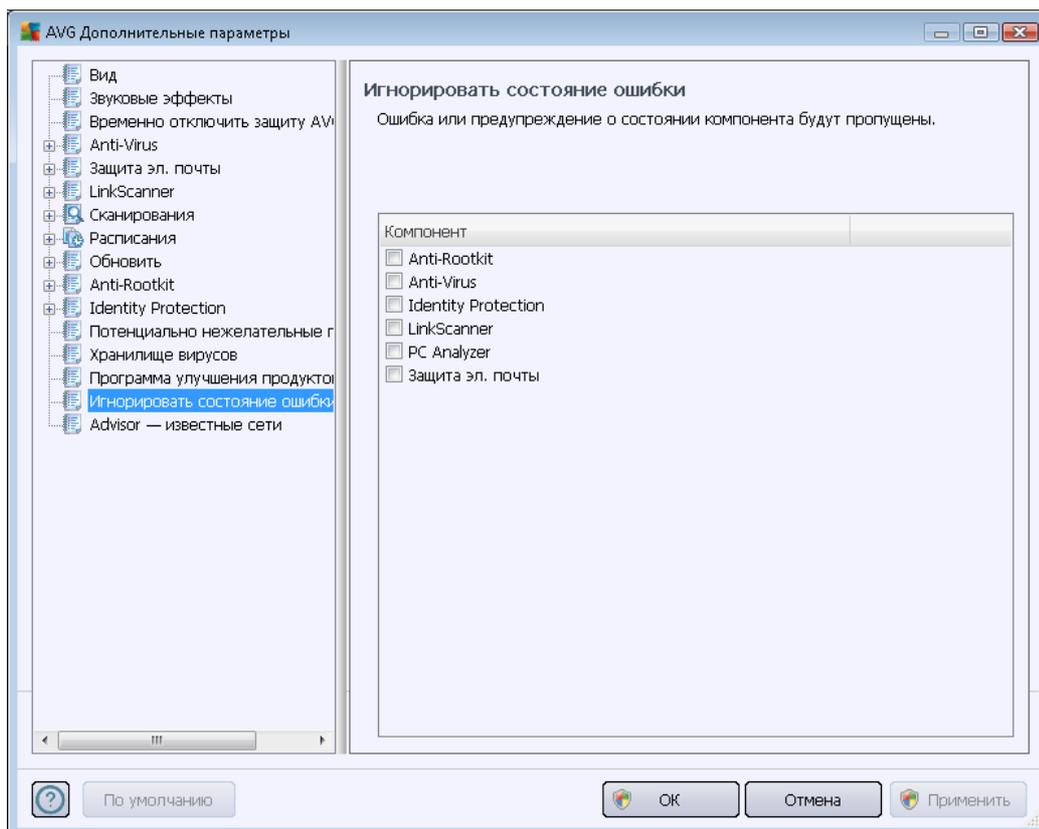
Интернете и другую аналогичную информацию.

- **Эксплойт.** Этот вредоносный код пользуется недостатками или уязвимыми местами операционной системы, интернет-браузера и других важных программ.
- **Фишинг.** Способ получения важных личных данных, при котором мошенники представляются сотрудниками надежных и хорошо известных организаций. Обычно потенциальным жертвам отправляются сообщения электронной почты с запросом, например на обновление сведений о банковском счете. В этих сообщениях пользователям предлагается перейти по ссылке, которая ведет на поддельный веб-сайт банка.
- **Программа-мистификация Ноах.** Данная угроза представляет собой нежелательное сообщение электронной почты, содержащее опасные, подозрительные или просто бесполезные сведения. Многие из вышеперечисленных угроз распространяются посредством сообщений электронной почты Ноах.
- **Вредоносные веб-сайты.** Сайты, которые преднамеренно устанавливают вредоносное ПО на вашем компьютере, а также взломанные сайты, которые являются законными и распространяют вирусы в результате взлома.

Для защиты от всех перечисленных угроз AVG Anti-Virus 2012 предлагает ряд специальных компонентов. Краткое описание см. в разделе [Обзор компонентов](#) данного документа.

10.15. Игнорировать состояние ошибки

В диалоговом окне *Игнорировать состояние ошибки* можно отметить компоненты, о которых не требуется получать уведомления.



По умолчанию в этом списке не выбрано никаких компонентов. Это означает, что при возникновении статуса ошибки компонента сразу же появится уведомление с помощью следующих сигналов.

- [Значок на панели задач](#). Во время безупречной работы всех компонентов AVG значок отображается четырьмя цветами; при появлении ошибок на значке появляется желтый восклицательный знак.
- Текстовое описание существующей проблемы в разделе [Сведения о состоянии безопасности](#) на главном окне AVG.

Может возникнуть ситуация, при которой понадобится временно отключить компонент (*Данное действие не рекомендуется. По возможности не отключайте компоненты и не изменяйте настройки, установленные по умолчанию. Но необходимость в данном действии может возникнуть*). В данном случае значок на панели задач автоматически оповестит о состоянии ошибки компонента. Тем не менее, в данной ситуации настоящей ошибки не возникает, так как пользователь преднамеренно ее вызвал и был предварительно предупрежден о возможном риске. В то же время, если значок отобразился серым цветом, он не может оповещать о дальнейших возможных ошибках.



В такой ситуации в диалоговом окне выше можно выбрать компоненты, которые могут находиться в состоянии ошибки (*или быть отключены*), и о которых не требуется получать уведомления. Аналогичный параметр (*Игнорировать состояние компонента*) также доступен для некоторых компонентов непосредственно из [обзора компонентов в главном окне AVG](#).

10.16. Advisor — известные сети

[AVG Advisor](#) выполняет функцию отслеживания сетей, с которыми работает пользователь. Если обнаруживается новая сеть (*с уже используемым сетевым именем, в связи с чем может возникнуть путаница*), появляется уведомление с рекомендацией проверить ее безопасность. Если пользователь сочтет новую сеть безопасной, он может занести ее в этот список. Тогда [AVG Advisor](#) сохранит ее уникальные атрибуты (*в частности, MAC-адрес*), и это уведомление больше не появится.

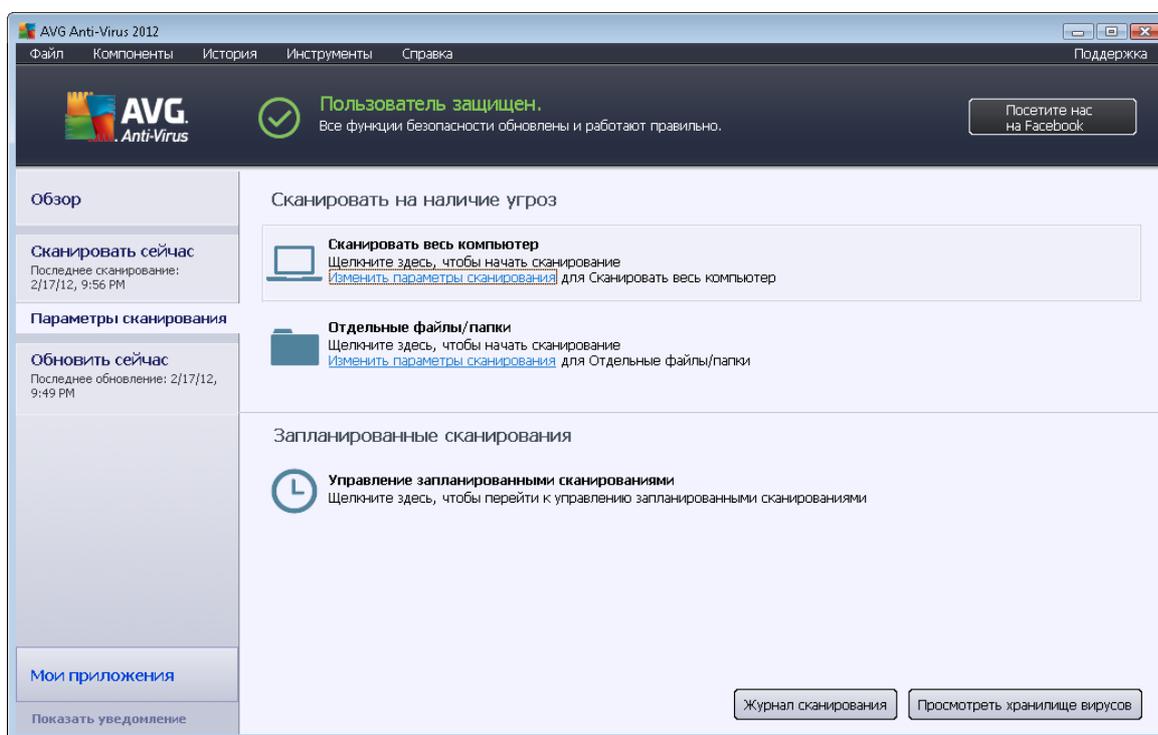
В этом диалоговом окне можно проверить, какие сети были сохранены как известные. С помощью кнопки **Удалить** можно исключить любые записи. Соответствующая сеть снова будет считаться неизвестной и потенциально опасной.



11. Сканирование AVG

По умолчанию **AVG Anti-Virus 2012** не запускает операции сканирования, так как после начального сканирования вы будете полностью защищены благодаря компонентам **AVG Anti-Virus 2012**, которые всегда на страже и не позволяют вредоносным кодам проникать в систему. Однако при необходимости можно [запланировать сканирование](#), которое будет выполняться через определенные промежутки времени или запустить сканирование вручную.

11.1. Интерфейс сканирования



Интерфейс сканирования AVG доступен при нажатии [быстрой ссылки](#) **Параметры сканирования**. Щелкните эту ссылку, чтобы открыть диалоговое окно **Сканирование на наличие угроз**. Данное диалоговое окно содержит следующие разделы:

- обзор [предопределенных сканирований](#) — три типа сканирований, определенных поставщиком ПО, готовые к использованию по расписанию или при необходимости:
 - [Сканирование всего компьютера](#)
 - [Сканировать отдельные файлы или папки](#)
- [Расписание сканирования](#) — настройка новых проверок и создание новых расписаний при необходимости.

Кнопки управления



В интерфейсе проверки доступны следующие кнопки управления:

- **Журнал сканирования.** Открывает диалоговое окно [Обзор результатов сканирования](#), содержащее полную историю сканирования
- **Просмотреть хранилище вирусов.** Открывает новое окно [Хранилище вирусов](#) — место хранения обнаруженных вирусов

11.2. Предопределенные сканирования

Одна из главных функций **AVG Anti-Virus 2012** — сканирование по требованию. Проверка по требованию разработана для сканирования различных частей компьютера при подозрении на заражение вирусом. Рекомендуется проводить такие проверки регулярно, даже в случае видимого отсутствия вируса на компьютере.

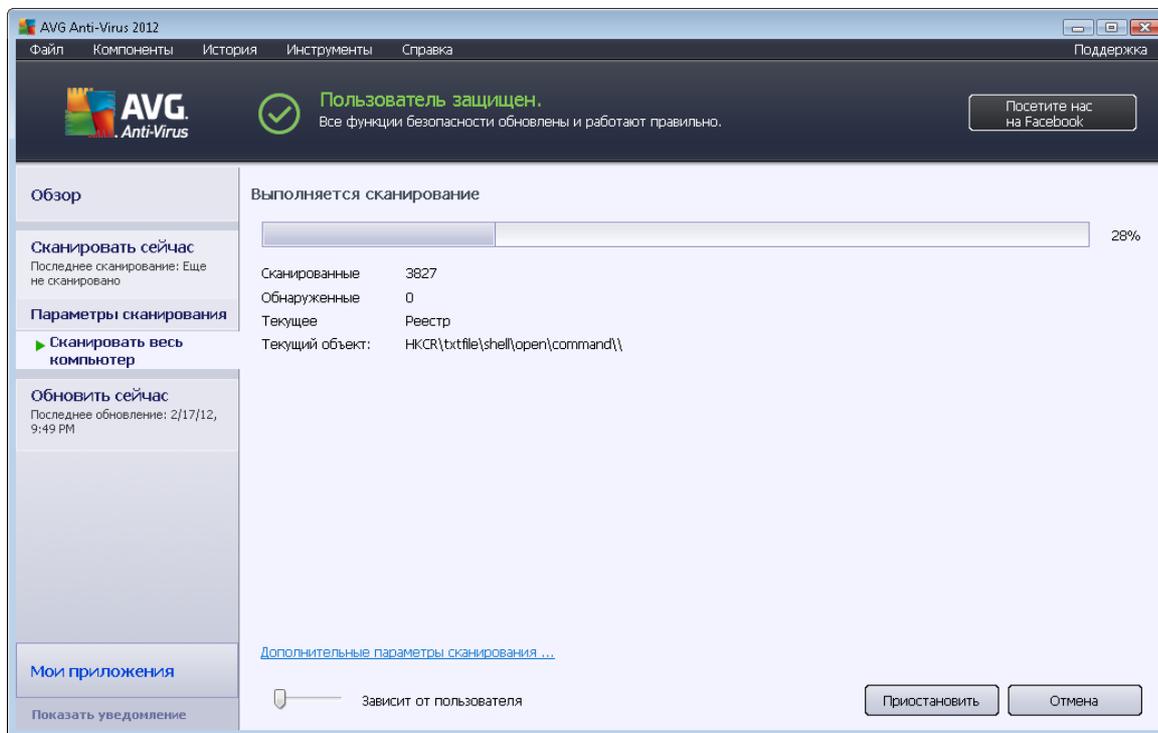
В системе **AVG Anti-Virus 2012** доступны следующие типы сканирования, настроенные поставщиком программного обеспечения.

11.2.1. Сканирование всего компьютера

Сканирование всего компьютера. Сканирование всего компьютера на наличие заражений и/или потенциально нежелательных программ. При данном типе проверки выполняется сканирование всех жестких дисков компьютера, производится обнаружение и лечение зараженных объектов или перемещение в [хранилище вирусов](#). Сканирование всего компьютера необходимо выполнять на рабочих станциях как минимум один раз в неделю.

