



AVG Internet Security 2011

Руководство пользователя

Версия документа 2011.21 (16.5.2011)

© 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	8
2. Требования для установки AVG	9
2.1 Поддерживаемые операционные системы	9
2.2 Минимальные требования и рекомендуемое оборудование	9
3. Варианты установки AVG	10
4. Процесс установки AVG	11
4.1 Добро пожаловать	11
4.2 Активация лицензии AVG	12
4.3 Выбор типа установки	13
4.4 Пользовательские параметры	14
4.5 Установка панели инструментов безопасности AVG	15
4.6 Состояние процесса установки	16
4.7 Установка выполнена успешно	16
5. После установки	18
5.1 Регистрация продукта	18
5.2 Доступ к интерфейсу пользователя	18
5.3 Сканирование всего компьютера	18
5.4 Тестирование Eicar	18
5.5 Конфигурация AVG по умолчанию	19
6. Интерфейс пользователя AVG	20
6.1 Системное меню	21
6.1.1 Файл	21
6.1.2 Компоненты	21
6.1.3 История	21
6.1.4 Инструменты	21
6.1.5 Справка	21
6.2 Информация о состоянии безопасности	24
6.3 Быстрые ссылки	25
6.4 Обзор компонентов	26
6.5 Статистика	27
6.6 Значок на панели задач	28
6.7 Гаджет AVG	29



7. Компоненты AVG	32
7.1 Anti-Virus	32
7.1.1 Принципы работы Anti-Virus	32
7.1.2 Интерфейс Anti-Virus	32
7.2 Anti-Spyware	33
7.2.1 Принципы работы Anti-Spyware	33
7.2.2 Интерфейс Anti-Spyware	33
7.3 Anti-Spam	35
7.3.1 Принципы работы Anti-Spam	35
7.3.2 Интерфейс Anti-Spam	35
7.4 Firewall	37
7.4.1 Принципы работы Firewall	37
7.4.2 Профили Firewall	37
7.4.3 Интерфейс Firewall	37
7.5 Link Scanner	41
7.5.1 Принципы работы Link Scanner	41
7.5.2 Интерфейс Link Scanner	41
7.5.3 Search-Shield	41
7.5.4 Surf-Shield	41
7.6 Resident Shield	45
7.6.1 Принципы работы Resident Shield	45
7.6.2 Интерфейс Resident Shield	45
7.6.3 Обнаружение Resident Shield	45
7.7 Защита семьи	50
7.8 AVG LiveKive	50
7.9 E-mail Scanner	50
7.9.1 Принципы работы E-mail Scanner	50
7.9.2 Интерфейс E-mail Scanner	50
7.9.3 Обнаружение E-mail Scanner	50
7.10 Диспетчер обновлений	55
7.10.1 Принципы работы диспетчера обновления	55
7.10.2 Интерфейс диспетчера обновления	55
7.11 Лицензия	57
7.12 Удаленное администрирование	58
7.13 Online Shield	59
7.13.1 Принципы работы Online Shield	59
7.13.2 Интерфейс Online Shield	59



7.13.3 Обнаружение Online Shield	59
7.14 Anti-Rootkit	62
7.14.1 Принципы работы Anti-Rootkit	62
7.14.2 Интерфейс Anti-Rootkit	62
7.15 Системные средства	64
7.15.1 Процессы	64
7.15.2 Сетевые подключения	64
7.15.3 Автозапуск	64
7.15.4 Расширения браузера	64
7.15.5 Средство просмотра LSP	64
7.16 PC Analyzer	70
7.17 ID Protection	72
7.17.1 Принципы работы ID Protection	72
7.17.2 Интерфейс ID Protection	72
7.18 Панель инструментов безопасности	75
8. Панель инструментов безопасности AVG	76
8.1 Интерфейс панели инструментов безопасности AVG	76
8.1.1 Кнопка со значком AVG	76
8.1.2 Поле поиска AVG Secure Search (powered by Google)	76
8.1.3 Состояние страницы	76
8.1.4 Новости AVG	76
8.1.5 Новости	76
8.1.6 Очистить историю	76
8.1.7 Уведомление о сообщениях эл. почты	76
8.1.8 Сведения о погоде	76
8.1.9 Facebook	76
8.2 Параметры панели инструментов безопасности AVG	83
8.2.1 Вкладка Общее	83
8.2.2 Вкладка Полезные кнопки	83
8.2.3 Вкладка Безопасность	83
8.2.4 Вкладка Дополнительные параметры	83
9. Дополнительные параметры AVG	88
9.1 Внешний вид	88
9.2 Звуки	90
9.3 Игнорирование ошибочных условий	92
9.4 Identity Protection	93
9.4.1 Параметры компонента Identity Protection	93



9.4.2	Список разрешенных объектов	93
9.5	Хранилище вирусов	97
9.6	Исключения PUP	97
9.7	Anti-Spam	99
9.7.1	Параметры	99
9.7.2	Производительность	99
9.7.3	RBL	99
9.7.4	Белый список	99
9.7.5	Черный список	99
9.7.6	Дополнительные параметры	99
9.8	Online Shield	111
9.8.1	Интернет-защита	111
9.8.2	Обмен мгновенными сообщениями	111
9.9	Link Scanner	115
9.10	Сканирования	116
9.10.1	Сканирование всего компьютера	116
9.10.2	Сканирование расширения оболочки	116
9.10.3	Сканирование отдельных файлов или папок	116
9.10.4	Сканирование съемного устройства	116
9.11	Расписания	122
9.11.1	Запланированное сканирование	122
9.11.2	Расписание обновления вирусной базы данных	122
9.11.3	Расписание обновления программы	122
9.11.4	Расписание обновления компонента Anti-Spam	122
9.12	E-mail Scanner	134
9.12.1	Сертификация	134
9.12.2	Фильтрация электронной почты	134
9.12.3	Серверы	134
9.13	Resident Shield	143
9.13.1	Дополнительные параметры	143
9.13.2	Исключенные элементы	143
9.14	Сервер кэширования	147
9.15	Anti-Rootkit	148
9.16	Обновление	149
9.16.1	Прокси-сервер	149
9.16.2	Подключение по коммутируемой линии	149
9.16.3	URL-адрес	149
9.16.4	Управление	149



9.17 Временное отключение защиты AVG	156
9.18 Программа улучшения продуктов	156
10. Параметры Firewall	160
10.1 Общие	160
10.2 Безопасность	162
10.3 Области и профили адаптеров	163
10.4 IDS	164
10.5 Журналы	166
10.6 Профили	167
11. Сканирование AVG	169
11.1 Интерфейс сканирования	169
11.2 Предопределенные сканирования	170
11.2.1 Сканирование всего компьютера	170
11.2.2 Сканирование отдельных файлов или папок	170
11.2.3 Сканирование Anti-Rootkit	170
11.3 Сканирование в Проводнике Windows	181
11.4 Сканирование с помощью командной строки	182
11.4.1 Параметры сканирования с помощью командной строки	182
11.5 Расписание сканирования	185
11.5.1 Параметры расписания	185
11.5.2 Способы сканирования	185
11.5.3 Объекты сканирования	185
11.6 Обзор результатов сканирования	194
11.7 Сведения о результатах сканирования	195
11.7.1 Вкладка "Обзор результатов"	195
11.7.2 Вкладка "Заражения"	195
11.7.3 Вкладка "Шпионское ПО"	195
11.7.4 Вкладка "Предупреждения"	195
11.7.5 Вкладка Rootkits	195
11.7.6 Вкладка "Сведения"	195
11.8 Хранилище вирусов	203
12. Обновления AVG	205
12.1 Уровни обновлений	205
12.2 Типы обновлений	205
12.3 Процесс обновления	205



13. Журнал событий	207
14. Часто задаваемые вопросы и техническая поддержка	209



1. Введение

Руководство пользователя содержит полные сведения о системе **AVG Internet Security 2011**.

Поздравляем с приобретением AVG Internet Security 2011!

AVG Internet Security 2011 является одним из представителей линейки продуктов AVG, удостоенных различных наград, который создан для обеспечения вашего спокойствия и полной безопасности компьютера. Как и другие продукты AVG, система **AVG Internet Security 2011** была полностью переработана для обеспечения традиционно высокого уровня безопасности продуктов AVG, а также имеет новый более удобный и эффективный интерфейс. Новый продукт **AVG Internet Security 2011** имеет улучшенный интерфейс, а также более эффективные и быстрые возможности сканирования. Для удобства пользователей многие функции были автоматизированы. Кроме того, в программу были включены интеллектуальные пользовательские параметры, позволяющие настроить функции безопасности в соответствии с потребностями пользователя. Вам больше не потребуется выбирать между удобством и безопасностью!

Программа AVG разработана и предназначена для обеспечения безопасности во время работы за компьютером и в Интернете. Благодаря AVG вы будете получать удовольствие от работы за полностью защищенным компьютером.

Все предложения продуктов AVG

- Защита, которая подстраивается под вашу манеру работы на компьютере: совершение банковских операций и покупок в Интернете, поиск и просмотр веб-страниц, общение в чате и обмен мгновенными сообщениями, загрузка файлов и работа в социальных сетях — у компании AVG есть продукт, созданный специально для вас.
- Эффективная и удобная защита, которой доверяют более 110 миллионов пользователей по всему миру, основанная на работе глобальной сети высококвалифицированных исследователей.
- Защита с круглосуточной экспертной поддержкой



2. Требования для установки AVG

2.1. Поддерживаемые операционные системы

AVG Internet Security 2011 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 Internet Security 2011, но только без компонента IDP.

2.2. Минимальные требования и рекомендуемое оборудование

Минимальные требования к оборудованию для **AVG Internet Security 2011**.

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

Рекомендуемые требования к оборудованию для **AVG Internet Security 2011**.

- Процессор Intel Pentium 1,8 ГГц
- 512 МБ памяти ОЗУ
- 1400 МБ свободного места на жестком диске (для установки).



3. Варианты установки AVG

Программу AVG можно установить с помощью соответствующего файла на установочном компакт-диске или, загрузив последнюю версию программы на веб-сайте AVG (<http://www.avg.com/>).

Перед началом установки программы AVG настоятельно рекомендуется посетить веб-сайт AVG (<http://www.avg.com/>), чтобы проверить наличие нового файла установки. Это обеспечит установку последней версии AVG Internet Security 2011.

В процессе установки отобразится запрос на ввод номера лицензии или продажи. Убедитесь в наличии этих номеров перед началом установки. Номер продажи см. на упаковке компакт-диска. При покупке программы AVG в Интернете номер лицензии предоставляется пользователю по электронной почте.



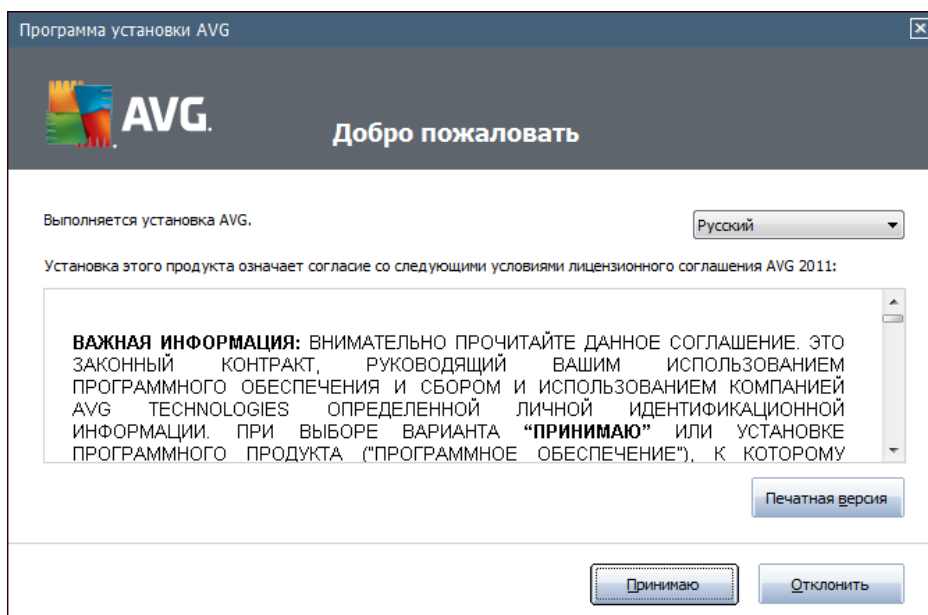
4. Процесс установки AVG

Для установки **AVG Internet Security 2011** на компьютер требуется файл установки последней версии. Можно использовать файл установки на компакт-диске, включенном в коробочную версию, но этот файл может устареть. Поэтому рекомендуется загружать последние файлы установки в Интернете. Этот файл можно загрузить с веб-сайта AVG (<http://www.avg.com/>), раздел [Центр поддержки/Загрузка](#).

Установка — это последовательность диалоговых окон с кратким описанием необходимых действий на каждом этапе. Далее приводится описание каждого диалогового окна.

4.1. Добро пожаловать

При запуске процесса установки открывается диалоговое окно **Добро пожаловать**. В этом окне можно выбрать язык установки и язык интерфейса пользователя AVG по умолчанию. В верхней части диалогового окна расположено раскрывающееся меню, содержащее список языков.



Внимание! Язык, выбранный в данном меню, будет использоваться в процессе установки. Выбранный язык будет использоваться в качестве языка интерфейса пользователя программы AVG по умолчанию вместе с английским языком, устанавливаемым автоматически. Чтобы установить дополнительные языки для отображения интерфейса пользователя, укажите их в диалоговом окне [Пользовательские параметры](#).

В следующем окне представлен полный текст лицензионного соглашения AVG. Просим внимательно ознакомиться с данным документом. 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.



4.2. Активация лицензии AVG

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

Номер продажи указан на футляре компакт-диска в поле **AVG Internet Security 2011**. Номер лицензии будет указан в подтверждающем сообщении электронной почты, которое будет получено после оформления покупки **AVG Internet Security 2011** 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.

Программа установки AVG

Активировать лицензию

Номер лицензии:

Например: 9FULL-NSDR5-KUL4L-UKSFR-L96M9-B2ALT-XWMX3

Если программное обеспечение AVG 2011 приобреталось в Интернете, номер лицензии должен быть доставлен по электронной почте. Чтобы избежать ошибок при вводе, рекомендуется вырезать и вставить номер из сообщения электронной почты в поле на этом экране.

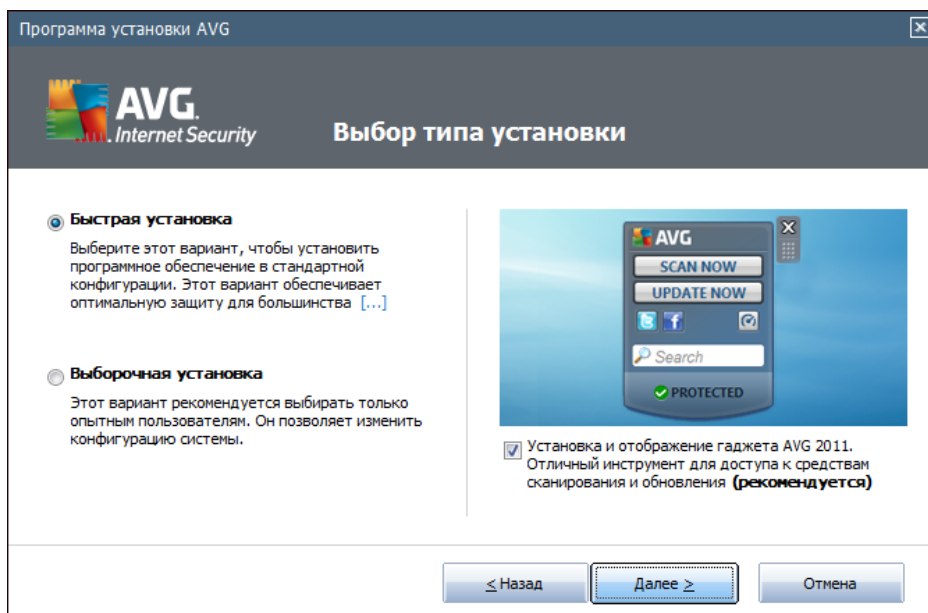
Если ПО приобретено в магазине розничной торговли, номер лицензии указан на регистрационной карточке продукта, которая находится в упаковке. Правильно скопируйте номер.

≤ Назад **Далее ≥** Отмена

Чтобы продолжить процесс установки, нажмите кнопку **Далее**.



4.3. Выбор типа установки



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

Для большинства пользователей рекомендуется выбирать вариант **Быстрая установка**. В этом случае установка AVG выполняется в полностью автоматическом режиме с параметрами, предварительно заданными поставщиком программного обеспечения. 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. Если выбран вариант **Быстрая установка**, нажмите кнопку **Далее**, чтобы перейти к следующему диалоговому окну [Установить панель инструментов безопасности AVG](#).

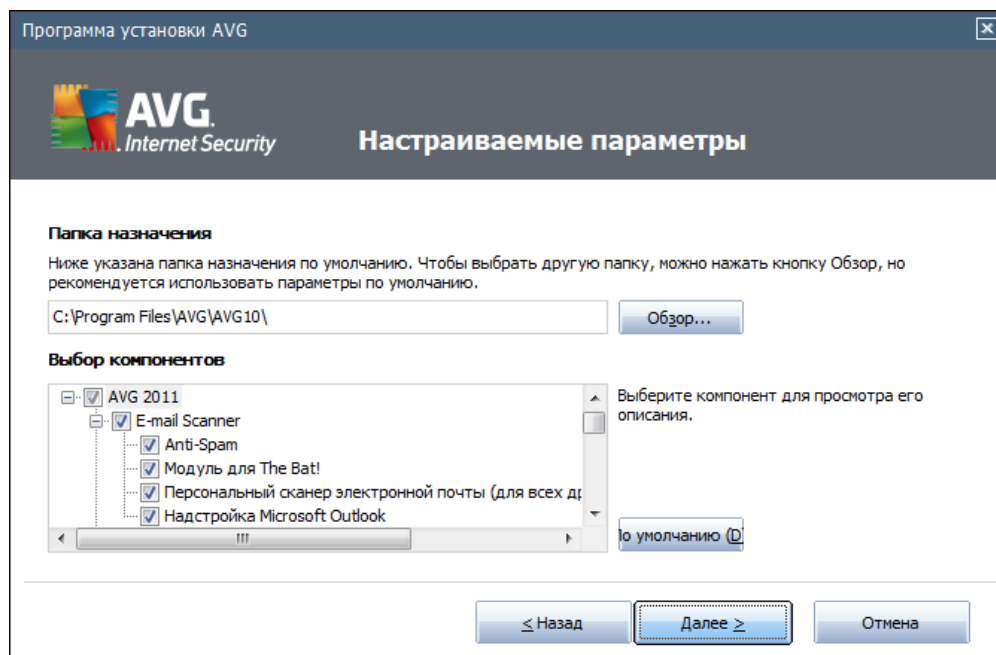
Выборочную установку следует использовать только опытным пользователям, у которых есть значительные основания для установки приложения AVG с параметрами, отличными от стандартных (например, при наличии специальных системных требований). При выборе данного параметра нажмите кнопку **Далее**, чтобы перейти к диалоговому окну [Пользовательские параметры](#).

В правой части данного диалогового окна отображается флажок, связанный с [гаджетом AVG](#) (поддерживается в ОС Windows Vista/Windows 7). Установите данный флажок, если требуется установить гаджет. После этого [гаджет AVG](#) будет доступен на боковой панели Windows. Данный гаджет позволяет мгновенно получить доступ к самым важным функциям **AVG Internet Security 2011**, например, к операциям [сканирования](#) и [обновления](#).



4.4. Пользовательские параметры

Диалоговое окно **Пользовательские параметры** позволяет настроить два параметра установки:



Папка назначения

В диалоговом окне **Папка назначения** можно выбрать папку, в которую будет установлена программа **AVG Internet Security 2011**. По умолчанию установка AVG выполняется в папку Program Files, которая расположена на диске C:. Чтобы изменить это местоположение, используйте кнопку **Обзор**, после нажатия которой отобразится структура дисков, в которой можно выбрать соответствующую папку.

Выбор компонентов

Диалоговое окно **Выбор компонентов** содержит обзор всех компонентов **AVG Internet Security 2011**, которые могут быть установлены. 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**.



Нажмите кнопку **Далее**, чтобы продолжить.

4.5. Установка панели инструментов безопасности AVG



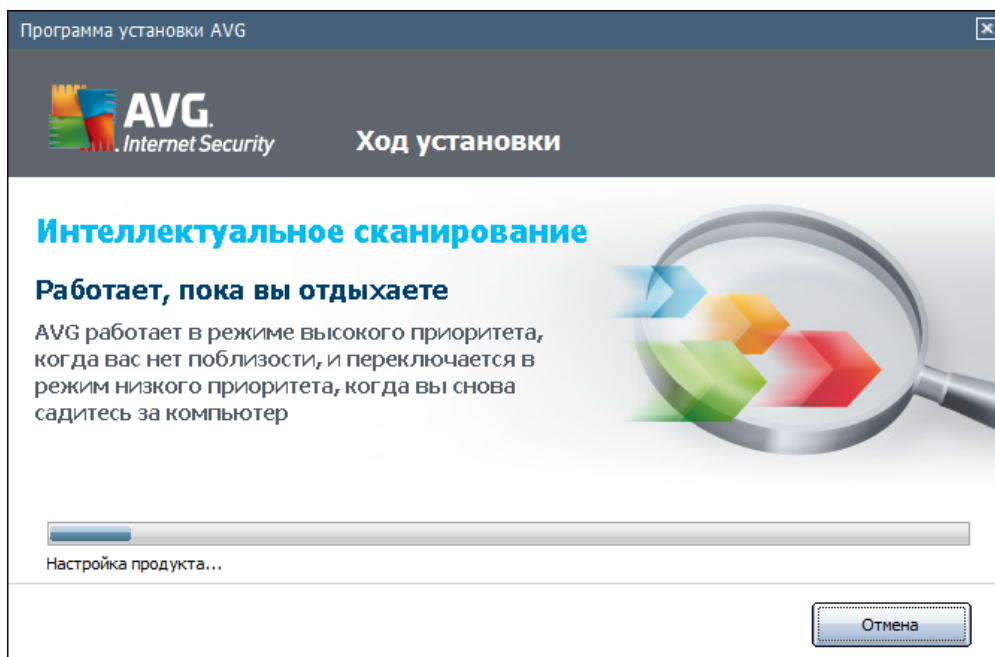
В диалоговом окне **Установка панели инструментов безопасности AVG** выберите, требуется ли установка **панели инструментов безопасности AVG**. Если значения параметров по умолчанию не изменены, этот компонент будет автоматически установлен в интернет-браузер (в данный момент поддерживаются браузеры *Microsoft Internet Explorer* версии 6.0 или выше и *Mozilla Firefox* версии 3.0 или 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.



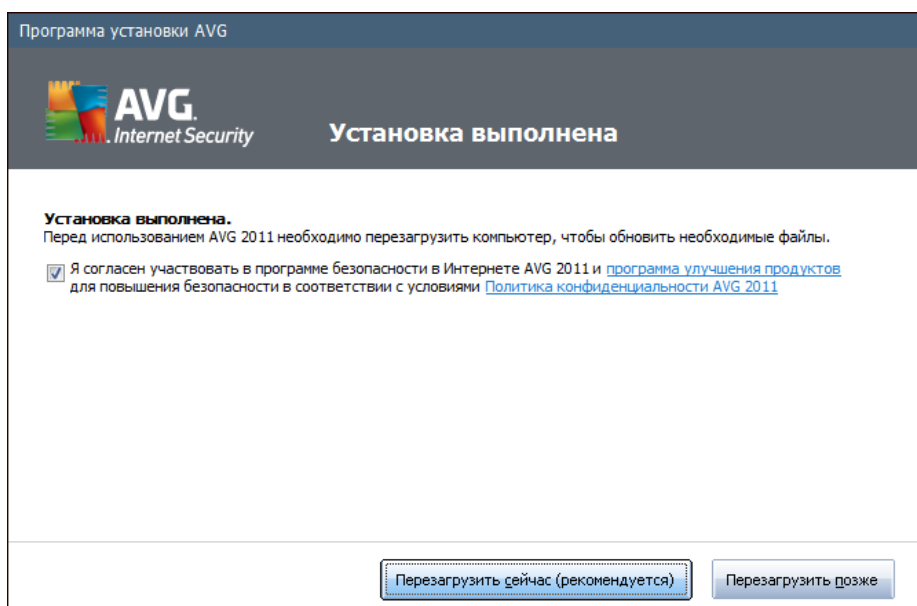
4.6. Состояние процесса установки

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



По завершении процесса установки будет выполнен переход к следующему диалоговому окну.

4.7. Установка выполнена успешно





Диалоговое окно **Установка выполнена успешно** отображается в подтверждение того, что программа **AVG Internet Security 2011** полностью установлена и настроена.

Укажите в данном диалоговом окне свои контактные данные, чтобы получать всю информацию и новости, связанные с продуктом. Под регистрационной формой доступны два варианта выбора.

- **Да, я хочу получать новости о безопасности и специальные предложения по AVG 2011 по электронной почте.** Установите данный флажок, чтобы получать информацию о новинках в области интернет-безопасности, специальных предложениях по продуктам AVG, улучшениях, обновлениях и т. п.
- **Я согласен(на) участвовать в программе интернет-безопасности и улучшения продуктов AVG 2011** Установите данный флажок, чтобы подтвердить свое согласие на участие в программе улучшения продуктов (дополнительные сведения см. в главе [Дополнительные параметры AVG / Программа улучшения продуктов](#)), в рамках которой выполняется сбор анонимных сведений об обнаруженных угрозах с целью повышения общего уровня безопасности в Интернете.

Для завершения установки необходимо перезагрузить компьютер: выберите **Перезагрузить сейчас** или, если необходимо отложить перезагрузку, — **Перезагрузить позже**.

Примечание. Если при использовании корпоративной лицензии AVG в начале установки была выбрана установка элемента Удаленное администрирование (см. [Пользовательские параметры](#)), отобразится диалоговое окно подтверждения успешности установки, имеющее следующий интерфейс.

Необходимо указать параметры центра данных AVG — укажите строку подключения к центру данных AVG в формате сервер:порт. Если в настоящий момент эта информация недоступна, оставьте поле незаполненным. Установить конфигурацию можно позже с помощью диалогового окна **Дополнительные параметры/Удаленное администрирование**. Для получения дополнительных сведений о компоненте Удаленное администрирование AVG обратитесь к руководству пользователя версии AVG Business Edition, которое можно загрузить на веб-сайте компании AVG (<http://www.avg.com/>).



5. После установки

5.1. Регистрация продукта

После завершения установки **AVG Internet Security 2011** выполните регистрацию продукта через Интернет на веб-сайте компании AVG (<http://www.avg.com/>) на странице **Регистрация** (следуйте инструкциям на странице). 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.

5.2. Доступ к интерфейсу пользователя

Доступ к [интерфейсу пользователя AVG](#) можно получить одним из следующих способов:

- дважды щелкните [значок AVG на панели задач](#)
- дважды щелкните значок AVG на рабочем столе
- дважды щелкните строку состояния в нижней части [гаджета AVG](#) (если установлен; поддерживается ОС Windows Vista/Windows 7)
- с помощью меню **Пуск/Программы/AVG 2011/Интерфейс пользователя AVG**
- на [панели инструментов безопасности AVG](#) с помощью параметра **Запустить AVG**

5.3. Сканирование всего компьютера

Существует потенциальная опасность того, что до установки **AVG Internet Security 2011** компьютер был заражен вирусом. Поэтому необходимо запустить [сканирование всего компьютера](#), чтобы убедиться, что компьютер не заражен.

Инструкции по запуску [сканирования всего компьютера](#) см. в главе [Сканирование AVG](#).

5.4. Тестирование Eicar

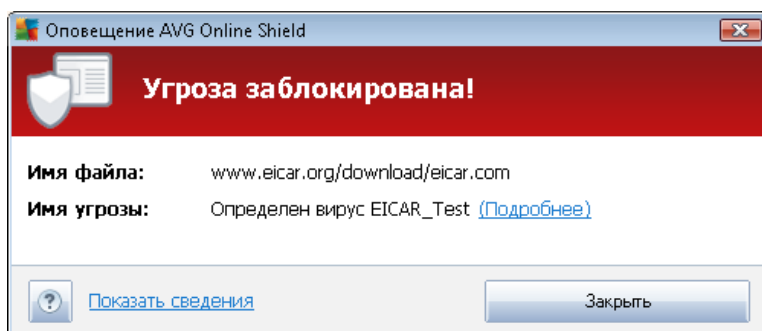
Чтобы проверить правильность установки **AVG Internet Security 2011**, можно выполнить тест EICAR.

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 компонент [Online Shield](#) отреагирует и выдаст предупреждение.



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*). **Online Shield** позволяет загрузить этот файл и сохранить его на локальном жестком диске, но затем компонент **Resident Shield** обнаруживает вирус и пытается извлечь его. **Если AVG не удалось определить тестовый файл EICAR как вирус, проверьте параметры программы еще раз.**

5.5. Конфигурация AVG по умолчанию

Параметры по умолчанию (*параметры приложения после установки*) **AVG Internet Security 2011** настроены поставщиком ПО таким образом, чтобы все компоненты и функции обеспечивали оптимальную производительность.

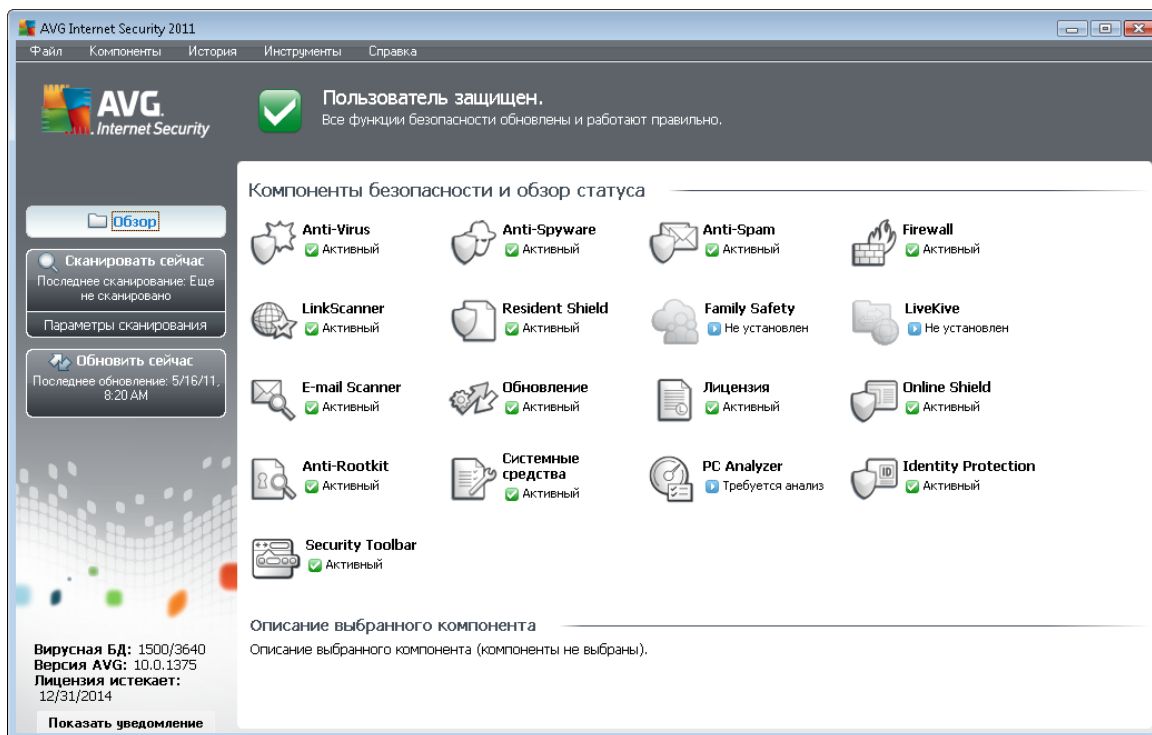
Не изменяйте настройки AVG без необходимости! Все изменения параметров должны выполняться опытным пользователем.

Допустимо незначительное изменение параметров **компонентов AVG** непосредственно с помощью интерфейса пользователя определенного компонента. Чтобы при необходимости изменить параметры AVG, используйте диалоговое окно **Дополнительные параметры AVG** : выберите элемент системного меню **Инструменты/Дополнительные параметры** и измените параметры AVG в отобразившемся диалоговом окне **Расширенные настройки AVG**.



6. Интерфейс пользователя AVG

AVG Internet Security 2011 открывается в главном окне.



- **Системное меню** (системная область в верхней части окна). Стандартное средство навигации, с помощью которого можно получить доступ ко всем компонентам, службам и функциям — [подробные сведения >>](#).
- **Информация о состоянии безопасности** (верхняя часть окна). Информация о текущем состоянии программы AVG. [Подробные сведения >>](#)
- **Быстрые ссылки** (левая часть окна). Позволяет получить быстрый доступ к наиболее важным и часто используемым задачам AVG. [Подробные сведения >>](#)
- **Обзор компонентов** (центральная часть окна). Обзор всех установленных компонентов — [Подробные сведения >>](#)
- **Статистика** (левая нижняя часть окна). Статистическая информация о работе программы — [Подробные сведения >>](#)
- **Значок на панели задач** (правая нижняя часть экрана, панель задач). Отображение текущего состояния AVG — [Подробные сведения >>](#)
- **Гаджет AVG** (боковая панель ОС Windows, поддерживает ОС Windows Vista/7). Позволяет получить быстрый доступ к функциям сканирования и обновления программы AVG — [Подробные сведения >>](#)



6.1. Системное меню

Системное меню — это стандартное средство навигации, которое используется во всех приложениях Windows. Оно расположено горизонтально в верхней части главного окна **AVG Internet Security 2011**. С помощью системного меню можно получить доступ к специальным компонентам, службам и функциям AVG.

Системное меню состоит из двух основных разделов.

6.1.1. Файл

- **Выход.** Закрытие интерфейса **AVG Internet Security 2011** пользователя. При нажатии данной кнопки приложение AVG продолжит свою работу в фоновом режиме, а компьютер будет находиться под защитой!

6.1.2. 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.** Обеспечивает защиту от вирусов, проникающих на компьютер — [Подробные сведения >>](#)
- **Anti-Spyware.** Обеспечивает защиту компьютера от шпионского и рекламного ПО — [Подробные сведения >>](#)
- **Anti-Spam.** Выполняет проверку всех входящих сообщений электронной почты и отмечает нежелательные сообщения как СПАМ — [Подробные сведения >>](#)
- **Firewall.** Предназначен для контроля обмена данными между используемым компьютером и другими компьютерами в Интернете и локальной сети — [Подробные сведения >>](#)
- **Link Scanner.** Проверяет результаты поиска, отображаемые в интернет-браузере — [Подробные сведения >>](#)
- **E-mail Scanner.** Проверяет входящие и исходящие сообщения электронной почты на наличие вирусов — [Подробные сведения >>](#)
- **Family Safety.** Позволяет отслеживать деятельность детей в Интернете и защитить их от посещения веб-сайтов, которые им не рекомендуется просматривать — [Подробные сведения >>](#)
- **LiveKive.** Позволяет выполнять автоматическое резервное копирование данных через Интернет — [Подробные сведения >>](#)
- **Resident Shield.** Работает в фоновом режиме и выполняет сканирование файлов во



время их копирования, открытия или сохранения — [подробные сведения >>](#)

- **Диспетчер обновления.** Предназначен для управления всеми обновлениями AVG — [подробные сведения >>](#)
- **Лицензия.** Отображает номер, тип и дату окончания срока действия лицензии — [Подробные сведения >>](#)
- **Online Shield.** Выполняет сканирование всех загружаемых веб-браузером данных — [Подробные сведения >>](#)
- **Anti-Rootkit.** Обнаружение программ и средств, пытающихся замаскировать вредоносное ПО — [Подробные сведения >>](#)
- **Системные средства.** Позволяет получить информацию о рабочей среде AVG и операционной системе — [Подробные сведения >>](#)
- **PC Analyzer.** Предоставляет сведения о состоянии компьютера — [Подробные сведения >>](#)
- **Identity Protection.** Компонент, защищающий от вредоносного ПО и направленный на предотвращение краж злоумышленниками важной личной информации — [Подробные сведения >>](#)
- **Security Toolbar.** Позволяет использовать выбранные функции AVG непосредственно в браузере — [Подробные сведения >>](#)
- **Удаленное администрирование.** Отображается только при использовании версий AVG Business Editions, если пользователь выбрал установку данного компонента [в процессе установки программы.](#)

6.1.3. История

- **[Результаты сканирования.](#)** Переход в интерфейс проверки AVG в диалоговое окно [Обзор результатов сканирования.](#)
- **[Обнаружение Resident Shield](#)** — отображение диалогового окна, содержащего обзор угроз, обнаруженных компонентом [Resident Shield](#)
- **[Обнаружение E-mail Scanner.](#)** Отображение диалогового окна с обзором вложений сообщений электронной почты, признанных опасными компонентом [E-mail Scanner.](#)
- **[Обнаружение Online Shield.](#)** Отображение диалогового окна с обзором угроз, обнаруженных компонентом [Online Shield](#)
- **[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 Internet Security 2011**.
- **Firewall**. Открытие интерфейса параметров компонента Firewall на вкладке **Журналы**, содержащей подробный обзор всех действий компонента Firewall

6.1.4. Инструменты

- **Сканировать компьютер**. Переключение к **интерфейсу сканирования AVG** и запуск сканирования всего компьютера.
- **Сканировать выбранную папку**. Переключение к **интерфейсу сканирования AVG**, который позволяет с помощью древовидной структуры определить, какие файлы и папки должны быть сканированы.
- **Сканировать файл**. Позволяет запустить проверку по требованию отдельного файла, выбранного в древовидной структуре диска.
- **Обновить**. Автоматический запуск процесса обновления **AVG Internet Security 2011**.
- **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.
- **Дополнительные параметры**. Открытие диалогового окна **Дополнительные параметры AVG**, которое позволяет изменять параметры программы **AVG Internet Security 2011**. В основном, рекомендуется не изменять стандартные параметры приложения, определенные производителем.
- **Параметры Firewall**. Открытие отдельного диалогового окна, содержащего дополнительные параметры компонента **Firewall**.

6.1.5. Справка

- **Содержание**. Открытие файла справки AVG.
- **Интерактивная справка**. Открытие веб-сайта AVG (<http://www.avg.com/>) на странице центра поддержки пользователей.
- **AVG Web**. Открытие веб-сайта 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 данном 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 нового продукта AVG).

- **Регистрация.** Переход на страницу регистрации веб-сайта 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 Internet Security 2011** вместо последних двух элементов будут отображаться пункты **Купить** и **Активировать**, которые позволяют сразу приобрести полную версию программы. Для программы **AVG Internet Security 2011**, при установке которой был указан номер продажи, будут отображаться пункты **Зарегистрировать** и **Активировать**. Для получения дополнительной информации см. раздел [Лицензия](#) данного документа.

- **О программе AVG.** Открытие диалогового окна **Сведения**, содержащего пять вкладок, на которых представлены данные о названии программы, версии программы и вирусной базы данных, системная информация, лицензионное соглашение, а также контактная информация **AVG Technologies CZ**.

6.2. Информация о состоянии безопасности

Раздел **Информация о состоянии безопасности** расположен в верхней части главного окна AVG. Этот раздел позволяет быстро определить текущее состояние безопасности **AVG Internet Security 2011**. Ознакомьтесь со значками, представленными в данном разделе, и их значением.



. Зеленый значок означает, что программа AVG работает правильно. Ваш компьютер полностью защищен, установлены все необходимые обновления. Все установленные компоненты также работают правильно.



. Оранжевый значок означает, что один или несколько компонентов настроены неправильно. Необходимо обратить внимание на их свойства или параметры. Никаких серьезных проблем, связанных с работой AVG, нет. Скорее всего, некоторые компоненты были отключены по какой-либо причине. Программа AVG также продолжает обеспечивать защиту компьютера. Однако необходимо уделить внимание настройке компонента. Его имя будет отображено в разделе **Информация о состоянии безопасности**.