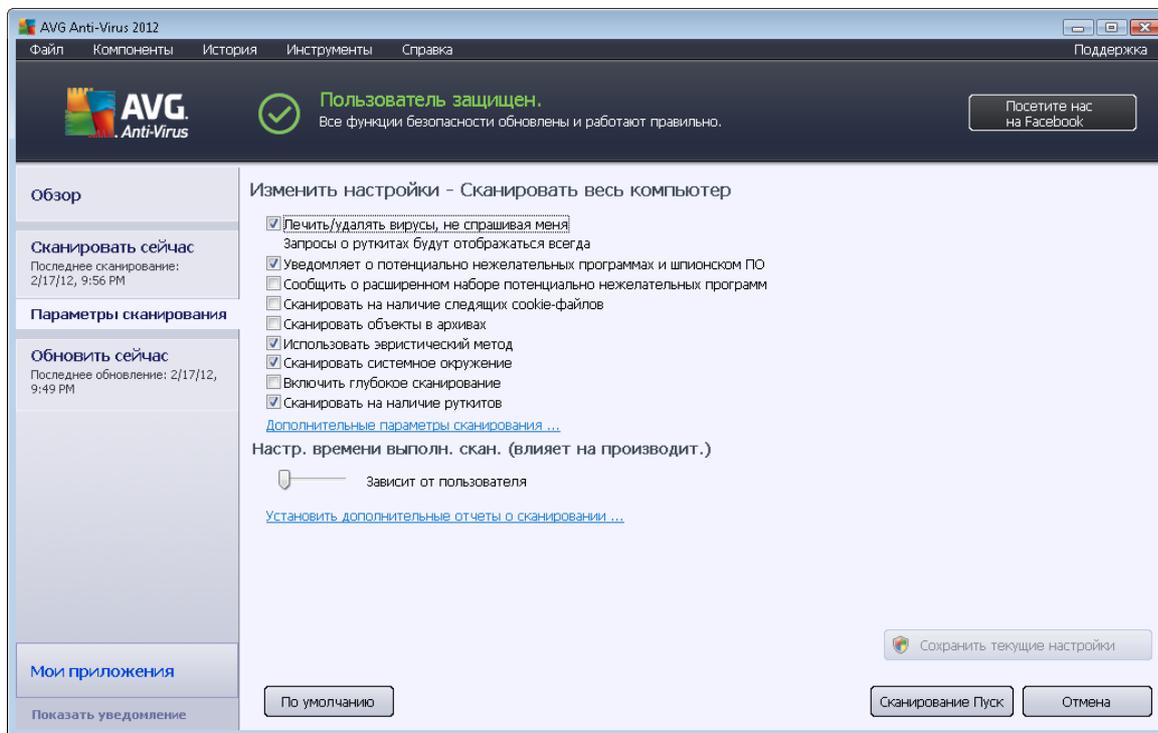
Запуск сканирования

Сканирование всего компьютера можно запустить непосредственно в [интерфейсе сканирования](#), щелкнув значок сканирования. При данном типе сканирования не требуются какие-либо дополнительные настройки, процесс сканирования начнется немедленно при открытии диалогового окна **Выполняется сканирование** (см. снимок экрана). При необходимости сканирование можно прервать (**Пауза**) или отменить (**Отмена**).



Изменение параметров сканирования

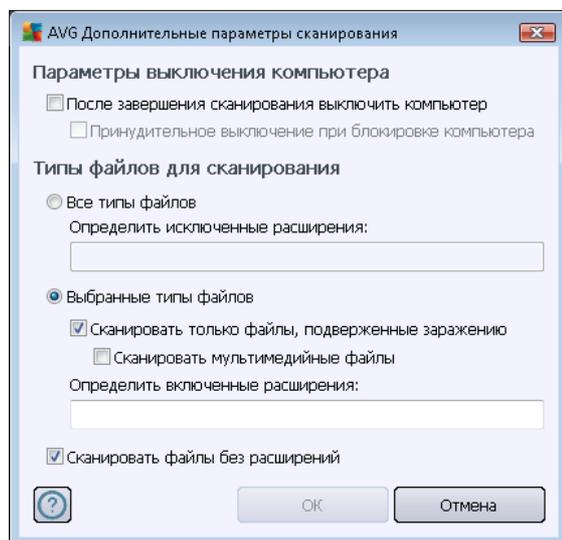
Существует возможность изменения предварительно определенных параметров **сканирования всего компьютера**. Нажмите ссылку **Изменить параметры сканирования** для открытия диалогового окна **Изменение параметров сканирования для сканирования всего компьютера** (доступно через [интерфейс сканирования](#) при щелчке ссылки **Изменить параметры сканирования для Сканирование всего компьютера**). **Рекомендуется сохранять установленные по умолчанию настройки до появления веской причины для их изменения!**



- **Параметры сканирования.** В списке параметров сканирования можно включить или выключить определенные параметры при необходимости.
 - **Автоматически лечить или удалять зараженные вирусами объекты (выбрано по умолчанию).** Обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если не удалось автоматически вылечить зараженный файл, зараженный объект будет перемещен в [хранилище вирусов](#).
 - **Уведомлять о потенциально нежелательных программах и угрозах появления шпионских программ (по умолчанию включено).** Установите данный флажок, чтобы активировать модуль [Anti-Spyware](#) и сканировать компьютер на наличие шпионских программ и вирусов. Шпионские программы относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.
 - **Уведомлять о расширенном наборе потенциально нежелательных программ (не выбрано по умолчанию).** Установите данный флажок для обнаружения расширенного пакета шпионских программ. Это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.



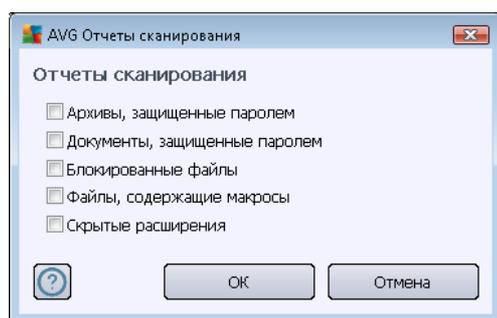
- **Сканировать на наличие следящих файлов cookie** (не выбрано по умолчанию). Благодаря данному параметру компонента [Anti-Spyware](#) осуществляется определение файлов cookie (файлы cookie протокола HTTP используются для аутентификации, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзины для покупок через Интернет).
 - **Сканировать объекты в архивах** (не выбрано по умолчанию). Благодаря данному параметру при сканировании проверяются все файлы, хранящиеся в архивах, например ZIP, RAR и т. п.
 - **Использовать эвристику** (выбрано по умолчанию). Эвристический анализ (динамическая эмуляция инструкций сканированных объектов в среде виртуального компьютера) — это один из способов, используемых для обнаружения вирусов при сканировании.
 - **Сканировать системную среду** (не выбрано по умолчанию). При сканировании также будут проверены системные области компьютера.
 - **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (например, при подозрении, что компьютер заражен) можно установить данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.
 - **Сканировать на наличие пакетов программ rootkit** (выбрано по умолчанию). Компонент [Anti-Rootkit](#) сканирует компьютер на возможное наличие пакетов программ rootkit (программы и технологии, позволяющие скрыть вредоносную активность на компьютере). Если программа rootkit обнаружена, это еще не значит, что компьютер заражен. В некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за средства rootkit.
- **Дополнительные параметры сканирования.** Эта ссылка открывает новое диалоговое окно **Дополнительные параметры сканирования**, где можно указывать следующие параметры.



- **Параметры выключения компьютера.** Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (**Выключить компьютер после завершения сканирования**) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (**Принудительное выключение при блокировке компьютера**).
- **Определение типов файлов для сканирования.** Далее необходимо указать типы файлов для сканирования.
 - **Все типы файлов** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет;
 - **Выбранные типы файлов.** Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.
 - Дополнительно можно установить флажок **Сканировать файлы без расширений**. Он установлен по умолчанию. Рекомендуется не снимать его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.
- **Настройка времени выполнения сканирования.** Для изменения приоритета процесса сканирования используйте ползунок. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить

нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).

- **Настроить дополнительные отчеты сканирования.** При нажатии этой ссылки открывается диалоговое окно **Отчеты сканирования**, в котором можно выбрать типы объектов, сведения о которых должны отображаться в отчете.



Предупреждение. Перечисленные параметры сканирования действительны также для вновь создаваемого сканирования, как описано в разделе [Сканирование AVG/Планирование сканирования/Способы сканирования](#). Если потребуются изменить конфигурацию по умолчанию параметра **Сканирование всего компьютера**, можно затем сохранить новые параметры в качестве конфигурации по умолчанию, чтобы они использовались каждый раз при сканировании всего компьютера.

11.2.2. Сканирование определенных файлов или папок

Сканирование файлов или папок. При данном типе сканирования проверяются только области компьютера, выбранные для сканирования (*выбранные папки, жесткие диски, гибкие диски, компакт-диски и т. п.*). Процессы обнаружения вирусов и лечения зараженных объектов при данном типе сканирования будут выполняться также, как и при сканировании всего компьютера: найденные вирусы подвергаются лечению или удаляются в [хранилище вирусов](#). Сканирование отдельных файлов и папок можно использовать при создании пользовательских проверок и их расписаний.

Запуск сканирования

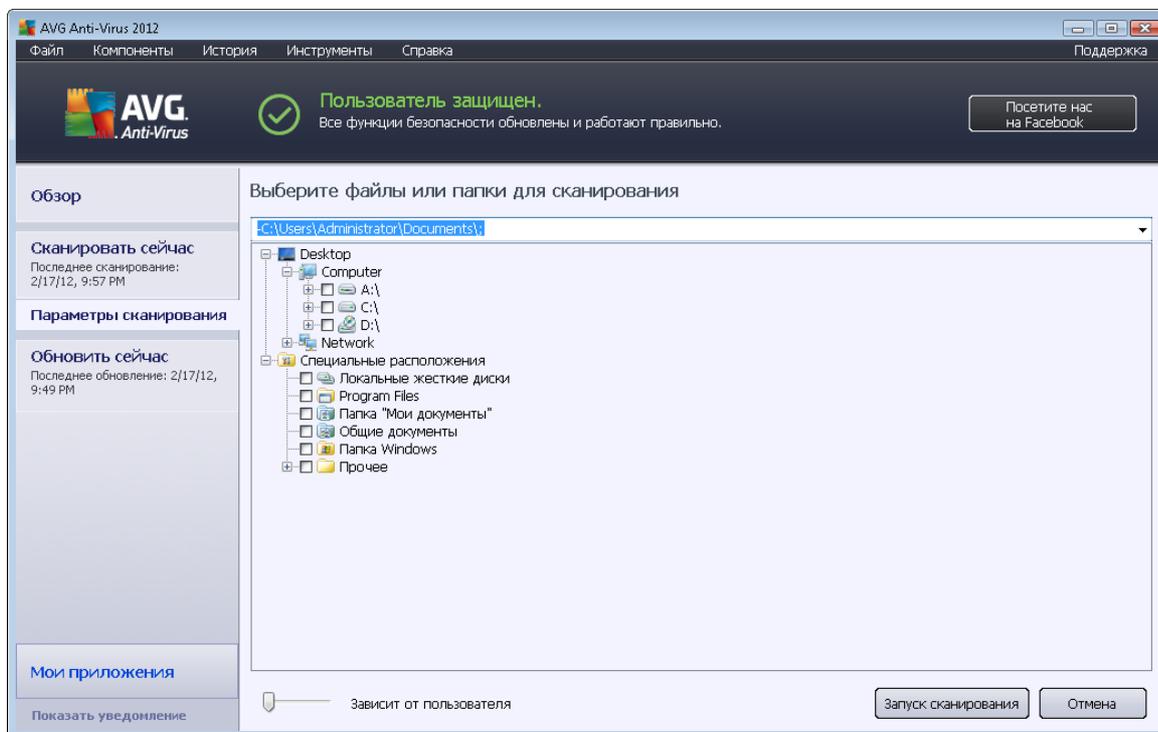
Сканирование файлов или папок можно запустить непосредственно в [интерфейсе сканирования](#), щелкнув значок сканирования. Откроется новое диалоговое окно **Выбор отдельных файлов или папок для сканирования**. В древовидной структуре компьютера выберите папки для сканирования. Путь к каждой выбранной папке будет создан автоматически и отобразится в текстовом поле в верхней части данного диалогового окна.

Существует также возможность сканирования определенных папок без сканирования соответствующих подпапок; чтобы выполнить такое сканирование, введите значок минус "-" перед автоматически созданным путем (*см. снимок экрана*). Чтобы исключить всю папку из процесса сканирования, используйте параметр "!".

Наконец, чтобы запустить сканирование, нажмите кнопку **Начать сканирование**; данный

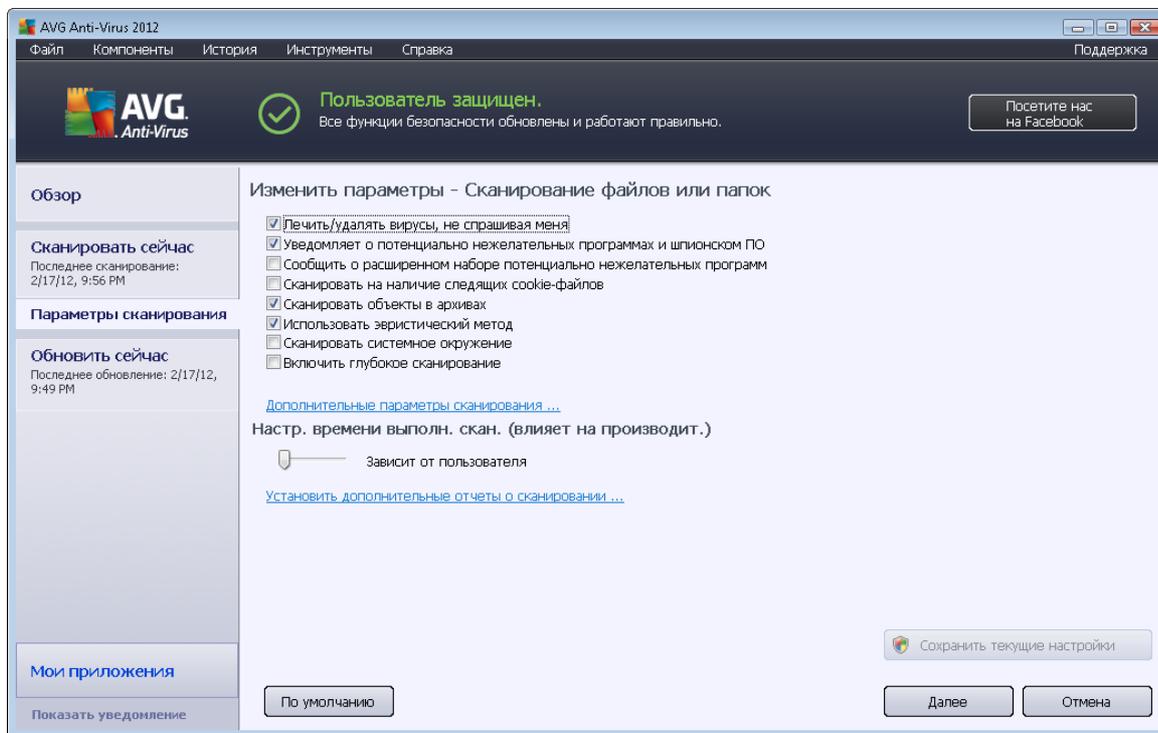


процесс сканирования практически идентичен процессу [сканирования всего компьютера](#).