Данный 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). Данный параметр может потребоваться в определенной ситуации, но настоятельно рекомендуется отключать параметр "**Игнорировать состояние компонента**" при отсутствии необходимости его использования.



. Красный значок означает критическое состояние AVG. Один или несколько компонентов работают неправильно, программа AVG не может защитить компьютер. Необходимо немедленно устранить указанные проблемы. Если проблему не удастся устранить самостоятельно, обратитесь в [службу технической поддержки компании AVG](#).

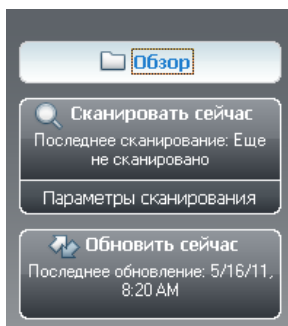
Если программа AVG не настроена для обеспечения оптимальной производительности, рядом со сведениями о состоянии безопасности отобразится новая кнопка **Исправить** (или **Исправить все** при возникновении проблемы с несколькими компонентами). Нажмите эту кнопку, чтобы запустить автоматический процесс проверки и настройки. Это наиболее простой способ настройки оптимальной производительности программы AVG 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 может быть получена в любое время с помощью [значка на панели задач](#).

6.3. Быстрые ссылки

Быстрые ссылки (в левой части [интерфейса пользователя AVG](#)) позволяют получить быстрый доступ к наиболее важным и часто используемым функциям AVG.



- **Обзор** . Используйте данную ссылку для переключения с открытого в настоящее время интерфейса AVG к стандартному интерфейсу, содержащему обзор всех установленных компонентов — см. [Обзор компонентов >>](#)
- **Сканировать** . По умолчанию данная кнопка позволяет получить сведения (*тип сканирования, дата последнего запуска*) о последнем запущенном сканировании. Можно выполнить команду **Сканировать**, чтобы повторить операцию сканирования, или щелкнуть ссылку **Параметры сканирования**, чтобы открыть интерфейс сканирования AVG, позволяющий запускать и планировать сканирования, а также редактировать их параметры — см. главу [Сканирование AVG >>](#)
- **Обновить сейчас** . Данная ссылка позволяет получить сведения о дате последнего запуска процесса обновления. Нажмите эту кнопку, чтобы открыть интерфейс



обновления и запустить процесс обновления программы AVG — см. главу [Обновления AVG>>](#)

Данные ссылки всегда доступны в интерфейсе пользователя. После того как ссылка будет использована для запуска определенного процесса, графический интерфейс пользователя переключится к новому диалоговому окну, но быстрые ссылки будут по-прежнему доступны. Кроме того, запущенный процесс будет представлен графически.

6.4. Обзор компонентов

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

- Обзор всех установленных компонентов, состоящих из панели со значком компонента и информации об активности компонента.
- Описание выбранного компонента

В **AVG Internet Security 2011** раздел **Обзор компонентов** содержит сведения о следующих компонентах.

- **Anti-Virus.** Обеспечивает защиту от вирусов, проникающих на компьютер — [подробные сведения >>](#).
- **Anti-Spyware.** Обеспечивает защиту компьютера от шпионского и рекламного ПО — [Подробные сведения >>](#)
- **Anti-Spam.** Выполняет проверку всех входящих сообщений электронной почты и отмечает нежелательные сообщения как СПАМ — [Подробные сведения >>](#)
- **Firewall.** Предназначен для контроля обмена данными между используемым компьютером и другими компьютерами в Интернете и локальной сети — [Подробные сведения >>](#)
- **Link Scanner.** Проверяет результаты поиска, отображаемые в интернет-браузере — [Подробные сведения >>](#)
- **E-mail Scanner.** Проверяет входящие и исходящие сообщения электронной почты на наличие вирусов — [Подробные сведения >>](#)
- **Resident Shield.** Работает в фоновом режиме и выполняет сканирование файлов во время их копирования, открытия или сохранения — [Подробные сведения >>](#)
- **Family Safety.** Позволяет отслеживать деятельность детей в Интернете и защитить их от посещения веб-сайтов, которые им не рекомендуется просматривать — [Подробные сведения >>](#)
- **LiveKive.** Позволяет выполнять автоматическое резервное копирование данных через Интернет — [Подробные сведения >>](#)
- **Диспетчер обновления.** Предназначен для управления всеми обновлениями AVG — [подробные сведения >>](#)



- **Лицензия.** Отображает номер, тип и дату окончания срока действия лицензии — [Подробные сведения >>](#)
- **Online Shield.** Выполняет сканирование всех загружаемых веб-браузером данных — [Подробные сведения >>](#)
- **Anti-Rootkit.** Обнаружение программ и средств, пытающихся замаскировать вредоносное ПО — [Подробные сведения >>](#)
- **Системные средства.** Позволяет получить информацию о рабочей среде AVG и операционной системе — [Подробные сведения >>](#)
- **PC Analyzer.** Предоставляет сведения о состоянии компьютера — [Подробные сведения >>](#)
- **Identity Protection.** Компонент, защищающий от вредоносного ПО и направленный на предотвращение краж злоумышленниками важной личной информации — [Подробные сведения >>](#)
- **Security Toolbar.** Позволяет использовать выбранные функции AVG непосредственно в браузере — [Подробные сведения >>](#)
- **Удаленное администрирование.** Отображается только при использовании версий AVG Business Editions, если пользователь выбрал установку данного компонента [в процессе установки программы.](#)

Щелкните значок компонента один раз, чтобы выделить этот компонент в окне обзора. При этом в нижней части интерфейса пользователя отобразится описание основных функций компонента. Дважды щелкните значок, чтобы открыть интерфейс компонента, содержащий список основных статистических данных.

Щелкните значок компонента правой кнопкой мыши, чтобы открыть контекстное меню. С помощью контекстного меню можно открыть графический интерфейс компонента, а также выбрать параметр **Игнорировать состояние компонента**. Выберите данный параметр, если известно о [состоянии ошибки компонента](#), но по какой-либо причине не требуется изменять состояние AVG и необходимо отключить оповещение с помощью [значка на панели задач](#).

6.5. Статистика

Раздел **Статистика** расположен в левой нижней части [интерфейса пользователя AVG](#). В нем представлены сведения, связанные с работой программы.

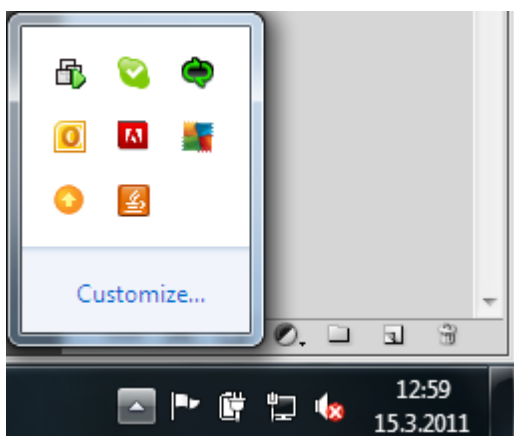
- **Вирусная БД** . Сведения о версии установленной вирусной базы данных.
- **Версия AVG.** Версия установленной программы AVG (*номер отображается в формате 10.0.xx, где 10.0 — это версия серии продуктов, а xxxx — номер сборки*)
- **Срок окончания действия лицензии.** Дата окончания срока действия лицензии



AVG.

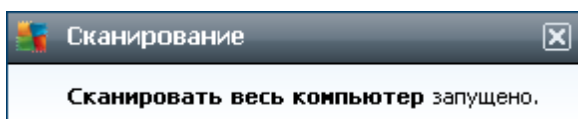
6.6. Значок на панели задач

Значок на панели задач (на панели задач Windows) указывает текущее состояние **AVG Internet Security 2011**. Этот значок всегда отображается на панели задач независимо от того, открыто ли главное окно AVG.



Если отображается полным цветом , **значок на панели задач** указывает, что все компоненты AVG активны и работают правильно. Кроме того, на панели задач отображается полноцветный значок AVG, если программа AVG находится в состоянии ошибки, но вам известно о проблеме и вы установили параметр [Игнорировать состояние компонентов](#). Значок с восклицательным знаком  указывает на наличие проблемы (неактивный компонент, состояние ошибки и т. д.). Дважды щелкните **значок на панели задач**, чтобы открыть главное окно и настроить необходимый компонент.

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



Кроме того, дважды щелкнув **значок на панели задач**, можно быстро получить доступ к главному окну AVG. Если щелкнуть правой кнопкой мыши **значок на панели задач**, откроется краткое контекстное меню, содержащее следующие пункты.

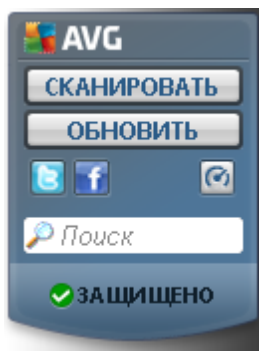
- **Открыть интерфейс пользователя AVG.** Открытие [интерфейса пользователя AVG](#)
- **Сканирования.** Щелкните, чтобы открыть контекстное меню



- **Firewall.** Щелкните, чтобы открыть контекстное меню параметров [Firewall](#), в котором можно редактировать большинство параметров: [состояние Firewall](#) (*Firewall включен/Firewall отключен/Экстренный режим*), [режим "Во время игры"](#) и [профили Firewall](#)
- **Запустить PC Analyzer.** Щелкните для запуска компонента [PC Analyzer](#).
- **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*.
- **Обновить сейчас.** Немедленный запуск [обновления](#)
- **Справка.** Открытие файла справки на начальной странице.

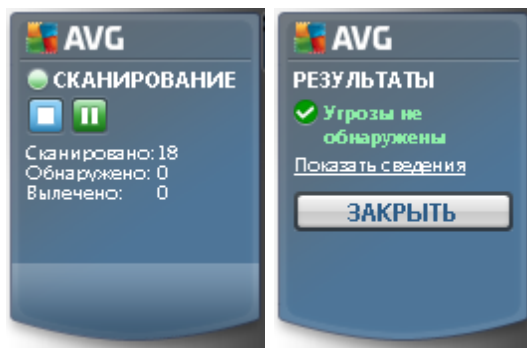
6.7. Гаджет AVG

Гаджет AVG отображается на рабочем столе ОС 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 Internet Security 2011**, например, к операциям [сканирования](#) и [обновления](#).

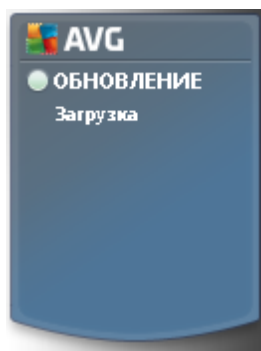


Гаджет AVG предоставляет доступ к следующим параметрам быстрого доступа:

- **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**, чтобы запустить процесс обновления AVG непосредственно в гаджете:



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



- **Ссылка Facebook** . Открытие в браузере страницы **сообщества AVG** сайта Facebook
- **LinkedIn** . Данный параметр доступен только во время сетевой установки (*т. е. предполагается, что программа AVG была установлена с помощью лицензии*)



версии *AVG Business edition*), он открывает веб-браузер на сайте сообщества **AVG SMB Community** в социальной сети LinkedIn

- **PC Analyzer**  . Открытие пользовательского интерфейса компонента [PC Analyzer](#) .
- **Поле поиска**. Отображение результатов поиска по ключевому слову в новом окне браузера по умолчанию.



7. Компоненты AVG

7.1. Anti-Virus

7.1.1. Принципы работы Anti-Virus

Модуль сканирования антивирусного ПО сканирует все файлы и их активность (открытие/ закрытие файлов и т. д.) на известные вирусы. Каждый обнаруженный вирус блокируется, удаляется или помещается в карантин. Большая часть антивирусного ПО также 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.

Важной чертой антивирусной защиты является тот факт, что ни один известный вирус не сможет запуститься на компьютере.

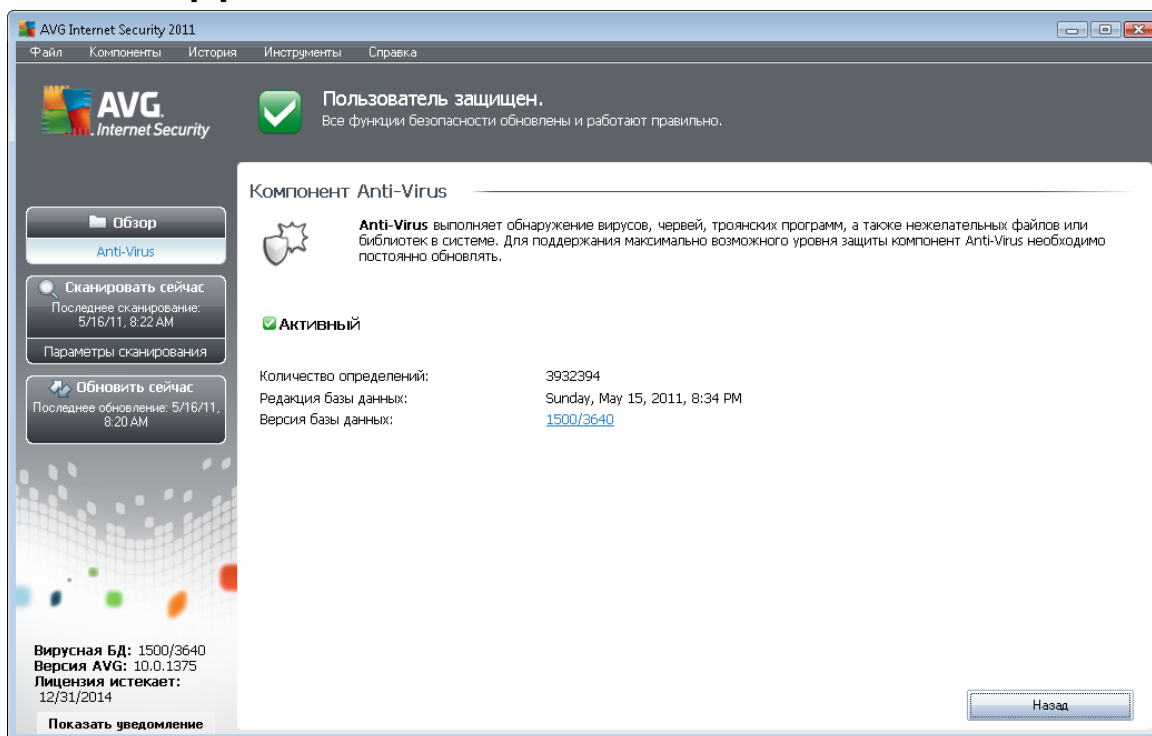
Когда одна технология не может справиться с обнаружением и определением вируса, компонент **Anti-Virus** использует несколько технологий, чтобы обеспечить защиту компьютера от вирусов.

- Сканирование. Поиск последовательности признаков, характерных для данного вируса.
- Эвристический анализ. Динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде.
- Типовое определение. Определение характерных команд данного вируса/группы вирусов.

Приложение AVG способно анализировать и обнаруживать исполняемые приложения или библиотеки DLL, использование которых в системе может быть потенциально нежелательным. Подобные угрозы называются потенциально нежелательными программами (различные виды шпионского ПО, рекламное ПО и прочее). Более того, AVG сканирует системный реестр на подозрительные записи, временные интернет-файлы, следящие cookie-файлы и позволяет поступать с потенциально вредоносными элементами так же, как и с другими зараженным объектами.



7.1.2. Интерфейс Anti-Virus



Интерфейс компонента **Anti-Virus** предоставляет краткий обзор функциональности компонента, сведения о текущем состоянии компонента (*Компонент Anti-Virus активен.*), а также краткий обзор статистики компонента **Anti-Virus**.

- **Количество определений.** Количество вирусов, определенных в последней версии вирусной базы данных.
- **Выпуск базы данных.** Указывает, когда и в какое время была обновлена вирусная база данных.
- **Версия базы данных.** Номер установленной версии вирусной базы данных; в результате каждого обновления вирусной базы данных номер увеличивается.

Для интерфейса данного компонента доступна только одна кнопка управления (**Назад**). Нажмите эту кнопку, чтобы вернуться к [интерфейсу пользователя AVG, установленному по умолчанию](#) (обзор компонентов).

7.2. Anti-Spyware



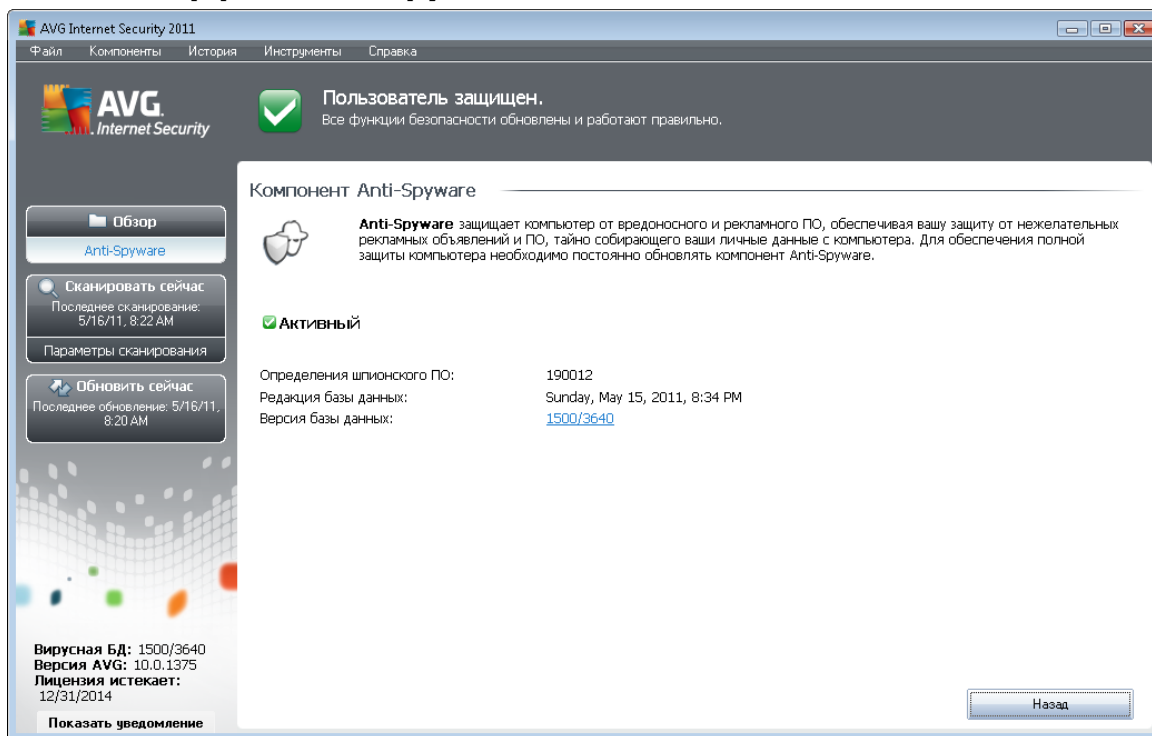
7.2.1. Принципы работы Anti-Spyware

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.

Также существует вероятность того, что вредоносное ПО может попасть на компьютер до установки программы AVG, а также если пользователь пренебрег обновлением [загрузкой обновлений программы и базы данных AVG Internet Security 2011](#). В таких случаях программа AVG предложит выполнить полное сканирование компьютера на наличие вредоносного или шпионского ПО с помощью функции сканирования. При сканировании также можно обнаружить "спящее" и неактивное вредоносное ПО, то есть вредоносное ПО, которое загружено, но еще не активировано.

7.2.2. Интерфейс Anti-Spyware



Интерфейс компонента **Anti-Spyware** содержит краткий обзор функций компонента, сведения о текущем состоянии компонента и некоторые статистические данные компонента **Anti-Spyware**.

- **Определение шпионского ПО.** Обеспечивает подсчет образцов шпионского ПО,



определенного в последней версии базы данных шпионского ПО.

- **Выпуск базы данных.** Указывает, когда и в какое время была обновлена база данных нежелательной почты.
- **Версия базы данных.** Определяет номер последней версии вирусной базы данных; в результате каждого обновления вирусной базы данных номер увеличивается.

Для интерфейса данного компонента доступна только одна кнопка управления (**Назад**). Нажмите эту кнопку, чтобы вернуться к [интерфейсу пользователя AVG, установленному по умолчанию](#) (обзор компонентов).

7.3. Anti-Spam

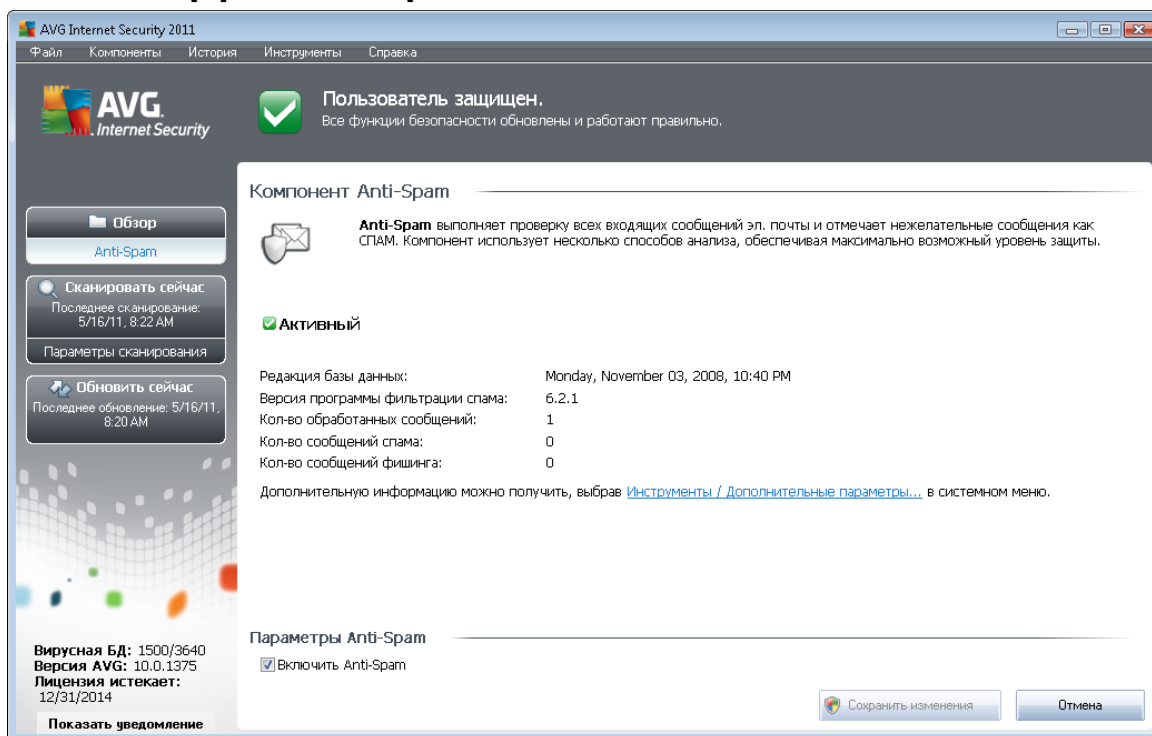
Спам относится к незапрашиваемым сообщениям электронной почты, в особенности к рекламным рассылкам о продуктах и услугах, которые массово рассылаются на большое количество адресов эл. почты одновременно, заполняя почтовые ящики получателей. Спам не является законной коммерческой рассылкой, на которую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

7.3.1. Принципы работы Anti-Spam

Компонент AVG Anti-Spam проверяет все входящие сообщения электронной почты и помечает нежелательные сообщения электронной почты как спам. **AVG 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 AVG Anti-Spam использует несколько способов анализа для обработки каждого сообщения электронной почты, обеспечивая максимальную защиту от спама. **AVG Anti-Spam** использует для определения спама регулярно обновляемую базу данных. 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).

7.3.2. Интерфейс Anti-Spam



С помощью диалогового окна компонента **Anti-Spam** можно получить краткие сведения о работе компонента, информацию о его текущем состоянии, а также следующие статистические данные:

- **Выпуск базы данных.** Указывает, когда и в какое время была обновлена и опубликована база данных нежелательной почты.
- **Версия модуля Spamcatcher.** Определяет номер последней версии модуля защиты от нежелательной почты.
- **Количество обработанных сообщений эл. почты.** Указывает количество сообщений эл. почты, которые были просканированы с момента последнего запуска модуля защиты от нежелательной почты.
- **Количество нежелательных сообщений эл. почты.** Указывает, сколько из просканированных сообщений были отмечены как спам.
- **Количество фишинговых сообщений эл. почты.** Указывает, сколько из просканированных сообщений были определены как попытки фишинга.

В диалоговом окне компонента **Anti-Spam** также содержится ссылка [Инструменты/Дополнительные параметры](#). Щелкните данную ссылку, чтобы перейти в меню расширенной конфигурации всех компонентов **AVG Internet Security 2011**.

Примечание. Все компоненты AVG настроены поставщиком ПО для обеспечения оптимальной производительности. Не изменяйте настройки AVG без необходимости. Все



изменения настроек должны выполняться опытным пользователем.

Для интерфейса данного компонента доступна только одна кнопка управления (**Назад**). Нажмите эту кнопку, чтобы вернуться к [интерфейсу пользователя AVG, установленному по умолчанию](#) (обзор компонентов).

7.4. Firewall

Компонент Firewall представляет собой систему, которая применяет политику контроля доступа между двумя или несколькими сетями с помощью блокировки/пропуска трафика. Firewall содержит ряд правил, которые обеспечивают защиту внутренней сети от внешних атак (главным образом из Интернета), и управляет соединениями на каждом сетевом порте. Выполняется оценка подключения в соответствии с определенными правилами, после чего оно будет разрешено или заблокировано. При обнаружении попыток взлома компонент Firewall "блокирует" данную попытку и не позволяет взломщику получить доступ к компьютеру.

Компонент Firewall настроен для разрешения или блокировки внешнего/внутреннего подключения (в обоих направлениях, входящего или исходящего) с помощью определенных портов и для определенных приложений. Например Firewall можно настроить только для разрешения получения и отправки веб-данных с помощью Microsoft Explorer. Любая попытка передачи веб-данных с помощью другого браузера будет заблокирована.

Компонент Firewall препятствует отправке с компьютера пользователя сведений, позволяющих установить личность пользователя без его ведома. Он контролирует обмен данными с другими компьютерами в Интернете и локальной сети. В пределах организации Firewall обеспечивает защиту отдельного компьютера от атак, исходящих от внутренних пользователей других компьютеров в сети.

Совет. Не рекомендуется использовать более одного брандмауэра на одном компьютере. Установка более одного брандмауэра не повысит безопасность компьютера. Но велика вероятность того, что это может привести к конфликту приложений. Таким образом, рекомендуется использовать на компьютере только один брандмауэр, а остальные отключить, чтобы устранить риск возникновения конфликтов и связанных с этим проблем.

7.4.1. Принципы работы Firewall

В программе AVG компонент **Firewall** контролирует весь трафик на каждом сетевом порте компьютера. На основе установленных правил компонент **Firewall** оценивает приложения, которые работают на компьютере (и пытаются подключиться к Интернету или локальной сети), либо приложения, пытающиеся подключиться к компьютеру извне. Для каждого из этих приложений компонент **Firewall** разрешает или запрещает обмен данными на сетевых портах. По умолчанию, если приложение неизвестно (например, не имеет установленных правил компонента **Firewall**), компонент **Firewall** отобразит запрос на разрешение или блокировку попытки обмена данными.

Примечание. AVG Firewall не предназначен для использования на серверных платформах.

Возможности компонента Firewall:



- Автоматическое разрешение или блокировка попыток обмена данными со стороны известных приложений или запрос подтверждения.
- Использование всех [профилей](#) с предварительно установленными правилами в соответствии с потребностями пользователя.
- [Переключение профилей](#) автоматически при подключении к различным сетям или при использовании различных сетевых адаптеров.

7.4.2. Профили Firewall

С помощью компонента [Firewall](#) можно установить специальные правила безопасности, основанные на том, является ли компьютер частью домена, автономным компьютером или ноутбуком. Для каждого варианта требуется определенный уровень защиты, который обеспечивается соответствующим профилем. Другими словами, профиль [Firewall](#) — это специальная конфигурация компонента [Firewall](#). Для пользователя доступен ряд подобных предопределенных конфигураций.

Доступные профили

- **Разрешить все.** Это системный профиль компонента [Firewall](#), предустановленный производителем по умолчанию. Если данный профиль активирован, разрешены все сетевые соединения и правила политики безопасности не действуют, как при отключенной защите компонента [Firewall](#) (например, все приложения разрешены, но проверка пакетов все еще выполняется — для полного отключения фильтрации необходимо отключить Firewall). Системный профиль невозможно копировать, удалить или изменить его параметры.
- **Блокировать все.** Это системный профиль компонента [Firewall](#), предустановленный производителем по умолчанию. Если данный профиль активен, все сетевые подключения блокируются, а компьютер становится недоступным для внешних сетей и не может связываться с ними. Системный профиль невозможно копировать, удалить или изменить его параметры.
- **Пользовательские профили:**
 - о **Прямое подключение к Интернету.** Подходит для обычных настольных компьютеров, имеющих прямое подключение к Интернету, а также для ноутбуков, подключаемых к Интернету за пределами безопасной корпоративной сети. Этот параметр следует выбрать при подключении с домашнего компьютера или компьютера в небольшой корпоративной сети, не имеющей централизованного управления. Также этот параметр можно использовать во время путешествий при подключении с помощью ноутбука из неизвестных и потенциально опасных мест (*интернет-кафе, гостиничного номера и т. д.*). Для этих компьютеров будут созданы более строгие правила, так как подразумевается, что они не имеют дополнительной защиты и потому требуют применения максимально возможного уровня защиты.
 - о **Компьютер, входящий в домен.** Подходит для компьютеров, находящихся в локальной сети, например школы или корпоративной сети. Предполагается, что



для защиты сети предприняты дополнительные меры безопасности, поэтому уровень безопасности может быть ниже, чем для автономного компьютера.

- о **Небольшая домашняя или офисная сеть**. Подходит для компьютеров, находящихся в небольших сетях, например дома или на небольшом предприятии. Обычно это несколько компьютеров, подключенных между собой без использования сервера.

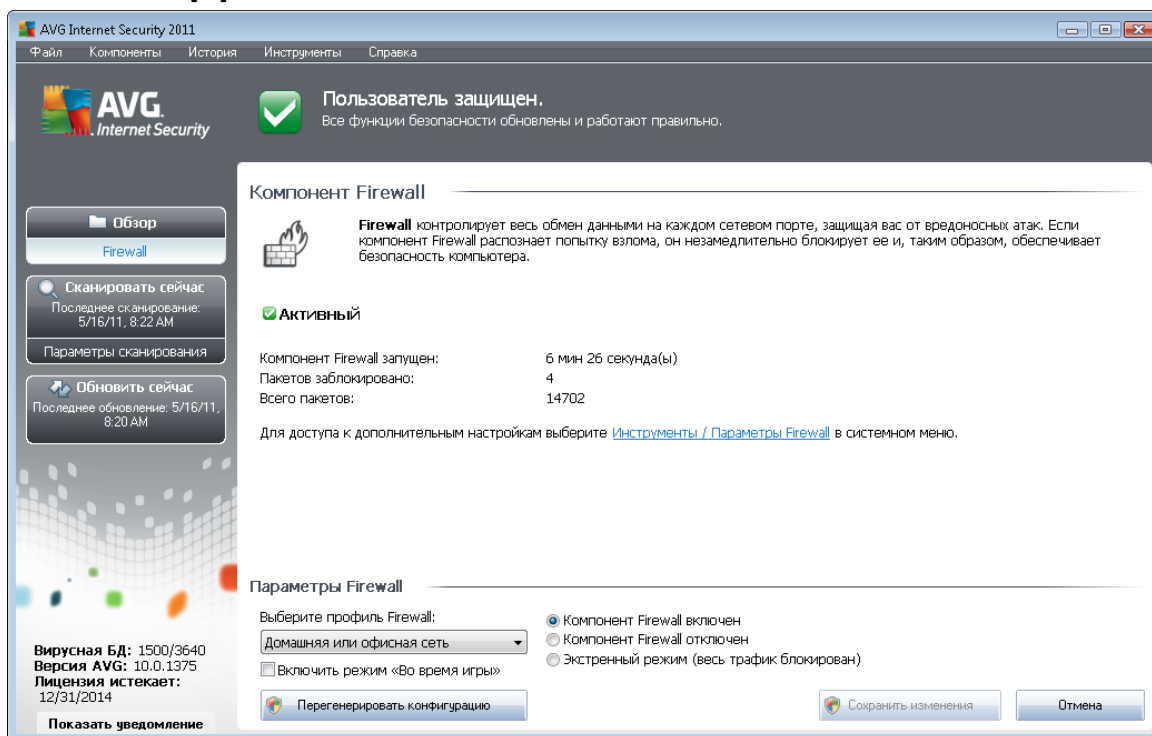
Переключение профиля

Функция переключения профиля позволяет компоненту [Firewall](#) автоматически переключаться на назначенный профиль при использовании определенного сетевого адаптера или при подключении к определенной сети. Если сетевой области еще не был назначен профиль, тогда при следующем подключении к данной области компонентом [Firewall](#) будет отображено диалоговое окно, с помощью которого можно назначить профиль.

Назначить профиль всем локальным сетевым интерфейсам или областям, а также указать дополнительные параметры можно в диалоговом окне [Области и профили адаптеров](#). Данное диалоговое окно также позволяет при необходимости отключить эту функцию (*при этом для каждого типа подключения будет использоваться профиль по умолчанию*).

Данная функция будет удобна пользователям ноутбука, которые используют различные виды подключений. При работе за настольным компьютером и использовании только одного вида подключения (*например, подключения к Интернету с помощью кабеля*) можно не тратить время на освоение функции переключения профиля, так как, вероятнее всего, данная функция никогда не будет использоваться.

7.4.3. Интерфейс Firewall



Интерфейс компонента **Firewall** содержит общие сведения о функциях и состоянии компонента, а также краткий обзор статистики компонента **Firewall**.

- **Время работы Firewall.** Время, прошедшее с момента последнего запуска компонента Firewall.
- **Пакетов заблокировано.** Количество заблокированных пакетов из общего числа проверенных пакетов.
- **Всего пакетов.** Количество пакетов, проверенных компонентом Firewall

Параметры Firewall

- **Выберите профиль Firewall.** В раскрывающемся меню выберите один из определенных профилей: два профиля по умолчанию доступны всегда (*профили Разрешить все и Блокировать все*). Другие профили были добавлены вручную при редактировании профиля в диалоговом окне [Профили](#) раздела [Параметры Firewall](#).
- **Включить режим "Во время игры".** Установите данный флажок, чтобы во время работы с полноэкранными приложениями (*играми, презентациями, фильмами и т. п.*), компонент [Firewall](#) не будет отображать запросы на разрешение или блокировку доступа неизвестным приложениям. В этом случае, если неизвестное приложение пытается получить доступ через сеть, компонент [Firewall](#) автоматически разрешит или заблокирует это приложение в соответствии с параметрами текущего профиля.



Примечание. Если режим "Во время игры" включен, все запланированные задачи (сканирования, обновления) будут отложены до завершения работы приложения.

- **Состояние компонента Firewall.**

- о **Firewall включен.** Выберите этот параметр, чтобы разрешить связь с приложениями, отмеченными как "разрешенные" в наборе правил, определенном в выбранном профиле [Firewall](#).
- о **Firewall отключен.** Данный параметр полностью отключает компонент [Firewall](#), весь сетевой трафик принимается без проверки.
- о **Экстренный режим (блокировка всего интернет-трафика).** Выберите данный параметр, чтобы блокировать трафик на всех сетевых портах; [Firewall](#) будет функционировать, однако прием трафика осуществляться не будет.

Примечание. Все компоненты AVG настроены поставщиком ПО для обеспечения оптимальной производительности. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться опытным пользователем. При необходимости изменить настройки Firewall выберите элемент системного меню **Инструменты/Параметры Firewall** и исправьте настройки Firewall в новом открытом диалоговом окне [Параметры Firewall](#).

Кнопки управления

- **Перегенерировать конфигурацию.** Нажмите данную кнопку, чтобы перезаписать текущую конфигурацию компонента **Firewall** и восстановить конфигурацию по умолчанию на основе автоматического обнаружения.
- **Сохранить изменения.** Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне.
- **Отмена.** Нажмите данную кнопку для возврата к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.5. Link Scanner

7.5.1. Принципы работы Link Scanner

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.

Технология **LinkScanner** включает в себя две функции: [Search-Shield](#) и [Surf-Shield](#).

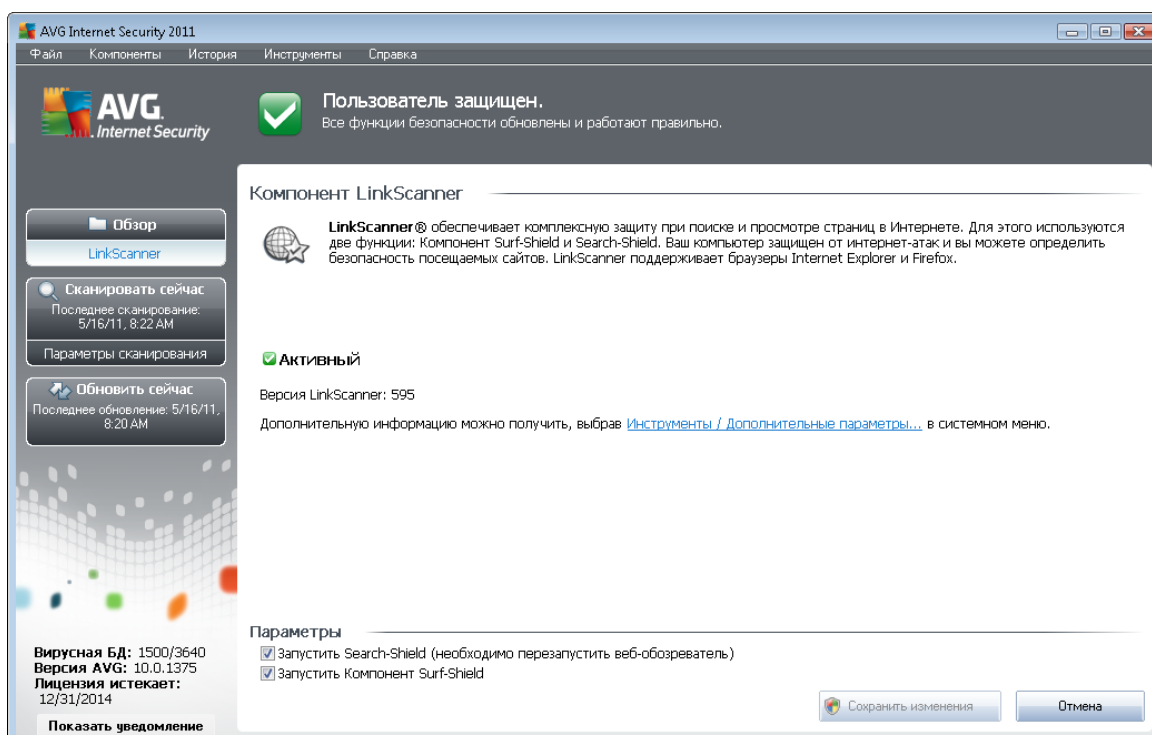


- **AVG Search-Shield** содержит список известных опасных веб-сайтов (URL-адресов). При выполнении поиска с помощью систем Google, Yahoo!, JP, WebHledani, Яндекс, Baidu, Bing, AOL, Altavista, EarthLink, Ask, Seznam, eBay, Twitter, Digg или SlashDot все результаты поиска проверяются в соответствии с этим списком. После этого отображается значок заключения (для результатов поиска Yahoo отображаются только значки заключения о наличии эксплойтов на веб-сайтах).
- **Surf-Shield** выполняет сканирование содержимого посещаемых веб-сайтов независимо от наличия их адресов в списке. Даже если опасный веб-сайт не 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 функцией **Surf-Shield** при попытке его посещения.

Примечание. Компонент Link Scanner не предназначен для использования на серверных платформах!

7.5.2. Интерфейс Link Scanner

Интерфейс компонента **LinkScanner** содержит краткое описание функций компонента и сведения о его текущем состоянии. Также можно просмотреть сведения о последней версии базы данных **LinkScanner** (версия Link Scanner).