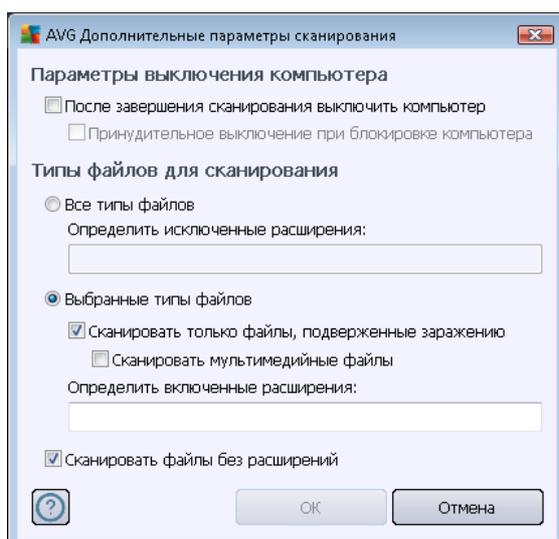
Изменение параметров сканирования

Существует возможность изменения предварительно определенных параметров **сканирования отдельных файлов и папок**. Щелкните ссылку **Изменить параметры сканирования**, чтобы открыть диалоговое окно **Изменение параметров сканирования для сканирования отдельных файлов и папок**. **Рекомендуется сохранять установленные по умолчанию настройки до появления веской причины для их изменения!**



- **Параметры сканирования.** В списке параметров сканирования можно включить или выключить определенные параметры при необходимости.
 - **Автоматически лечить или удалять зараженные вирусами объекты (выбрано по умолчанию).** Обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если зараженный файл не удалось вылечить автоматически, зараженный объект будет перемещен в [хранилище вирусов](#).
 - **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО (выбрано по умолчанию).** Установите данный флажок для активации модуля [Anti-Spyware](#) и сканирования компьютера на наличие шпионского ПО и вирусов. Шпионские программы относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.
 - **Уведомлять о расширенном наборе потенциально нежелательных программ (по умолчанию выключено).** Установите данный флажок для обнаружения расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

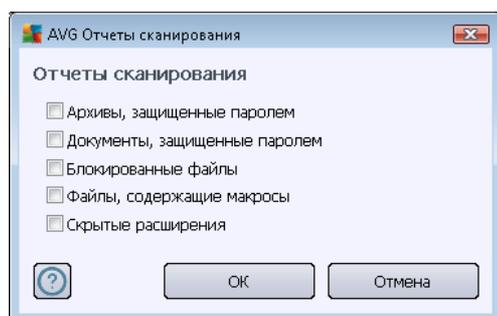
- **Сканировать на наличие следящих файлов cookie** (не выбрано по умолчанию): благодаря данному параметру компонента [Anti-Spyware](#) осуществляется поиск файлов cookie; (файлы cookie протокола HTTP используются для аутентификации, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзины для покупок через Интернет).
 - **Сканировать объекты в архивах** (выбрано по умолчанию). Благодаря данному параметру при сканировании проверяются все файлы, хранящиеся в архивах, например ZIP, RAR и т. п.
 - **Использовать эвристику** (выбрано по умолчанию). Эвристический анализ (динамическая эмуляция инструкций сканированных объектов в среде виртуального компьютера) — это один из способов, используемых для обнаружения вирусов при сканировании.
 - **Сканировать системную среду** (не выбрано по умолчанию). При сканировании также будут проверены системные области компьютера.
 - **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (например, при подозрении, что компьютер заражен) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.
- **Дополнительные параметры сканирования.** Эта ссылка открывает новое диалоговое окно **Дополнительные параметры сканирования**, где можно указывать следующие параметры.



- **Параметры выключения компьютера.** Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса

сканирования. После выбора этого параметра (**Выключить компьютер после завершения сканирования**) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (**Принудительное выключение при блокировке компьютера**).

- **Определение типов файлов для сканирования.** Далее необходимо указать типы файлов для сканирования.
 - **Все типы файлов** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет;
 - **Выбранные типы файлов.** Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.
 - Дополнительно можно установить флажок **Сканировать файлы без расширений**. Он установлен по умолчанию. Рекомендуется не снимать его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.
- **Приоритет процесса сканирования.** Для изменения приоритета процесса сканирования используйте ползунок. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).
- **Настроить дополнительные отчеты сканирования.** При нажатии этой ссылки открывается диалоговое окно **Отчеты сканирования**, в котором можно выбрать типы объектов, сведения о которых должны отображаться в отчете.

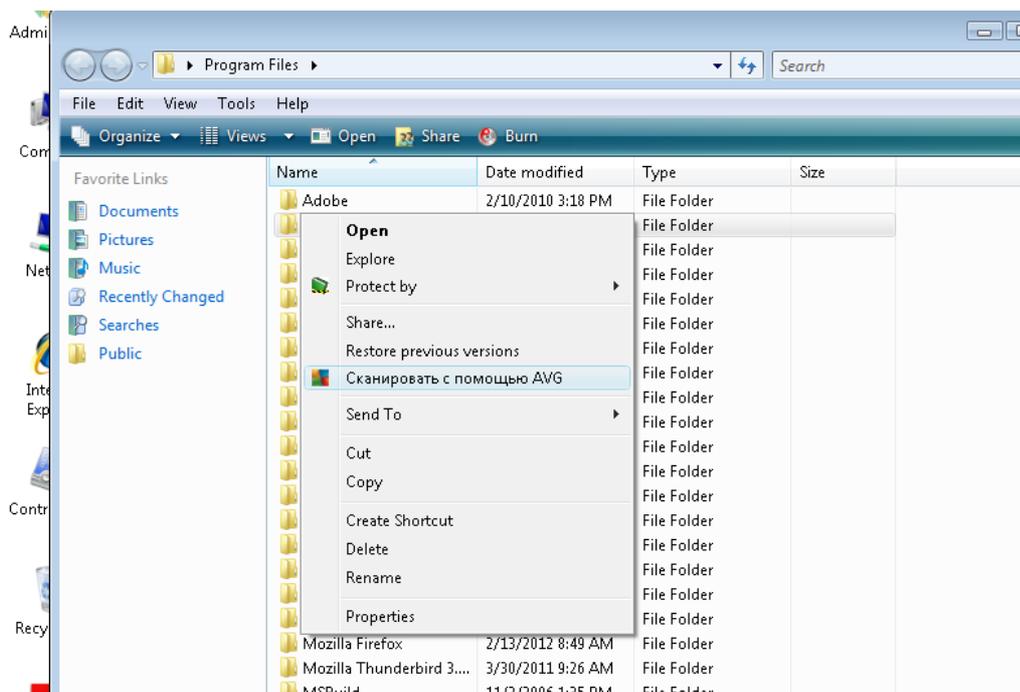


Предупреждение. Перечисленные параметры сканирования действительны также для вновь создаваемого сканирования, как описано в разделе [Сканирование AVG/Планирование](#)

[сканирования/Способы сканирования](#). Если потребуется изменить конфигурацию по умолчанию параметра **Сканирование отдельных файлов и папок**, можно сохранить новые параметры как конфигурацию по умолчанию, чтобы она использовалась каждый раз при сканировании отдельных файлов или папок. Кроме того, созданная конфигурация может затем использоваться в качестве шаблона для новых запланированных сканиваний ([все пользовательские сканирования основаны на текущей конфигурации сканирования выбранных файлов и папок](#)).

11.3. Сканирование в Проводнике Windows

Кроме predetermined сканиваний всего компьютера или выбранных областей, программа **AVG Anti-Virus 2012** также имеет функцию быстрого сканирования выбранного объекта непосредственно в Проводнике Windows. Если необходимо открыть неизвестный файл, содержимое которого не вызывает доверия, можно проверить такой файл по запросу. Выполните следующие действия.



- В проводнике Windows выделите файл (или папку), который необходимо проверить
- Откройте контекстное меню, щелкнув объект правой кнопкой мыши
- Выберите элемент меню **Сканировать с помощью AVG**, чтобы начать сканирование файла с помощью **AVG Anti-Virus 2012**

11.4. Сканирование с помощью командной строки

В **AVG Anti-Virus 2012** можно выбрать запуск сканирования из командной строки. Например, данный параметр может быть использован на серверах, а также при создании пакетного сценария, запускаемого автоматически при загрузке компьютера. Из командной строки можно



запустить сканирование со всеми основными параметрами, доступными в графическом интерфейсе пользователя AVG.

Чтобы запустить сканирование AVG из командной строки, выполните следующую команду в папке установки AVG:

- **avgscanx** для 32-разрядной ОС;
- **avgscana** для 64-разрядной ОС.

Синтаксис команды

Команда имеет следующий синтаксис.

- **avgscanx /parameter** ... например, **avgscanx /comp** для сканирования всего компьютера
- **avgscanx /parameter /parameter** .. несколько параметров в одной строке отделяются пробелом и косой чертой,
- если для параметров необходимо указать определенное значение (например, параметр **/scan**, которому необходимы сведения о том, какие области на компьютере необходимо сканировать, а также прямой путь к выбранному разделу), значения отделяются точкой с запятой, например **avgscanx /scan=C:\;D:**

Параметры сканирования

Для получения полного списка доступных параметров введите соответствующую команду вместе с параметром **/?** или **/HELP** (например, **avgscanx /?**). Единственный обязательный параметр — **/SCAN**, который определяет сканируемые области компьютера. Подробное описание параметров см. в [обзоре параметров командной строки](#).

Чтобы начать сканирование, нажмите клавишу **Enter**. Процесс сканирования можно остановить, нажав сочетание клавиш **Ctrl+C** или **Ctrl+Pause**.

Сканирование из командной строки запущено с помощью графического интерфейса

При запуске компьютера в безопасном режиме Windows также можно запустить сканирование из командной строки с помощью графического интерфейса пользователя. Сканирование запустится из командной строки, диалоговое окно **Конструктор командной строки** позволяет определить большинство основных параметров сканирования с помощью удобного графического интерфейса.

Так как данное диалоговое окно доступно только в безопасном режиме Windows, более подробное описание данного окна можно получить в файле справки, доступном непосредственно в этом диалоговом окне.



11.4.1. Параметры сканирования с помощью командной строки

Далее приведен список всех параметров для сканирования с помощью командной строки.

- **/SCAN** [Сканировать определенные файлы или папки](#) /SCAN=путь;
путь (например, /SCAN=C:\;D:\)
- **/COMP** [Сканирование всего компьютера](#)
- **/HEUR** Использовать [эвристический анализ](#)
- **/EXCLUDE** Исключить путь или файлы из сканирования
- **/@** Командный файл /имя файла/
- **/EXT** Сканировать эти расширения /например, EXT=EXE,DLL/
- **/NOEXT** Не сканировать эти расширения /например, NOEXT=JPG/
- **/ARC** Сканировать архивы
- **/CLEAN** Автоматическая очистка
- **/TRASH** Переместить зараженные файлы в [хранилище вирусов](#)
- **/QT** Быстрая проверка
- **/LOG** Создать файл результата сканирования
- **/MACROW** Сообщать о макросах
- **/PWDW** Сообщать о файлах, защищенных паролем
- **/ARCBOMBSW** Сообщать об "архивных бомбах" (*множественно сжатых архивах*)
- **/IGNLOCKED** Пропускать заблокированные файлы
- **/REPORT** Отчет в файл /имя файла/
- **/REPAPPEND** Добавить в файл отчета
- **/REPOK** Сообщать о незараженных файлах
- **/NOBREAK** Запретить остановку по нажатию CTRL-BREAK
- **/BOOT** Включить проверку сектора MBR/загрузочного сектора
- **/PROC** Сканировать активные процессы
- **/PUP** Сообщать о [потенциально нежелательных программах](#)



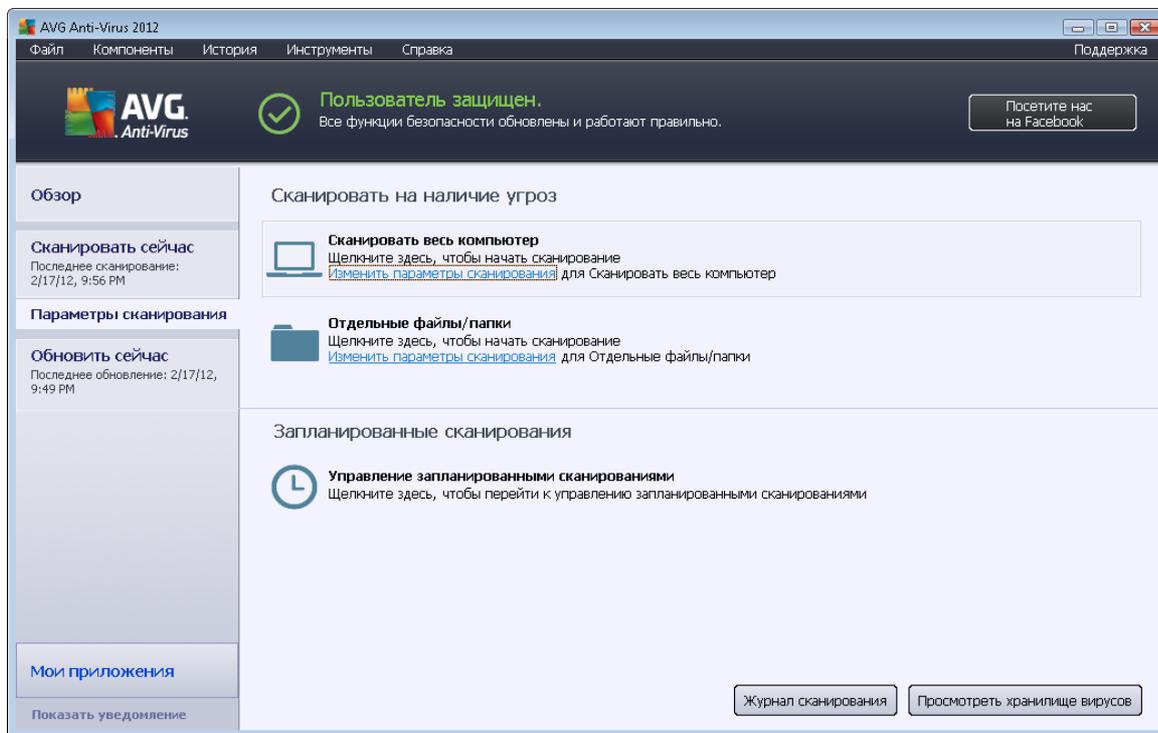
- **/PUPEXT** Сообщать о расширенном наборе [потенциально нежелательных программ](#)
- **/REG** Сканировать реестр
- **/COO** Сканировать файлы cookie
- **/?** Показать справку по этой теме
- **/HELP** Показать справку по этой теме
- **/PRIORITY** Установить приоритет сканирования /Низкий, Автоматический, Высокий/ (см. [Дополнительные параметры/Сканирование](#))
- **/SHUTDOWN** Выключить компьютер по завершении сканирования
- **/FORCESHUTDOWN** Принудительное выключение компьютера по завершении сканирования
- **/ADS** Сканировать альтернативные потоки данных (*только NTFS*)
- **/HIDDEN** Сообщать о файлах со скрытым расширением
- **/INFECTABLEONLY** Сканировать только файлы с подверженными заражению расширениями
- **/THOROUGHSCAN** Включить глубокое сканирование
- **/CLOUDCHECK** Проверять на наличие ложных обнаружений
- **/ARCBOMBSW** Сообщать о повторно сжатых архивных файлах

11.5. Расписание сканирования

С помощью **AVG Anti-Virus 2012** можно запустить сканирование по требованию (в случае предполагаемого заражения компьютера) или запланированное сканирование. Рекомендуется запускать сканирование согласно расписанию. В этом случае вы будете уверены, что компьютер надежно защищен от всех возможных заражений, и не придется волноваться о том, нужно ли и когда запускать сканирование.