Параметры LinkScanner

В нижней части диалогового окна можно изменить некоторые параметры.



- **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 и 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).

7.5.3. 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, **AVG Link Scanner** 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.



Страница, связанная со ссылкой, безопасна (данный значок не отображается в результатах поиска на сайте Yahoo! JP).



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.

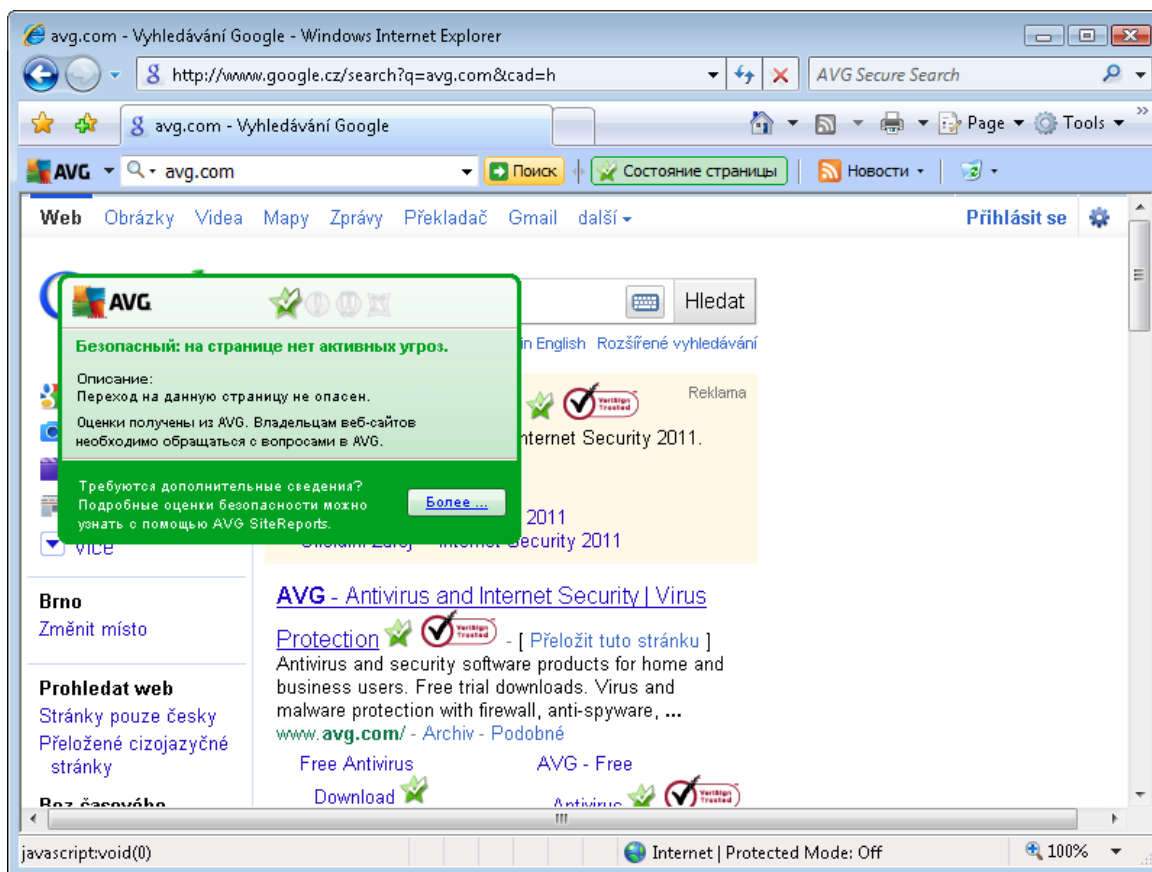


Связанная страница содержит активные угрозы! В целях безопасности доступ на подобные страницы будет закрыт.



Связанная страница недоступна, сканирование не может быть выполнено.

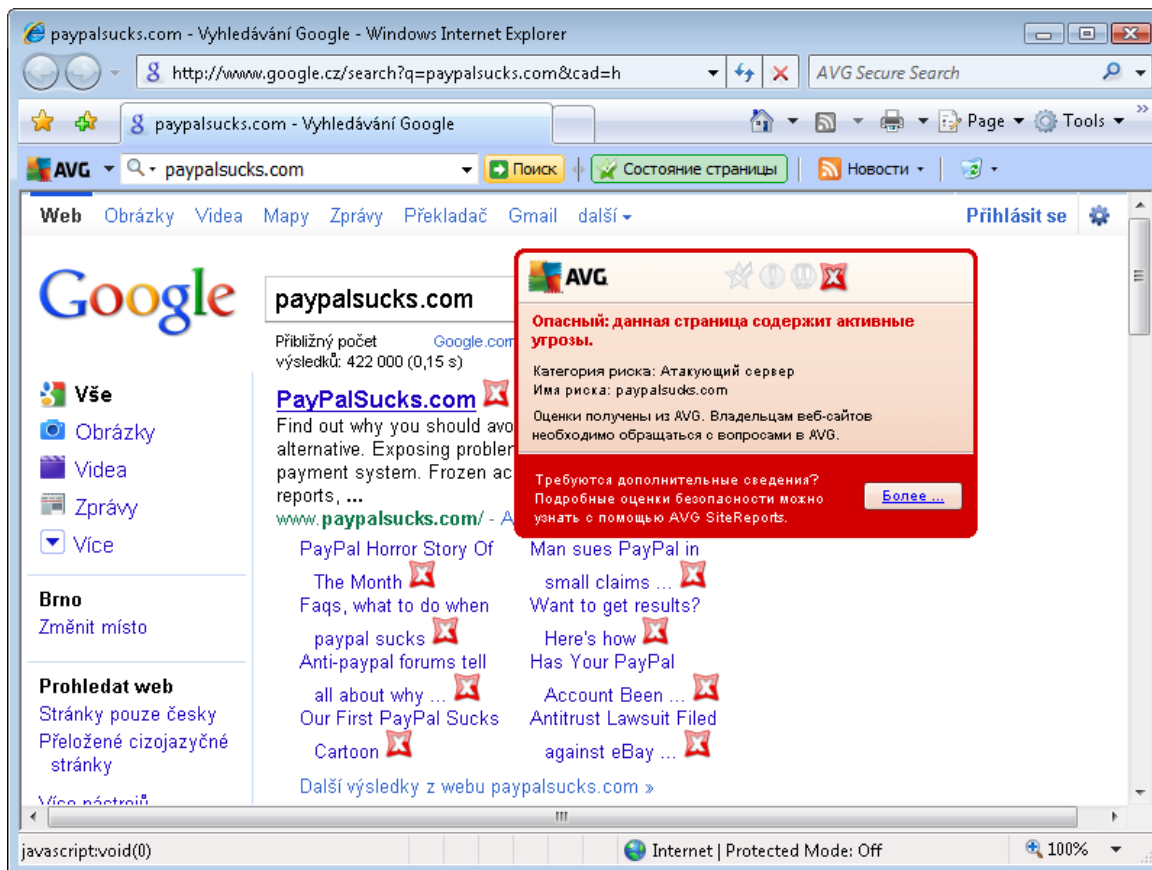
При наведении указателя мыши на значок отдельных рейтингов отобразятся сведения об определенной ссылке. Эти сведения содержат дополнительную информацию об угрозе (при ее наличии):



7.5.4. 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 **AVG Link Scanner** блокирует открытие такой страницы в браузере.

Если вам встретился зараженный веб-сайт, компонент браузера **AVG Security Toolbar** отобразит предупреждение, аналогичное следующему.



Посещение подобных сайтов чрезвычайно опасно и не рекомендуется.

7.6. Resident Shield

7.6.1. Принципы работы Resident Shield

Компонент **Resident Shield** обеспечивает непрерывную защиту компьютера. Он сканирует каждый файл при открытии, сохранении или копировании и защищает системные области компьютера. Если при доступе к файлу компонент **Resident Shield** обнаруживает вирус, все выполняемые в данный момент действия с файлом завершаются. Таким образом, вирус не может активировать себя. Обычно процесс сканирования незаметен, так как протекает в фоновом режиме, а уведомления отображаются только при обнаружении угроз. Однако компонент **Resident Shield** блокирует активацию угрозы и удаляет ее. Компонент **Resident Shield** загружается в память компьютера при запуске системы.

Возможности **Resident Shield**:

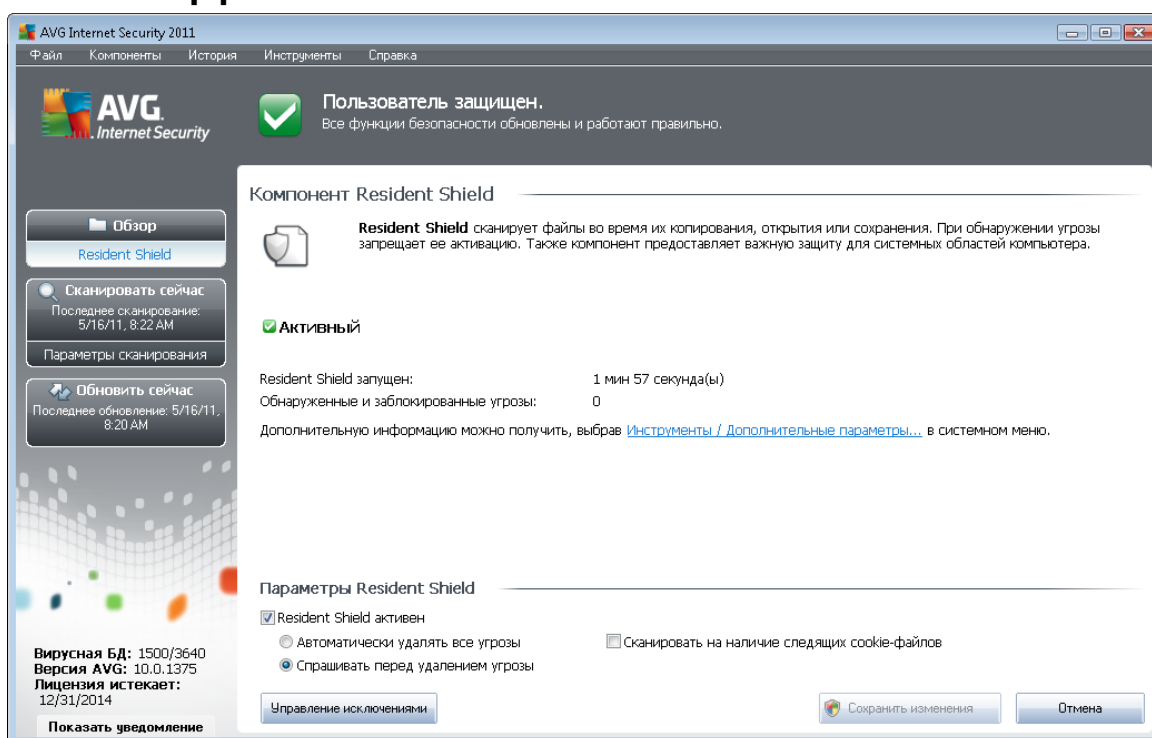
- Сканирование на наличие определенных видов угроз
- Сканирование съемных носителей (флэш-диск и т. п.)



- Сканирование файлов с определенными расширениями или без расширений
- Создание исключений из сканирования — определенные файлы и папки, которые не следует сканировать

Предупреждение. Компонент *Resident Shield* загружается в память компьютера при запуске системы — крайне необходимо, чтобы данный компонент всегда был запущен.

7.6.2. Интерфейс Resident Shield



Помимо обзора функций компонента *Resident Shield* и сведений о состоянии компонента, интерфейс *Resident Shield* содержит некоторые статистические данные.

- **Время работы компонента Resident Shield.** Время, прошедшее с момента запуска компонента.
- **Обнаруженные и заблокированные угрозы.** Количество обнаруженных заражений, запуск/открытие которых удалось предотвратить (при необходимости данное значение можно сбросить; например, в статистических целях — Сбросить значение).

Параметры Resident Shield

В нижней части диалогового окна расположен раздел *Параметры Resident Shield*, который позволяет изменять некоторые основные параметры компонента (подробные настройки, как и в других компонентах, доступны в системном меню *Инструменты/Дополнительные*



параметры).

Параметр **Компонент Resident Shield активен** позволяет легко включать и отключать постоянную защиту. По умолчанию данная функция включена. Если постоянная защита включена, можно определить действия, которые будут производиться с обнаруженными заражениями (удалено):

- о автоматически (**Удалять все угрозы автоматически**);
- о или только после подтверждения пользователем (**Запрашивать подтверждение перед удалением угроз**).

Данный параметр не влияет на уровень безопасности, поэтому может быть настроен на усмотрение пользователя.

Также можно выбрать параметр **Сканировать на наличие следящих файлов cookie**. В некоторых случаях может потребоваться включение данного параметра, чтобы обеспечить максимальный уровень безопасности. Однако по умолчанию параметр отключен. (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).

Примечание. 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 настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG в открывшемся диалоговом окне [Дополнительные параметры AVG](#).

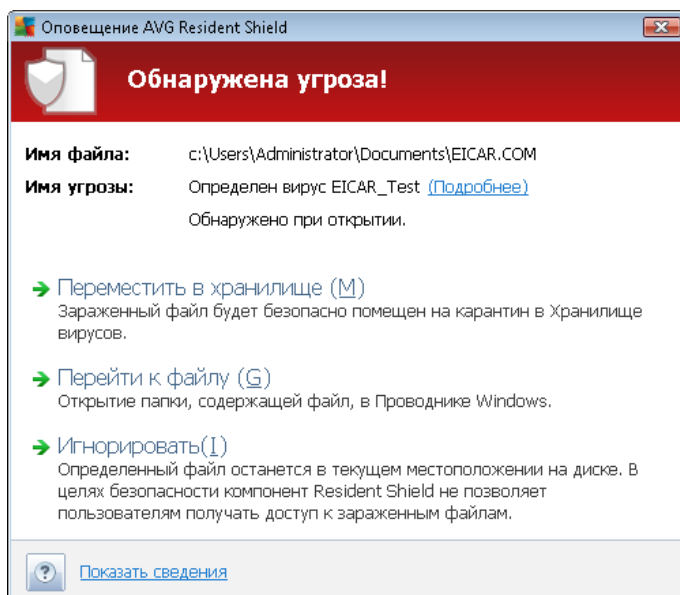
Кнопки управления

В интерфейсе компонента **Resident Shield** доступны следующие кнопки управления.

- **Управление исключениями.** Открытие диалогового окна [Resident Shield — исключенные элементы](#), которое позволяет определить папки, которые не должны сканироваться компонентом [Resident Shield](#).
- **Сохранить изменения.** Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне.
- **Отмена.** Нажмите данную кнопку для возврата к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.6.3. Обнаружение Resident Shield

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 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 (*Дополнительные сведения*).

Далее необходимо выбрать действие, которое будет применено к заражениям. Доступны следующие варианты:

Обратите внимание, что при определенных условиях (зависит от типа зараженного файла и его месторасположения) могут быть доступны не все варианты.

- **Удалить угрозу от имени опытного пользователя.** Установите этот флажок, если у вас недостаточно прав для удаления данной угрозы. Опытные пользователи имеют расширенные права доступа, поэтому для успешного удаления угрозы, расположенной в определенной системной папке, может потребоваться установить данный флажок.
- **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.** Вирус будет помещен в [хранилище вирусов AVG](#)
- **Перейти к файлу.** Перенаправление в папку размещения подозрительного объекта (в новом окне *Проводника Windows*).
- **Игнорировать.** Категорически НЕ рекомендуется использовать данный параметр.

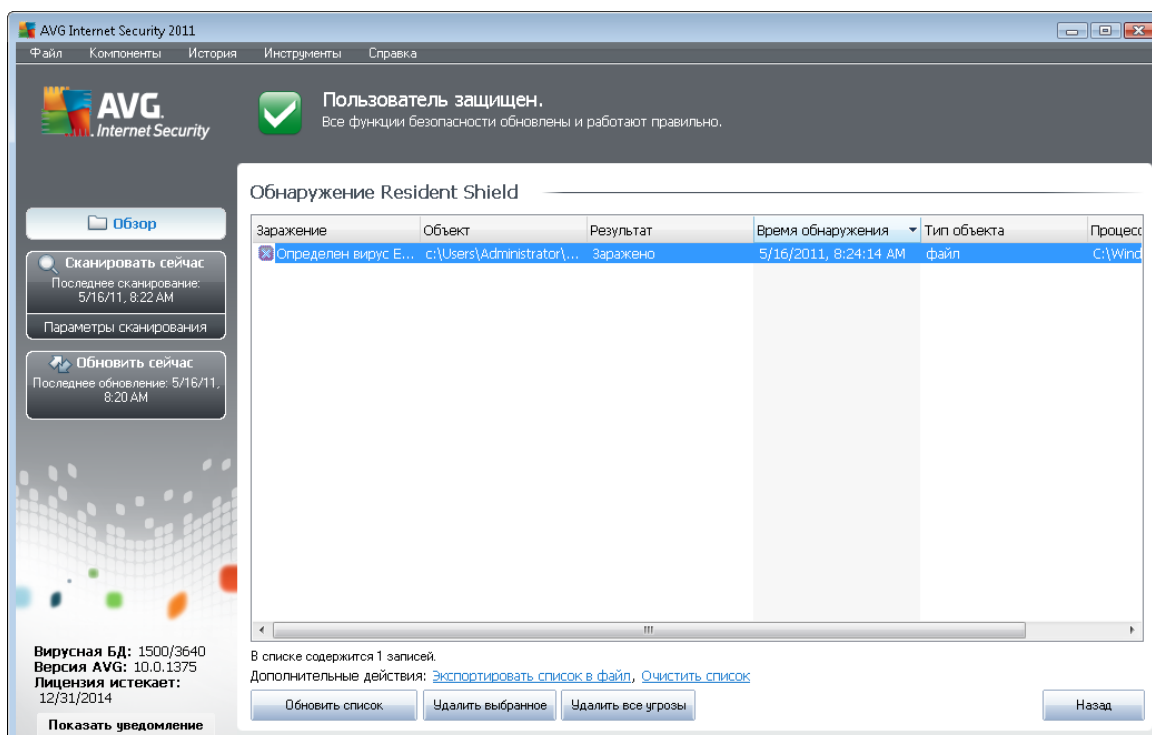
Примечание. Размер обнаруженного объекта может превышать объем свободного места в



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.

Полный обзор всех угроз, обнаруженных компонентом [Resident Shield](#), доступен в окне **Обнаружение 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 обратный переход к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.7. Защита семьи

AVG защита семьи 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. Можно назначить необходимый уровень защиты для каждого ребенка, а затем отслеживать их по отдельности с помощью уникальных имен пользователей.

Данный компонент будет активен, только если продукт **AVG защита семьи** установлен на компьютере. Если продукт **AVG защита семьи** не установлен на компьютере, щелкните соответствующий значок в интерфейсе пользователя **AVG Internet Security 2011**. Откроется веб-сайт продукта, на котором можно найти все необходимые сведения.

7.8. AVG LiveKive

Программа **AVG LiveKive** позволяет автоматически выполнять резервное копирование файлов, фотографий и музыки в общее безопасное пространство. 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.

Соответствующий компонент будет активен, только если программа **AVG LiveKive** установлена на компьютере. Если программа **AVG LiveKive** не установлена на компьютере, щелкните соответствующий значок в интерфейсе пользователя **AVG Internet Security 2011**. Откроется веб-сайт продукта, на котором можно найти все необходимые сведения.

7.9. E-mail Scanner

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.



7.9.1. Принципы работы 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 и The Bat*). В первую очередь, данный компонент предназначен для использования с такими приложениями, как Outlook Express, Mozilla, Incredimail и т. п.

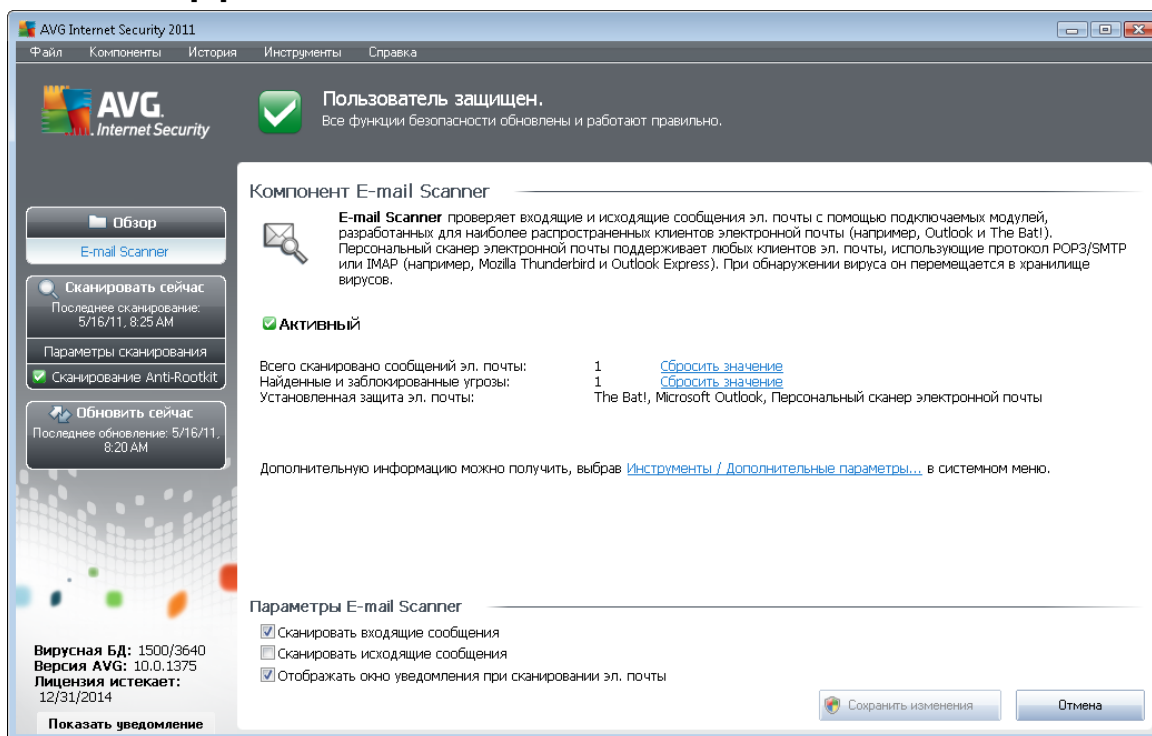
При [установке](#) AVG создаются автоматические серверы для управления электронной почтой: один для проверки входящих сообщений электронной почты, второй для проверки исходящих сообщений. С помощью этих двух серверов сообщения электронной почты автоматически проверяются на портах 110 и 25 (*стандартные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

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

7.9.2. Интерфейс E-mail Scanner



С помощью диалогового окна компонента **E-mail Scanner** можно получить краткие сведения о работе компонента, информацию о текущем состоянии компонента и следующие статистические данные.

- **Всего сканировано сообщений электронной почты.** Количество сканированных сообщений электронной почты со времени последнего запуска **E-mail Scanner** (при необходимости можно сбросить это значение, например в целях ведения статистики — "Сбросить значение")
- **Найденные и заблокированные угрозы.** Количество заражений, обнаруженных в сообщениях электронной почты со времени последнего запуска компонента **E-mail Scanner**.
- **Установленная защита электронной почты** — сведения о специальном модуле защиты электронной почты, встроенном в установленный по умолчанию почтовый клиент

Параметры E-mail Scanner

В нижней части диалогового окна расположен раздел **Параметры E-mail Scanner**, в котором можно редактировать некоторые основные функции компонента.

- **Сканировать входящие сообщения** Установите данный параметр, чтобы подтвердить проверку на вирусы всех сообщений, получаемых в используемую



учетную запись. По умолчанию данный параметр включен, рекомендуется не изменять значение для этого параметра.

- **Сканировать исходящие сообщения.** Установите данный параметр, чтобы подтвердить проверку на вирусы всех сообщений, отправляемых с используемой учетной записи. По умолчанию данный параметр отключен.
- **Отображать окно уведомления при сканировании эл. почты.** Установите этот флажок, чтобы на значке AVG на панели задач отображалось оповещение во время сканирования электронной почты с помощью компонента [E-mail Scanner](#). По умолчанию данный параметр включен, рекомендуется не изменять значение для этого параметра.

Дополнительные настройки компонента **E-mail Scanner** доступны в разделе системного меню **Инструменты/Дополнительные параметры**; однако использование дополнительных параметров рекомендуется только опытным пользователям.

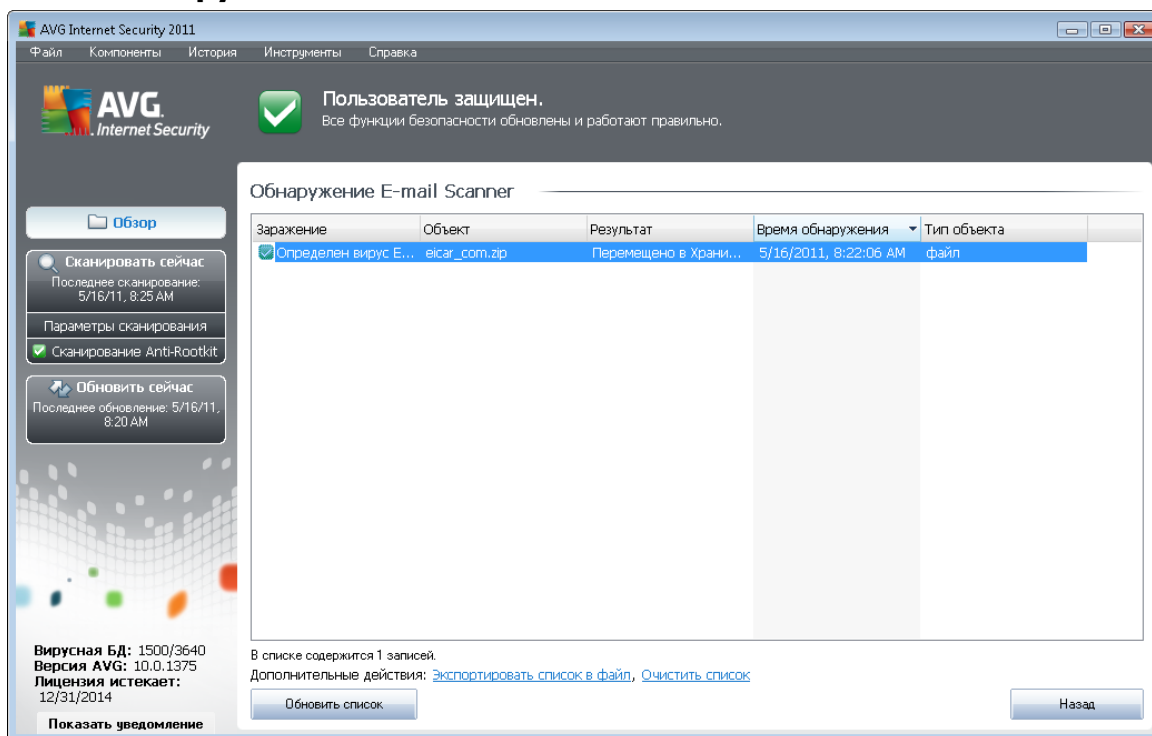
Примечание. Все компоненты AVG настроены поставщиком ПО для обеспечения оптимальной производительности. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться опытным пользователем. При необходимости изменить настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG в открывшемся диалоговом окне [Дополнительные параметры AVG](#).

Кнопки управления

В интерфейсе компонента **E-mail Scanner** 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 установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.9.3. Обнаружение E-mail Scanner



Диалоговое окно **Обнаружение E-mail Scanner** (доступное при выборе *История/Обнаружение E-mail Scanner*) содержит список всех объектов, обнаруженных компонентом **E-mail Scanner**. 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

7.10. Диспетчер обновлений

7.10.1. Принципы работы диспетчера обновления

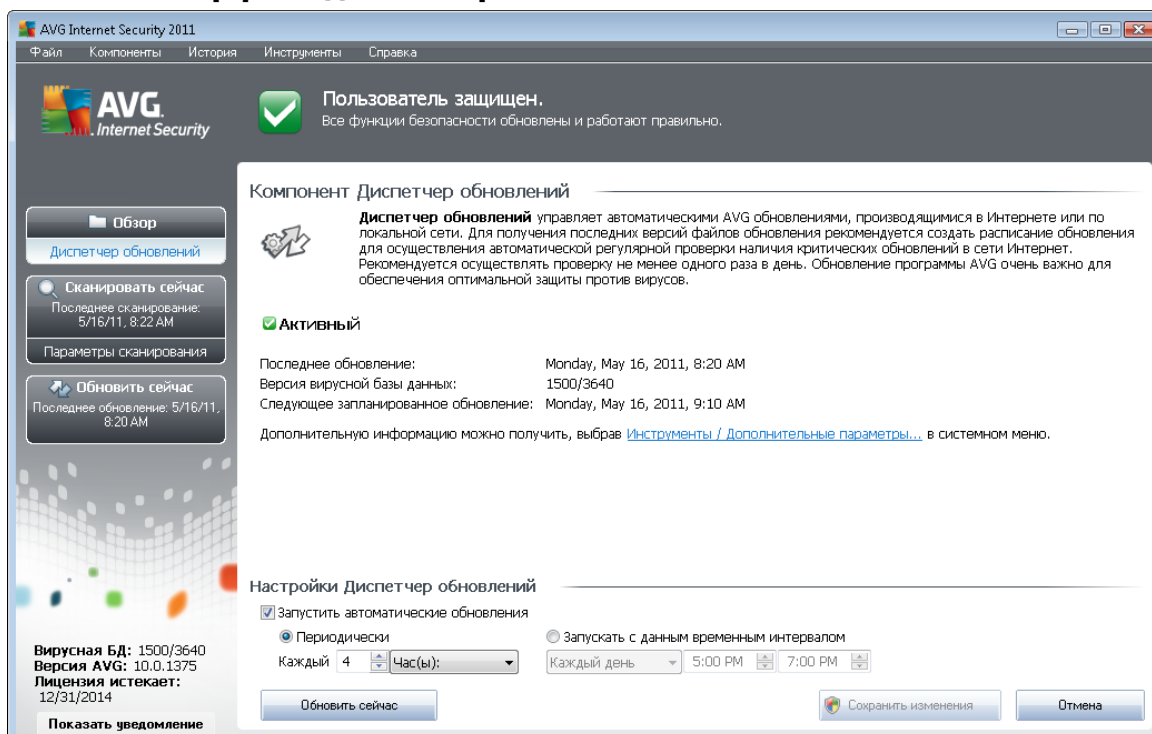
Ни один из программных продуктов по обеспечению безопасности не может гарантировать полноценную защиту от различных типов угроз без регулярного обновления. Создатели вирусов ищут новые уязвимые места для взлома программного обеспечения и операционных систем. Ежедневно совершаются попытки несанкционированного 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.

Очень важно выполнять регулярное обновление продуктов AVG!

Управлять регулярными обновлениями можно с помощью компонента **Диспетчер обновлений**. Данный компонент позволяет запланировать автоматическую загрузку файлов обновлений через Интернет или локальную сеть. Важные обновления определений вирусов должны выполняться ежедневно, если это возможно. Обновление менее важных программ может выполняться один раз в неделю.

Примечание. Для получения дополнительной информации о типах и уровнях обновлений внимательно ознакомьтесь с главой [Обновления AVG](#).

7.10.2. Интерфейс диспетчера обновления





В интерфейсе компонента **Диспетчер обновления** можно просмотреть сведения о функциях и текущем состоянии компонента, а также соответствующие статистические данные.

- **Последнее обновление.** Дата и время последнего обновления базы данных.
- **Версия вирусной базы данных.** Номер установленной версии вирусной базы данных; в результате каждого обновления вирусной базы данных номер увеличивается
- **Следующее запланированное обновление.** Дата и время следующего обновления базы данных.

Параметры диспетчера обновления

В нижней части диалогового окна расположен раздел **Параметры компонента "Диспетчер обновления"**, где можно изменить правила запуска процесса обновления. Файлы обновления могут загружаться автоматически (**Запустить автоматические обновления**) или по требованию. Функция **Запустить автоматические обновления** включена по умолчанию. Данную настройку изменять не рекомендуется. Регулярная загрузка последних файлов обновлений имеет критическое значение для правильной работы ПО по обеспечению безопасности!

Также можно определить время запуска процесса обновления.

- о **Периодически.** Позволяет определить временной интервал.
- о **Запускать через определенный интервал.** Позволяет определить точные дату и время запуска процесса обновления.

По умолчанию обновление выполняется каждые 4 часа. Рекомендуется изменять данную настройку только в случае крайней необходимости.

Примечание. 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 настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG в открывшемся диалоговом окне [Дополнительные параметры AVG](#).

Кнопки управления

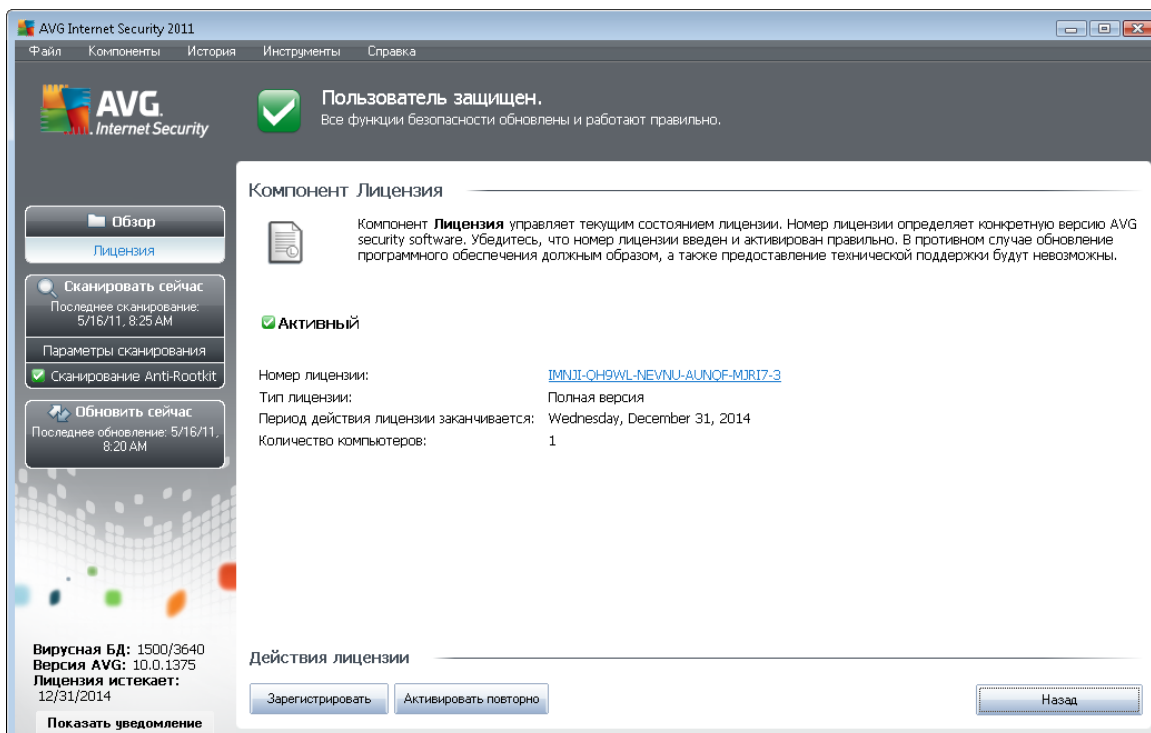
В интерфейсе компонента **Диспетчер обновления** имеются следующие кнопки управления.

- **Обновить сейчас** — запускает [немедленное обновление](#) по требованию
- **Сохранить изменения.** Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне.



- **Отмена.** Нажмите данную кнопку для возврата к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.11. Лицензия



С помощью интерфейса компонента **Лицензия** можно получить краткие сведения о работе компонента, информацию о его текущем состоянии, а также следующие сведения.

- **Номер лицензии.** В данном поле отображается краткая форма номера лицензии (*в целях безопасности скрыты последние четыре символа*). Необходимо правильно ввести номер лицензии. Настоятельно рекомендуется использовать способ "копировать/вставить" для любых операций с номером лицензии.
- **Тип лицензии.** Тип устанавливаемого продукта.
- **Срок окончания действия лицензии.** Данная дата определяет период действия лицензии. Чтобы использовать **AVG Internet Security 2011** после окончания срока действия лицензии, потребуется выполнить продление срока действия лицензии. Продление лицензии может быть выполнено в Интернете на [веб-сайте AVG](#).
- **Количество компьютеров.** Количество рабочих станций, на которые пользователь может установить приложение **AVG Internet Security 2011**.

Кнопки управления

- **Регистрация.** Переход на страницу регистрации веб-сайта компании AVG (<http://www.avg.com/>). Введите данные для регистрации. Только клиенты, зарегистрировавшие



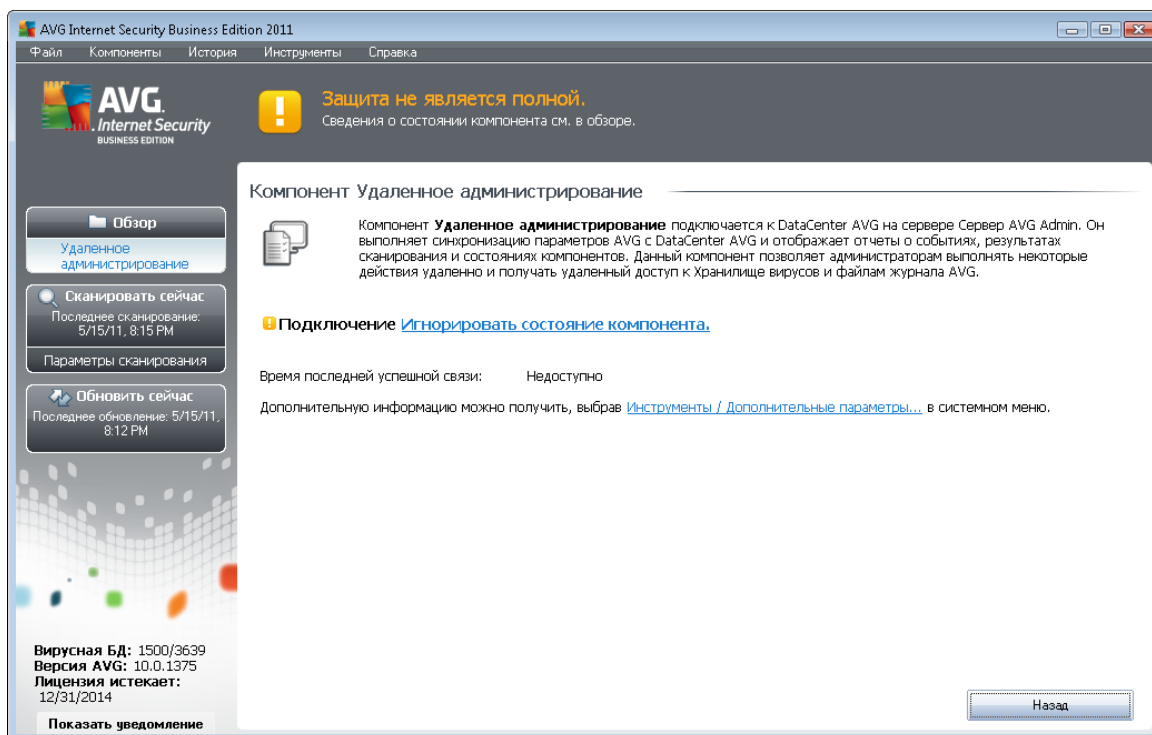
продукт AVG, могут получать бесплатную техническую поддержку.

- **Активировать повторно.** Открытие диалогового окна **Активация AVG**, содержащего сведения, введенные в диалоговое окно [Персонализация AVG при установке](#). В данном 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 нового продукта AVG).

Примечание. При использовании пробной версии **AVG Internet Security 2011** кнопки будут называться **Купить** и **Активировать**. С их помощью можно сразу купить полную версию программы. Для программы **AVG Internet Security 2011**, при установке которой был указан номер продажи, будут отображаться кнопки **Зарегистрировать** и **Активировать**.

- **Назад.** Нажмите данную кнопку для возврата к [интерфейсу пользователя AVG](#) по умолчанию (обзор компонентов).

7.12. Удаленное администрирование



Компонент **Удаленное администрирование** отображается в интерфейсе пользователя программы **AVG Internet Security 2011** только в случае установки версии продукта Business Edition (см. компонент [Лицензия](#)). В диалоговом окне **Удаленное администрирование** можно узнать, активен ли компонент и подключен ли он к серверу. Для настройки параметров компонента **Удаленное администрирование** выберите **Дополнительные параметры/Удаленное администрирование**.

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 \(www.avg.com\)](http://www.avg.com) в разделе **Центр поддержки/Загрузка/Документация**.

Кнопки управления

- **Назад.** Нажмите данную кнопку для возврата к [интерфейсу пользователя AVG](#) по умолчанию (обзор компонентов).

7.13. Online Shield

7.13.1. Принципы работы Online Shield

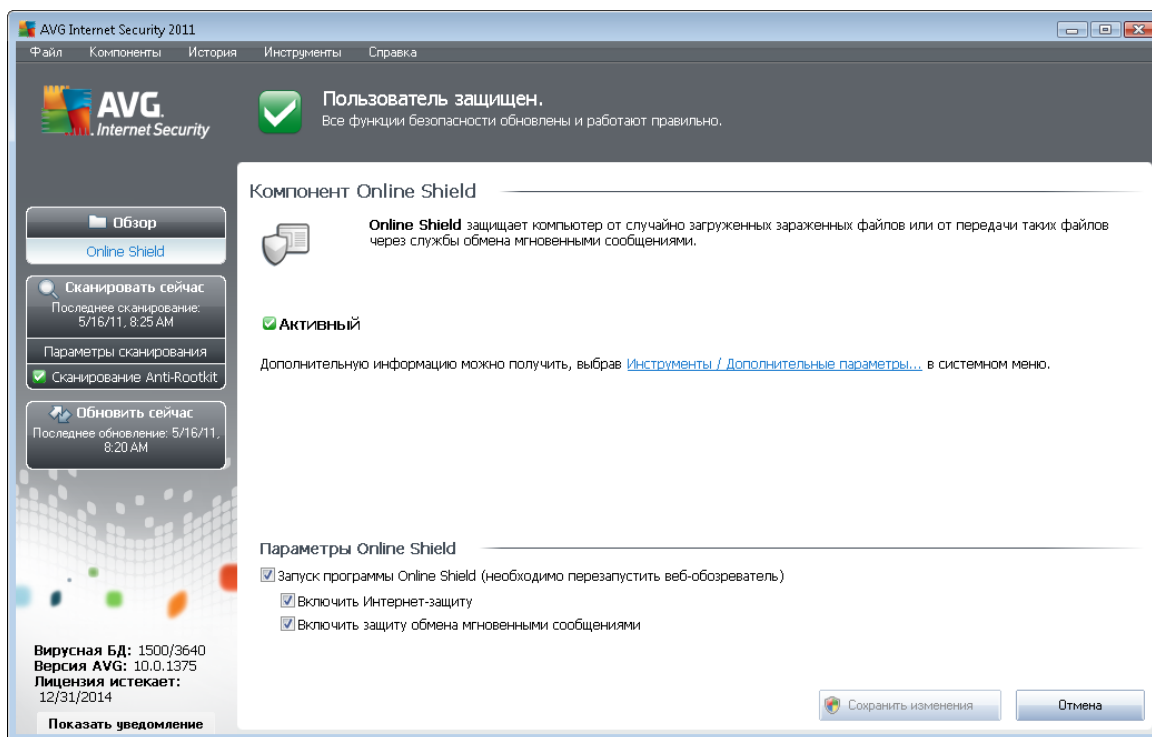
Online Shield — это разновидность постоянной защиты в режиме реального времени, которая сканирует содержимое посещаемых веб-страниц и *файлов, которые содержат эти страницы*, до того, как они отобразятся в веб-браузере или будут загружены на компьютер.

Компонент **Online Shield** предназначен для обнаружения на открываемой веб-странице небезопасных объектов javascript и предотвращения отображения данной страницы. Кроме того, она способна определить наличие вредоносного ПО на странице и остановить его загрузку, чтобы оно не попало на компьютер.

Примечание. Компонент AVG Online Shield не предназначен для использования на серверных платформах.

7.13.2. Интерфейс Online Shield

Интерфейс компонента **Online Shield** позволяет определить особенности работы данного типа защиты. Также здесь можно найти сведения о текущем состоянии компонента. В нижней части диалогового окна находятся начальные параметры функционирования данного компонента.



Параметры Online Shield

Прежде всего, имеется возможность быстрого включения и отключения компонента **Online Shield** путем установки флажка **Активировать Online Shield**. Данный параметр установлен по умолчанию, компонент **Online Shield** активен. Не рекомендуется изменять данные настройки без необходимости: желательно, чтобы компонент был всегда активен. Если элемент отмечен флажком, а компонент **Online Shield** запущен, становятся активны еще два параметра.

- **Включить интернет-защиту.** Данный параметр подтверждает, что компонент **Online Shield** должен выполнять сканирование содержимого интернет-страниц.
- **Включить защиту обмена мгновенными сообщениями.** Установите данный флажок, если требуется, чтобы компонент **Online Shield** проверял мгновенные сообщения (например, при использовании служб ICQ, MSN Messenger, ...) на наличие вирусов.

Примечание. 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 настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG в открывшемся диалоговом окне [Дополнительные параметры AVG](#).

Кнопки управления

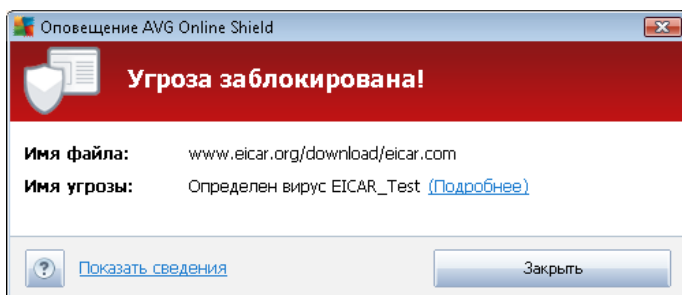


В окне компонента **Online Shield** имеются следующие кнопки управления.

- **Сохранить изменения.** Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне.
- **Отмена.** Нажмите данную кнопку для возврата к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.13.3. Обнаружение Online Shield

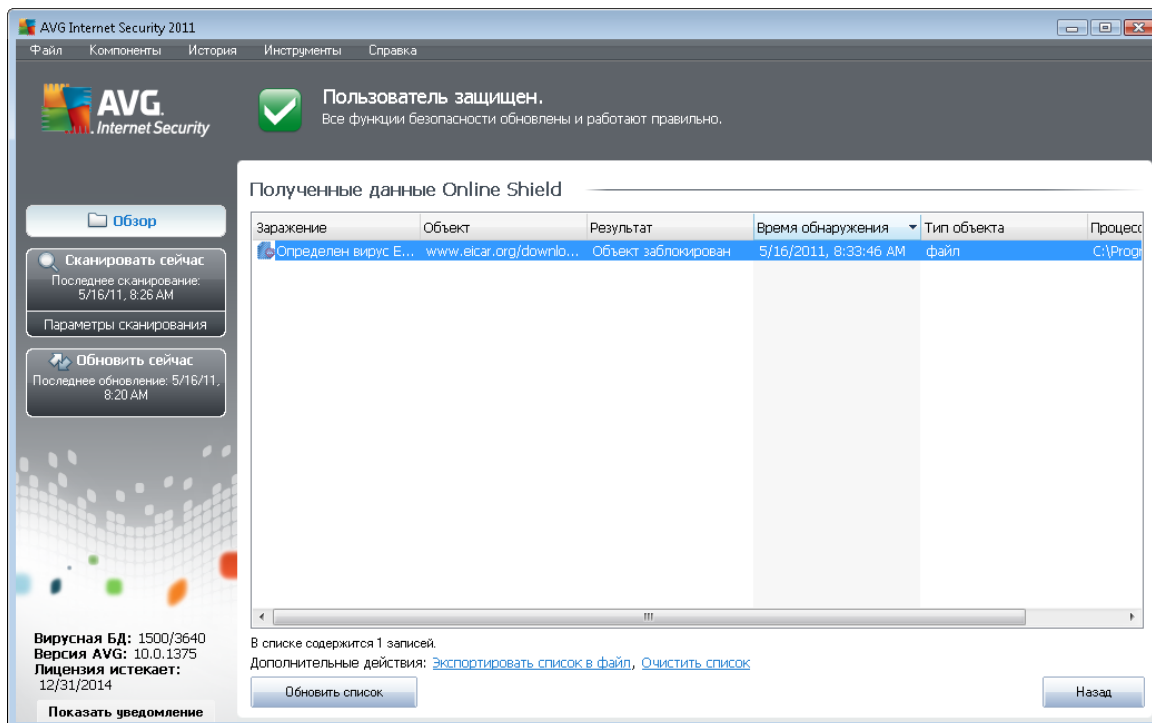
Компонент **Online Shield** выполняет сканирование содержимого посещаемых веб-страниц и файлов, которые могут на них содержаться, еще до того, как данное содержимое будет отображено в веб-браузере или загружено на компьютер. При обнаружении угрозы сразу же отобразится предупреждение в виде следующего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



Для каждого обнаруженного объекта 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**). Кнопка **Обновить список** обновит список объектов, найденных **Online Shield**. Кнопка **Назад** выполняет обратный переход к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.14. Anti-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

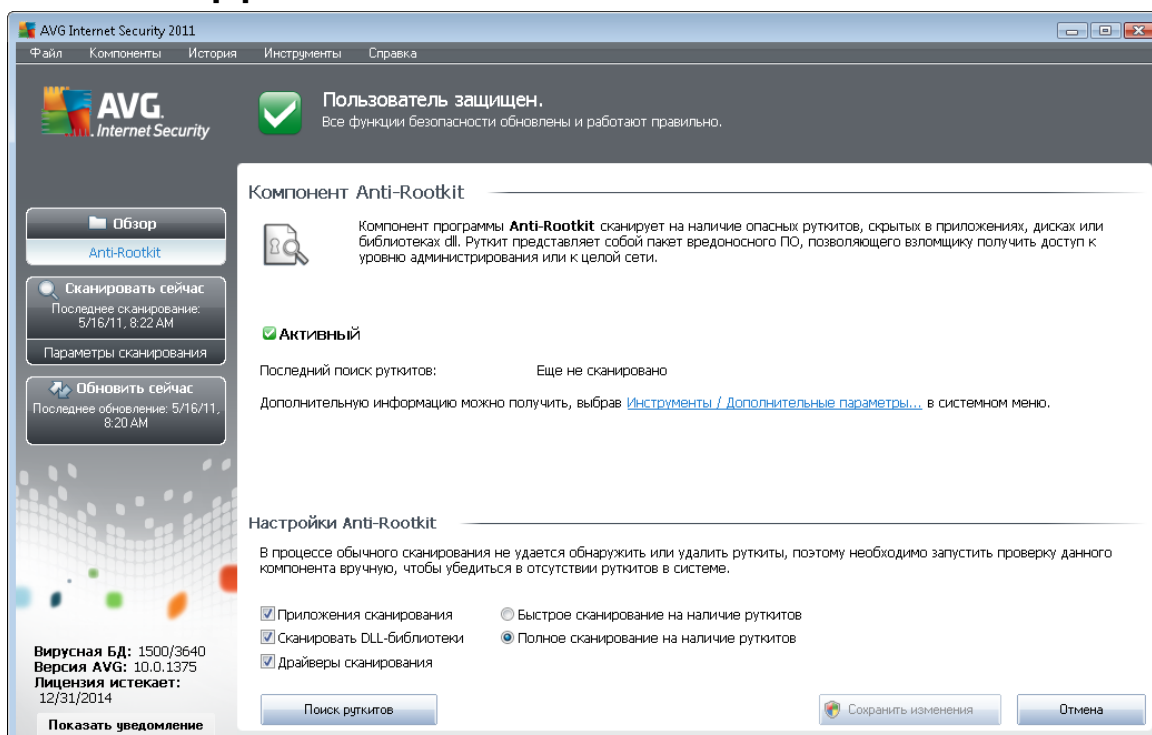


скрывают свое присутствие в системе с помощью замены информации или обхода стандартных механизмов безопасности операционных систем. Кроме того, они могут попадать на компьютер в виде троянских программ, которые пользователи уверенно запускают, не подозревая об опасности. Используемые для этого технические приемы включают в себя скрытие запущенных процессов от следящих программ, а файлов и системных данных — от операционных систем.

7.14.1. Принципы работы Anti-Rootkit

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

7.14.2. Интерфейс Anti-Rootkit



В интерфейсе пользователя компонента **Anti-Rootkit** приводится краткое описание функций компонента, сведения о текущем состоянии компонента, а также о последнем запуске проверки **Anti-Rootkit** (*последний поиск средств rootkit*). В диалоговом окне компонента **Anti-Rootkit** также содержится ссылка [Инструменты/Дополнительные параметры](#). Щелкните данную ссылку, чтобы перейти в меню расширенной конфигурации компонента **Anti-Rootkit**.

Примечание. Все компоненты AVG настроены поставщиком ПО для обеспечения



оптимальной производительности. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться опытным пользователем.

Параметры Anti-Rootkit

В нижней части диалогового окна расположен раздел **Параметры Anti-Rootkit**, в котором можно настроить некоторые из основных функций сканирования на наличие средств rootkit. Чтобы указать объекты, которые должны сканироваться, установите соответствующие флажки.

- **Сканировать приложения**
- **Сканировать DLL-библиотеки**
- **Сканировать драйверы**

Далее можно включить режим сканирования на наличие средств rootkit.

- **Быстрое сканирование rootkits.** 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 приводов компакт-дисков).

Кнопки управления

- **Поиск rootkits.** 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 [интерфейсу пользователя AVG](#) по умолчанию (обзор компонентов).
- **Отмена.** Используйте данную кнопку для возврата к [интерфейсу пользователя AVG](#) по умолчанию (обзор компонентов) без сохранения изменений

7.15. Системные средства

Системные средства. Средства, обеспечивающие просмотр подробной информации о среде **AVG Internet Security 2011** и операционной системе. Компонент содержит обзор следующих элементов:

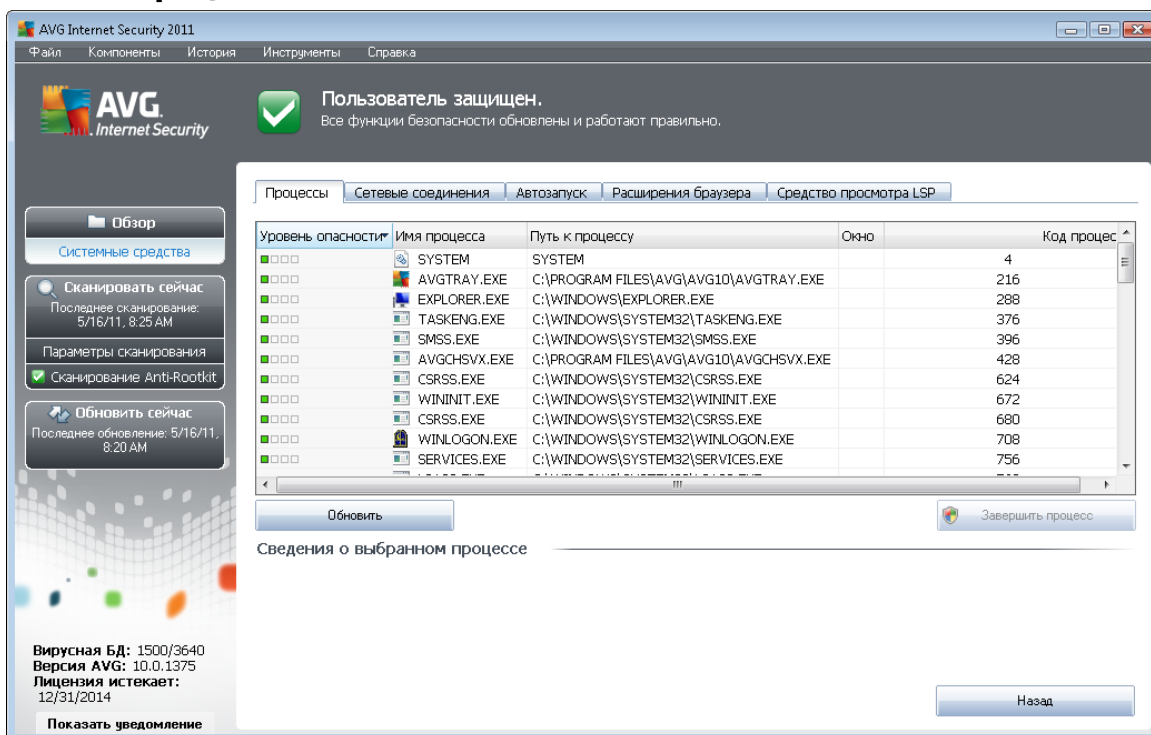
- [Процессы.](#) Список процессов (*т. е. запущенных приложений*), активных на компьютере в данный момент.
- [Сетевые подключения.](#) Список подключений, активных в данный момент.



- [Автозапуск](#). Список всех приложений, запускаемых при загрузке ОС Windows.
- [Расширения браузера](#). Список модулей (т. е. приложений), установленных в веб-браузере.
- [Средство просмотра LSP](#). Список поставщиков многоуровневых услуг (LSP).

Специальные обзоры могут быть также изменены, однако данное действие рекомендуется выполнять только опытным пользователям.

7.15.1. Процессы



Диалоговое окно Процессы содержит список процессов (например, запущенные приложения), которые в данный момент активны на компьютере. Список разделен на следующие столбцы:

- **Уровень серьезности.** Графическое определение уровня серьезности соответствующих процессов по 4-уровневой шкале от наименее важного (■□□□) до критического (■□■□).
- **Имя процесса.** В данном столбце отображается имя запущенного процесса.
- **Путь процесса.** В данном столбце отображается физический путь к запущенному процессу.
- **Окно.** В данном столбце указывается имя окна приложения.
- **PID.** Идентификационный номер процесса является уникальным идентификатором внутреннего процесса Windows.

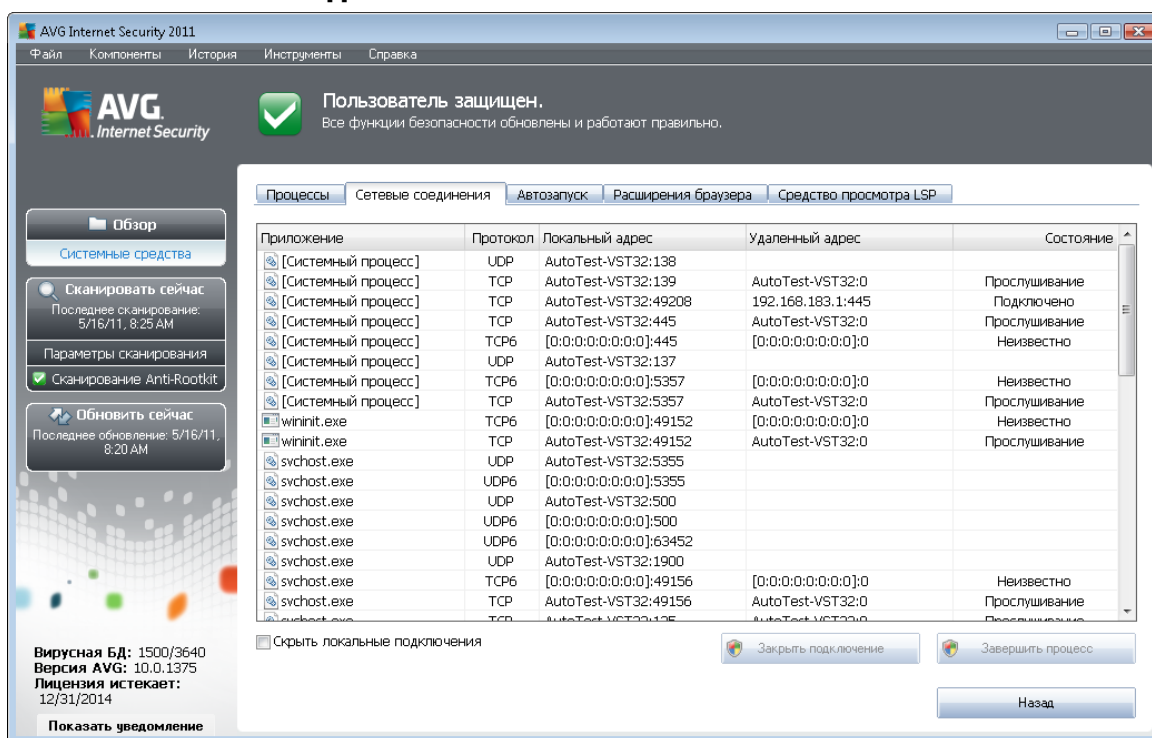


Кнопки управления

В интерфейсе компонента **System Tools** имеются следующие кнопки управления.

- **Обновить.** Обновление списка процессов в соответствии с текущим состоянием.
- **Завершить процесс.** Можно выбрать одно или несколько приложений и завершить их работу с помощью этой кнопки. **Настоятельно не рекомендуется завершать работу приложений при отсутствии уверенности в том, что они представляют реальную угрозу.**
- **Назад.** Переход к [интерфейсу пользователя AVG](#) по умолчанию (обзор компонентов).

7.15.2. Сетевые подключения



Диалоговое окно **Сетевые соединения** содержит список активных в данный момент соединений. Список разделен на следующие столбцы.

- **Приложение.** Название приложения, связанного с подключением (за исключением Windows 2000, где данные сведения недоступны).
- **Протокол.** Тип протокола передачи, используемого в соединении.

о Протокол TCP. Протокол, используемый в сочетании с интернет-протоколом (IP) для передачи информации через Интернет.



о Протокол UDP. Альтернатива протоколу TCP.

- **Локальный адрес.** IP-адрес локального компьютера и используемый номер порта.
- **Удаленный адрес.** IP-адрес удаленного компьютера и номер используемого для соединения порта. По возможности будет также отображено имя хост-системы удаленного компьютера.
- **Состояние.** В данном столбце отображается наиболее достоверное текущее состояние (*Подключено, Сервер необходимо закрыть, Сбор сведений, Активное закрытие завершено, Пассивное закрытие, Активное закрытие*)

Чтобы в списке отображались только внешние соединения, установите флажок **Скрыть локальные подключения** в нижнем разделе диалогового окна под списком.

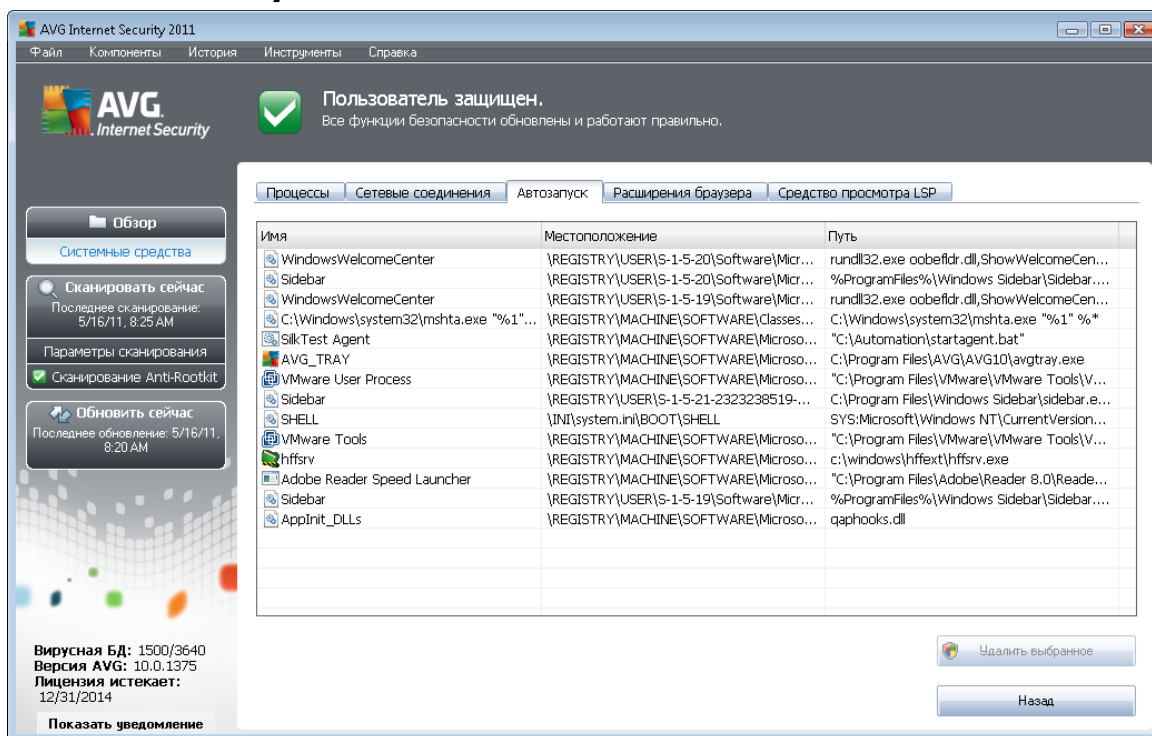
Кнопки управления

Доступны следующие кнопки управления.

- **Завершение соединения.** Закрывает одно или несколько подключений, выбранных в списке.
- **Завершить процесс.** Завершение работы одного или нескольких приложений, связанных с соединениями, выбранными в списке.
- **Назад.** Переход к [интерфейсу пользователя AVG](#) по умолчанию (обзор компонентов).

Иногда возможно отключить только приложения, находящиеся в подключенном состоянии. Настоятельно не рекомендуется завершать работу приложений при отсутствии уверенности в том, что они представляют реальную угрозу.

7.15.3. Автозапуск

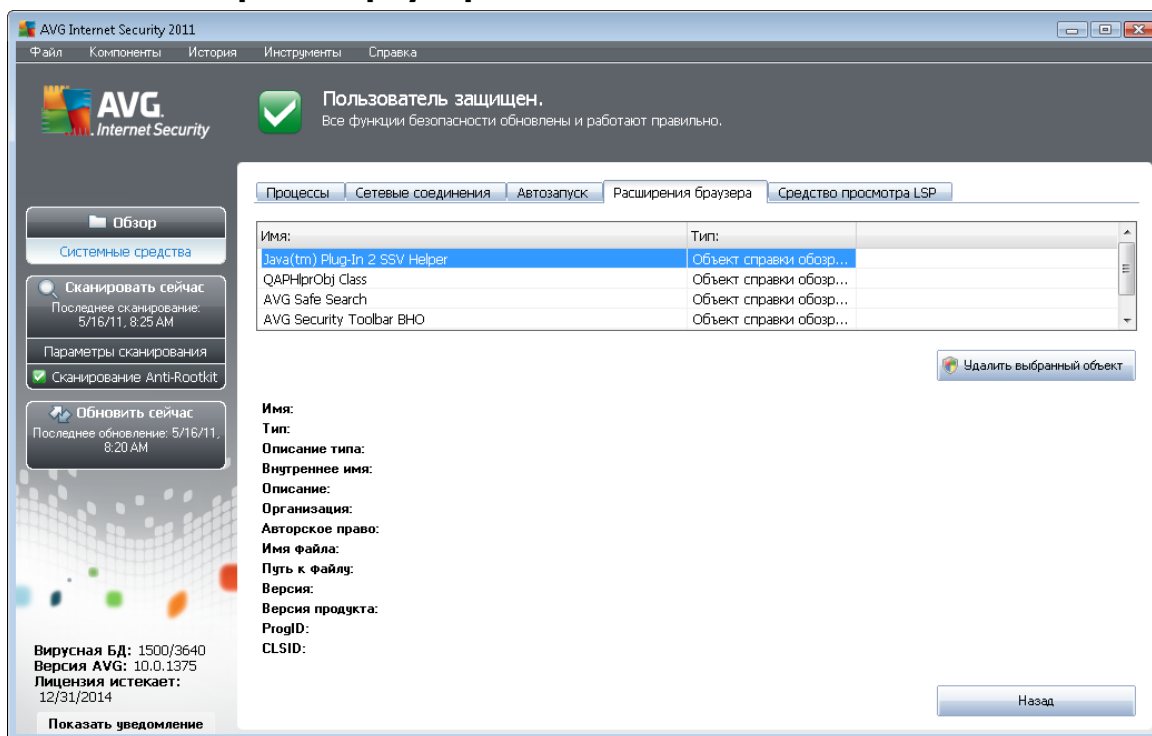


В диалоговом окне **Автозапуск** отображается список всех приложений, которые запускаются при загрузке ОС Windows. Очень часто некоторые вредоносные приложения автоматически прописывают свой запуск в реестре.

Чтобы удалить одну или несколько записей реестра, выберите необходимые записи и нажмите кнопку **Удалить выбранное**. Кнопка **Назад** выполняет обратный переход к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

Настоятельно рекомендуется не удалять приложения из списка, если нет уверенности, что они представляют реальную угрозу.

7.15.4. Расширения браузера



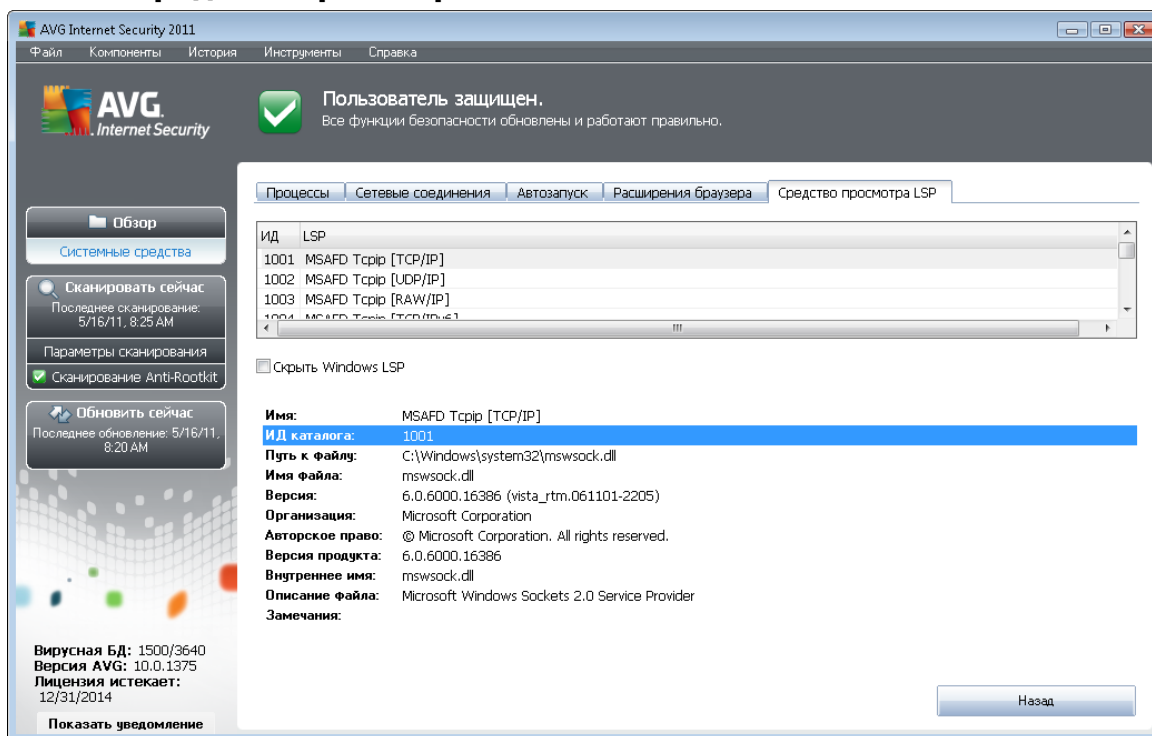
Диалоговое окно **Расширения браузера** содержит список подключаемых модулей (например, модулей приложений), которые встраиваются в интернет-браузер. В данном списке могут содержаться как обычные модули приложения, так и потенциально вредоносные программы. Для получения подробных сведений о выбранном модуле щелкните объект в списке, который отобразится в нижней части диалогового окна.

Кнопки управления

Кнопки управления, доступные на вкладке **Расширение веб-браузера**:

- **Удалить выбранный объект** — удаляет модуль, выделенный в списке в данный момент. **Настоятельно рекомендуется не удалять модули из списка, если нет уверенности, что они представляют реальную угрозу.**
- **Назад** — переход к интерфейсу пользователя AVG по умолчанию (обзор компонентов)

7.15.5. Средство просмотра LSP



В диалоговом окне **Средство просмотра LSP** отображается список поставщиков многоуровневых услуг (LSP).

Поставщик многоуровневых услуг (LSP). Это системный драйвер, связанный с сетевыми службами операционной системы Windows. Он имеет доступ ко всей входящей и исходящей информации компьютера и может вносить изменения в эту информацию. Некоторые LSP необходимы, чтобы разрешить Windows выполнять подключение к другим компьютерам, а также к Интернету. Однако некоторые вредоносные программы могут выполнить установку под видом LSP, получив тем самым доступ ко всей передаваемой компьютером информации. Поэтому данный обзор может помочь обнаружить все возможные LSP угрозы.

При определенных условиях также иногда возможно восстановить поврежденные LSP (например, когда файл был удален, а элементы реестра не были затронуты). При обнаружении LSP, который может быть восстановлен, будет отображена новая кнопка, которая позволяет устранить данную проблему.

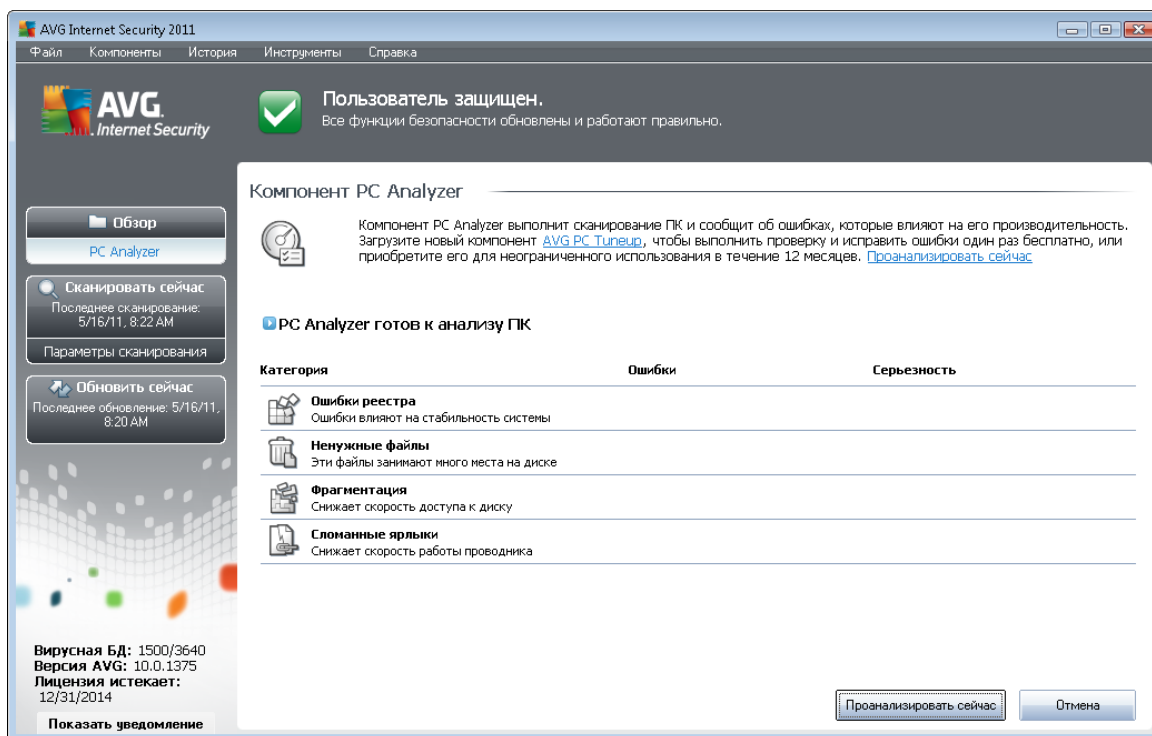
Чтобы включить Windows LSP в список, снимите флажок **Скрыть Windows LSP**. Кнопка **Назад** выполняет обратный переход к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).

7.16. 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

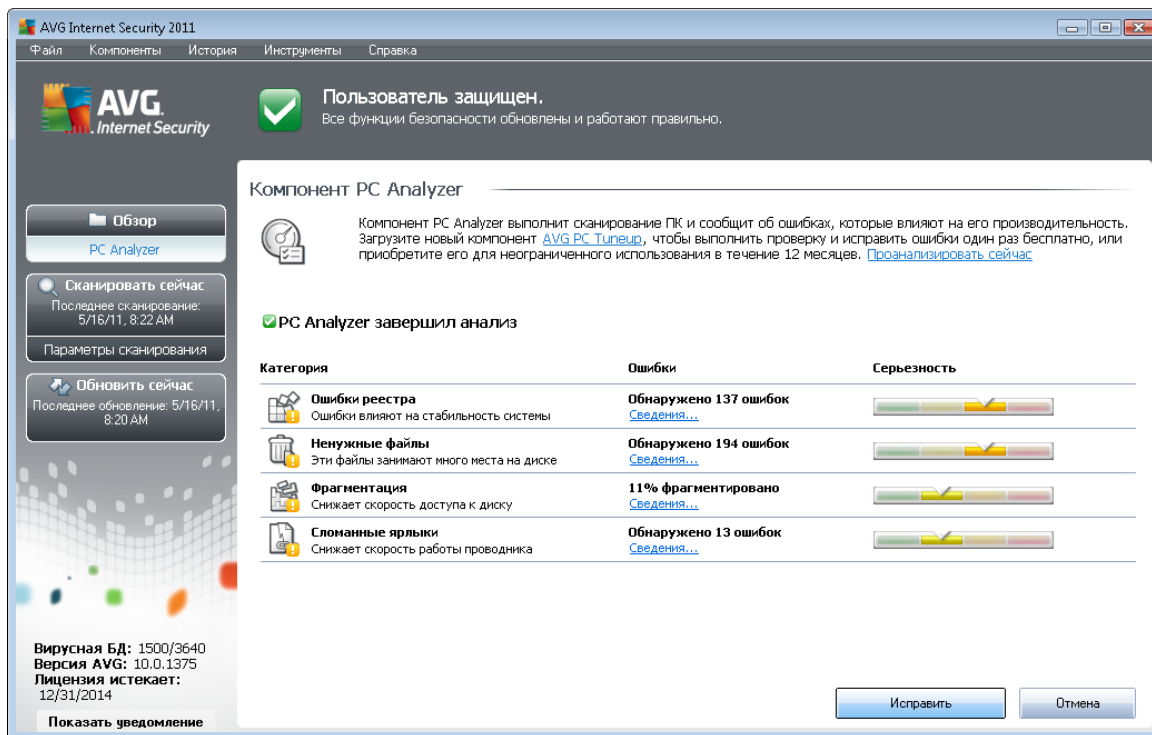


таблица, разделенная на четыре строки, относящиеся к соответствующим категориям. ошибки реестра, ненужные файлы, фрагментация и сломанные ярлыки.



- **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

- **Проанализировать 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 открыть [интерфейс пользователя AVG](#) по умолчанию (обзор компонента) по завершении анализа.

7.17. ID Protection

AVG Identity Protection — это продукт для защиты от вредоносного ПО, главной задачей которого является предотвращение кражи паролей, сведений о банковских счетах, номеров кредитных карт и другой важной личной информации с помощью вредоносных программ (вредоносного ПО), нацеленных на ваш ПК. Данная программа обеспечивает правильную работу всех программ на компьютере. Компонент **AVG Identity Protection** непрерывно ищет и блокирует подозрительные объекты, защищая таким образом компьютер от всех новых разновидностей вредоносного ПО.