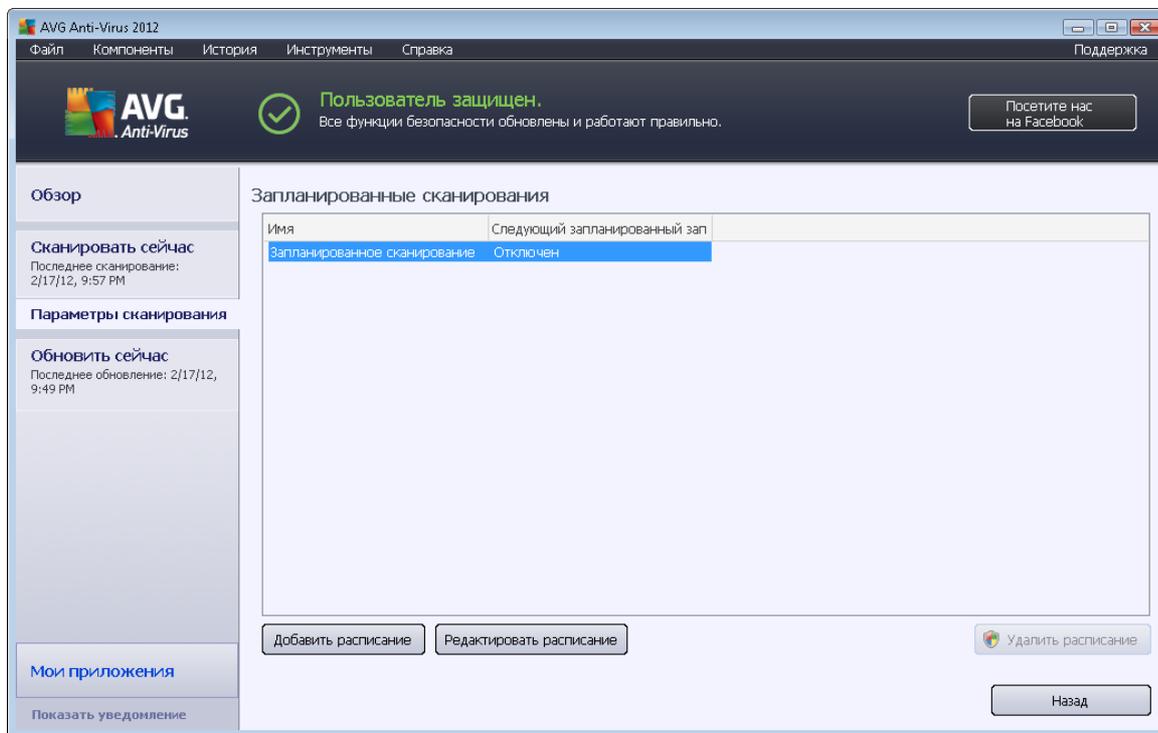
[Сканирование всего компьютера](#) необходимо запускать как минимум раз в неделю. Все же, если это возможно, рекомендуется запускать сканирование всего компьютера ежедневно (как настроено в конфигурации расписания сканирования по умолчанию). Если компьютер всегда включен, можно назначить сканирование на нерабочее время. Если пользователь иногда выключает компьютер, сканирование начинается [сразу же при включении компьютера, если сканирование в заданное время было пропущено](#).

Для создания новых расписаний сканирования откройте [Интерфейс сканирования AVG](#) и см. раздел **Запланированные сканирования**, расположенный в нижней части интерфейса сканирования.



Запланированные сканирования

Щелкните графический значок в разделе **Запланированные сканирования**, чтобы открыть новое диалоговое окно **Запланированные сканирования**, в котором находится список текущих запланированных сканирований.



Сканирования можно редактировать или добавлять с помощью следующих кнопок управления.

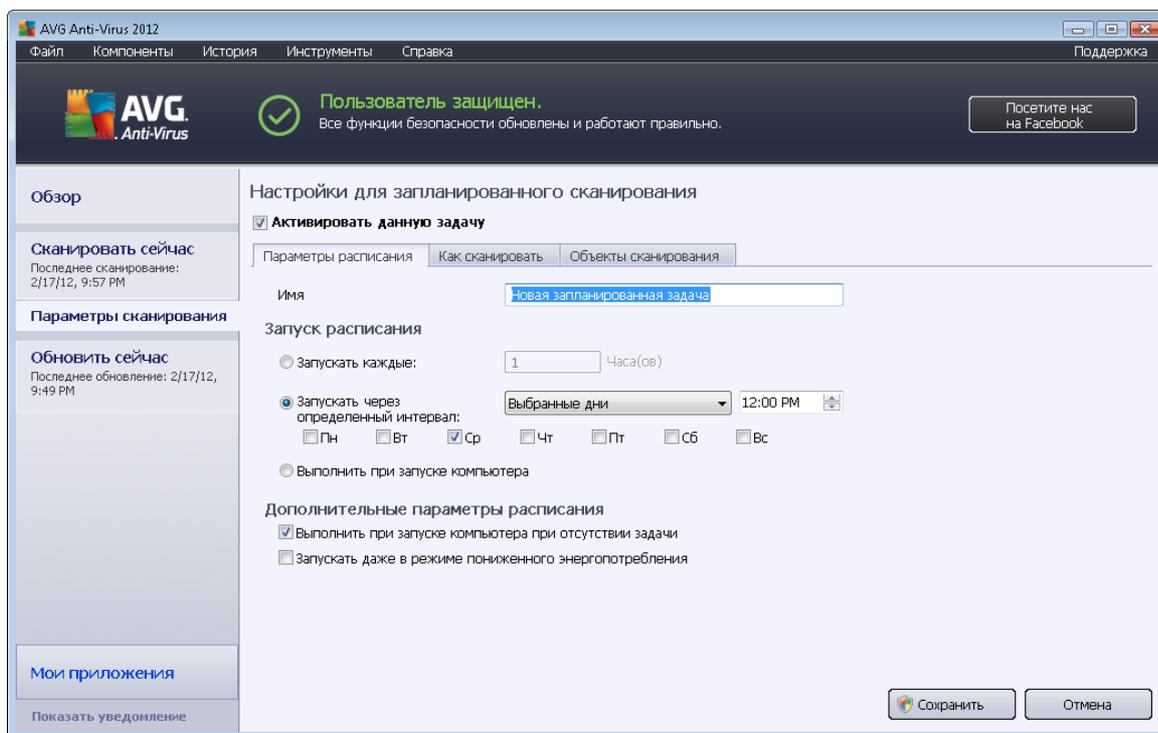
- **Добавить расписание сканирования.** Открытие диалогового окна **Параметры запланированного сканирования**, вкладки [Параметры расписания](#). В данном диалоговом окне можно указать параметры новой созданной проверки.
- **Редактировать расписание сканирования.** Используется, только если текущая проверка была предварительно выбрана в списке запланированных проверок. В данном случае кнопка активна и может использоваться для перехода к диалоговому окну **Параметры запланированного сканирования**, вкладке [Параметры расписания](#). Параметры выбранной проверки уже указаны и могут быть изменены.
- **Удалить расписание сканирования.** Данная кнопка также активна, если текущая проверка была предварительно выбрана в списке запланированных проверок. Далее проверку можно удалить из списка, нажав кнопку управления. При этом пользователь может удалять только собственные проверки; удаление **расписания полного сканирования компьютера**, предварительно определенного параметрами по умолчанию, недоступно.
- **Назад.** Возврат к [интерфейсу сканирования AVG](#)

11.5.1. Параметры расписания

При необходимости запланировать новую проверку и ее регулярный запуск войдите в диалоговое окно **Параметры запланированной проверки** (нажмите кнопку **Добавить расписание сканирования** в диалоговом окне **Запланированные сканирования**). Диалоговое окно состоит из трех вкладок. **Параметры расписания** — см. рисунок ниже



(вкладка по умолчанию, на которую пользователь перенаправляется автоматически),
[Способы сканирования](#) и [Объекты сканирования](#).



На вкладке **Параметры расписания** можно сначала установить или снять флажок элемента **Активировать данную задачу**, чтобы временно отключить запланированную проверку и включить ее при необходимости.

Далее необходимо указать название сканирования, которое будет создано и запланировано. Введите название в текстовое поле рядом с элементом **Имя**. Старайтесь использовать краткие, содержательные и понятные названия расписаний обновления, так как позже это облегчит их поиск среди остальных расписаний обновления.

Пример. Названия "Новое сканирование" или "Мое сканирование" не являются содержательными, так как не связаны с объектами, которые будут проверяться. И наоборот, название "Сканирование системных областей" является хорошим содержательным названием. Хотя и не обязательно указывать в названии сканирования, является ли оно сканированием всего компьютера или только сканированием выбранных файлов или папок, созданные сканирования будут определяться как разновидности [сканирования выбранных файлов и папок](#).

В данном диалоговом окне можно определить следующие параметры сканирования.

- **Выполняемое расписание.** Укажите временные интервалы запуска нового запланированного сканирования. Можно определить время запуска сканирования через определенные промежутки времени (**Запускать каждые ...**), указать точные дату и время запуска сканирования (**Запускать в определенное время ...**), а также определить событие, с которым должен быть связан запуск сканирования (**Действие**



связано с включением компьютера).

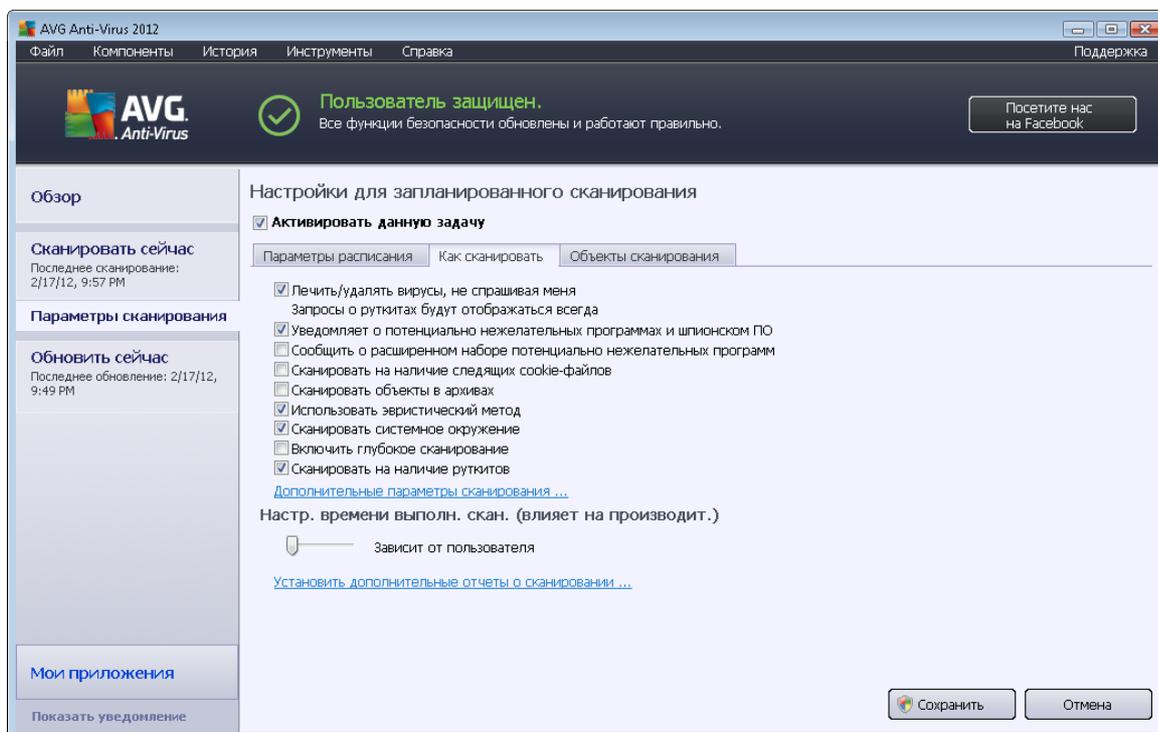
- **Дополнительные параметры расписания** — данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск сканирования, если компьютер работает в энергосберегающем режиме или выключен.

Кнопки управления параметрами диалогового окна запланированного сканирования

На каждой из трех вкладок (*Параметры расписания*, [Способы сканирования](#) и [Объекты сканирования](#)) диалогового окна **Параметры запланированного сканирования** расположены две кнопки управления, которые имеют одинаковые функции независимо от того, какая вкладка выбрана.