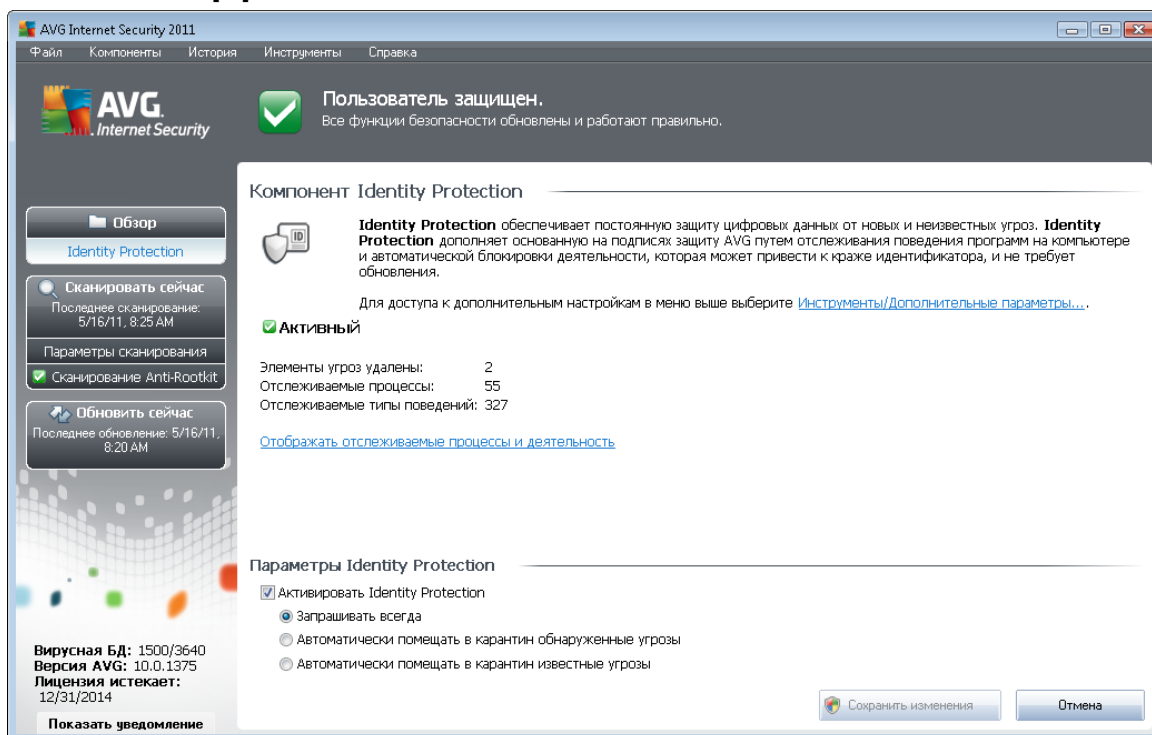


7.17.1. Принципы работы ID Protection

AVG 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. Вредоносное ПО является поддельным ПО и выглядит как обычная программа, которую пользователь открывает на компьютере и через которую злоумышленник может удаленно завладеть личными данными пользователя. Средство **AVG Identity Protection** обеспечивает защиту пользователя от этого нового типа вредоносного ПО, основанного на запуске программ. Это бесплатное дополнение к компоненту **AVG Anti-Virus**, обеспечивающее защиту пользователей от известных вирусов и вирусов, основанных на файлах, с помощью технологии подписей и сканирования.

Настоятельно рекомендуется установить как компонент **AVG Anti-Virus, так и приложение **AVG Identity Protection**, чтобы обеспечить полную защиту компьютера.**

7.17.2. Интерфейс ID Protection



Интерфейс компонента **Identity Protection** содержит краткое описание основных функций компонента, его состояние 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.

Ниже доступна ссылка [Отображать отслеживаемые процессы и деятельность](#), которая позволяет перейти к интерфейсу пользователя компонента [Системные средства](#), в котором приводится подробный обзор всех отслеживаемых процессов.

Параметры Identity Protection

В нижней части диалогового окна расположен раздел **Параметры Identity Protection**, который позволяет изменять некоторые 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.

- o **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).
- o **Автоматически помещать в карантин обнаруженные угрозы.** Все приложения, определенные как вредоносные, будут автоматически заблокированы
- o **Автоматически помещать в карантин известные угрозы.** Будут заблокированы только те приложения, которые точно являются вредоносными.

Кнопки управления

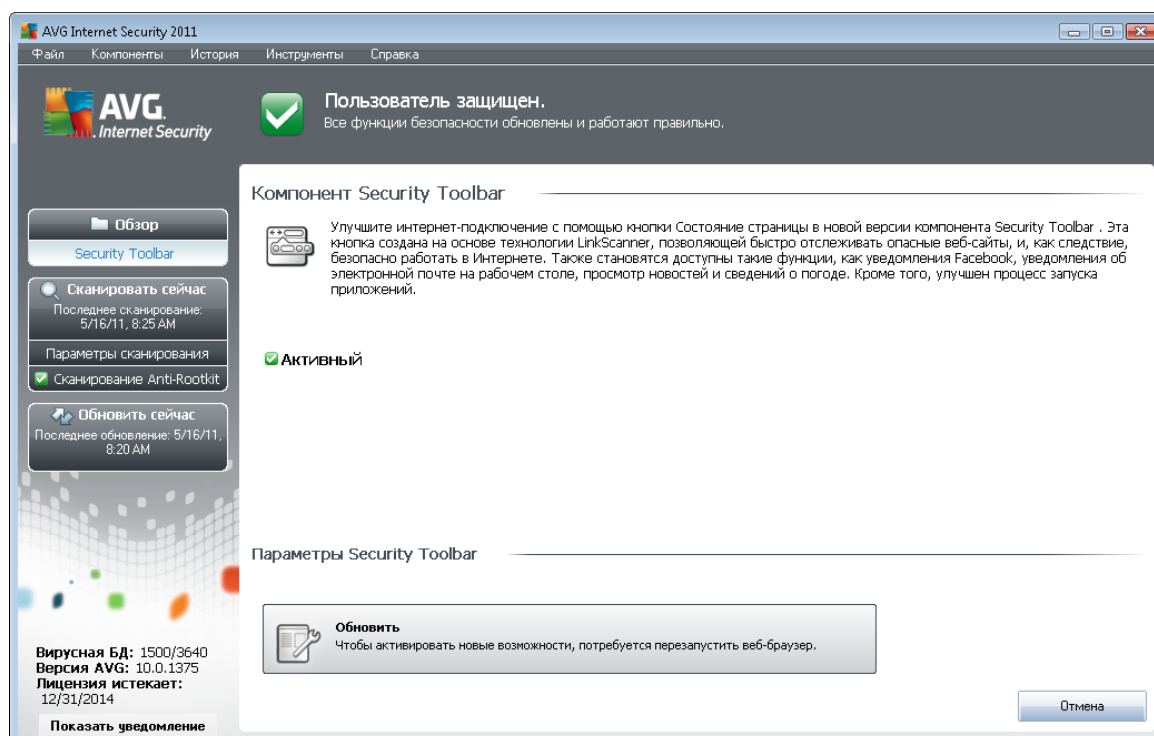
В интерфейсе компонента **Identity Protection** доступны следующие кнопки управления.

- **Сохранить изменения.** Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне.
- **Отмена.** Нажмите данную кнопку для возврата к установленному по умолчанию [интерфейсу пользователя AVG](#) (обзор компонентов).



7.18. Панель инструментов безопасности

Панель инструментов безопасности — это дополнительная панель инструментов для веб-браузера, которая обеспечивает улучшенную защиту AVG, а также позволяет получать быстрый доступ к различным функциям и инструментам во время работы в Интернете. В настоящее время **панель инструментов безопасности** поддерживает браузеры Internet Explorer (6.0 или выше) и Mozilla Firefox (3.0 или выше).



Все параметры компонента **Security Toolbar** доступны непосредственно на [панели инструментов](#) в браузере.



8. Панель инструментов безопасности AVG

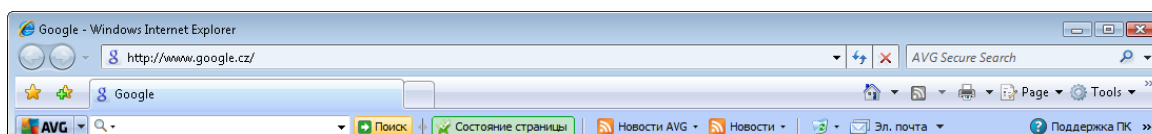
Панель инструментов безопасности AVG — это новый инструмент, работающий совместно с компонентом [LinkScanner](#). **Панель инструментов безопасности AVG** можно использовать для управления функциями компонента [Link Scanner](#) и настройки его поведения.

При установке панели инструментов во время установки **AVG Internet Security 2011** она будет добавлена в веб-браузер (*Internet Explorer 6.0/Mozilla Firefox 3.0 или более поздней версии*) автоматически. В настоящее время поддерживаются только вышеперечисленные браузеры.

Примечание. При использовании альтернативного веб-браузера (например веб-браузера Avant) могут произойти неожиданные ошибки.

8.1. Интерфейс панели инструментов безопасности AVG

Панель инструментов безопасности AVG работает вместе с браузерами **MS Internet Explorer** (6.0 или более поздней версии) и **Mozilla Firefox** (3.0 или более поздней версии). Если необходимо установить **панель инструментов безопасности AVG** (при [установке AVG](#) пользователю будет предложено выбрать, устанавливать компонент или нет), компонент будет размещен в веб-браузере прямо под адресной строкой.



Панель инструментов безопасности AVG включает в себя следующие элементы:

8.1.1. Кнопка со значком AVG

Данная кнопка позволяет получить доступ к основным элементам панели инструментов. Нажмите кнопку с логотипом, чтобы перейти на [веб-сайт компании AVG](#). Щелкнув указатель, расположенный рядом со значком AVG, можно открыть следующие элементы:

- **Сведения о панели инструментов.** Ссылка на домашнюю страницу **панели инструментов безопасности AVG** с подробными сведениями о защите панели инструментов.
- **Запустить AVG.** Открытие интерфейса пользователя **AVG Internet Security 2011**.
- **Сведения об AVG.** Открытие контекстного меню со следующими ссылками к важной информации о безопасности, связанной с **AVG Internet Security 2011**.
 - о Об угрозах. Открытие страницы [веб-сайта компании AVG](#), на которой содержатся самые важные данные о наиболее опасных угрозах, рекомендации по удалению вирусов, сведения об обновлении AVG, сведения о получении доступа к [вирусной базе данных](#) и другая подобная информация.
 - о Новости AVG. Открытие веб-страницы, содержащей последние пресс-релизы



компании AVG.

о *Текущий уровень угрозы*. Открытие веб-страницы лаборатории вирусов с графическим отображением текущего уровня угроз в Интернете.

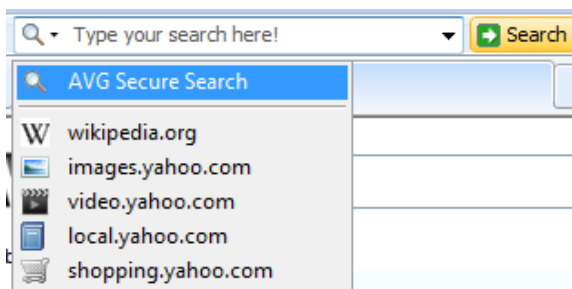
о *Лаборатория угроз компании AVG*. Открытие веб-сайта [отчетов AVG о сайтах](#), на котором можно осуществить поиск определенных угроз по имени и получить подробные сведения о каждой из них.

- **Параметры**. Открытие диалогового окна конфигурации, в котором можно настроить параметры **панели инструментов безопасности AVG** в соответствии с требованиями пользователя — см. следующую главу [Параметры панели инструментов безопасности AVG](#)
- **Очистить историю**. Данный параметр позволяет удалить всю историю, или историю поиска, историю браузера, историю загрузок и файлы cookie по отдельности непосредственно на **панели инструментов безопасности AVG**.
- **Обновление**. Проверка новых обновлений для **панели инструментов безопасности AVG**
- **Справка**. Позволяет открыть файл справки, обратиться в [службу технической поддержки компании AVG](#), отправить отзыв о продукте, а также просмотреть информацию о текущей версии панели инструментов

8.1.2. Поле поиска AVG Secure Search (powered by Google)

Поле **AVG Secure Search (powered by Google)** позволяет удобно и безопасно выполнять поиск в Интернете с помощью системы AVG Secure Search (powered by Google). Введите слово или фразу в поле поиска и нажмите кнопку **Поиск** или клавишу **Enter**, чтобы начать поиск непосредственно на сервере AVG Secure Search (powered by Google) независимо от отображаемой в текущий момент страницы. В поле поиска также отображается история поисковых запросов. Операции поиска, выполняемые с помощью поля поиска, анализируются компонентом защиты [Search-Shield](#).

Кроме того, в поле поиска можно переключиться на поиск в Wikipedia или других поисковых службах (см. рисунок):





8.1.3. Состояние страницы

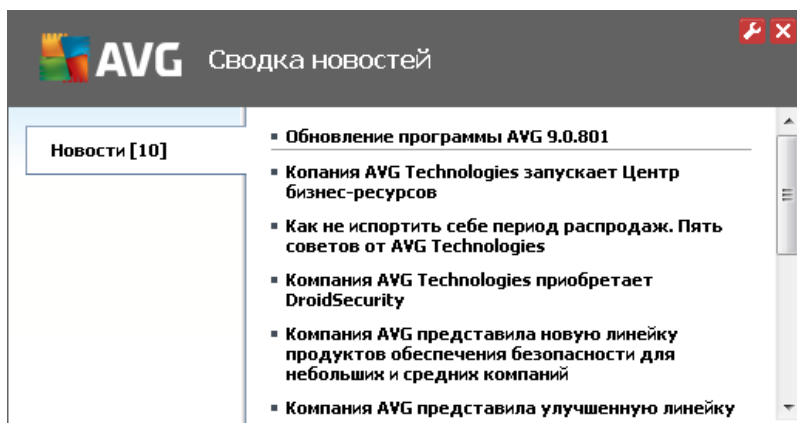
Данная кнопка панели инструментов показывает состояние безопасности отображаемой веб-страницы на основе критериев компонента [Surf-Shield](#).

- . Связанная страница безопасна.
- . Страница является подозрительной.
- . Страница содержит ссылки на фактически зараженные страницы.
- . Связанная страница содержит активные угрозы! В целях безопасности доступ на подобные страницы будет закрыт.
- . Страница недоступна, сканирование не может быть выполнено.

Нажмите эту кнопку, чтобы открыть панель сведений, содержащую подробные данные об указанной веб-странице.

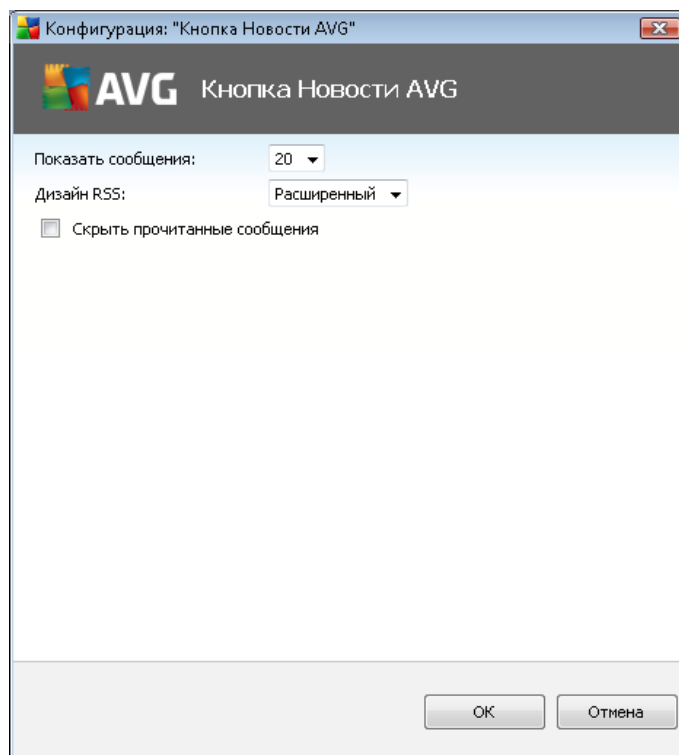
8.1.4. Новости AVG

При нажатии данной кнопки на **панели инструментов безопасности AVG** открывается окно сводки последних **заголовков новостей** компании AVG: пресс-релизы компании и прочие статьи:



В правом верхнем углу расположены две красные кнопки управления.

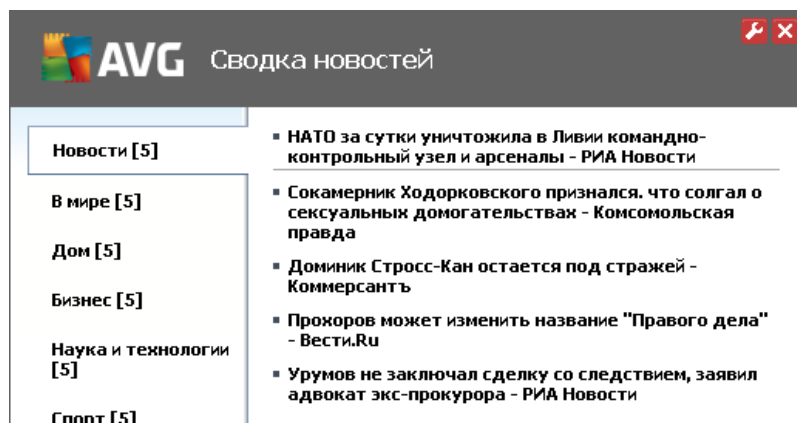
- . При нажатии данной кнопки открывается диалоговое окно настройки параметров кнопки **Новости AVG** , отображаемой на **панели инструментов безопасности AVG**.



- о **Показать сообщения.** Выбор количества отображаемых сообщений.
 - о **Дизайн RSS.** Выбор расширенного или базового режима отображения сводки новостей (*по умолчанию выбран расширенный режим, см. изображение выше*).
 - о **Скрыть прочитанные сообщения.** Установите данный флажок, чтобы прочитанные сообщения не отображались в сводки заголовков и заменялись новыми сообщениями.
-  . Нажмите данную кнопку, чтобы закрыть окно сводки новостей.

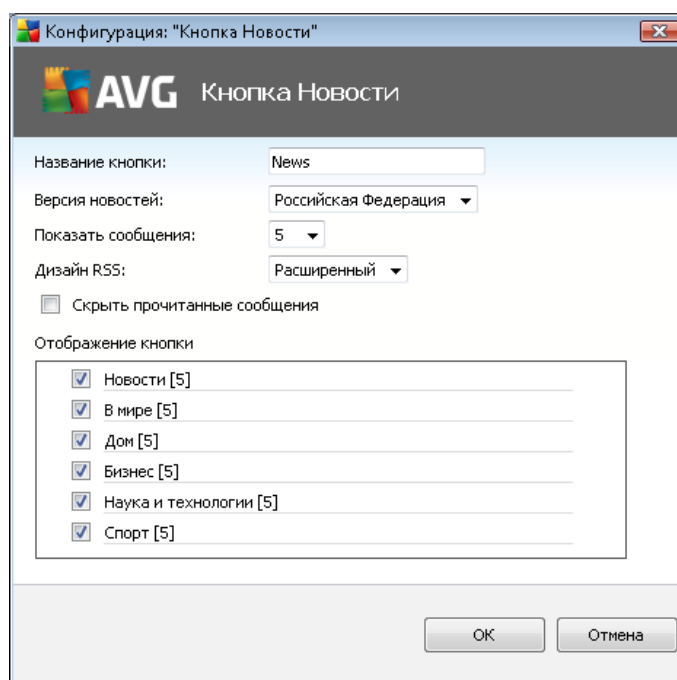
8.1.5. Новости

Аналогичным образом при нажатии данной кнопки на **панели инструментов безопасности AVG** открывается окно сводки последних новостей от выбранных СМИ, разделенное на несколько разделов.



В правом верхнем углу расположены две красные кнопки управления:

-  При нажатии данной кнопки открывается диалоговое окно настройки параметров кнопки **Новости**, отображаемой на **панели инструментов безопасности AVG**.



- о **Название кнопки.** Изменение названия кнопки, отображаемого на **панели инструментов безопасности AVG**
- о **Версия новостей.** Выбор страны, новости из которой будут отображаться.
- о **Показать сообщения.** Выбор количества отображаемых сообщений.
- о **Дизайн RSS.** Выбор базового или расширенного режима отображения окна сводки новостей (**по умолчанию выбран расширенный режим, см. изображение выше**).
- о **Скрыть прочитанные сообщения.** Установите данный флажок, чтобы прочитанные сообщения не отображались в сводке новостей и заменялись новыми заголовками.
- о **Разделы новостей.** Выбор групп новостей, которые необходимо отображать в окне сводки новостей **панели инструментов безопасности AVG**.



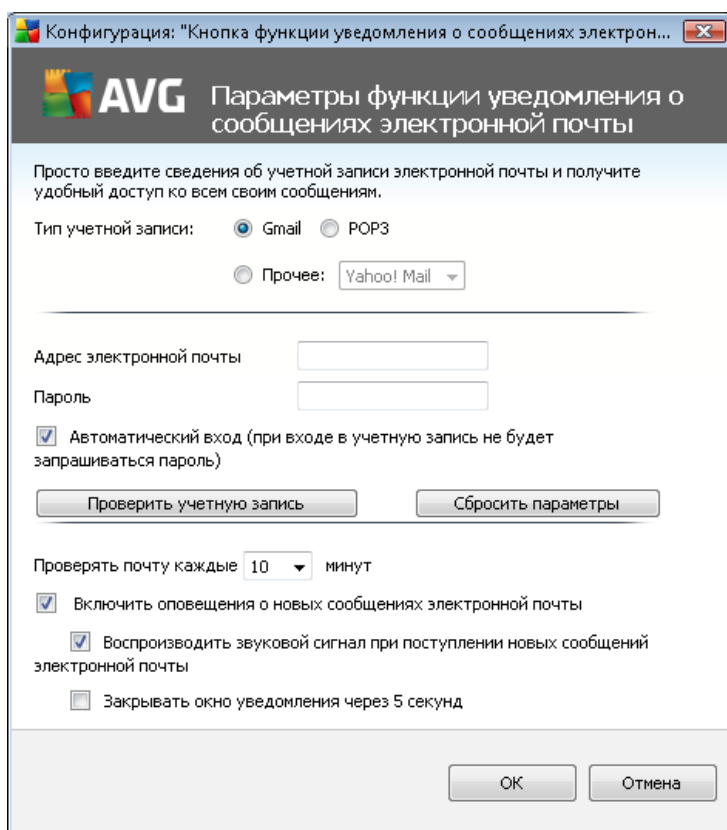
-  Нажмите данную кнопку, чтобы закрыть окно сводки новостей.

8.1.6. Очистить историю

С помощью данной кнопки можно очистить историю браузера (как при нажатии **значка AVG -> Очистить историю**).

8.1.7. Уведомление о сообщениях эл. почты

С помощью кнопки **функции уведомления о сообщениях электронной почты** можно активировать функцию получения уведомлений о новых сообщениях эл. почты при их поступлении непосредственно на **панели инструментов безопасности AVG**. При нажатии данной кнопки открывается следующее диалоговое окно редактирования, в котором можно определить параметры учетной записи и правила отображения эл. почты. Следуйте инструкциям в диалоговом окне.



Конфигурация: "Кнопка функции уведомления о сообщениях электрон..."

AVG Параметры функции уведомления о сообщениях электронной почты

Просто введите сведения об учетной записи электронной почты и получите удобный доступ ко всем своим сообщениям.

Тип учетной записи: ☒ Gmail ☐ POP3
☐ Прочее: Yahoo! Mail

Адрес электронной почты:
Пароль:

☒ Автоматический вход (при входе в учетную запись не будет запрашиваться пароль)

Проверять почту каждые 10 минут

☒ Включить оповещения о новых сообщениях электронной почты
☒ Воспроизводить звуковой сигнал при поступлении новых сообщений электронной почты
☐ Закрывать окно уведомления через 5 секунд

- **Тип учетной записи.** Тип протокола, который использует учетная запись эл. почты. Можно выбрать один из следующих вариантов: *Gmail*, *POP3* или выберите имя сервера в раскрывающемся меню элемента *Другие* (в настоящее время данный параметр доступен только для владельцев учетных записей *Yahoo! JP Mail* или *Hotmail*). Если неизвестно, какой тип сервера эл. почты использует ваша учетная запись, обратитесь за данными сведениями к поставщику услуг электронной почты или Интернета.
- **Вход.** В разделе ниже укажите свой *адрес эл. почты* и соответствующий *пароль*. Не

снимайте флажок *Автоматический вход*, чтобы не вводить каждый раз заново данные для входа.

- **Проверить учетную запись.** Данная кнопка позволяет проверить правильность введенных данных.
- **Сбросить параметры.** Быстрое удаление введенных выше сведений электронной почты.
- **Проверять почту каждые ... минут.** Определение временного интервала, через который должна выполняться проверка новых сообщений эл. почты (*в диапазоне 5–120 минут*), а также настройка уведомлений о получении новых сообщений.
- **Включить оповещения о новых сообщениях эл. почты.** Снимите данный флажок, чтобы отключить отображение уведомлений о получении новых сообщений электронной почты.
 - **Воспроизводить звуковой сигнал при поступлении новых сообщений эл. почты.** Снимите данный флажок, чтобы отключить звуковые уведомления при получении новых сообщений электронной почты.
 - **Закрывать окно уведомления через 5 сек.** Установите данный флажок для автоматического закрытия окна уведомлений о получении новых сообщений электронной почты по истечении 5 секунд.

8.1.8. Сведения о погоде

При нажатии кнопки **Погода** отображаются сведения о текущей температуре (*обновляются каждые 3–6 часов*) в выбранном местоположении. Данные сведения отображаются непосредственно в интерфейсе **панели инструментов безопасности AVG**. Нажмите данную кнопку, чтобы открыть новую информационную панель с подробным обзором погоды.

Brno, CZ
[изменить место]

 **14° C**

Скорость ветра: 16,09 км/ч
Восход: 05:08
Закат: 20:29

**Пн**
Выс.: 17 °C
Низ.: 8 °C

**Вт**
Выс.: 21 °C
Низ.: 9 °C

Обновлено 05/16/2011 11:02:30 **YANOO! NEWS** [Полный прогноз >](#)

Доступны следующие параметры настройки:



- **Изменить место.** Щелкните текст **Изменить место**, чтобы открыть новое диалоговое окно **Поиск места**. В текстовом поле введите название необходимого местоположения, а затем подтвердите его, нажав кнопку **Поиск**. Затем в отобразившемся списке выберите необходимое местоположение. После этого снова отобразится информационная панель, содержащая сведения о погоде для выбранного местоположения.
- **Преобразователь шкалы Фаренгейта/Цельсия.** В правом верхнем углу информационной панели можно выбрать шкалу Фаренгейта или Цельсия. После этого сведения о температуре изменятся в соответствии с выбранной шкалой.
- **Полный прогноз.** Чтобы просмотреть полный и подробный прогноз погоды, щелкните ссылку **Полный прогноз**. После этого откроется специализированный веб-сайт погоды.

8.1.9. Facebook

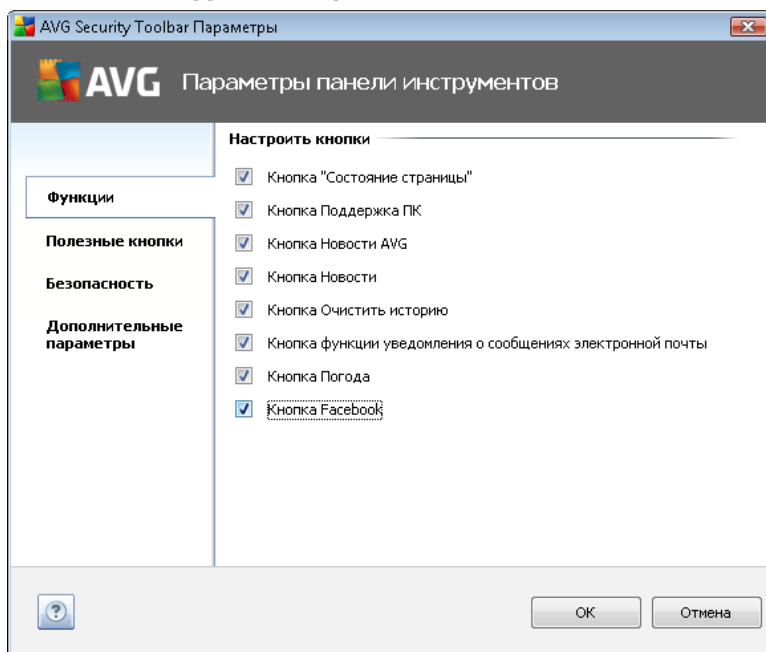
Кнопка **Facebook** позволяет подключиться к социальной сети [Facebook](#) непосредственно на **панели инструментов безопасности AVG**. После нажатия данной кнопки отобразится предложение выполнить вход; нажмите ее еще раз, чтобы открыть диалоговое окно **Вход на Facebook**. Введите данные для входа и нажмите кнопку **Вход**. Если у вас нет учетной записи [Facebook](#), вы можете создать ее с помощью ссылки **Зарегистрироваться на Facebook**.

По завершении процесса регистрации учетной записи [Facebook](#) вам будет предложено активировать приложение **Расширение AVG для социальных сетей**. Главным назначением данного приложения является подключение к сети [Facebook](#), поэтому рекомендуется его разрешить. После подключения к [Facebook](#) при нажатии кнопки **Facebook** на **панели инструментов безопасности AVG** будет открываться меню стандартных параметров [Facebook](#).

8.2. Параметры панели инструментов безопасности AVG

Настройку всех параметров **AVG Security Toolbar** можно выполнять непосредственно на панели **AVG Security Toolbar**. Интерфейс редактирования открывается с помощью пункта меню панели инструментов **AVG/Параметры** в новом диалоговом окне **Параметры панели инструментов**, разделенном на четыре части:

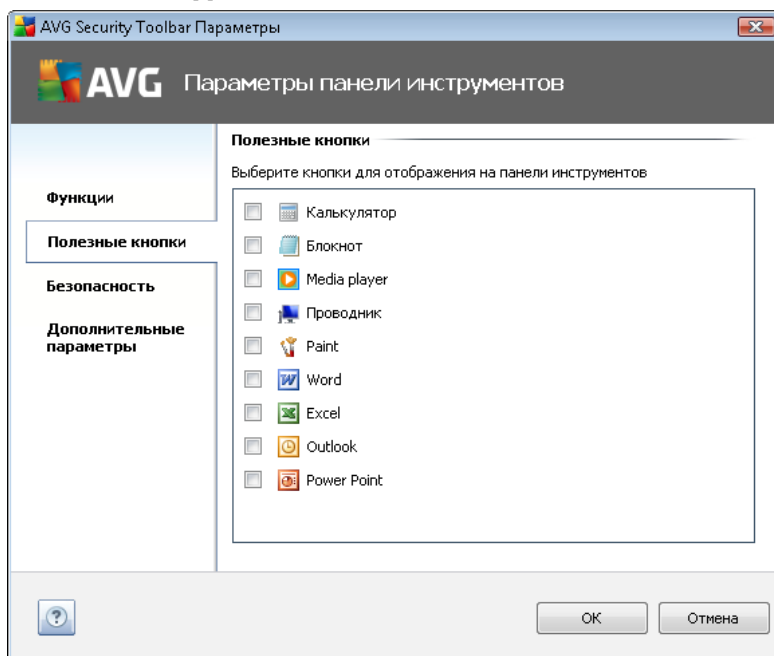
8.2.1. Вкладка **Общее**



На этой вкладке можно указать кнопки, которые должны быть отображены или скрыты на **панели инструментов безопасности AVG**. Пометьте кнопки, которые должны отображаться на панели. Ниже приведено описание каждой кнопки панели управления.

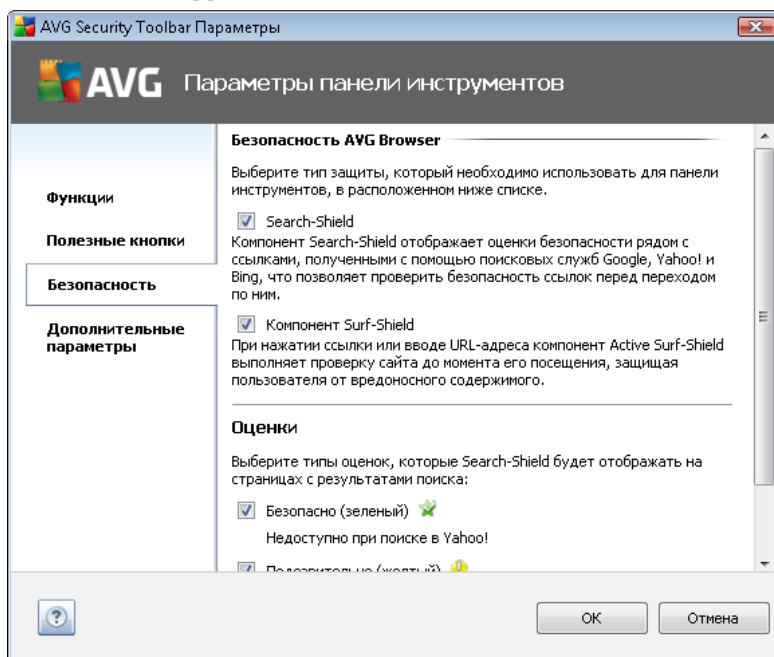
- **Кнопка *Состояние страницы*.** Данная кнопка позволяет просмотреть сведения о безопасности отображаемой веб-страницы непосредственно на **панели инструментов безопасности AVG**
- **Новости AVG.** Эта кнопка открывает веб-страницу, содержащую последние пресс-релизы компании AVG.
- **Новости.** Эта кнопка обеспечивает структурированный обзор текущих новостей из прессы.
- **Кнопка *Очистить историю*.** Эта кнопка позволяет полностью очистить историю или очистить историю поиска, очистить историю браузера, очистить историю загрузок либо удалить файлы cookie прямо на панели инструментов безопасности AVG.
- **Кнопка *уведомления о сообщениях эл. почты*.** Данная кнопка позволяет просматривать новые сообщения эл. почты непосредственно в интерфейсе **панели инструментов безопасности AVG**.
- **Кнопка *Погода*.** Данная кнопка позволяет мгновенно получить сведения о погоде в выбранном местоположении.
- **Кнопка *Facebook*.** Данная кнопка позволяет подключиться к социальной сети [Facebook](https://www.facebook.com/AVG).

8.2.2. Вкладка Полезные кнопки



Вкладка **Полезные кнопки** позволяет выбрать приложения в списке и включить отображение их значков на панели инструментов. Эти значки будут обеспечивать быстрый доступ к соответствующим приложениям.

8.2.3. Вкладка Безопасность



Вкладка **Безопасность** состоит из двух разделов: **Безопасность браузера AVG** и **Оценки**.

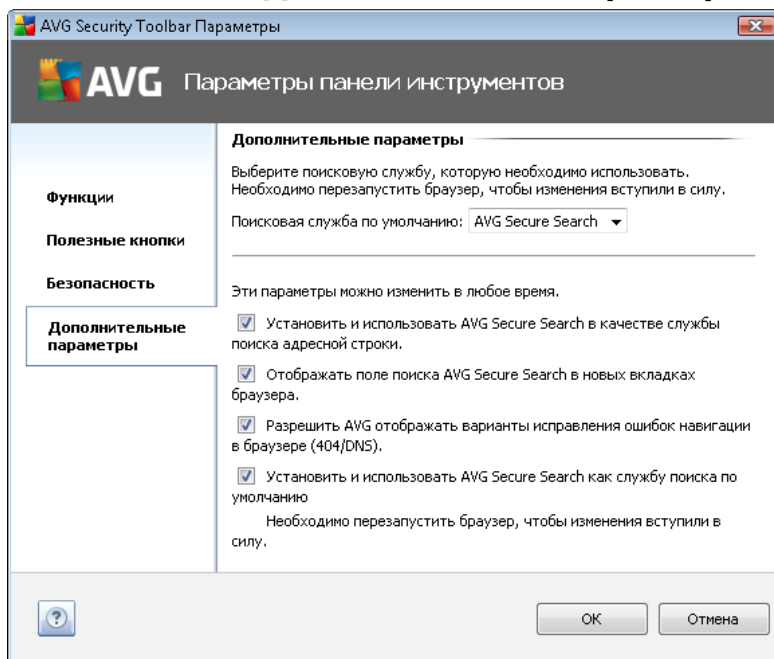


На вкладке можно установить определенные флажки, чтобы назначить компоненту **AVG Security Toolbar** ряд необходимых функций:

- **Безопасность браузера** . Установите этот флажок, чтобы активировать или отключить [AVG Search-Shield](#) и/или службу [Surf-Shield](#).
- **Оценки**. Выберите графические символы, используемые компонентом [Search-Shield](#) для отображения оценок страниц в результатах поиска:
 - o страница безопасна
 - o страница является подозрительной
 - o страница содержит ссылки на фактически зараженные страницы
 - o страница содержит активные угрозы
 - o страница недоступна, сканирование не может быть выполнено

Выберите соответствующий параметр для подтверждения необходимости информирования о данном уровне угрозы. Но при этом отображение красных значков, назначенных страницам, содержащим активные и опасные угрозы, отключить нельзя. **Не рекомендуется изменять стандартную конфигурацию, установленную поставщиком программы, без крайней необходимости.**

8.2.4. Вкладка Дополнительные параметры





На вкладке **Дополнительные параметры** сначала выберите поисковую систему, которую требуется использовать по умолчанию. Можно выбрать службу *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*, *Yandex* или *Yahoo! JP*. После изменения поисковой системы, используемой по умолчанию, перезапустите интернет-браузер, чтобы изменение вступило в силу.

Также можно включить или отключить определенные параметры **панели инструментов безопасности AVG** (отображаемая подпись относится к параметрам *AVG Secure Search (powered by Google)* по умолчанию).

- **Установить и использовать AVG Secure Search (powered by Google) в качестве службы поиска адресной строки.** Данный параметр позволяет вводить ключевые слова поиска непосредственно в адресной строке интернет-браузера, а служба Google будет автоматически производить поиск соответствующих веб-сайтов.
- **Разрешить AVG отображать варианты исправления ошибок навигации в браузере (404/DNS).** Если при переходе на страницу возникнет ошибка отсутствия страницы или страницу нельзя будет отобразить (ошибка 404), будет автоматически выполнен переход на страницу, позволяющую выбрать одну из альтернативных страниц по данной теме.
- **Установить и использовать AVG Secure Search (powered by Google) как службу поиска по умолчанию.** Google является службой поиска **панели инструментов безопасности AVG** по умолчанию. При активации данного параметра она также может стать службой поиска веб-браузера по умолчанию.

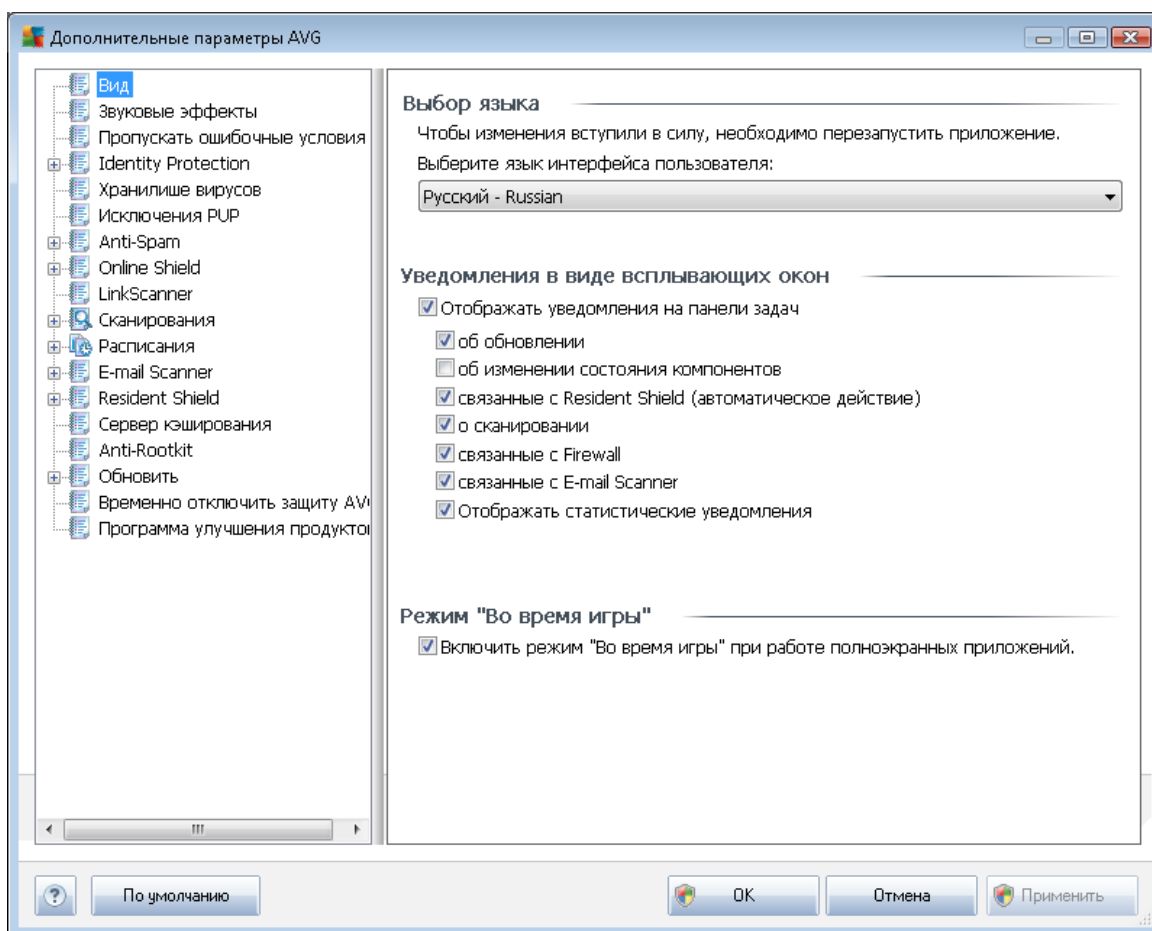


9. Дополнительные параметры AVG

Параметры дополнительной настройки **AVG Internet Security 2011** 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.

9.1. Внешний вид

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



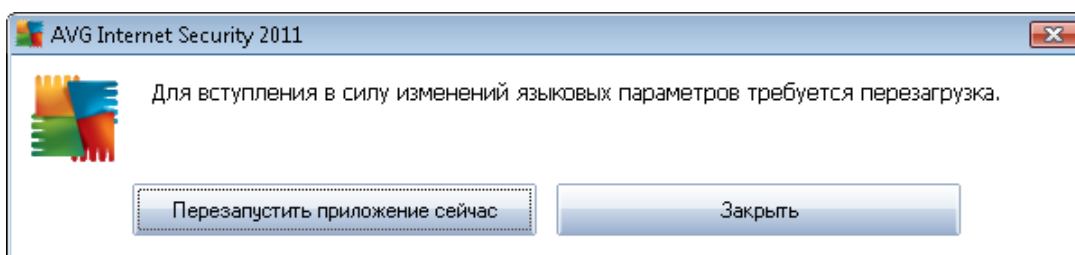
Выбор языка

В раскрывающемся меню раздела **Выбор языка** можно выбрать необходимый язык; после этого [интерфейс пользователя AVG](#) 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 смены языка приложения, необходимо перезапустить



интерфейс пользователя; выполните следующие действия.

- Выберите необходимый язык приложения и подтвердите выбор, нажав кнопку **Применить** (в правом нижнем углу).
- Для подтверждения нажмите кнопку **ОК**
- Новые всплывающие диалоговые окна информируют о том, что для повторного запуска приложения требуется смена языка интерфейса пользователя AVG:



Уведомления в виде всплывающих окон на панели задач

В данном разделе можно отключить отображение уведомлений о состоянии приложения в виде всплывающих окон на панели задач. По умолчанию отображение уведомлений в виде всплывающих окон включено. Рекомендуется не отключать данный параметр. Уведомления в виде всплывающих окон обычно информируют пользователя об изменениях состояния какого-либо компонента AVG. Необходимо обращать на них внимание.

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

- **Отображать уведомления на панели задач.** По умолчанию данный параметр отмечен флажком (*включен*), а уведомления отображаются. Снимите флажок с данного параметра, чтобы отключить отображение всех всплывающих уведомлений. Если данный параметр включен, можно настроить отображение отдельных уведомлений.
 - о **Отображать уведомления об обновлении** на панели задач. Позволяет определить, следует ли отображать информацию о запуске процесса обновления AVG, его состоянии и завершении.
 - о **Отображать уведомления об изменении состояния компонентов.** 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](#) (изменение цвета), информирующего пользователя о проблеме, связанной с компонентом AVG;
 - о **Отображать уведомления компонента Resident Shield на панели задач (выполняется автоматически).** Определяет, должна ли отображаться



информация о сохранении, копировании и открытии файлов (такая конфигурация доступна только в том случае, если функция [Автоматическое лечение](#) Resident Shield включена);

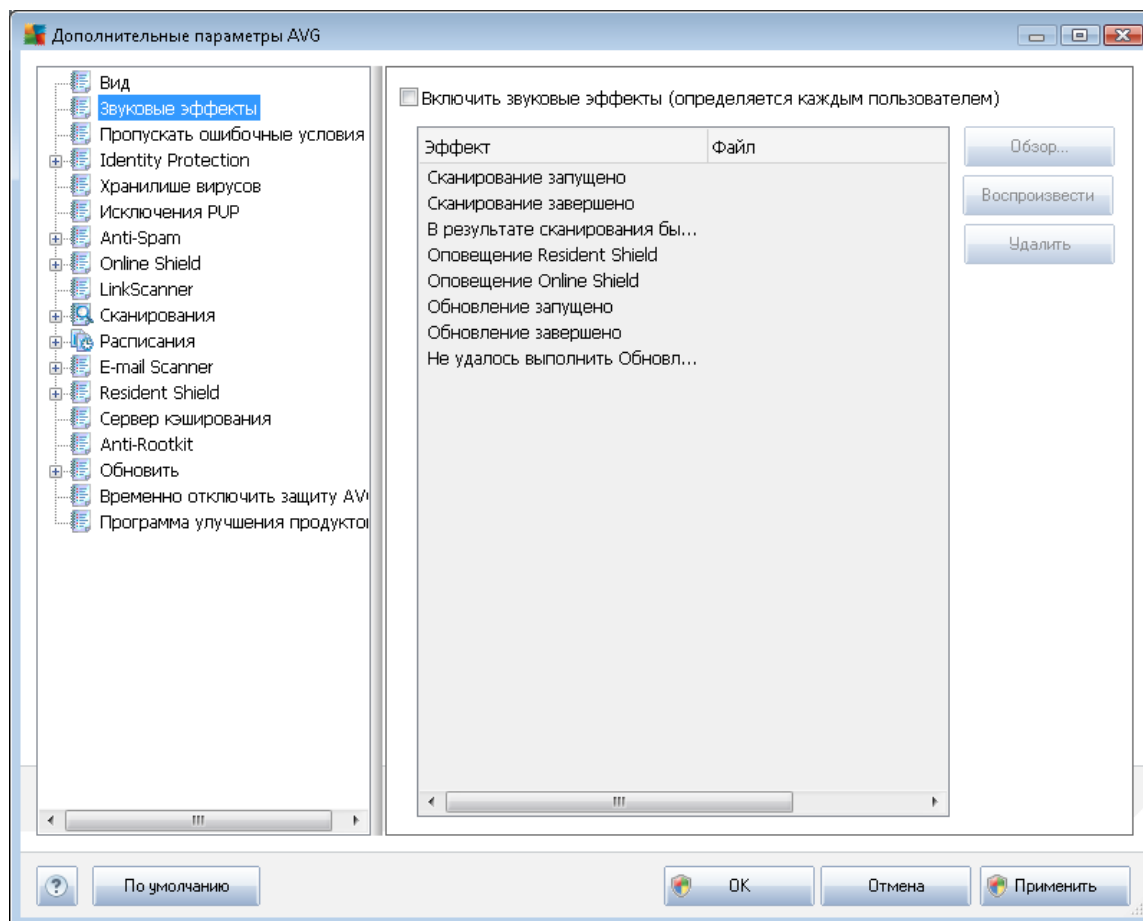
- о **Отображать уведомления о сканировании** на панели задач. Позволяет определить, должна ли отображаться информация об автоматическом запуске запланированного сканирования, его состоянии и результатах.
- о **Отображать уведомления компонента Firewall на панели задач**. Позволяет определить, должна ли отображаться информация о состоянии и процессах (предупреждения об активации/деактивации компонента, возможная блокировка трафика и т. п.). компонента Firewall.
- о **Отображать уведомления E-mail Scanner на панели задач**. Позволяет определить, должна ли отображаться информация о сканировании всех входящих и исходящих сообщений электронной почты.
- о **Отображать статистические уведомления**. Не снимайте данный флажок, чтобы на панели задач отображались уведомления о регулярных статистических обзорах.

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).

9.2. Звуки

В окне **Звуки** можно указать, следует ли включить оповещение об определенных действиях AVG с помощью звуковых уведомлений. Чтобы включить эту функцию, установите флажок **Включить звуки для событий** (по умолчанию отключено), чтобы активировать список действий AVG:



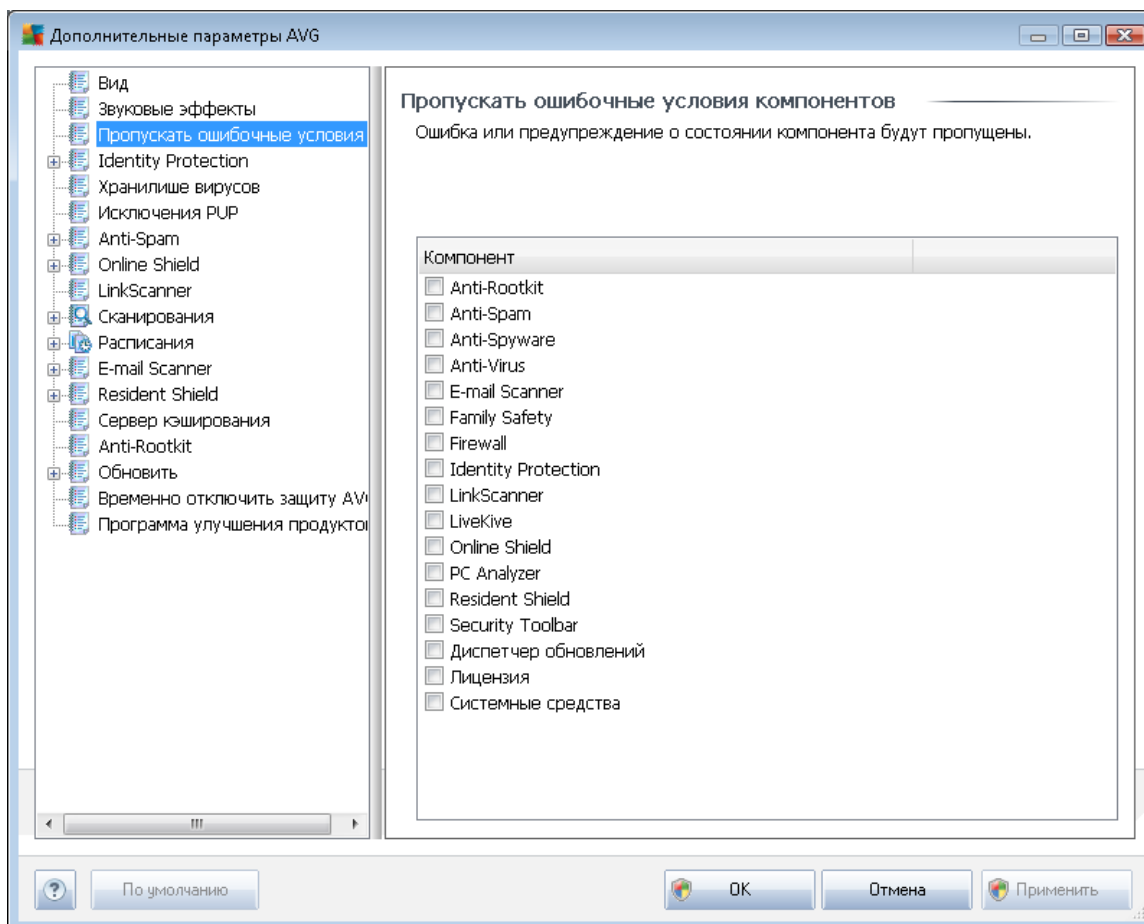
Затем выберите в списке событие и укажите (**Обзор**) на диске аудиофайл, который необходимо назначить для этого события. Чтобы прослушать выбранный аудиофайл, выделите событие в списке и нажмите кнопку **Воспроизвести**. Чтобы удалить звук, назначенный определенному событию, нажмите кнопку **Удалить**.

Примечание. Поддерживаются только файлы в формате *.wav.



9.3. Игнорирование ошибочных условий

В диалоговом окне **Пропустить ошибочные условия компонентов** 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



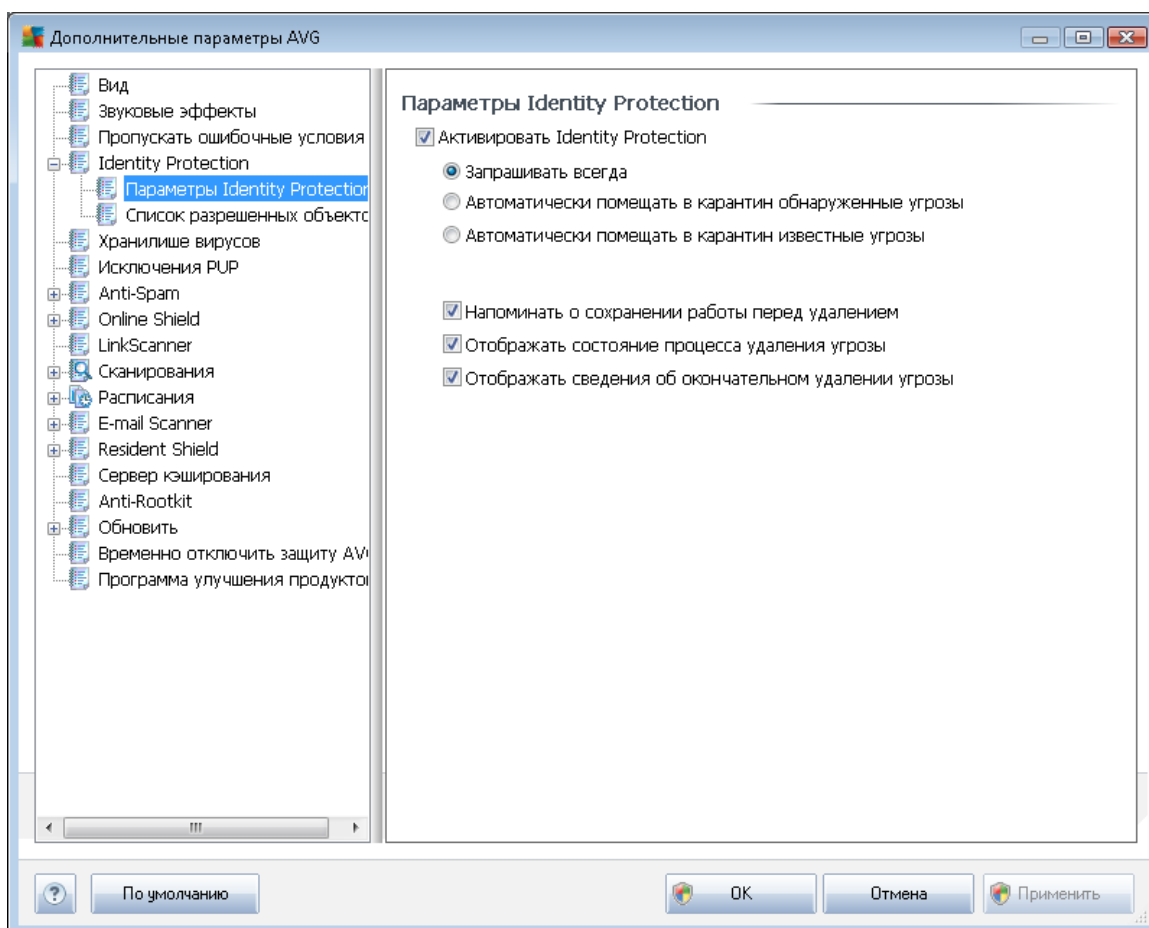
пользователь преднамеренно ее вызвал и был предварительно предупрежден о возможном риске. В то же время, если значок отображился серым цветом, он не может оповещать о дальнейших возможных ошибках.

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. Этот же параметр **Игнорирование состояния компонента** также доступен для специальных компонентов непосредственно из [обзора компонентов в главном окне AVG](#).

9.4. Identity Protection

9.4.1. 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.

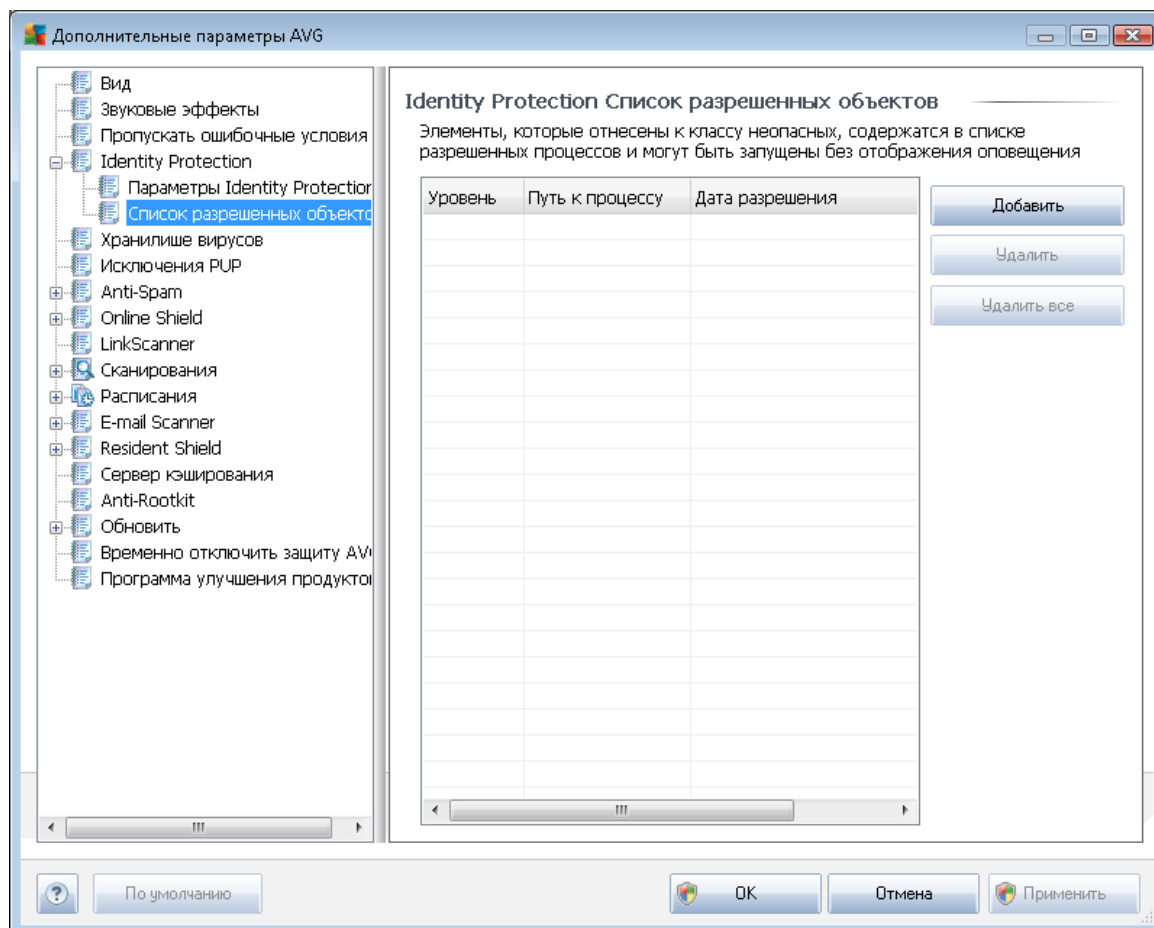
- **Запрашивать всегда** (выбрано по умолчанию). При обнаружении угрозы отобразится запрос на перемещение опасного объекта в карантин, чтобы избежать случайного удаления запускаемых приложений.
- **Автоматически помещать в карантин обнаруженные угрозы**. Установите флажок, чтобы все обнаруженные угрозы сразу же помещались в безопасное место — [хранилище вирусов AVG](#). 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 AVG](#).

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 вредоносного ПО** (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 финальные сведения об удалении вредоносного ПО** (выбрано по умолчанию). Если данный параметр включен, **Identity Protection** будет отображать подробные сведения о каждом объекте, перемещенном в карантин (уровень опасности, местоположение и т. д.).

9.4.2. 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.



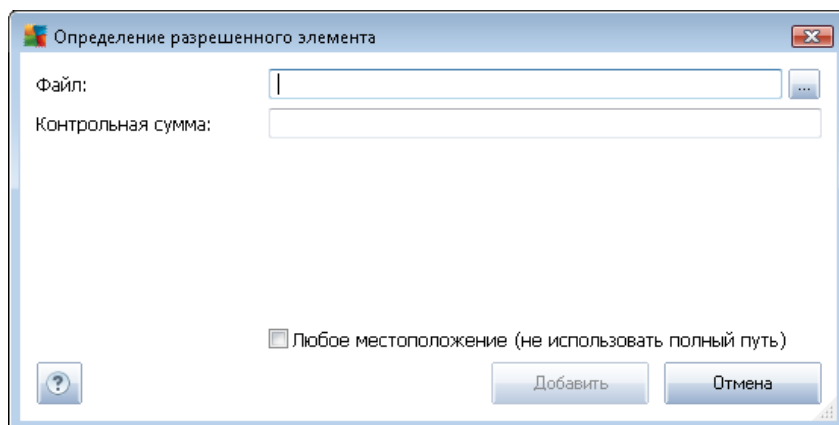
Список разрешенных процессов Identity Protection предоставляет следующие сведения по каждому элементу:

- **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

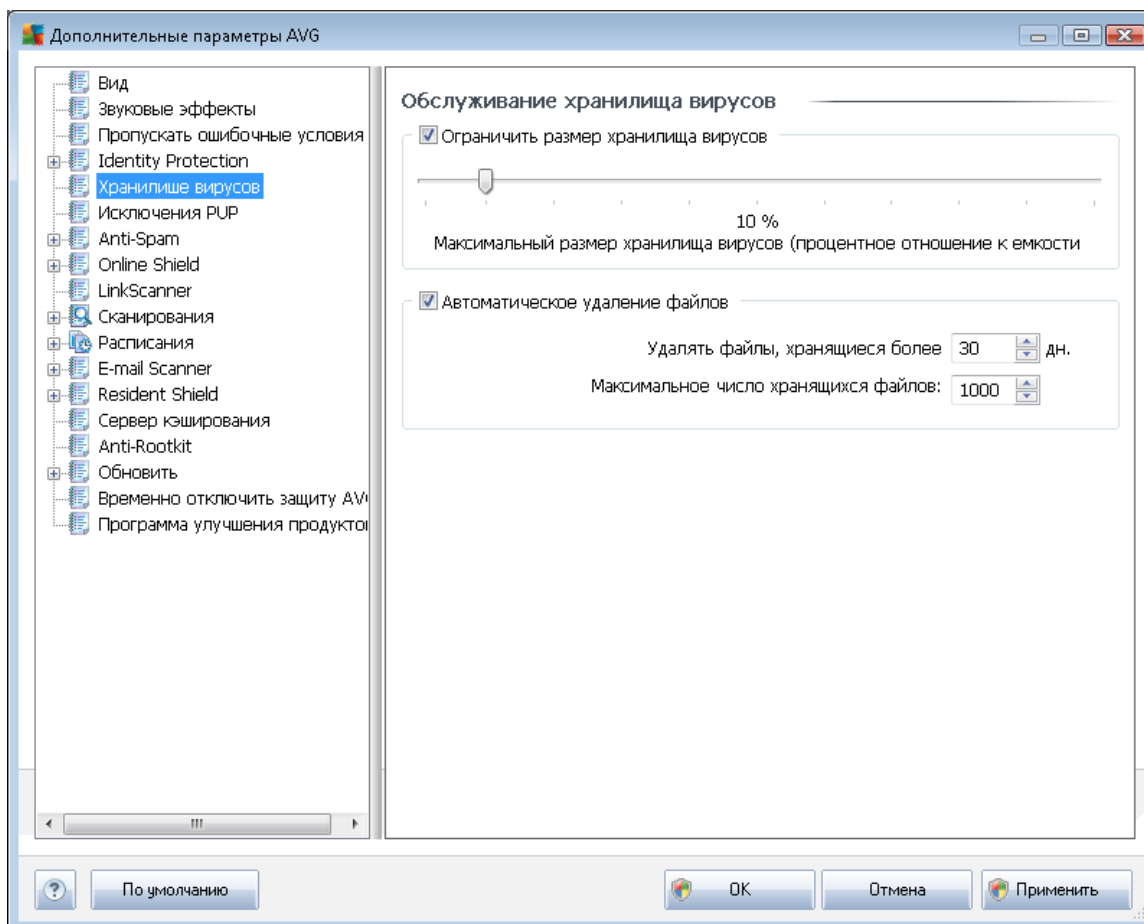
В диалоговом окне **Список разрешенных элементов Identity Protection** имеются следующие кнопки управления.

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



- о **Файл**. Введите полный путь к файлу (*приложению*), который необходимо отметить как исключение.
 - о **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.
 - о **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.

9.5. Хранилище вирусов



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

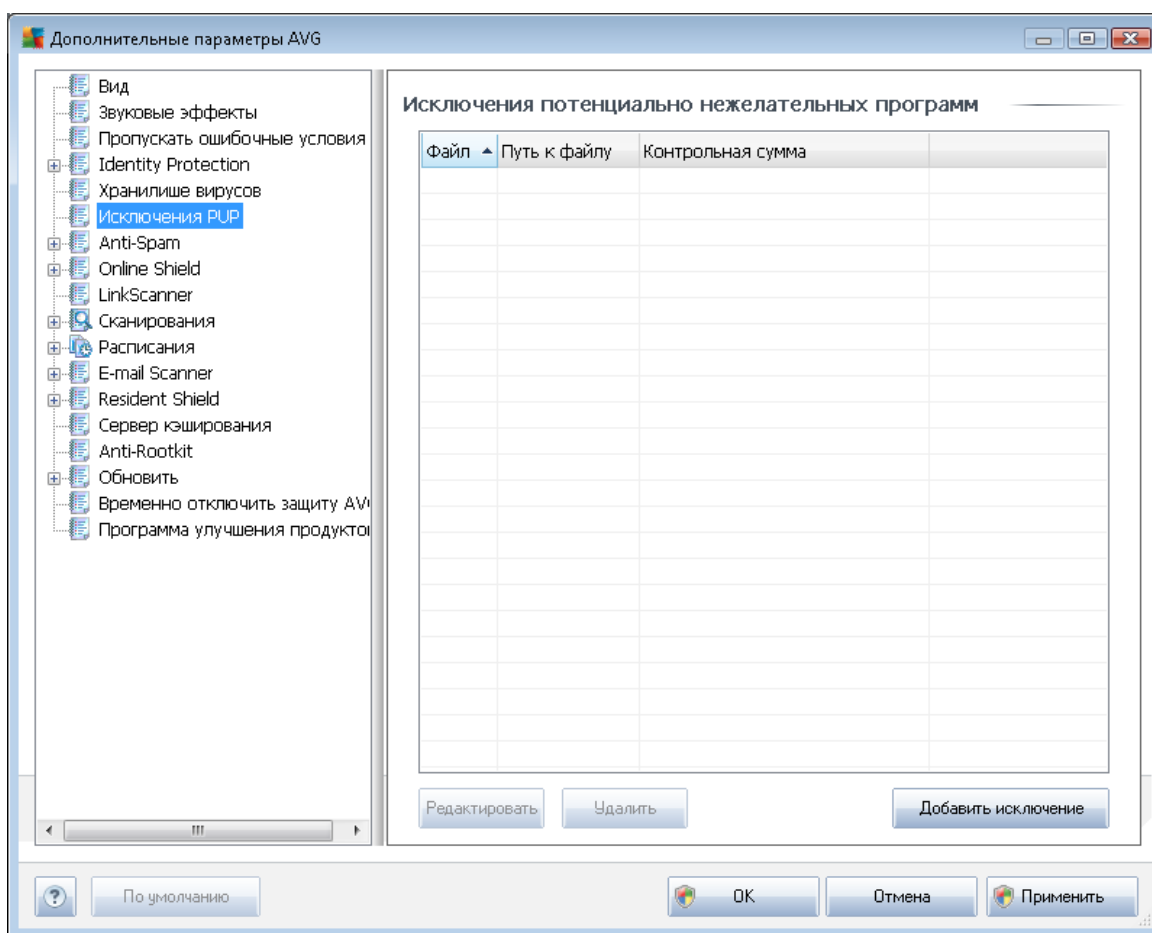
- **Предельный размер хранилища вирусов.** Установите максимальный размер [хранилища вирусов](#) с помощью ползунка. Размер хранилища указывается пропорционально размеру локального диска.
- **Автоматическое удаление файлов** — в данном разделе можно указать максимальное время хранения объектов в [хранилище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

9.6. Исключения PUP

AVG Internet Security 2011 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 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:

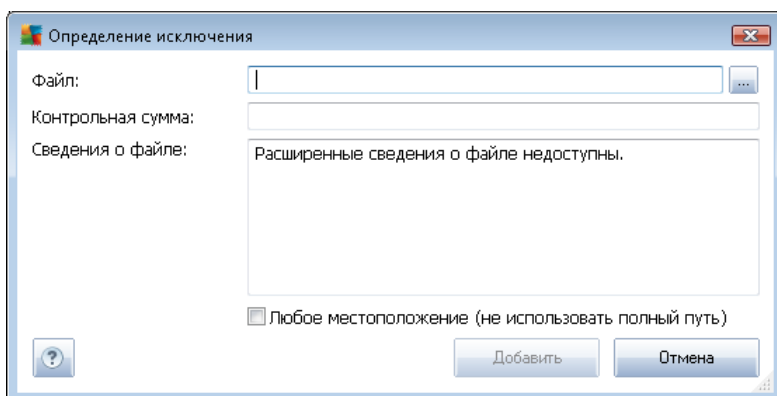


В диалоговом окне **Исключения потенциально нежелательных программ** отобразится список уже определенных исключений из числа потенциально нежелательных программ, которые на данный момент являются допустимыми исключениями. Список можно изменить, удалить из него существующие элементы или добавить новые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

- **Файл.** Указание 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

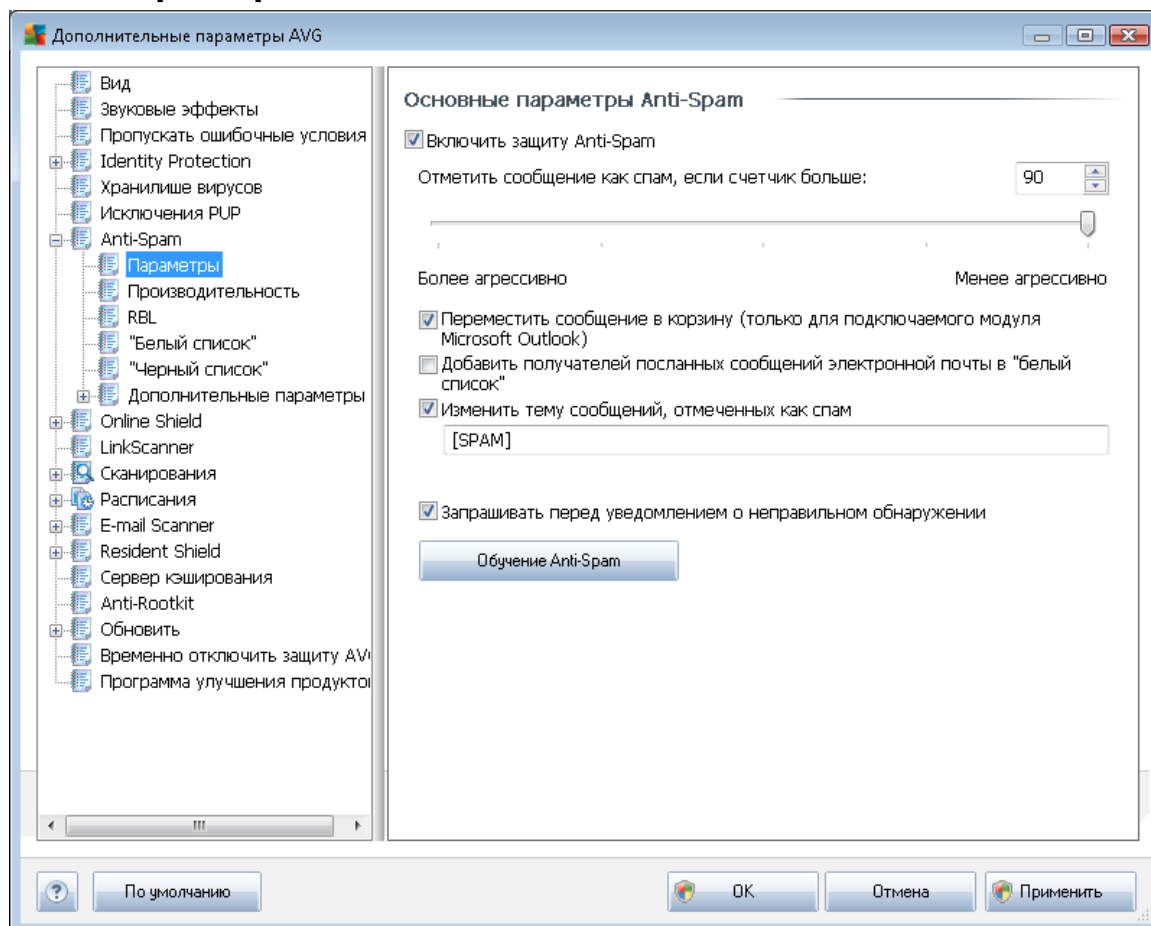
- **Редактировать.** Открытие диалогового окна редактирования (*соответствующего окну определения новых исключений, см. ниже*) определенного исключения, с помощью которого можно изменять параметры исключения.
- **Удалить** . Удаление выбранного элемента из списка исключений.
- **Добавить исключение.**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



- о **Файл.** Введите полный путь к файлу, который необходимо отметить как исключение.
- о **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.
- о **Сведения о файле.** Отображение другой дополнительной информации о файле (*информация о лицензии или версии и т. п.*).
- о **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; файл будет использоваться в качестве уникального примера возможности существования в системе двух файлов с одинаковым именем*).

9.7. Anti-Spam

9.7.1. Параметры



В диалоговом окне **Основные параметры Anti-Spam** можно установить или снять флажок **Включить защиту Anti-Spam**, чтобы включить или отключить сканирование сообщений электронной почты на наличие спама. По умолчанию данный параметр включен, и рекомендуется не снимать данный флажок без крайней необходимости.

Далее можно выбрать более или менее точные способы определения. Фильтр **Anti-Spam** определяет рейтинг каждого сообщения (то есть насколько содержимое сообщения соответствует критериям СПАМА) на основе нескольких способов динамического сканирования. Можно определить параметр **Отметить сообщение как спам, если рейтинг превышает**, указав необходимое значение или переместив ползунок влево или вправо (при использовании ползунка диапазон значений ограничен значениями от 50 до 90).

Как правило, рекомендуется установить пороговое значение в диапазоне от 50 до 90. Или, если вы не уверены, установить значение 90. Ниже представлен общий обзор пороговых значений рейтинга.

- **Значения в диапазоне 80-90.** Будет производиться фильтрация сообщений электронной почты, которые возможно являются [спамом](#). Некоторые сообщения, которые не являются спамом, могут быть неверно помечены как спам.



- **Значения в диапазоне 60–79.** Значения в данном диапазоне обеспечивают довольно высокий уровень защиты. Будет производиться фильтрация сообщений электронной почты, которые скорее всего являются [спамом](#). Сообщения, которые не являются спамом, могут быть определены как спам.
- **Значения в диапазоне 50–59.** Значения в данном диапазоне обеспечивают очень высокую степень защиты. Сообщения, которые не являются спамом, могут быть определены как настоящий [спам](#). Обычно не рекомендуется использовать пороговые значения из данного диапазона.

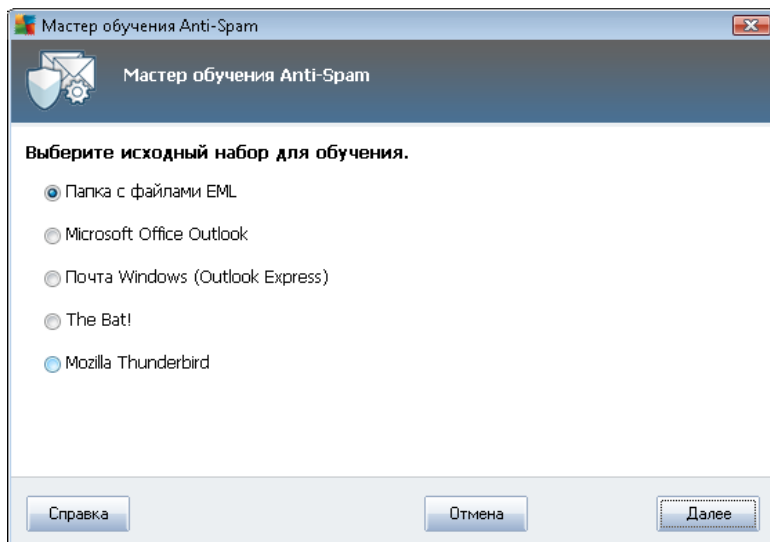
В окне **Основные параметры Anti-Spam** можно определить действия в отношении обнаруженных сообщений электронной почты, которые были определены как [спам](#).

- **Переместить сообщение в папку нежелательной почты.** Установите данный флажок, чтобы каждое сообщение электронной почты, определенное как спам, было автоматически перемещено в папку нежелательной почты используемого клиента электронной почты.
- **Добавить получателей отправленных сообщений эл. почты в [белый список](#).** Установите данный флажок, чтобы подтвердить, что всем получателям отправленных сообщений электронной почты можно доверять, а все сообщения электронной почты, приходящие с их учетных записей электронной почты, должны быть доставлены.
- **Изменить тему сообщений, отмеченных как СПАМ.** Установите данный флажок, если необходимо, чтобы все сообщения, определенные как [спам](#), были отмечены специальным словом или символом в поле темы сообщения. Необходимый текст можно ввести в текстовое поле, которое станет активным.
- **Запрашивать перед уведомлением о неправильном обнаружении.** Установив данный флажок в [процессе установки](#), вы соглашаетесь участвовать в [программе улучшения продуктов](#). В этом случае вы будете отправлять отчеты об обнаруженных угрозах в компанию AVG. Отправка отчетов осуществляется автоматически. Однако в случае установки данного флажка перед отправкой отчетов об обнаруженном спаме в компанию AVG вы будете получать запрос, позволяющий подтвердить, что сообщение, о котором вы сообщаете, действительно является спамом.

Кнопки управления

Кнопка **Обучение Anti-Spam** открывает [Мастер обучения Anti-Spam](#), подробно описанный в [следующей главе](#).

В первом диалоговом окне **мастера обучения Anti-Spam** необходимо выбрать источник сообщений электронной почты, которые будут использованы для обучения. Обычно используются сообщения электронной почты, ошибочно помеченные как СПАМ, или сообщения со спамом, которые не были опознаны.



Необходимо выбрать один из приведенных ниже вариантов.