- **Сохранить.** Сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, а также обратный переход к [стандартному диалоговому окну интерфейса сканирования AVG](#). Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.
- **Отмена.** Отмена любых изменений, выполненных на этой или других вкладках данного диалогового окна, а также возврат к [диалоговому окну по умолчанию интерфейса сканирования AVG](#).

11.5.2. Способы сканирования



На вкладке **Способ сканирования** приведен список параметров сканирования, которые при



необходимости можно включить или отключить. По умолчанию большинство параметров включены и используются при сканировании. Если нет веских оснований для изменения данных параметров, рекомендуется не изменять стандартные настройки.

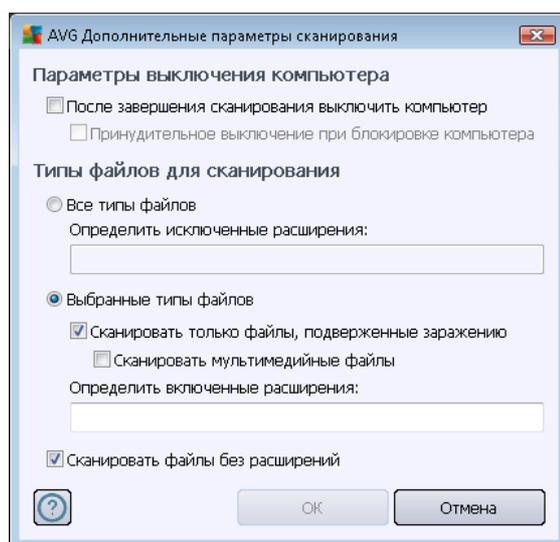
- **Автоматически лечить или удалять зараженные вирусами объекты** (выбрано по умолчанию): обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если зараженный файл невозможно вылечить автоматически или данный параметр отключен, отобразится уведомление об обнаружении вируса с выбором действия по отношению к зараженному объекту. Рекомендуется переместить зараженный файл в [хранилище вирусов](#).
- **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО** (по умолчанию включено). Установите флажок для активации модуля [Anti-Spyware](#) и сканирования на наличие шпионского ПО и вирусов. Шпионские программы относят к категории сомнительного вредоносного ПО: несмотря на то, что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуется включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.
- **Уведомлять о расширенном наборе потенциально нежелательных программ** (по умолчанию выключено). Установите данный флажок для обнаружения расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.
- **Сканировать на наличие следящих файлов cookie** (не выбрано по умолчанию). Этот параметр компонента [Anti-Spyware](#) включает поиск файлов cookie при сканировании; (файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержанием корзины для покупок через Интернет).
- **Сканировать объекты в архивах** (не выбрано по умолчанию). Данный параметр означает, что при сканировании должны быть проверены все файлы, даже те, которые находятся в архивах некоторых типов, например ZIP, RAR и других.
- **Использовать эвристический анализ** (выбрано по умолчанию). Эвристический анализ (динамичная эмуляция команд сканированных объектов в виртуальной компьютерной среде) является одним из способов, используемых для выявления вирусов при сканировании.
- **Сканировать системную среду** (выбрано по умолчанию): при сканировании будут также проверяться системные области компьютера.
- **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (например, при подозрении, что компьютер заражен) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера,

которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

- **Сканировать на наличие пакетов программ rootkit** (выбрано по умолчанию). Компонент [Anti-Rootkit](#) сканирует компьютер на возможное наличие пакетов программ rootkit (программы и технологии, позволяющие скрыть вредоносную активность на компьютере). Если программа rootkit обнаружена, это еще не значит, что компьютер заражен. В некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за средства rootkit.

Затем, чтобы изменить параметры сканирования, выполните следующие действия.

- **Дополнительные параметры сканирования.** Эта ссылка открывает новое диалоговое окно **Дополнительные параметры сканирования**, где можно указывать следующие параметры.

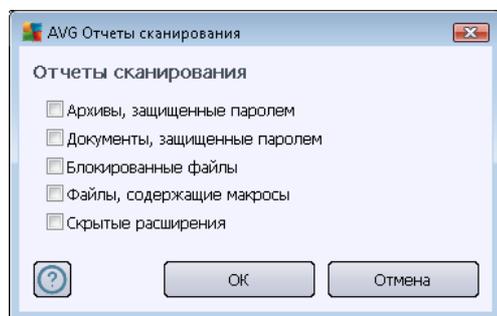


- **Параметры выключения компьютера.** Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (**Выключить компьютер после завершения сканирования**) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (**Принудительное выключение при блокировке компьютера**).
- **Определение типов файлов для сканирования.** Далее необходимо указать типы файлов для сканирования.
 - **Все типы файлов** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет;
 - **Выбранные типы файлов.** Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые*

файлы или другие неисполняемые файлы), включая мультимедийные файлы (видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.

➤ Дополнительно можно установить флажок **Сканировать файлы без расширений**. Он установлен по умолчанию. Рекомендуется не снимать его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

- **Настройка времени выполнения сканирования.** Для изменения приоритета процесса сканирования используйте ползунок. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).
- **Настроить дополнительные отчеты сканирования.** При нажатии этой ссылки открывается диалоговое окно **Отчеты сканирования**, в котором можно выбрать типы объектов, сведения о которых должны отображаться в отчете.



Кнопки управления

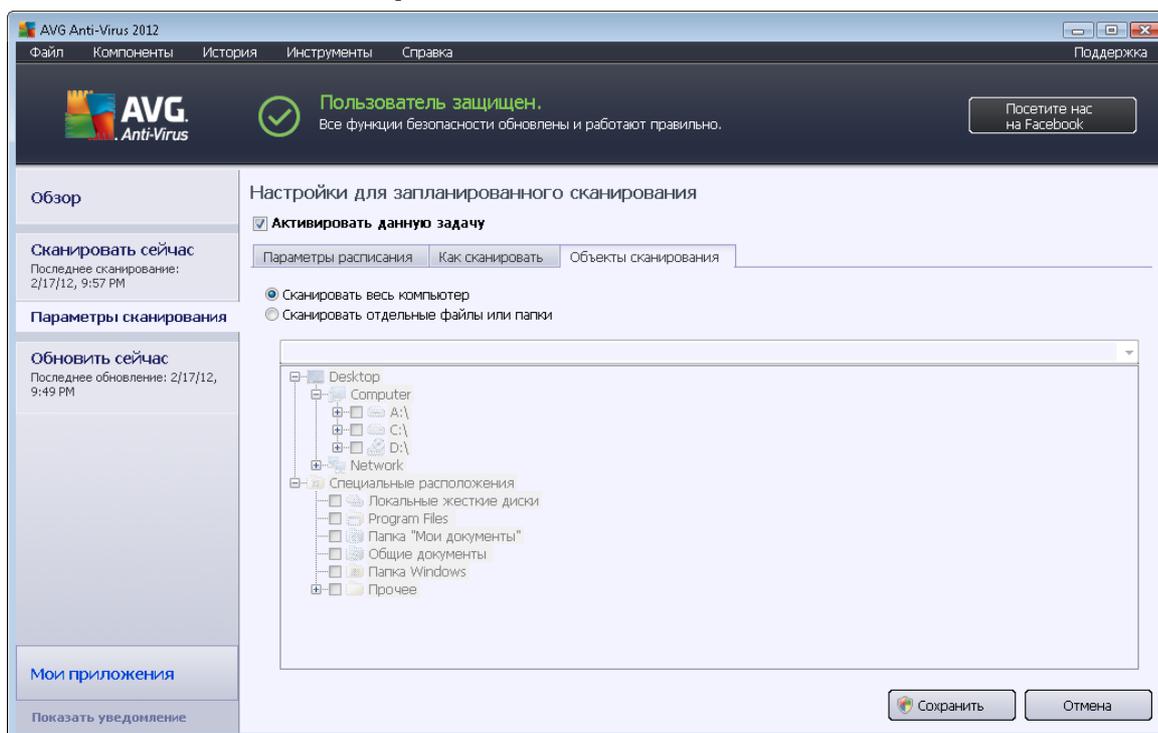
На каждой из трех вкладок ([Настройки расписания](#), [Способы сканирования](#) и [Объекты сканирования](#)) диалогового окна **Настройки запланированного сканирования** расположены две кнопки управления с одинаковыми функциями независимо от того, какая вкладка выбрана.

- **Сохранить.** Сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, а также обратный переход к [стандартному диалоговому окну интерфейса сканирования AVG](#). Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.
- **Отмена.** Отмена любых изменений, выполненных на этой или других вкладках данного диалогового окна, а также возврат к [диалоговому окну по умолчанию](#)



[интерфейса сканирования AVG.](#)

11.5.3. Объекты сканирования



На вкладке **Объекты сканирования** можно запланировать [сканирование всего компьютера](#) или [сканирование отдельных файлов и папок](#).

При выборе сканирования отдельных файлов или папок в нижней части этого диалогового окна станет доступно дерево структуры, позволяющее выбрать папки, которые необходимо сканировать (*нажимайте на узел со значком плюса, чтобы раскрывать элементы*). Установив соответствующие флажки, можно выбрать несколько папок. Выбранные папки будут отображены в текстовом поле в верхней части диалогового окна, а в раскрывающемся списке будет сохранена история сканирования, которую можно использовать в дальнейшем. Также можно вручную ввести полный путь к нужной папке (*при указании нескольких путей необходимо использовать в качестве разделителя точку с запятой без дополнительных пробелов*).

В структуре дерева также отображается ветвь **Специальные расположения**. Ниже приведен список мест, которые будут отсканированы после установки соответствующего флажка.

- **Локальные жесткие диски**. Все жесткие диски компьютера.
- **Program Files**
 - C:\Program Files\



○ в 64-разрядной версии C:\Program Files (x86)

• **Папка Мои документы**

○ для Win XP: C:\Documents and Settings\Default User\My Documents\

○ для Windows Vista/7: C:\Users\user\Documents\

• **Общие документы**

○ для Win XP: C:\Documents and Settings\All Users\Documents\

○ для Windows Vista/7: C:\Users\Public\Documents\

• **Папка Windows** — C:\Windows\

• **Прочее**

○ **Системный диск.** Жесткий диск, на котором установлена операционная система (обычно диск C:).

○ **Системная папка** — C:\Windows\System32\

○ **Папка временных файлов** — C:\Documents and Settings\User\Local\ (Windows XP); или C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)

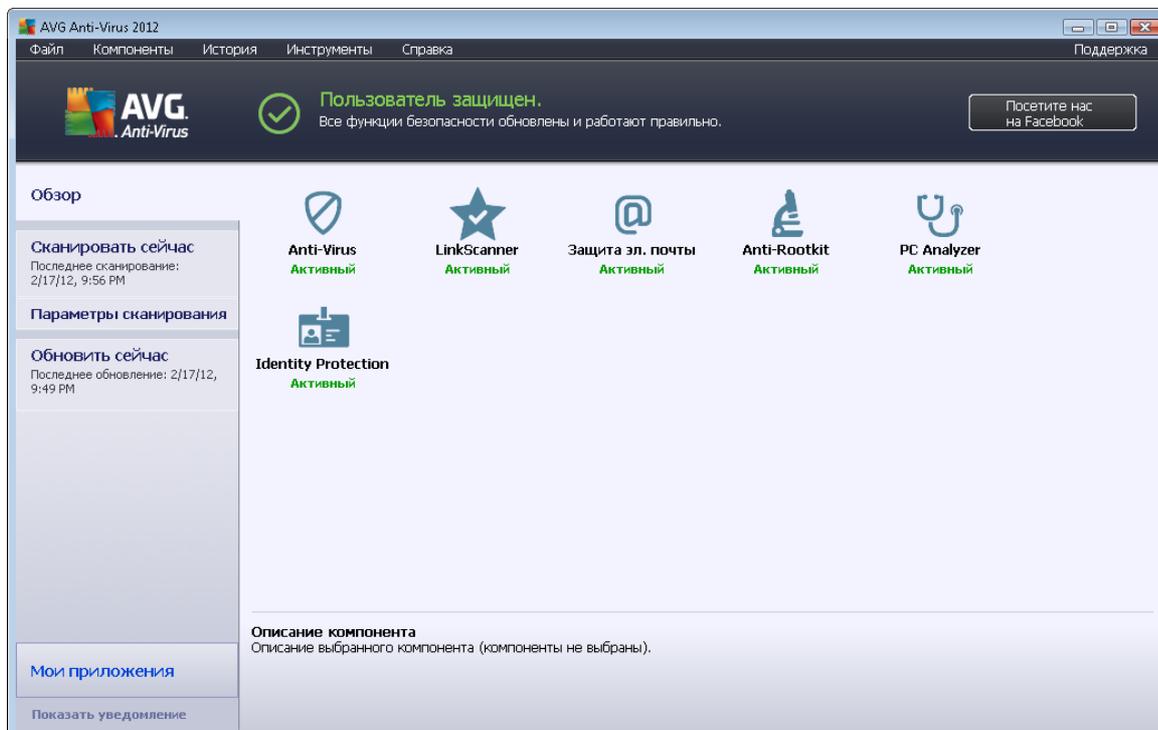
○ **Временные файлы Интернета** — C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); или C:\Users\user\AppData\Local\Temp\Microsoft\Windows\Временные файлы Интернета (Windows Vista/7)

Кнопки управления

На каждой из трех вкладок ([Настройки расписания](#), [Способы сканирования](#) и [Объекты сканирования](#)) диалогового окна **Настройки запланированного сканирования** расположены две кнопки управления с одинаковыми функциями независимо от того, какая вкладка выбрана.

- **Сохранить.** Сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, а также обратный переход к [стандартному диалоговому окну интерфейса сканирования AVG](#). Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.
- **Отмена.** Отмена любых изменений, выполненных на этой или других вкладках данного диалогового окна, а также возврат к [диалоговому окну по умолчанию интерфейса сканирования AVG](#).

11.6. Обзор результатов сканирования



Диалоговое окно **Обзор результатов сканирования** можно просмотреть, нажав в [интерфейсе сканирования AVG](#) кнопку **Журнал сканирования**. В данном диалоговом окне приводится список всех запущенных ранее процессов сканирования, а также сведения о полученных результатах.

- **Имя** – наименование сканирования; это может быть [предварительно определенное название сканирования](#) или [пользовательское наименование запланированного сканирования](#). Рядом с каждым именем отображается значок, обозначающий результат сканирования:

 – зеленый значок отображается, если при сканировании не было обнаружено заражений

 – синий значок отображается, если при сканировании были обнаружены заражения, но зараженные объекты были автоматически удалены

 – красный значок отображается, если при сканировании были обнаружены заражения, но не удалось удалить зараженные объекты

Значки могут быть цельными или разделенными – цельные значки обозначают сканирования, которые были полностью завершены; разделенные значки обозначают отмененные или прерванные сканирования.