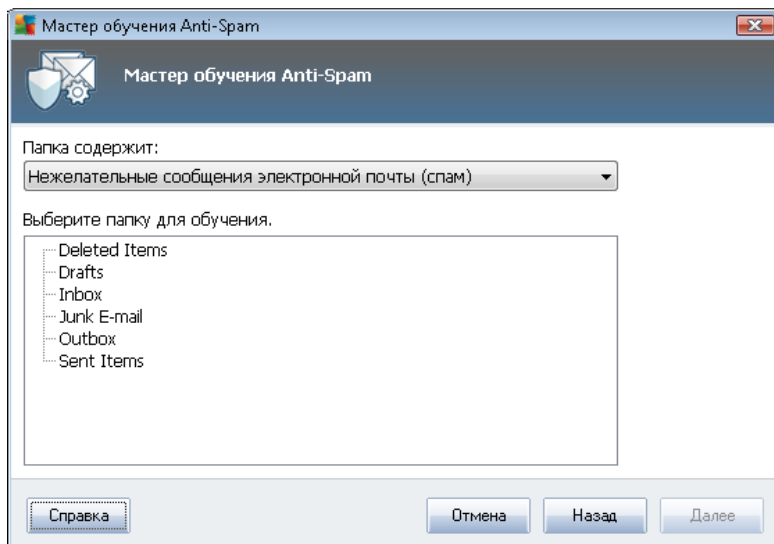
- **Определенный клиент электронной почты.** Если используется один из перечисленных клиентов электронной почты (*MS Outlook, Outlook Express, The Bat!*), выберите соответствующий вариант
- **Папка с файлами EML** — при использовании другой почтовой программы сначала необходимо сохранить сообщения в специальной папке (*в формате eml*) или узнать точное расположение папки с сообщениями используемого клиента электронной почты. Затем необходимо выбрать пункт **Папка с файлами EML**, чтобы на следующем шаге указать необходимую папку

Чтобы упростить и ускорить процесс обучения, можно заранее отсортировать сообщения электронной почты в папке так, чтобы папка, которая используется для обучения, содержала только учебные сообщения (желательные или нежелательные). Однако в этом нет необходимости, так как данный мастер позволяет выполнить сортировку сообщений электронной почты позже.

Выберите необходимый параметр и щелкните **Далее**, чтобы продолжить работу с мастером.

Отображаемое на данном шаге диалоговое окно определяется выбором, сделанным в предыдущем шаге.

Папки с файлами EML



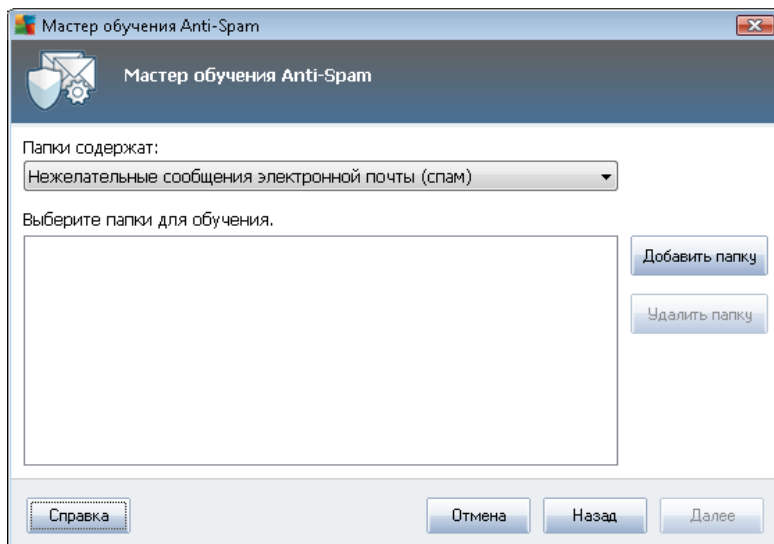
В данном диалоговом окне нужно указать папку с сообщениями, которые необходимо использовать для обучения. Нажмите **Добавить папку**, чтобы указать местоположение папки с файлами .eml (*сохраненные сообщения электронной почты*). Выбранная папка будет отображена в диалоговом окне.

В раскрывающемся меню **Содержимое папок:** выберите один из двух вариантов — выбранные папки содержат допустимые сообщения (ХАМ) или нежелательные сообщения (СПАМ). Обратите внимание, что на следующем шаге имеется возможность выполнить фильтрацию сообщений, поэтому папка может содержать не только тренировочные сообщения электронной почты. Нежелательные папки могут быть удалены из списка нажатием кнопки **Удалить папку**.

По завершении щелкните **Далее** и перейдите к [параметрам фильтрации сообщений](#).

Определенный клиент электронной почты

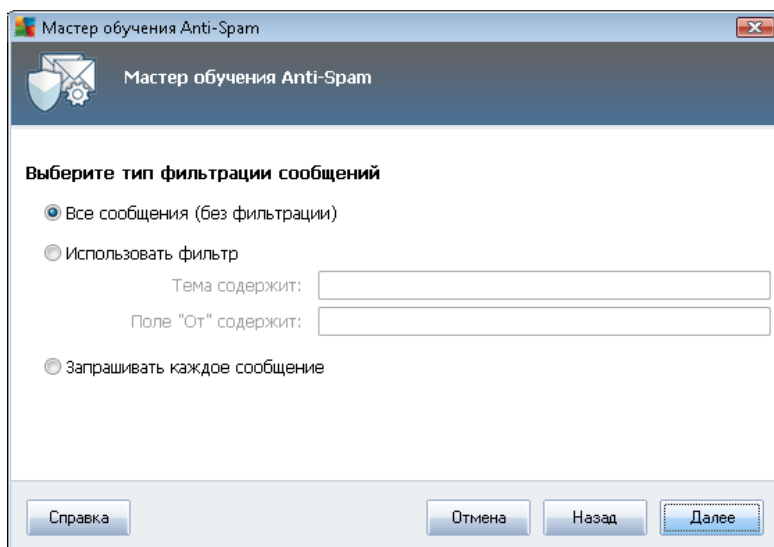
После подтверждения какого-либо из параметров откроется новое диалоговое окно.



Примечание. При использовании Microsoft Office Outlook будет предложено сначала выбрать профиль MS Office Outlook.

В раскрывающемся меню **Содержимое папок:** выберите один из двух вариантов — выбранные папки содержат допустимые сообщения (ХАМ) или нежелательные сообщения (СПАМ). Обратите внимание, что на следующем шаге имеется возможность выполнить фильтрацию сообщений, поэтому папка может содержать не только тренировочные сообщения электронной почты. Дерево навигации выбранного клиента электронной почты уже отображается в основном разделе данного диалогового окна. Выберите необходимую папку в дереве и выделите ее с помощью мыши.

По завершении щелкните **Далее** и перейдите к [параметрам фильтрации сообщений](#).



В данном окне можно настроить фильтрацию сообщений электронной почты.



Если выбранная папка действительно содержит только сообщения, которые необходимо использовать для обучения, выберите параметр **Все сообщения (без фильтрации)**.

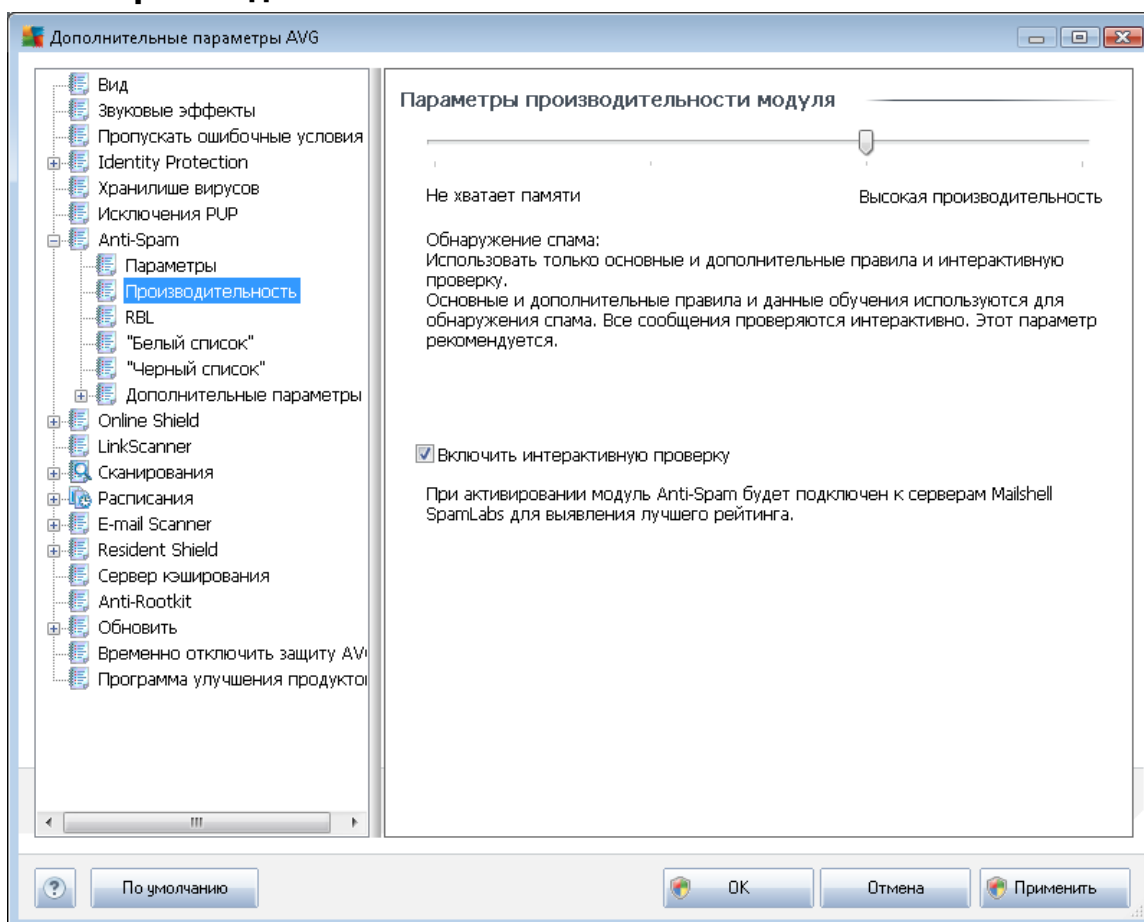
Если сообщения, находящиеся в папке, неизвестны и необходимо, чтобы мастер отображал запрос о каждом отдельном сообщении (чтобы определить, использовать его для обучения или нет), выберите параметр **Запрашивать каждое сообщение**.

Для получения дополнительных параметров фильтрации выберите параметр **Использовать фильтр**. Можно ввести слово (имя), часть слова или фразу для поиска в теме сообщения или поле отправителя. Все сообщения, точно соответствующие указанным критериям, будут использованы для обучения без предварительного уведомления.

Внимание! Если заполнены оба текстовых поля, адреса, соответствующие одному из двух указанных условий, также будут использоваться.

Выбрав соответствующий параметр, нажмите кнопку **Далее**. Следующее диалоговое окно носит исключительно информативный характер, уведомляя о готовности мастера к обработке сообщений. Чтобы начать обучение, снова нажмите кнопку **Далее**. Начнется процесс обучения в соответствии с предварительно выбранными условиями.

9.7.2. Производительность





Диалоговое окно **Параметры производительности модуля** (доступно при выборе элемента **Производительность** на панели навигации слева) позволяет настроить параметры производительности компонента **Anti-Spam**. Переместите ползунок влево или вправо, чтобы изменить уровень производительности при сканировании в диапазоне от **Малое использование памяти** до **Высокая производительность**.

- **Малая загрузка памяти.** В процессе сканирования будет определяться только [спам](#), правила использоваться не будут. Для определения будут использоваться только данные обучения. Данный режим рекомендуется использовать только на компьютерах с действительно низкой конфигурацией.
- **Высокая производительность.** При работе в данном режиме программа использует большой объем памяти компьютера. Для определения [спама](#) при сканировании будут использоваться следующие функции: правила и кэш базы данных [спама](#), основные и дополнительные правила, IP-адреса и базы данных распространителей спама.

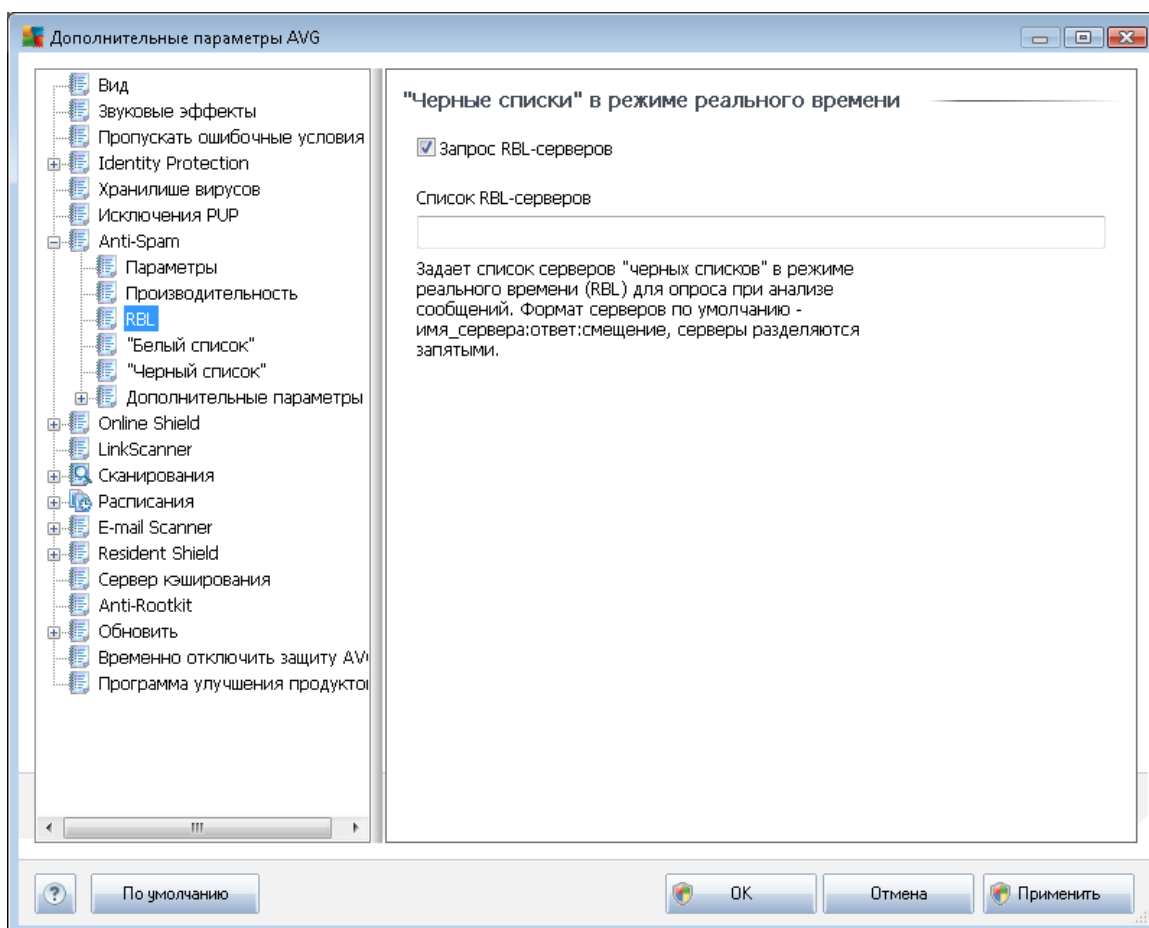
Параметр **Включить интерактивную проверку** включен по умолчанию. Таким образом обеспечивается более точное обнаружение [спама](#) посредством связи с серверами [Mailshell](#) — сканируемые данные будут сравниваться с базами данных [Mailshell](#) через Интернет.

Рекомендуется оставить параметры по умолчанию без изменений и вносить изменения, только если это действительно необходимо. Любые изменения конфигурации должны осуществляться только опытными пользователями!



9.7.3. RBL

Элемент **RBL** открывает диалоговое окно редактирования **Черные списки в режиме реального времени**.



Данное диалоговое окно позволяет включить или отключить функцию **Запрос RBL-серверов**.

Сервер RBL ("**черный список**" в режиме реального времени) — это сервер DNS с расширенной базой данных известных отправителей спама. Если данная функция включена, все сообщения электронной почты будут при проверке сопоставлены с базой данных сервера RBL и отмечены как [спам](#) в случае совпадения с одной из записей в базе данных. Базы данных серверов RBL содержат наиболее свежие идентификационные отметки спама, благодаря чему обеспечивается наилучшее и наиболее точное обнаружение [спама](#). Данная функция будет особенно полезна пользователям, получающим большое количество спама, который не распознается правильно модулем [Anti-Spam](#).

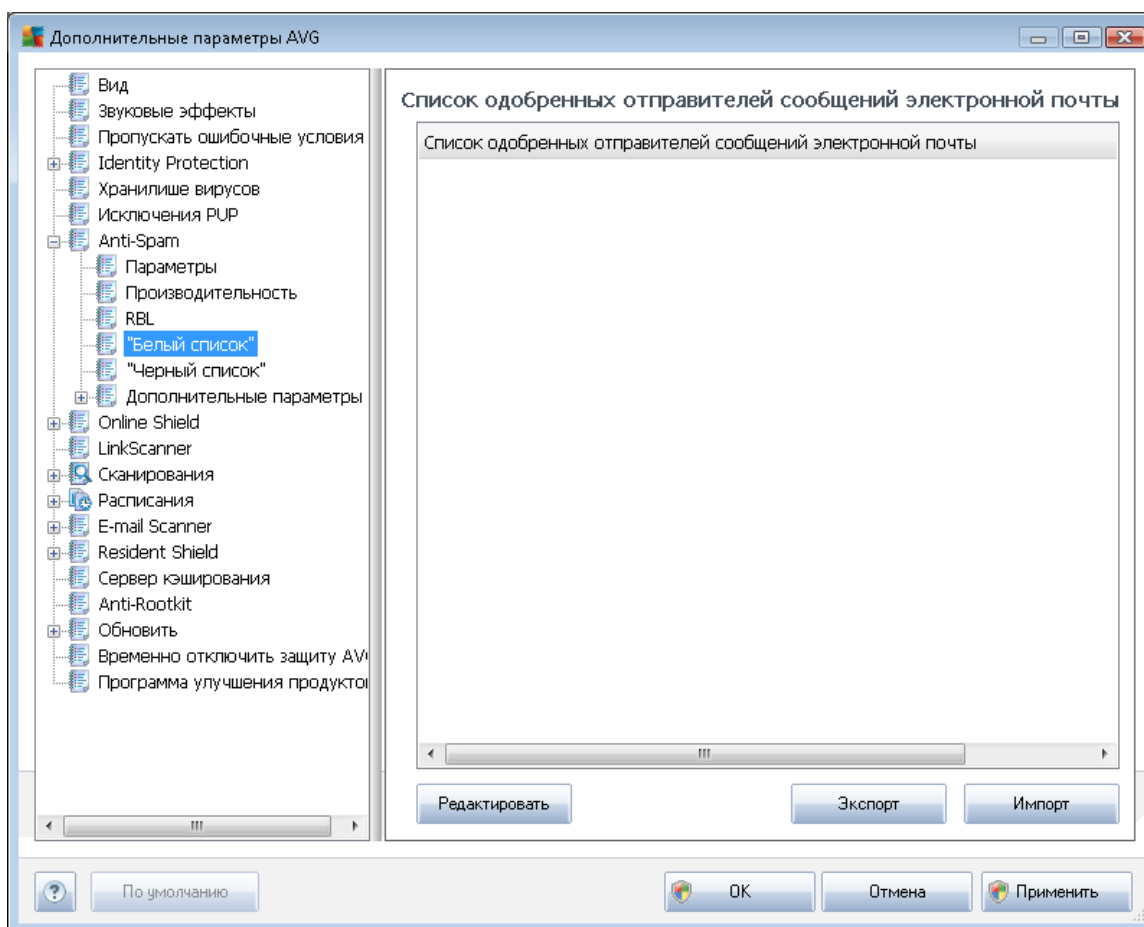
Список RBL-серверов позволяет указать местоположения серверов RBL.

Примечание. В результате включения данной функции процесс получения электронной почты может быть замедлен на некоторых системах и конфигурациях, так как происходит сопоставление каждого отдельного сообщения с базой данных сервера RBL.

Отправка личных данных на сервер не выполняется.

9.7.4. Белый список

Элемент **Белый список** представляет собой диалоговое окно **Список одобренных отправителей сообщений электронной почты**, содержащее общий список подтвержденных адресов отправителей электронной почты и имен доменов, сообщения которых никогда не будут отмечены как [спам](#).



В интерфейсе редактирования можно указать список отправителей, которые, как вы считаете, никогда не отправляют нежелательных сообщений ([спам](#)). Можно также указать список полных имен доменов (например, *avg.com*), которые, как вы уверены, не генерируют нежелательных сообщений электронной почты.

Список отправителей и/или доменных имен можно ввести двумя способами: отдельно ввести каждый адрес электронной почты или сразу импортировать весь список адресов. Доступны следующие кнопки управления.

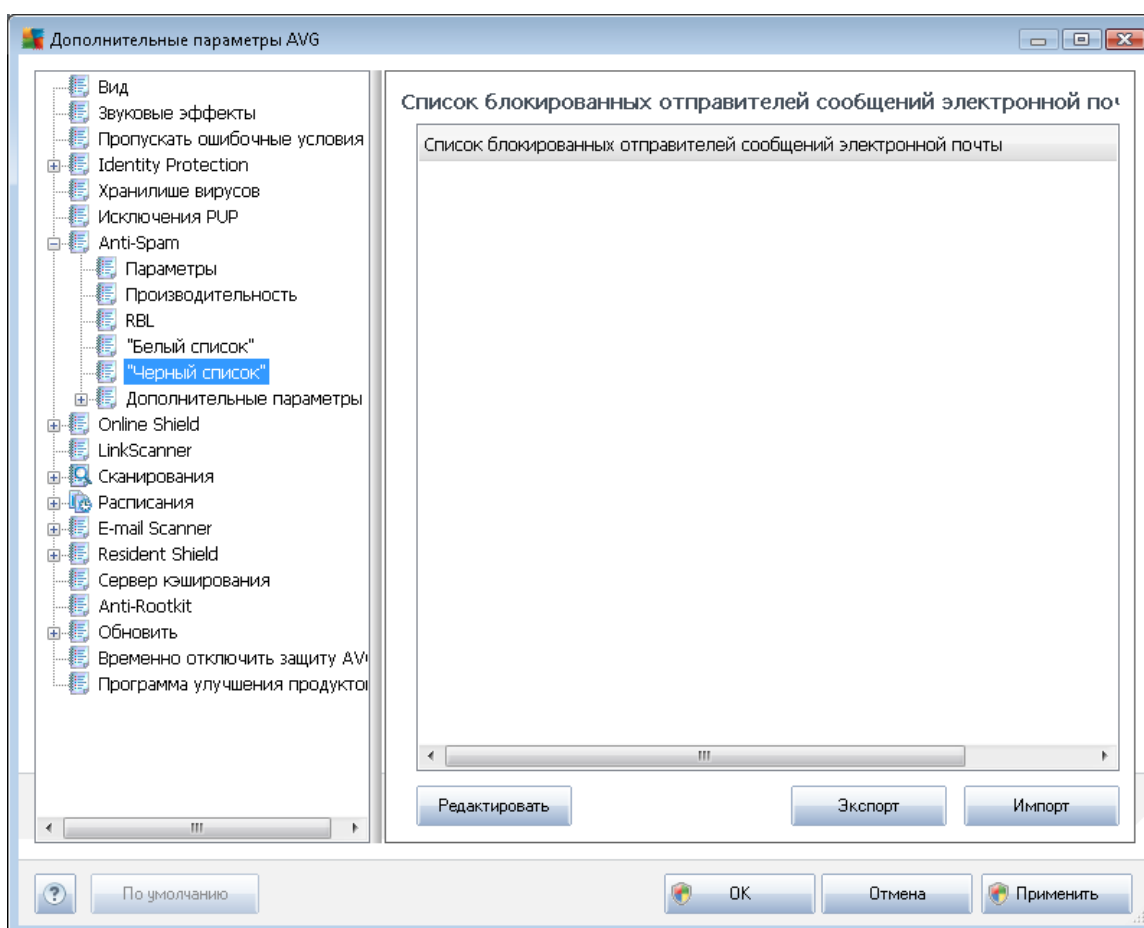
- **Редактировать** — при нажатии этой кнопки откроется диалоговое окно, в котором можно вручную ввести список адресов (*также можно использовать способ "копировать/вставить"*). Можно вставлять только один элемент (*отправитель, имя домена*) в каждую строку.



- **Экспорт** — если по какой-либо причине необходимо экспортировать записи, это можно сделать, нажав данную кнопку. Все записи будут сохранены в формате обычного текста.
- **Импорт** — заранее подготовленный текстовый файл с адресами электронной почты или именами доменов можно импортировать, нажав эту кнопку. В каждой строке файла должен содержаться только один элемент (*адрес, имя домена*).

9.7.5. Черный список

Элемент **Черный список** открывает диалоговое окно с общим списком заблокированных адресов отправителей электронной почты и имен доменов. Сообщения таких отправителей всегда будут отмечаться как [спам](#).



В интерфейсе редактирования можно указать список отправителей, рассылающих нежелательные сообщения ([спам](#)). Также можно составить список полных имен доменов (например, *spammingcompany.com*), рассылающих нежелательные сообщения. Все сообщения электронной почты с указанных адресов/доменов будут расцениваться как спам.

Список отправителей и/или доменных имен можно ввести двумя способами: отдельно ввести каждый адрес электронной почты или сразу импортировать весь список адресов. Доступны следующие кнопки управления.

- **Редактировать** — при нажатии этой кнопки откроется диалоговое окно, в котором можно вручную ввести список адресов (*также можно использовать способ "копировать/вставить"*). Можно вставлять только один элемент (*отправитель, имя домена*) в каждую строку.
- **Экспорт** — если по какой-либо причине необходимо экспортировать записи, это можно сделать, нажав данную кнопку. Все записи будут сохранены в формате обычного текста.
- **Импорт** — заранее подготовленный текстовый файл с адресами электронной почты или именами доменов можно импортировать, нажав эту кнопку.

9.7.6. Дополнительные параметры

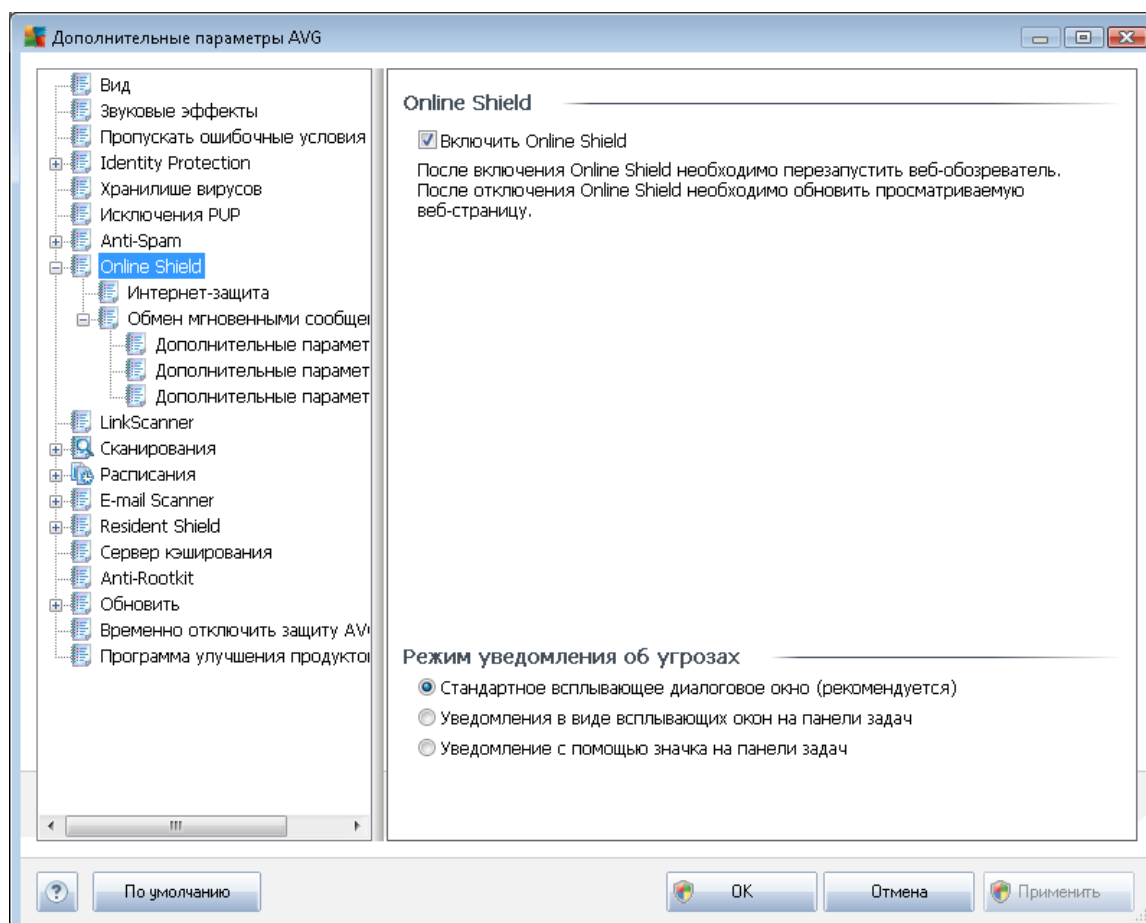
Ветвь Дополнительные параметры содержит расширенные параметры компонента Anti-Spam. Данные параметры предназначены для опытных пользователей, в основном для администраторов сети, которым требуется произвести подробные настройки защиты от спама для обеспечения наилучшего уровня защиты почтовых серверов. По этой причине дополнительная справочная информация по отдельным диалоговым окнам отсутствует, однако непосредственно в пользовательском интерфейсе имеется краткое описание каждого параметра.

Настоятельно рекомендуется не изменять никакие параметры без предварительного ознакомления со всеми дополнительными параметрами компонента Spamcatcher (MailShell Inc.). Любые неправильные изменения могут привести к снижению производительности или неправильной работе компонента.

Чтобы изменить расширенные параметры компонента [Anti-Spam](#), следуйте инструкциям, предоставленным непосредственно в интерфейсе пользователя. В каждом диалоговом окне указана одна определенная функция, которую можно редактировать. Описание функции приведено в диалоговом окне.

- **Кэш**. Отпечаток, репутация домена, LegitRepute.
- **Обучение**. Максимальное количества слов, порог автоматического обучения, вес.
- **Фильтрация**. Список языков, список стран, одобренные IP-адреса, блокируемые IP-адреса, блокируемые страны, блокируемые кодировки, ложные отправители.
- **RBL**. Серверы RBL, множественные совпадения, порог, время ожидания, максимальное количество IP-адресов.
- **Интернет-соединение**. Время ожидания, прокси-сервер, проверка подлинности прокси-сервера.

9.8. Online Shield



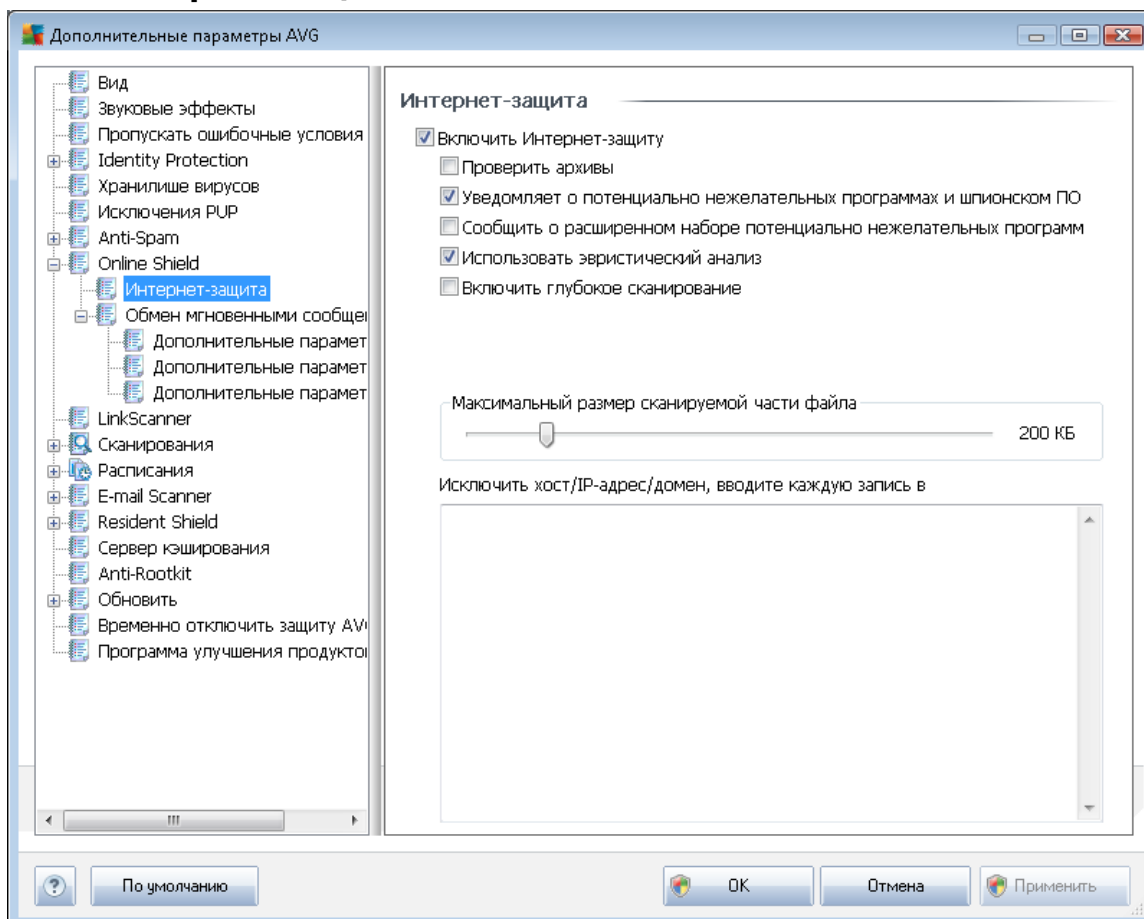
Диалоговое окно **Online Shield** позволяет активировать и отключать компонент [Online Shield](#) с помощью параметра **Включить Online Shield** (активирован по умолчанию). Для доступа к остальным дополнительным параметрам данного компонента перейдите к последующим диалоговым окнам в соответствии со списком в навигационном дереве.

- [Интернет-защита](#)
- [Обмен мгновенными сообщениями](#)

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.

9.8.1. Интернет-защита

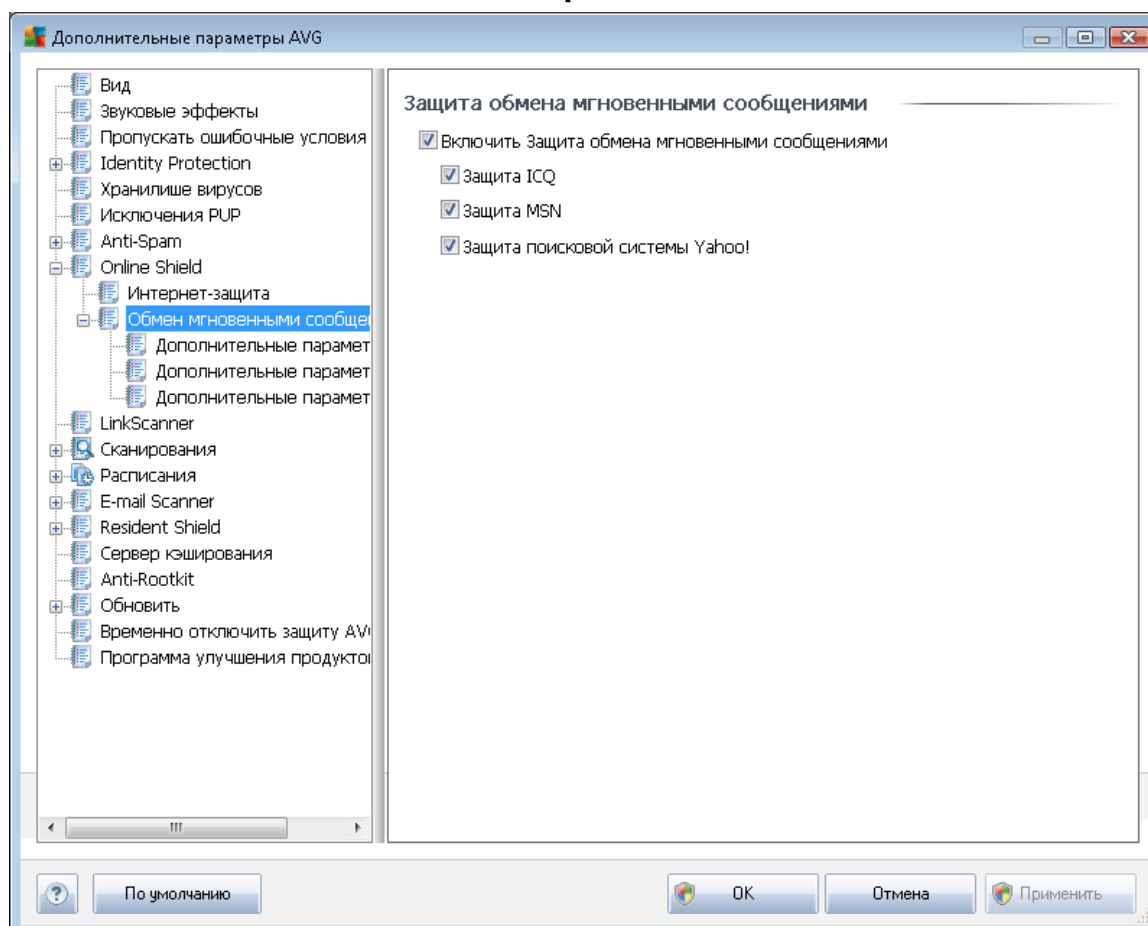


Диалоговое окно **Интернет-защита** позволяет изменять настройки компонента, относящиеся к сканированию содержимого веб-сайта. Интерфейс редактирования позволяет настроить следующие начальные параметры.

- **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.
 - о **Проверка архивов** (не выбрано по умолчанию). Сканирование содержимого архивов, которые могут содержаться на отображаемых интернет-страницах.
 - о **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.

- о **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 законные программы, поэтому по умолчанию параметр отключен.
- о **Использовать эвристический анализ** (выбрано по умолчанию). сканирование содержимого отображаемой страницы с использованием метода [эвристического анализа](#) (динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде).
- о **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.
- о **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.
- о **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.

9.8.2. Обмен мгновенными сообщениями

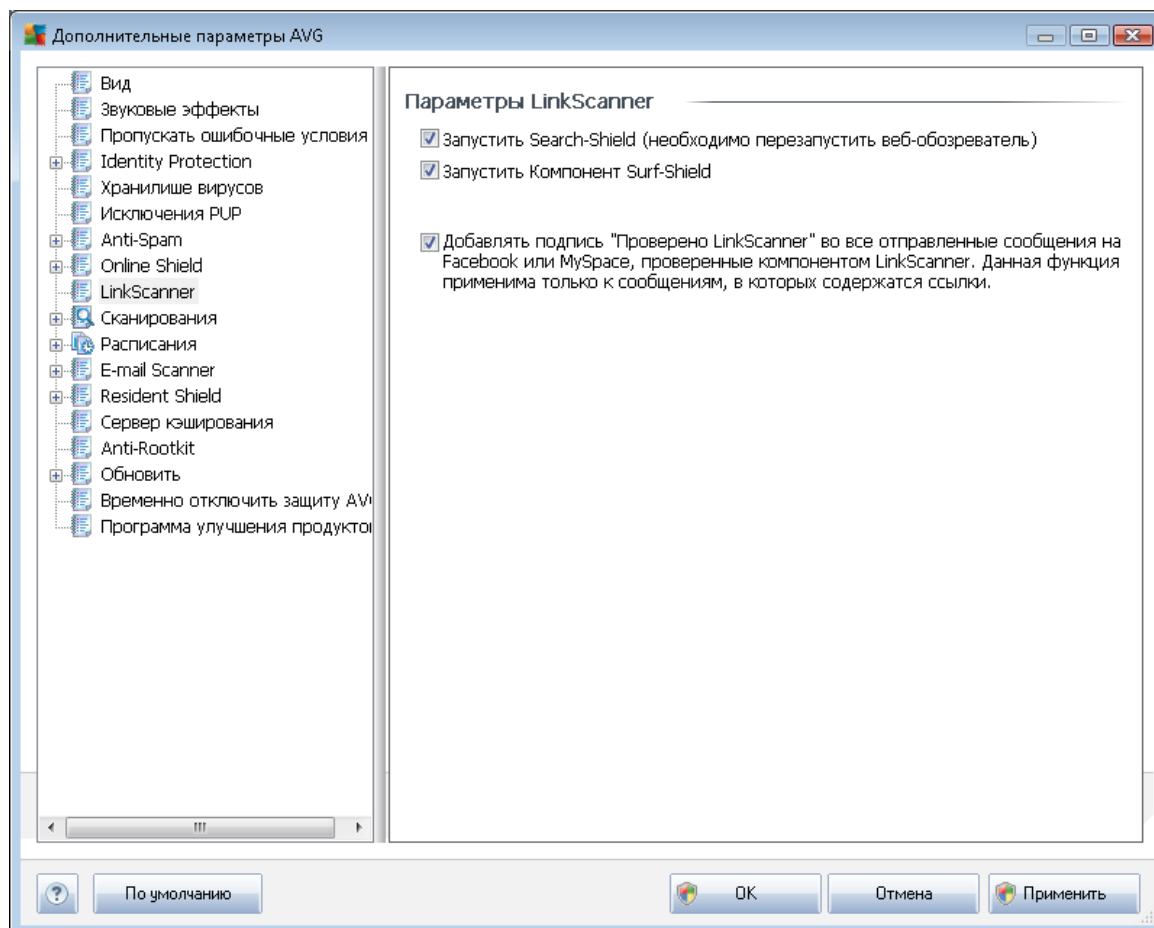


В окне **Защита обмена мгновенными сообщениями** можно изменять параметры компонентов **Online Shield**, относящихся к сканированию мгновенных сообщений. В настоящее время поддерживаются три следующие программы обмена мгновенными сообщениями: **ICQ**, **MSN** и **Yahoo**. Установите флажок в соответствующем поле для каждой программы, если необходимо, чтобы компонент **Online Shield** проверял сообщения на наличие вирусов во время общения в режиме реального времени.