Примечание. Подробные сведения об операциях сканирования см. в диалоговом окне [Результаты сканирования](#), доступном при нажатии кнопки



Просмотреть сведения (в нижней части данного диалогового окна).

- **Время запуска.** дата и время запуска процесса сканирования
- **Время окончания.** дата и время завершения процесса сканирования
- **Проверенные объекты.** количество объектов, проверенных в процессе сканирования
- **Вирусы.** Количество обнаруженных и удаленных вирусов
- **Шпионское ПО.** Количество обнаруженных и удаленных объектов шпионского ПО.
- **Предупреждения.** Количество [обнаруженных подозрительных объектов](#)
- **Rootkit.** Количество обнаруженных [средств rootkit](#)
- **Сведения журнала сканирования.** сведения, связанные с процессом и результатами сканирования (обычно при завершении или прерывании процесса сканирования)

Кнопки управления

В диалоговом окне **Обзор результатов сканирования** доступны следующие кнопки управления.

- **Просмотреть сведения.** Нажмите, чтобы перейти в окно [Результаты сканирования](#) для просмотра подробных сведений о выбранном сеансе сканирования.
- **Удалить результат.** Нажмите, чтобы удалить выбранный объект из обзора результатов сканирования.
- **Назад.** Данная кнопка служит для повторного открытия диалогового окна [интерфейса сканирования AVG](#)

11.7. Сведения о результатах сканирования

Если в диалоговом окне [Обзор результатов сканирования](#) выбрано определенное сканирование, можно нажать кнопку **Просмотреть сведения** для перехода к диалоговому окну **Результаты сканирования**. В данном окне приведены подробные сведения о процессе и результате выбранного сканирования. Данное диалоговое окно состоит из нескольких вкладок.

- **Обзор результатов.** Данная вкладка отображается каждый раз при выполнении сканирования и предоставляет статистические данные с описанием процесса сканирования.
- **Заражения.** Данная вкладка отображается только в том случае, если во время сканирования было обнаружено заражение вирусом.
- **Шпионское ПО.** Данная вкладка отображается только в том случае, если во время



сканирования было обнаружено шпионское ПО.

- [Предупреждения](#). Данная вкладка отображается, например, в том случае, если во время сканирования были обнаружены файлы cookie.
- [Rootkit](#). Данная вкладка отображается только в том случае, если во время сканирования были обнаружены средства rootkit.
- [Сведения](#). Данная вкладка отображается только в том случае, если были обнаружены потенциальные угрозы, не попадающие ни под одну из перечисленных выше категорий; в данном случае на вкладке отображается предупреждающее сообщение об обнаружении. Также на ней приведены сведения об объектах, которые не удалось отсканировать (например, защищенные паролем архивы).

11.7.1. Вкладка "Обзор результатов"

AVG Anti-Virus 2012

Файл Компоненты История Инструменты Справка Поддержка

Пользователь защищен.
Все функции безопасности обновлены и работают правильно.

Посетите нас на Facebook

Обзор

Обзор сканирования Сведения Заражения Шпионское ПО

Сканирование "Сканирование файлов или папок" завершено.
Неудаленные или невылеченные объекты требуют вашего внимания.

	Обнаружено	Удалено и вылечено	Не удалено или не вылечено
Заражения	5	0	5
Шпионское ПО	11	0	11

Выбранные папки: -C:\Users\Administrator\Documents\;
Сканирование запущено: Friday, February 17, 2012, 9:57:02 PM
Сканирование завершено: Friday, February 17, 2012, 9:57:06 PM (3 секунда(ы))
Всего сканировано объектов: 20
Пользователь: Administrator
[Экспорт отчета в файл ...](#)

Удалить все невылеченные объекты

Закрыть результаты

На вкладке **Результаты сканирования** содержатся следующие подробные статистические сведения:

- обнаруженные заражения/шпионское ПО
- удаленные заражения/шпионское ПО
- количество заражений/шпионского ПО, которые не могут быть удалены или вылечены

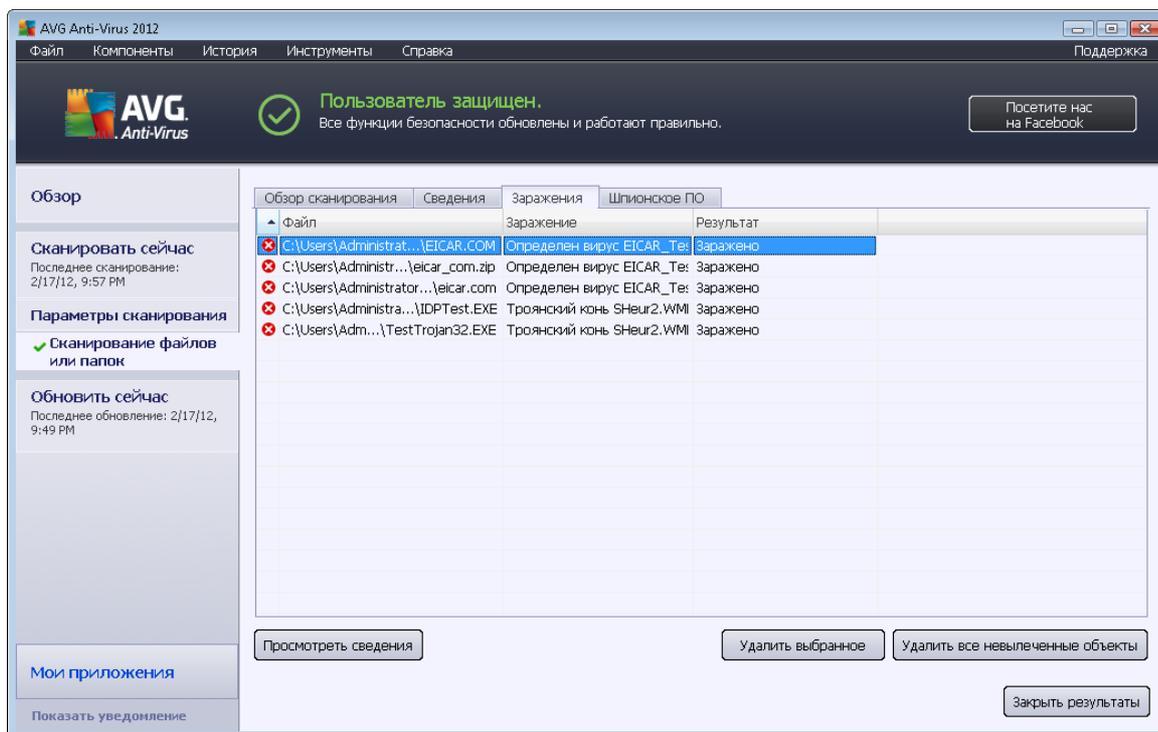
Кроме того, здесь содержится информация о дате и точном времени запуска сканирования, общем количестве сканированных объектов, продолжительности сканирования и количестве ошибок, произошедших при сканировании.



Кнопки управления

В данном диалоговом окне имеется только одна кнопка управления. Кнопка **Закр~~ыть~~ результаты** выполняет переход обратно к диалоговому окну [Обзор результатов сканирования](#).

11.7.2. Вкладка "Заражения"



Вкладка **Заражения** отображается в диалоговом окне **Результаты сканирования** только в том случае, если во время сканирования было обнаружено заражение вирусом. Вкладка разделена на три части, содержащие следующие данные.

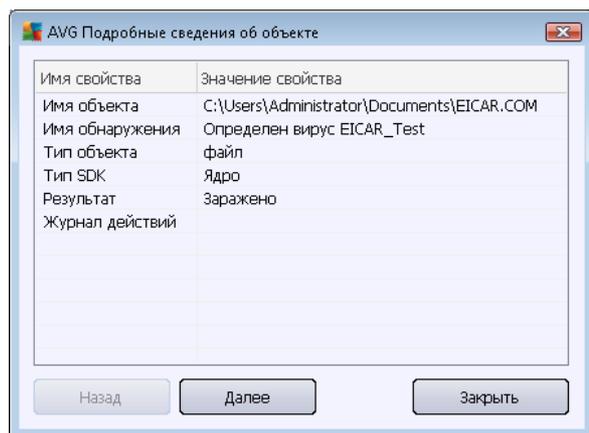
- **Файл.** Полный путь к исходному местоположению зараженного объекта.
- **Зараженный объект.** Имя обнаруженного вируса (*подробные сведения об определенных вирусах см. в интерактивной [энциклопедии вирусов](#)*).
- **Результат.** Определение текущего состояния объекта, обнаруженного при сканировании.
 - **Заражен.** Зараженный объект обнаружен и не перемещен (*например, если в настройках сканирования отключен параметр автоматического лечения*).
 - **Вылечен.** Зараженный объект вылечен автоматически, его начальное местоположение сохранено.

- **Перемещен в хранилище вирусов.** Зараженный объект помещен на карантин в [хранилище вирусов](#).
- **Удален.** Зараженный объект удален.
- **Добавлен в список исключений PUP.** Обнаруженный объект получил статус исключения и добавлен в список исключений PUP (настроенный в диалоговом окне дополнительных параметров [Исключения PUP](#)).
- **Заблокированный файл — не проверен.** Объект заблокирован, поэтому AVG не может выполнить его сканирование.
- **Потенциально опасный объект.** Объект является потенциально опасным, но не заражен (*например, содержит макросы*); данная информация имеет лишь предупредительный характер.
- **Для завершения процесса требуется перезагрузка.** Невозможно удалить зараженный объект; необходимо перезагрузить компьютер, чтобы полностью удалить объект.

Кнопки управления

В данном диалоговом окне доступны три кнопки управления.

- **Просмотреть сведения.** В результате нажатия данной кнопки открывается новое диалоговое окно **Подробная информация об объектах**.



В данном диалоговом окне приведена подробная информация об обнаруженном зараженном объекте (*например, имя, местонахождение, тип объекта, результаты обнаружения и история событий, связанных с обнаруженным объектом*). С помощью кнопок **Назад/Далее** можно просматривать сведения об определенных обнаруженных объектах. Чтобы закрыть диалоговое окно, нажмите кнопку **Заккрыть**.

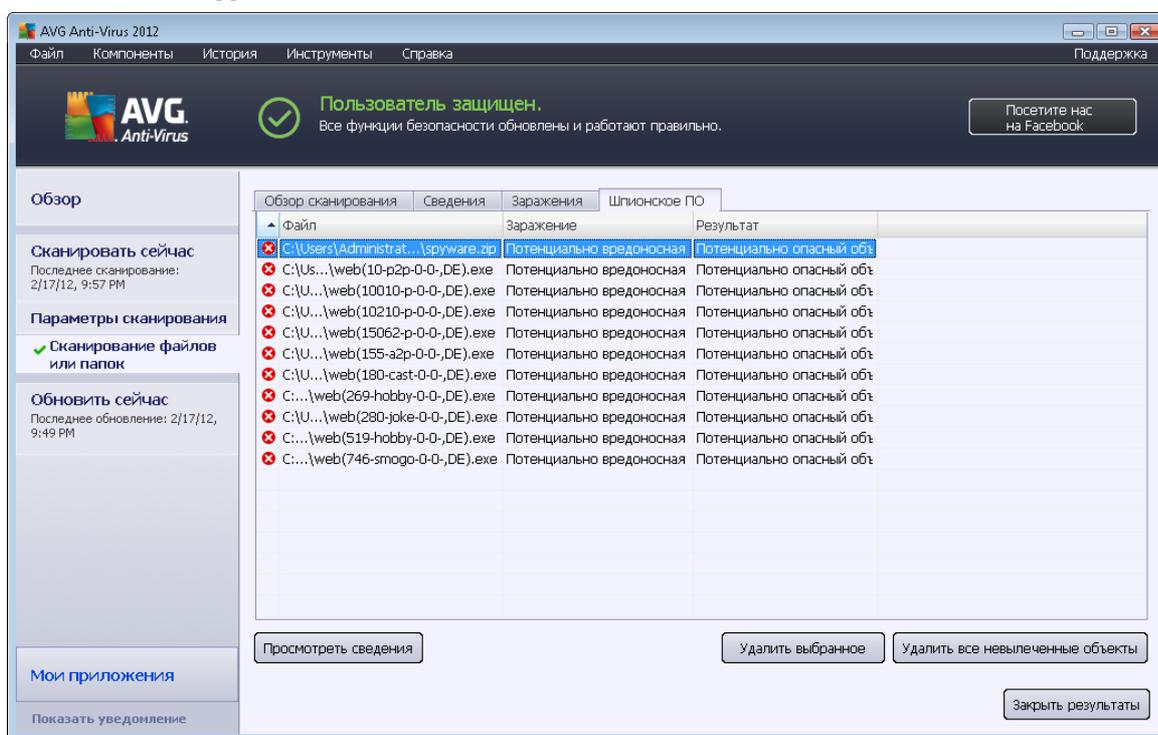
- **Удалить выбранные.** С помощью этой кнопки можно переместить выбранные



обнаруженные объекты в [хранилище вирусов](#)

- **Удалить все зараженные объекты, лечение которых невозможно.** С помощью этой кнопки можно удалить все обнаруженные объекты, которые не могут быть вылечены или перемещены в [хранилище вирусов](#)
- **Закреть результаты.** Закрытие окна просмотра сведений и возврат к окну [Просмотр результатов сканирования](#).

11.7.3. Вкладка "Шпионское ПО"



Вкладка **Шпионское ПО** отображается в диалоговом окне **Результаты сканирования**, только если при сканировании было обнаружено шпионское программное обеспечение.

Вкладка разделена на три части, содержащие следующие данные.

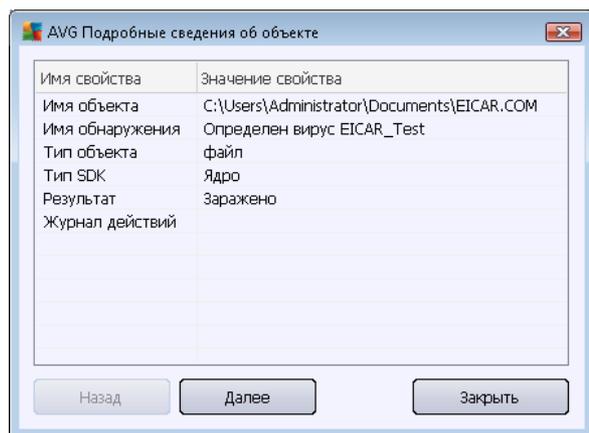
- **Файл.** Полный путь к исходному местоположению зараженного объекта.
- **Заражения.** Имя обнаруженного шпионского ПО (*подробные сведения об определенных вирусах см. в интерактивной [Энциклопедии вирусов](#)*).
- **Результат.** Определяет текущее состояние объекта, обнаруженного при сканировании.
 - **Заражен.** Зараженный объект обнаружен и не перемещен (*например, если в настройках сканирования [отключен параметр автоматического лечения](#)*).
 - **Вылечен.** Зараженный объект вылечен автоматически, его начальное местоположение не изменено.

- **Перемещен в хранилище вирусов.** Зараженный объект помещен на карантин в [хранилище вирусов](#).
- **Удален.** Зараженный объект удален.
- **Добавлен в список исключений PUP.** Обнаруженный объект получил статус исключения и добавлен в список исключений PUP (*настроенный в диалоговом окне дополнительных параметров [Исключения PUP](#)*).
- **Заблокированный файл — не проверен.** Объект заблокирован, поэтому AVG не может выполнить его сканирование.
- **Потенциально опасный объект.** Объект является потенциально опасным, но не заражен (например, содержит макросы); данная информация имеет лишь предупредительный характер.
- **Для завершения процесса требуется перезагрузка.** Невозможно удалить зараженный объект; необходимо перезагрузить компьютер, чтобы полностью удалить объект.

Кнопки управления

В данном диалоговом окне доступны три кнопки управления.

- **Просмотреть сведения.** В результате нажатия данной кнопки открывается новое диалоговое окно **Подробная информация об объектах**.



В данном диалоговом окне приведена подробная информация об обнаруженном зараженном объекте (*например, имя, местонахождение, тип объекта, результаты обнаружения и история событий, связанных с обнаруженным объектом*). С помощью кнопок **Назад/Далее** можно просматривать сведения об определенных обнаруженных объектах. Чтобы закрыть диалоговое окно, нажмите кнопку **Заккрыть**.

- **Удалить выбранные.** С помощью этой кнопки можно переместить выбранные



обнаруженные объекты в [хранилище вирусов](#)

- **Удалить все зараженные объекты, лечение которых невозможно.** С помощью этой кнопки можно удалить все обнаруженные объекты, которые не могут быть вылечены или перемещены в [хранилище вирусов](#)
- **Закрыть результаты.** Закрытие окна просмотра сведений и возврат к окну [Просмотр результатов сканирования](#)

11.7.4. Вкладка "Предупреждения"

Вкладка **Предупреждения** содержит сведения о подозрительных объектах (*обычно это файлы*), обнаруженных при сканировании. При обнаружении компонентом Resident Shield доступ к данным файлам блокируется. Типичные примеры данных объектов: скрытые файлы, файлы cookie, подозрительные ключи реестра, защищенные паролем документы или архивы, а также некоторые другие объекты. Данные файлы не представляют прямой угрозы компьютеру или безопасности. Сведения о данных файлах могут быть полезны в случае обнаружения на компьютере шпионского или рекламного ПО. Если в результатах проверки выводятся только предупреждения **AVG Anti-Virus 2012**, не требуется предпринимать каких-либо действий.

Ниже приведено краткое описание наиболее распространенных подозрительных объектов.

- **Скрытые файлы** — файлы, которые по умолчанию не отображаются в ОС Windows. Поэтому некоторые вирусы и другие угрозы могут попытаться избежать обнаружения, присвоив своим файлам атрибут "Скрытый". Если программа **AVG Anti-Virus 2012** сообщает об обнаружении скрытого файла, который кажется подозрительным, его можно переместить в [хранилище вирусов](#).
- **Файлы cookie** — это обычные текстовые файлы, используемые веб-сайтами для хранения определенной информации о пользователе, которая используется для последующей загрузки пользовательской компоновки веб-сайта, автоматического ввода имени пользователя и для других целей.
- **Подозрительные ключи реестра.** Некоторое вредоносное ПО размещает информацию в реестре Windows, чтобы обеспечить загрузку ПО при запуске ОС, а также для расширения своего воздействия на операционную систему.

11.7.5. Вкладка Rootkits

Вкладка **Rootkits** содержит информацию о пакетах программ rootkit, обнаруженных при сканировании, если была запущена функция [Сканирование всего компьютера](#).

Rootkit — это программа, предназначенная для полного управления системой компьютера без разрешения владельцев систем или законных управляющих. Средствам rootkit обычно не требуется доступ к оборудованию, так как они предназначены для управления операционными системами, установленными на этом оборудовании. В большинстве случаев средства rootkit скрывают свое присутствие в системе с помощью замены информации или обхода стандартных механизмов безопасности операционных систем. Кроме того, они могут попадать на компьютер в виде троянских программ, которые пользователи уверенно запускают, не подозревая об опасности. Используемые для этого технические приемы включают в себя скрытие запущенных процессов от следящих программ, а файлов и системных данных — от операционных систем.



Структура данной вкладки идентична структуре вкладок [Заражения](#) или [Шпионское ПО](#).

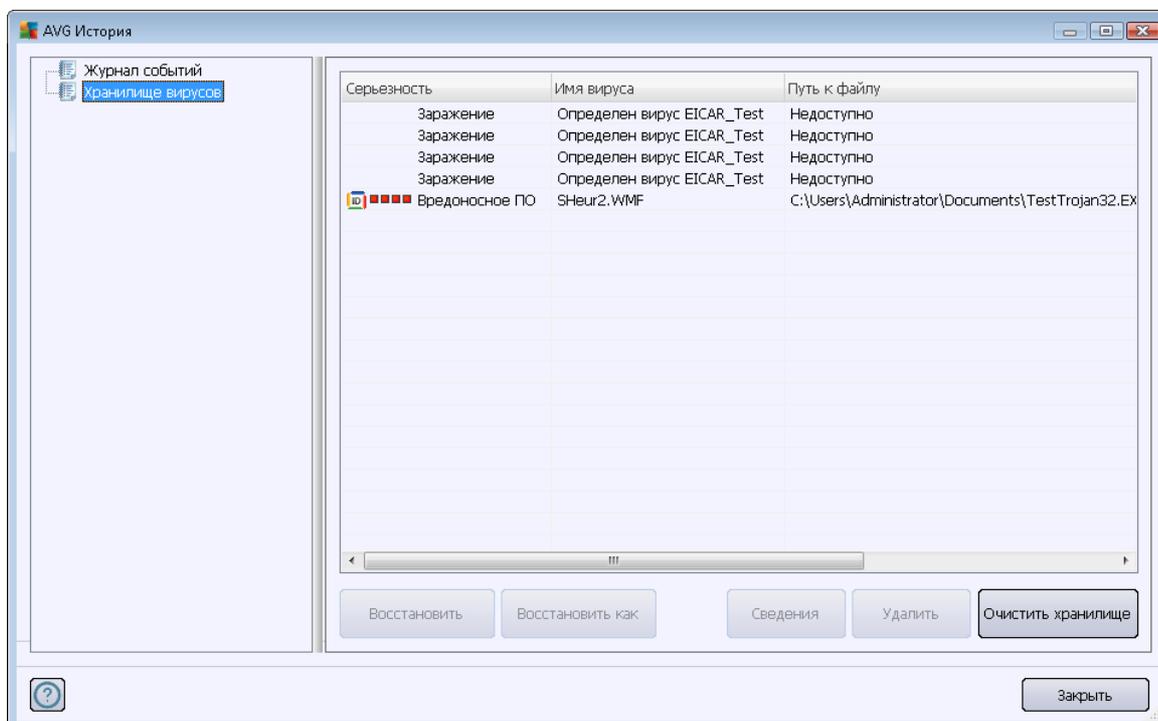
11.7.6. Вкладка "Сведения"

На вкладке **Сведения** содержатся данные о найденных объектах, которые не удалось отнести к доступным категориям (заражения, шпионское ПО и т. п.). Данные объекты не были отмечены как "опасные", но они являются подозрительными. Сканирование **AVG Anti-Virus 2012** позволяет определять файлы, которые могут быть не заражены, но являются подозрительными. Сообщение о таких файлах отображается в виде [предупреждения](#) или сведений.

Сообщения со **сведениями** об уровне опасности отображаются в следующих случаях.

- **Упаковывание в среде выполнения.** упаковывание файла с помощью нераспространенного упаковщика среды выполнения, что может указывать на попытку предотвращения сканирования такого файла. Однако не каждое сообщение о таком файле указывает на наличие вируса.
- **Рекурсивное упаковывание в среде выполнения.** случай, похожий на описанный выше, но встречающийся реже при использовании распространенного ПО. Такие файлы являются подозрительными и могут быть удалены или отправлены на анализ.
- **Архив или документ, защищенные паролем.** Файлы, защищенные паролем, не могут быть проверены программой **AVG Anti-Virus 2012** (или другой антивирусной программой).
- **Документ, содержащий макросы.** документ, указанный в отчете, содержит макросы, которые могут быть вредоносными.
- **Скрытое расширение.** файлы со скрытым расширением могут отображаться, например как изображения, но в действительности являться исполняемыми файлами (например, *изображение.jpg.exe*). Второе расширение не отображается в ОС Windows по умолчанию, и **AVG Anti-Virus 2012** предоставляет отчет о таких файлах, чтобы предотвратить их случайное открытие.
- **Неправильный путь к файлу.** Если при запуске некоторых важных системных файлов используется путь, отличный от пути по умолчанию (например, *файл winlogon.exe* запускается не из папки Windows), **AVG Anti-Virus 2012** программа сообщает о таком расхождении. В некоторых случаях вирусы используют имена стандартных системных процессов, чтобы скрыть свое присутствие в системе.
- **Заблокированный файл.** Файл заблокирован, **AVG Anti-Virus 2012** не сможет выполнить его проверку. Обычно это означает, что некоторые файлы в настоящий момент используются системой (например, *файл подкачки*).

11.8. Хранилище вирусов



Хранилище вирусов. это безопасная среда для управления зараженными или подозрительными объектами во время проведения тестов AVG. При обнаружении во время сканирования зараженного объекта, который программе AVG не удалось вылечить автоматически, отобразится запрос на выбор дальнейших действий в отношении данного объекта. Рекомендуется переместить объект в **хранилище вирусов** для дальнейшего лечения. Основное назначение **хранилища вирусов** — хранить удаленный файл в течение определенного времени, чтобы дать возможность принять решение о необходимости удаления файла из исходного места. Если отсутствие файла вызывает проблемы, можно отправить его на анализ или восстановить в исходном месте.

Интерфейс **хранилища вирусов** открывается в отдельном окне и предоставляет обзор сведений о зараженных объектах, помещенных в карантин.

- **Серьезность.** при установке компонента [Identity Protection](#) в **AVG Anti-Virus 2012** в этом разделе будет показано графическое обозначение уровня опасности по шкале, имеющей 4 уровня, от безопасного (■□□□) до очень опасного (■□□■), а также информация о типе заражения (в зависимости от уровня заражения все объекты могут быть заражены или потенциально заражены).
- **Имя вируса.** Имя обнаруженного заражения в соответствии с [энциклопедией вирусов](#) (в Интернете).
- **Путь к файлу.** Полный путь к исходному местоположению зараженного объекта.
- **Исходное имя объекта.** В процессе сканирования всем объектам, заносимым в



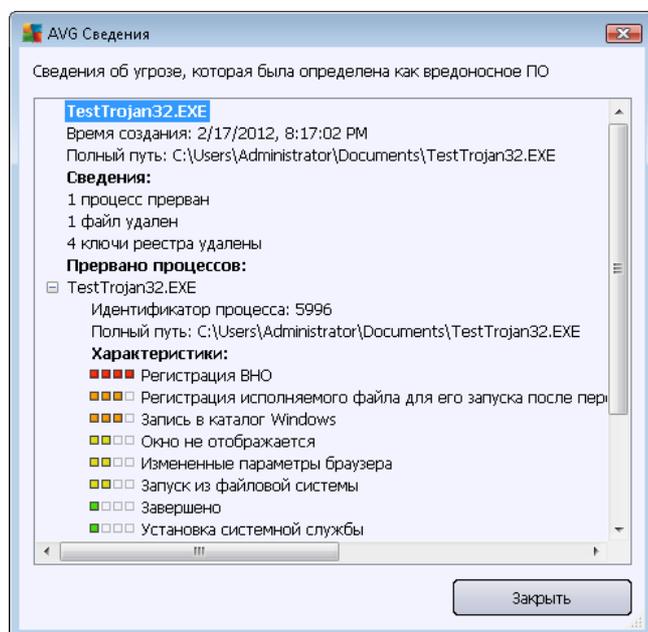
список, программа AVG присваивает стандартное имя. Если же объект имел свое известное исходное имя (*например, имя вложения электронной почты, не соответствующее фактическому содержимому вложения*), оно отобразится в данном столбце.

- **Дата хранения.** Дата и время обнаружения подозрительного файла и его перемещения в хранилище вирусов

Кнопки управления

В интерфейсе **хранилища вирусов** доступны следующие кнопки управления.

- **Восстановить.** Перемещение зараженного файла в исходное местоположение на диске.
- **Восстановить как.** Перемещение зараженного файла в выбранную папку
- **Сведения.** Данную кнопку можно применить только к угрозам, обнаруженным компонентом [Identity Protection](#). При ее нажатии отображаются сводные сведения об угрозе (*какие файлы/процессы были затронуты, характеристики процесса и т. д.*). Обратите внимание, что для всех других элементов, не обнаруженных компонентом IDP, данная кнопка недоступна и неактивна!



- **Удалить.** Полное удаление зараженного файла из **хранилища вирусов**.
- **Очистить хранилище.** Удаление всех файлов из **хранилища вирусов**. При удалении файлов из **хранилища вирусов** они будут также удалены с диска без возможности восстановления (*то есть они не будут помещены в корзину*).



12. Обновления AVG

Ни один из программных продуктов для защиты данных не может гарантировать полноценную защиту от различных типов угроз без регулярного обновления. Создатели вирусов ищут новые уязвимые места для взлома программного обеспечения и операционных систем. Ежедневно совершаются попытки несанкционированного доступа, появляются новые вирусы и вредоносное ПО. Именно поэтому поставщиками программного обеспечения постоянно выпускаются обновления и исправления для систем безопасности, предназначенные для исправления обнаруженных уязвимостей.

Учитывая все новые возникающие угрозы и скорость их распространения, очень важно регулярно выполнять обновление **AVG Anti-Virus 2012**. Оптимальным решением является сохранение параметров по умолчанию, где автоматическое обновление уже настроено. Обратите внимание, что если не обновлять вирусную базу данных **AVG Anti-Virus 2012**, программа не сможет обнаруживать новые угрозы.

Очень важно выполнять регулярное обновление продуктов AVG. Важные обновления определений вирусов должны выполняться ежедневно, если это возможно. Обновление менее важных программ может выполняться один раз в неделю.

12.1. Запуск обновления

Для обеспечения максимальной защиты программа **AVG Anti-Virus 2012** по умолчанию проверяет новые обновления каждые четыре часа. Так как обновления AVG выпускаются не по расписанию, а в ответ на количество и опасность появляющихся новых угроз, крайне важно регулярно обновлять вирусную базу данных AVG.

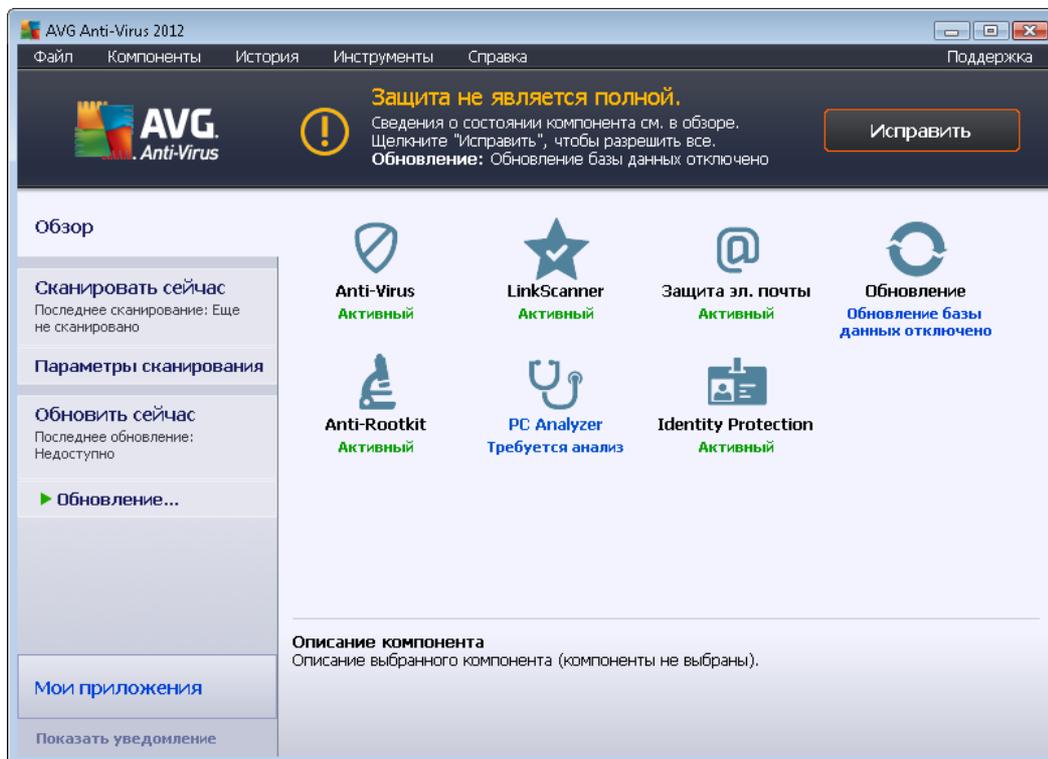
При необходимости можно уменьшить количество запусков обновления установив свои параметры запуска обновления. Тем не менее, настоятельно рекомендуется запускать обновление как минимум раз в день. Данную конфигурацию можно настроить в разделе [Дополнительные параметры/Расписания](#) в следующих окнах:

- [Расписание обновления определений](#)
- [Расписание обновления программы](#)

Если необходимо немедленно произвести проверку новых файлов обновления, щелкните ссылку [Обновить сейчас](#) в главном интерфейсе пользователя. Данная ссылка постоянно доступна в диалоговом окне [Интерфейс пользователя](#).

12.2. Ход обновления

После подтверждения начала обновления программа AVG сначала проверит наличие новых доступных файлов обновления. Если файлы имеются, **AVG Anti-Virus 2012** начнет их загрузку и выполнит запуск обновления самостоятельно. В процессе обновления откроется интерфейс **Обновление**, где можно просмотреть выполняемый процесс в графическом представлении, а также ознакомиться с соответствующими статистическими параметрами (*размер файла обновления, полученные данные, скорость загрузки, время выполнения и т. п.*)



Примечание. Перед запуском обновления программы AVG создается точка восстановления системы. Если не удастся выполнить обновление или произойдет сбой в работе ОС, всегда можно будет восстановить начальную конфигурацию ОС с этой точки. Этот параметр доступен из меню Windows: Пуск/Все программы/Стандартные/Служебные/Восстановление системы. Рекомендуется использовать только опытным пользователям.

12.3. Уровни обновлений

AVG Anti-Virus 2012 предлагает два уровня обновлений на выбор.

- **Обновление определений** содержит изменения, необходимые для обеспечения надежной защиты от вирусов. Как правило, сюда не включены изменения кода, а только обновления базы данных определений. Обновление необходимо выполнять сразу после его выпуска.
- **Обновление программы.** Содержит различные изменения, исправления и улучшения программы.

При [планировании обновления](#) можно настроить определенные параметры для обеих уровней обновлений.

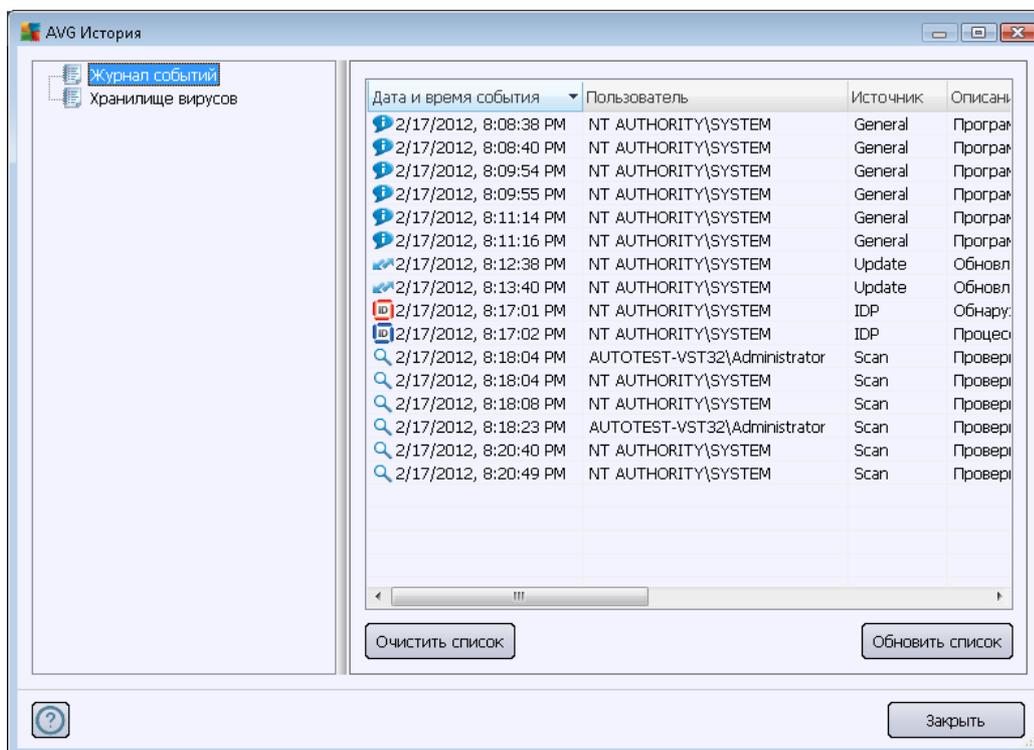
- [Расписание обновления определений](#)
- [Расписание обновления программы](#)

Примечание. Если запланированное обновление программы и сканирование пересекутся по



времени, сканирование будет прервано, так как процесс обновления имеет более высокий приоритет.

13. Журнал событий



Диалоговое окно **История** доступно в [СИСТЕМНОМ МЕНЮ](#) при выборе элемента **История/Журнал событий**. В этом окне можно посмотреть перечень важных событий, произошедших во время работы **AVG Anti-Virus 2012**. В журнале **История** регистрируются следующие типы событий.

- Сведения об обновлениях приложения AVG
- Данные о начале, завершении или приостановке процесса сканирования (*включая автоматически проведенные тесты*).
- Данные о событиях, связанных с обнаружением вирусов (*компонентом [Resident Shield](#) или при [сканировании](#)*), включая местонахождение угрозы.
- Другие важные события

Для каждого события отображаются следующие сведения.

- **Дата и время события.** Указание точной даты и времени события.
- **Имя пользователя.** Указание имени пользователя, зарегистрированного в системе во время события.
- **Источник.** Предоставление информации об исходном компоненте или другом элементе системы AVG, который запустил событие



- **Описание события.** Краткое описание произошедшего события

Кнопки управления

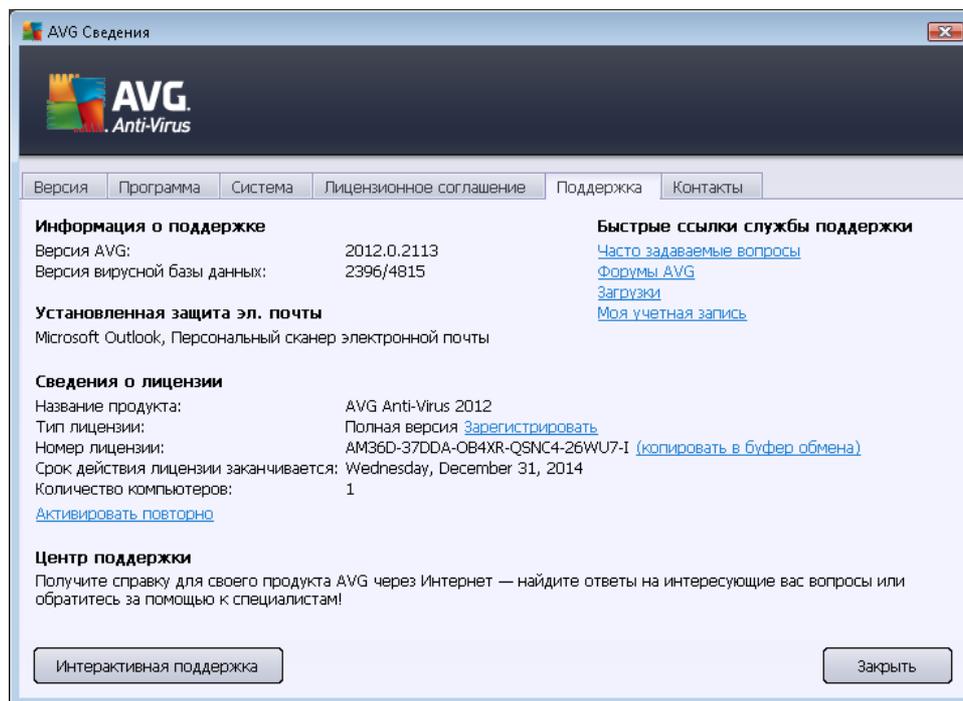
- **Очистить список.** Удаление всех записей из списка событий.
- **Обновить список.** Нажатие этой кнопки обновляет все записи в списке событий.



14. Часто задаваемые вопросы и техническая поддержка

При возникновении вопросов о продажах или технических проблем, связанных с использованием приложения **AVG Anti-Virus 2012**, существует несколько способов получения справочной информации. Выберите один из следующих вариантов:

- **Получить поддержку.** С помощью меню приложения AVG можно перейти на страницу службы поддержки пользователей на веб-сайте AVG (<http://www.avg.com/>). Выберите пункт главного меню **Справка / Получить поддержку** для перехода на веб-сайт AVG с доступными средствами поддержки. Далее следуйте приведенным на веб-странице инструкциям.
- **Поддержка (ссылка в главном меню).** Меню приложения AVG (в верхней части основного пользовательского интерфейса) содержит ссылку **Поддержка**, при нажатии на которую открывается новое диалоговое окно со всей необходимой информацией для решения проблемы. В этом окне содержится основная информация об установленной программе AVG (*программа/версия базы данных*), сведения о лицензии и список ссылок для быстрого перехода в соответствующий раздел поддержки.



- **Устранение неполадок в файле справки.** Новый раздел **Устранение неполадок** можно найти в файле справки **AVG Anti-Virus 2012** (чтобы открыть файл справки, нажмите клавишу **F1** в любом диалоговом окне приложения). Данный раздел содержит список наиболее часто возникающих ситуаций, в которых пользователю может понадобиться профессиональная помощь в технических вопросах. Выберите ситуацию, которая наиболее полно описывает возникшую проблему, и щелкните на ней, чтобы открыть подробные инструкции для решения этой проблемы.



- **Центр поддержки веб-сайта компании AVG.** Также можно поискать решение возникшей проблемы на веб-сайте компании AVG (<http://www.avg.com/>). В разделе **Центр поддержки** можно найти структурированный по тематическим группам обзор, содержащий вопросы как технического характера, так и связанные с продажами.
- **Часто задаваемые вопросы.** На веб-сайте компании AVG (<http://www.avg.com/>) также можно ознакомиться с хорошо структурированным специальным разделом часто задаваемых вопросов. Данный раздел доступен из пункта меню **Центр поддержки/Часто задаваемые вопросы**. Все вопросы удобно разделены на категории, относящиеся к продажам, техническим неполадкам и вирусам.
- **Сведения о вирусах и угрозах.** Специальный раздел веб-сайта AVG (<http://www.avg.com/>) посвящен проблемам вирусов (*перейти на эту веб-страницу можно с помощью главного меню через пункт "Справка / О вирусах и угрозах"*). Для перехода на страницу с подробным обзором сетевых угроз выберите в меню пункт **Центр поддержки/Сведения о вирусах и угрозах**. Здесь можно найти инструкции по удалению вирусов и шпионского ПО, а также советы о том, как защититься.
- **Дискуссионный форум.** Проблему также можно обсудить на форуме для пользователей AVG, доступном по адресу <http://forums.avg.com>.