Дополнительные параметры разрешенных и заблокированных пользователей можно просматривать и изменять с помощью соответствующего диалогового окна (**Дополнительные параметры ICQ**, **Дополнительные параметры MSN**, **Дополнительные параметры Yahoo**), а также можно указать **белый список** (список пользователей, которым разрешено общение с вами) и **черный список** (список пользователей, которых следует заблокировать).

9.9. 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).
- **Добавить "Проверено AVG LinkScanner"** Установите данный флажок для ввода текста сертификации во все проверенные компонентом [Link Scanner](#) сообщения, содержащие активные гиперссылки, отправленные из социальных сетей Facebook и MySpace.



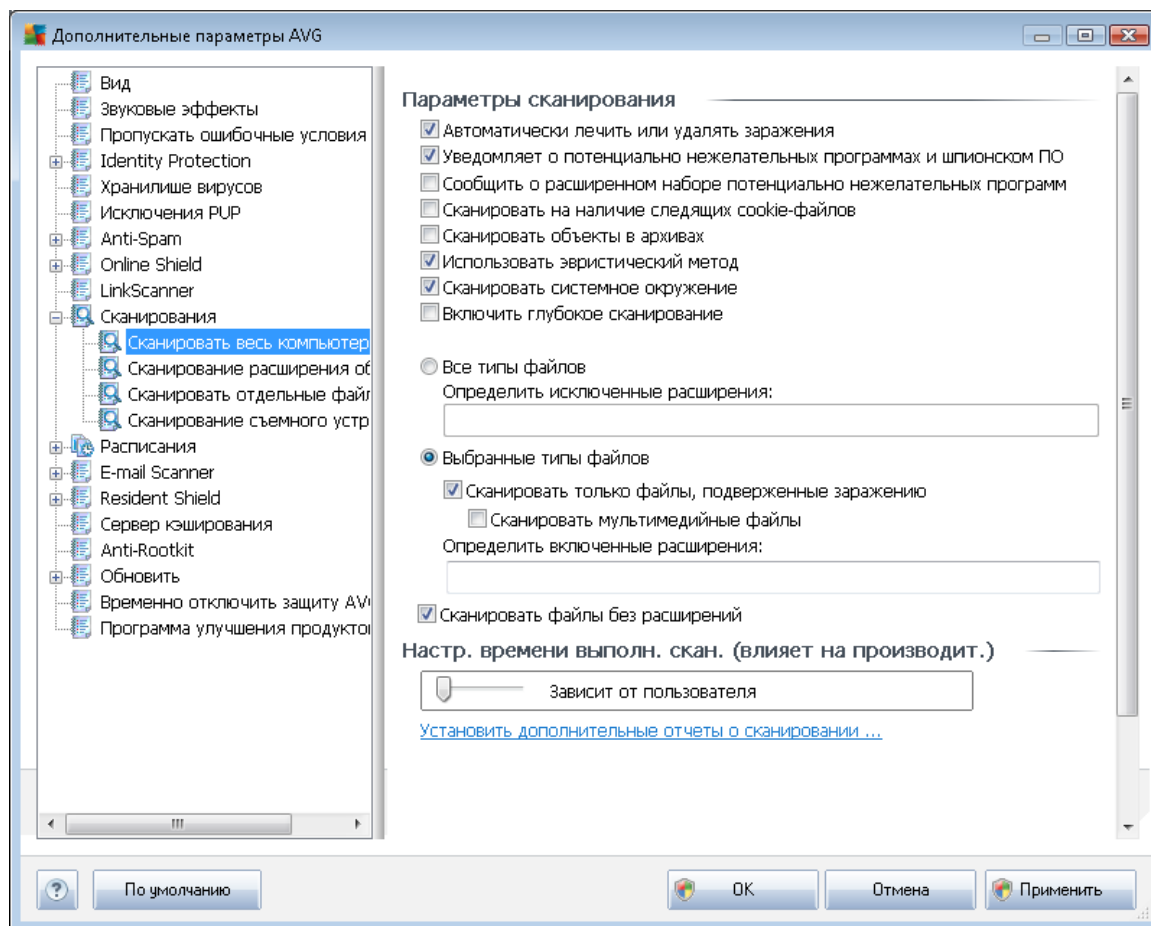
9.10. Сканирования

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 отдельных файлов или папок](#). Стандартное предварительно настроенное сканирование выбранных областей компьютера.
- [Сканирование съемного устройства](#). Особое сканирование съемных устройств, подключенных к компьютеру.

9.10.1. Сканирование всего компьютера

С помощью параметра **Сканирование всего компьютера** можно изменять 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 заражения** (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**



(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 законные 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 содержанием 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 (динамичная 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.

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**.



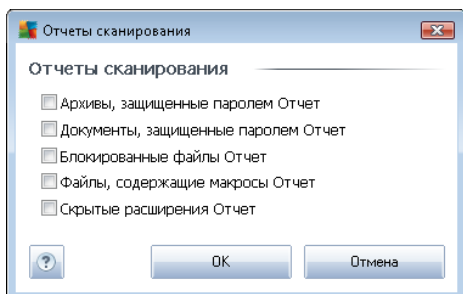
Он установлен по умолчанию. Рекомендуется не снимать его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

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.

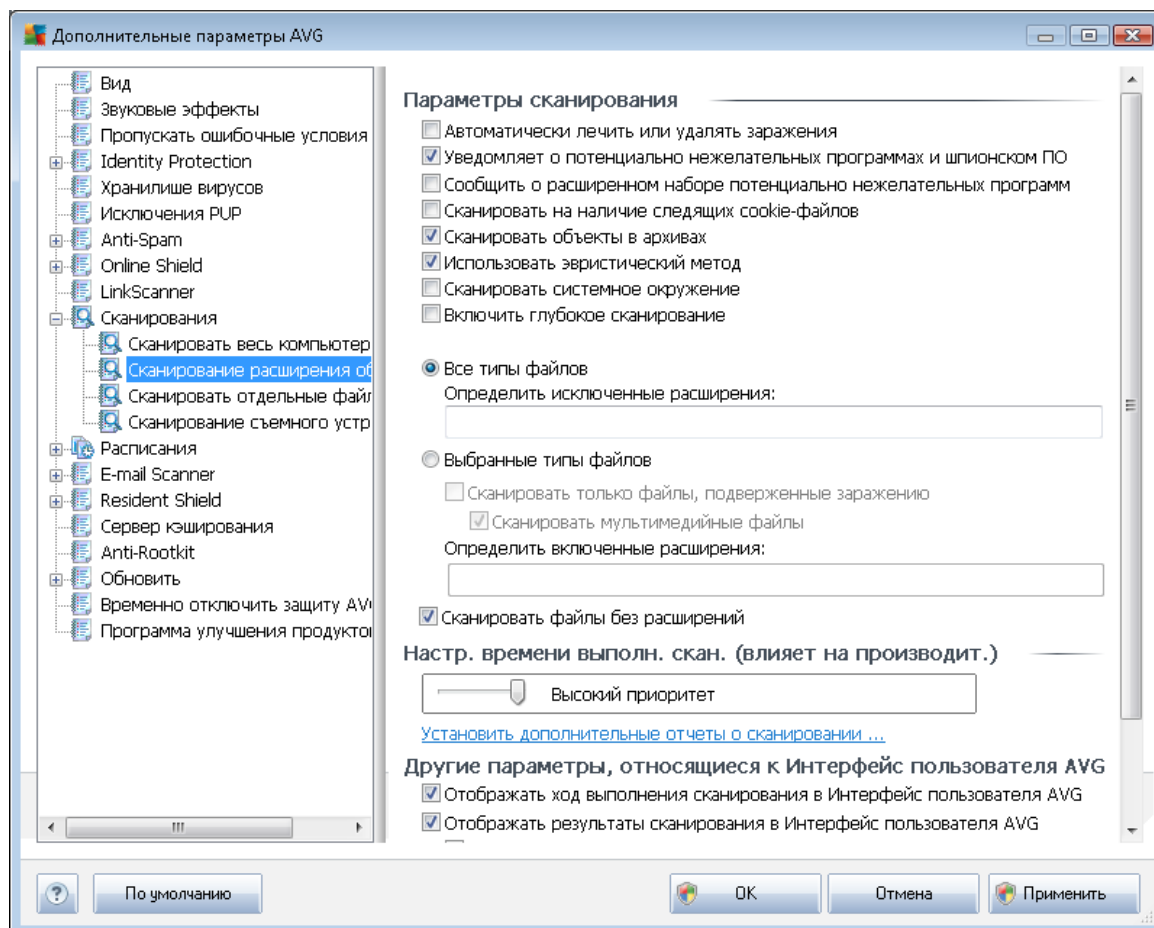
Установить дополнительные отчеты о сканировании ...

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.



9.10.2. Сканирование расширения оболочки

Как и предыдущий элемент [Сканирование всего компьютера](#), элемент **Сканирование расширения оболочки** также содержит несколько предварительно установленных 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](#).



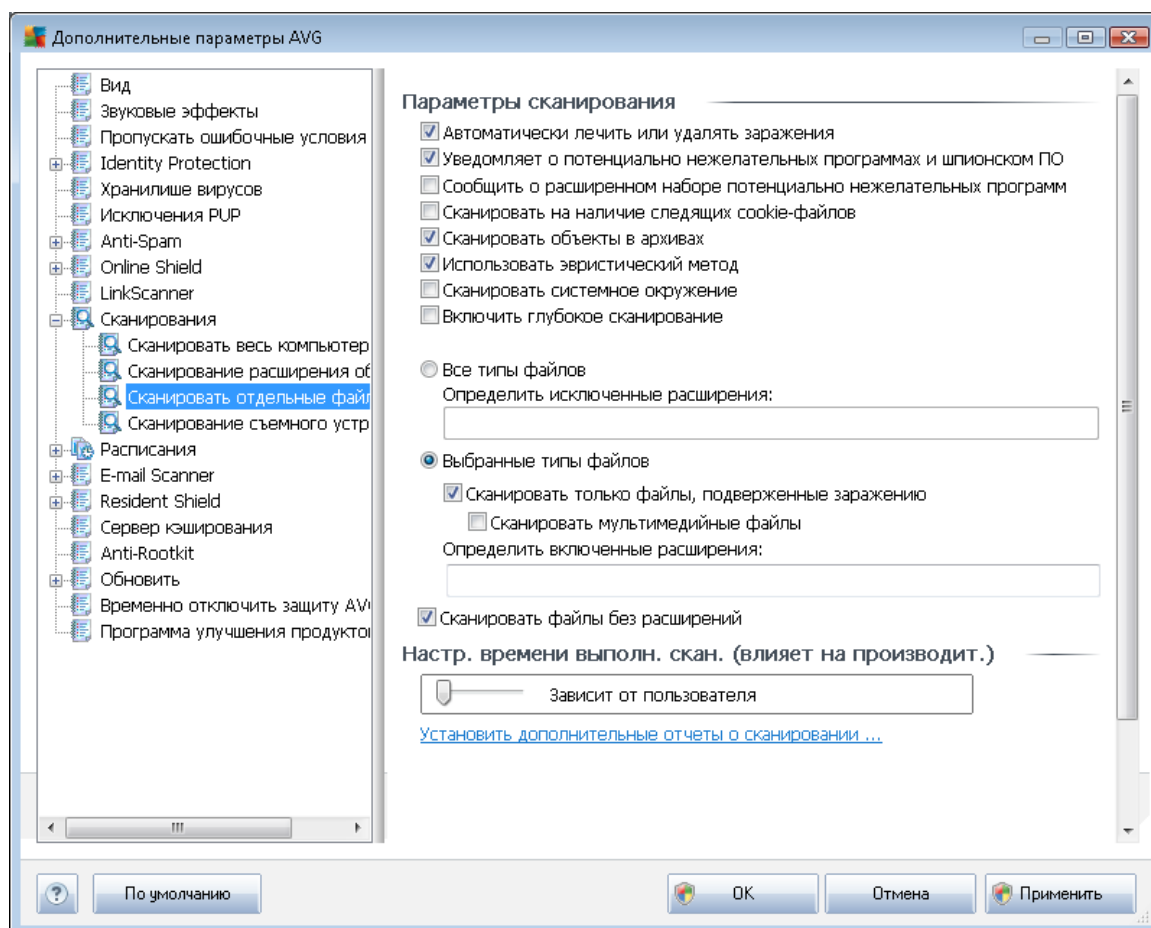
Список параметров соответствует параметрам элемента [Сканирование всего компьютера](#). Однако параметры по умолчанию отличаются (например, при сканировании всего компьютера по умолчанию не выполняется проверка архивов, однако выполняется сканирование системной среды, в то время как при сканирования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

9.10.3. Сканирование отдельных файлов или папок

Интерфейс редактирования **Сканирование отдельных 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](#):

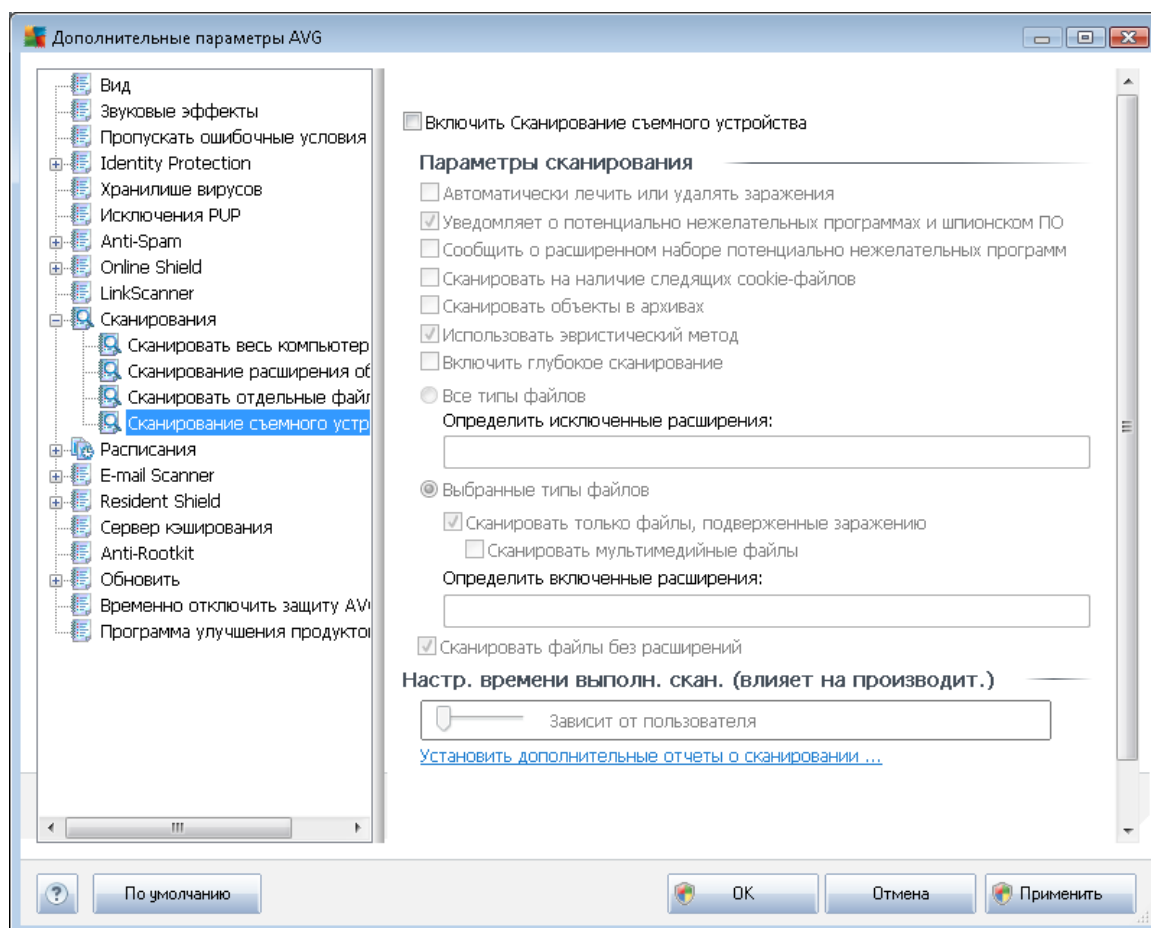


Все параметры, настроенные в этом диалоговом окне конфигурации, применяются только в выбранным для сканирования областям с помощью [Сканирование определенных файлов или папок!](#)

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

9.10.4. 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](#).

9.11. Расписания

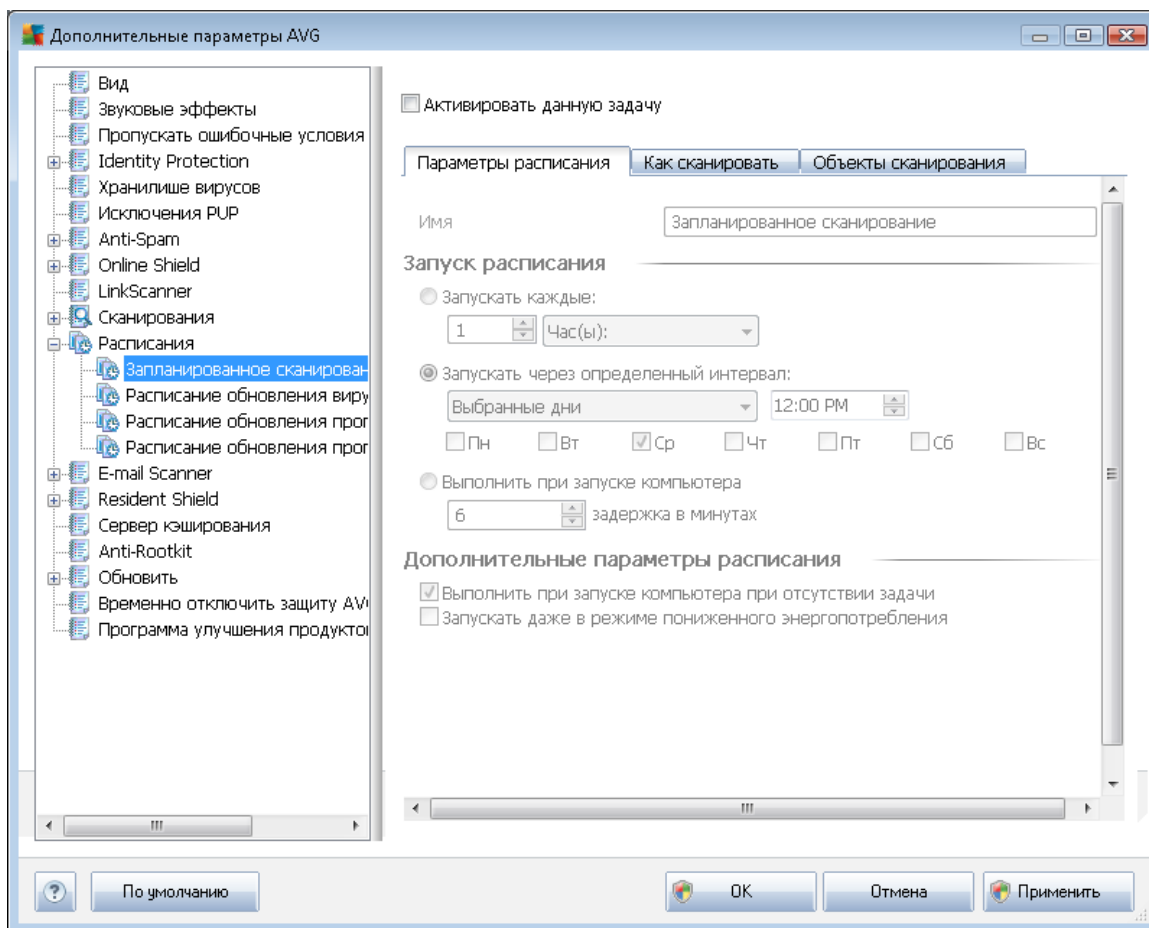
Раздел *Расписания* позволяет изменить стандартные настройки расписания.

- [Запланированное сканирование](#)
- [Расписание обновления вирусной базы данных](#)

- [Расписание обновления программы](#)
- [Расписание обновления Anti-Spam](#)

9.11.1. 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.

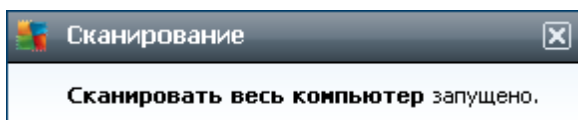
Выполняемое расписание

Здесь можно указать временные интервалы запуска нового запланированного сканирования. 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**).

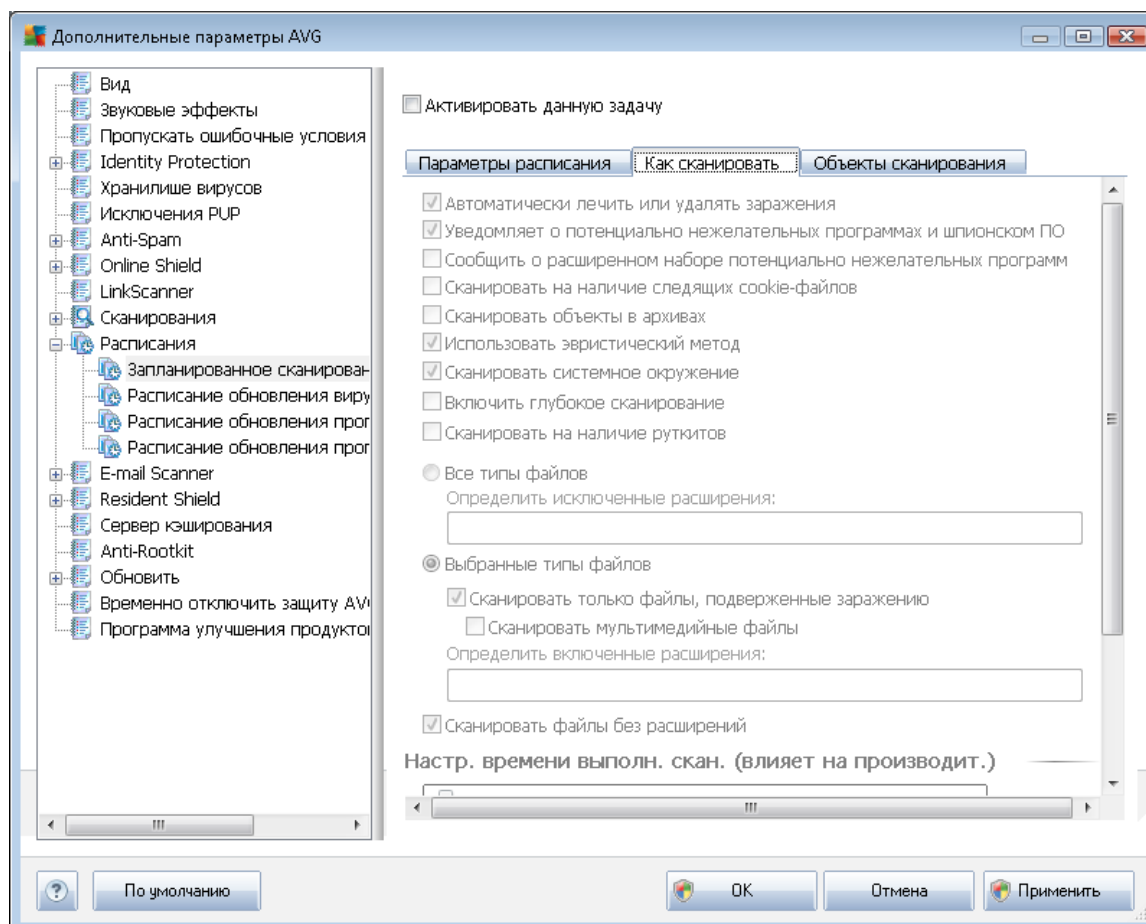
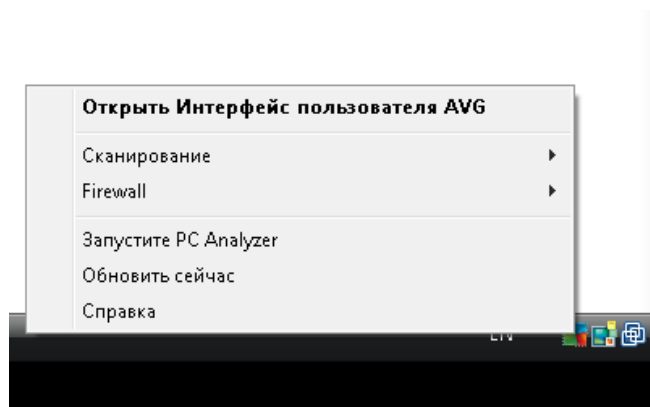
Дополнительные параметры расписания

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

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 значок с белой стрелкой), 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 заражения** (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** (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 законные 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 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). 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 (динамическая 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, 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 rootkits** (не выбрано по умолчанию). Установите этот флажок, чтобы искать средства rootkit при сканировании всего компьютера. Определение средств rootkit можно выполнить отдельно с помощью компонента [Anti-Rootkit](#).



Далее необходимо выбрать файлы для сканирования

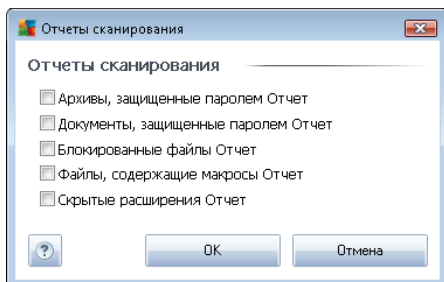
- **Все типы файлов** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми (*после сохранения запятые изменяются на точки с запятой*), сканирование которых проводиться не будет;
- **Выбранные типы файлов.** Можно указать сканирование 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

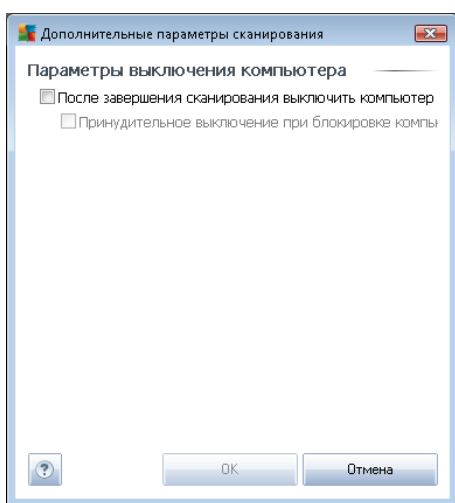
Щелкните ссылку **Установить дополнительные отчеты о сканировании**, чтобы открыть диалоговое окно **Отчеты сканирования**, в котором можно выбрать типы объектов, о которых будут выводиться отчеты при сканировании.

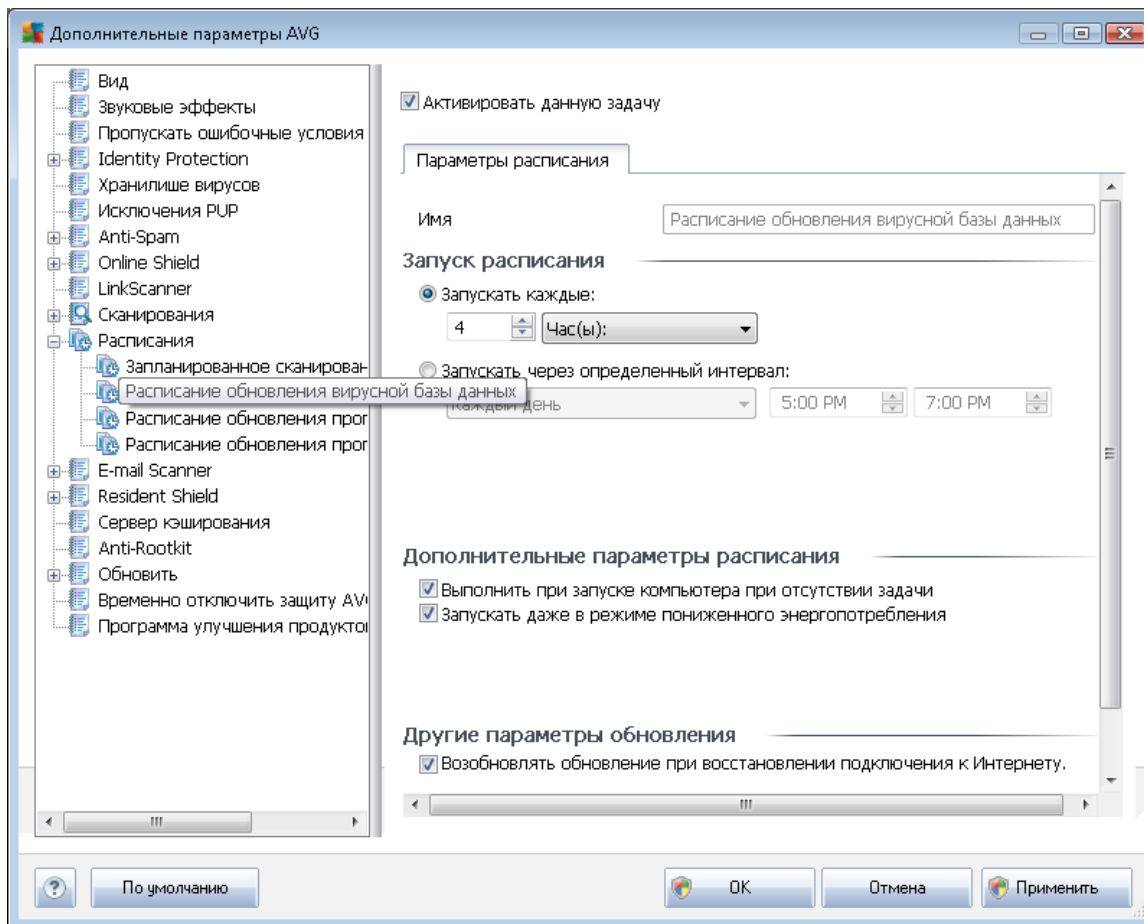




Дополнительные параметры сканирования

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**).





Основное расписание обновления вирусной базы данных может быть настроено с помощью компонента [Диспетчер обновления](#). В данном диалоговом окне могут быть настроены параметры расписания обновления вирусной базы данных. 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 запланированного запуска обновления вирусной базы данных. 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 вирусной базы данных, если компьютер работает в энергосберегающем режиме или выключен.



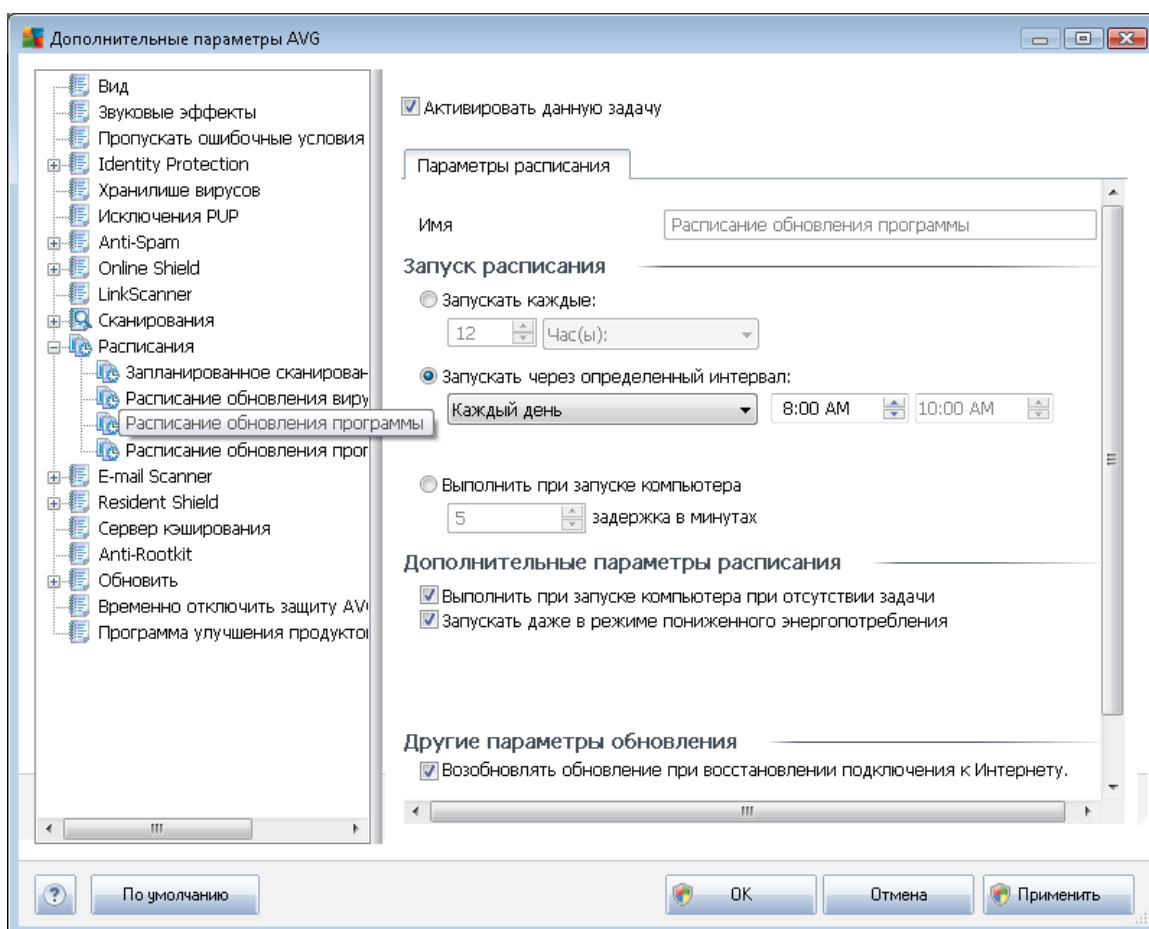
Другие параметры обновления

Установите флажок **Возобновлять обновление при восстановлении подключения к Интернету**, чтобы в случае разрыва соединения с Интернетом и 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).

9.11.3. 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

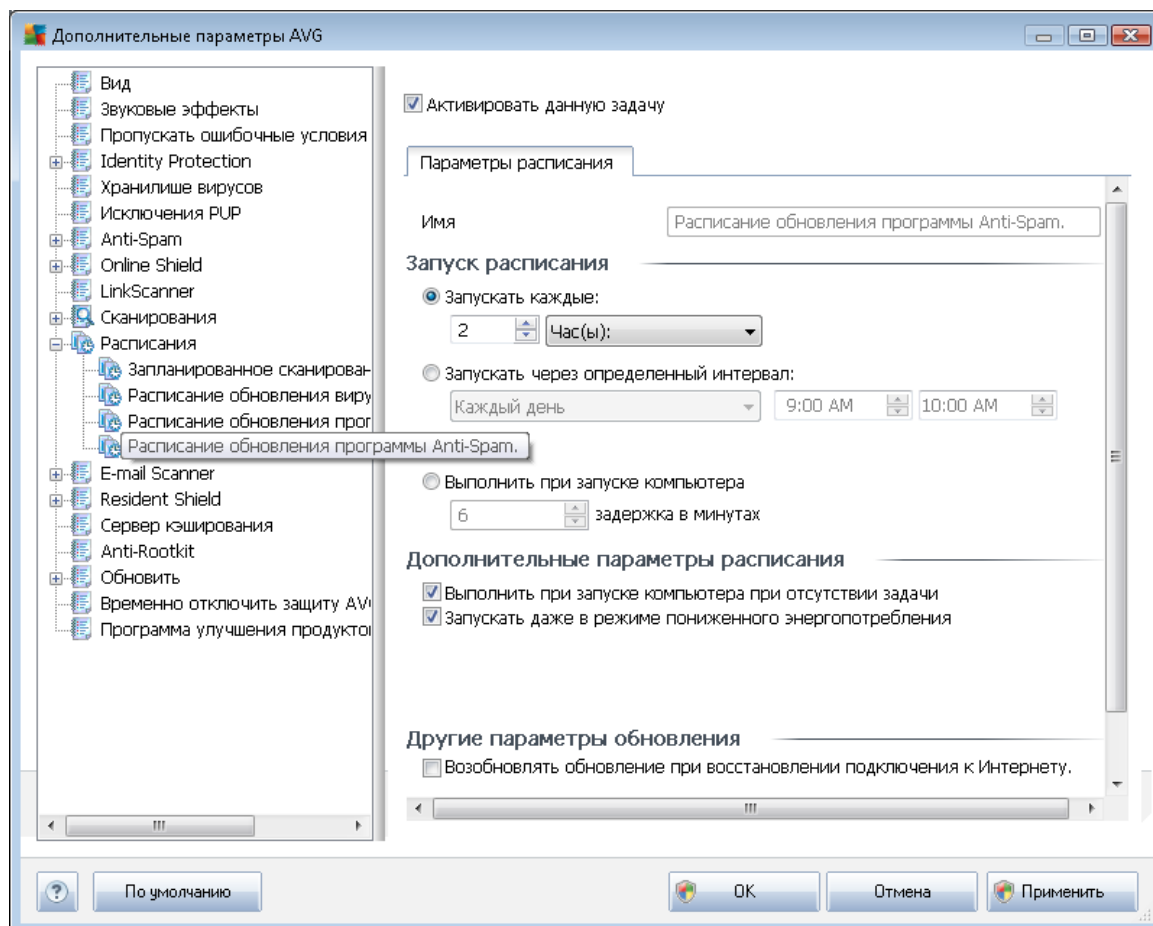
Установите флажок **Возобновлять обновление при восстановлении подключения к Интернету**, чтобы в случае разрыва соединения с Интернетом и сбое процесса обновления компонента обновление выполнялось сразу же после восстановления подключения к Интернету.

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 проверка пересекаются по времени, процесс обновления имеет более высокий приоритет и сканирование будет прервано.

9.11.4. Расписание обновления компонента Anti-Spam

В случае **крайней необходимости** можно снять флажок **Активировать данную задачу**, чтобы временно деактивировать запланированное обновление [Anti-Spam](#). Обновление можно включить позже в любое время.



Основное расписание обновления компонента [Anti-Spam](#) можно настроить с помощью компонента [Диспетчер обновлений](#). В данном диалоговом окне можно настроить параметры расписания обновления. 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 компонента [Anti-Spam](#). Временные интервалы также могут быть определены с помощью повторного запуска обновления компонента [Anti-Spam](#) через определенный промежуток времени (**Запускать через каждые ...**), указания точной даты и времени (**Запускать в определенное время ...**), а также определения события, 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 компонента [Anti-Spam](#), если компьютер работает в энергосберегающем режиме или выключен.



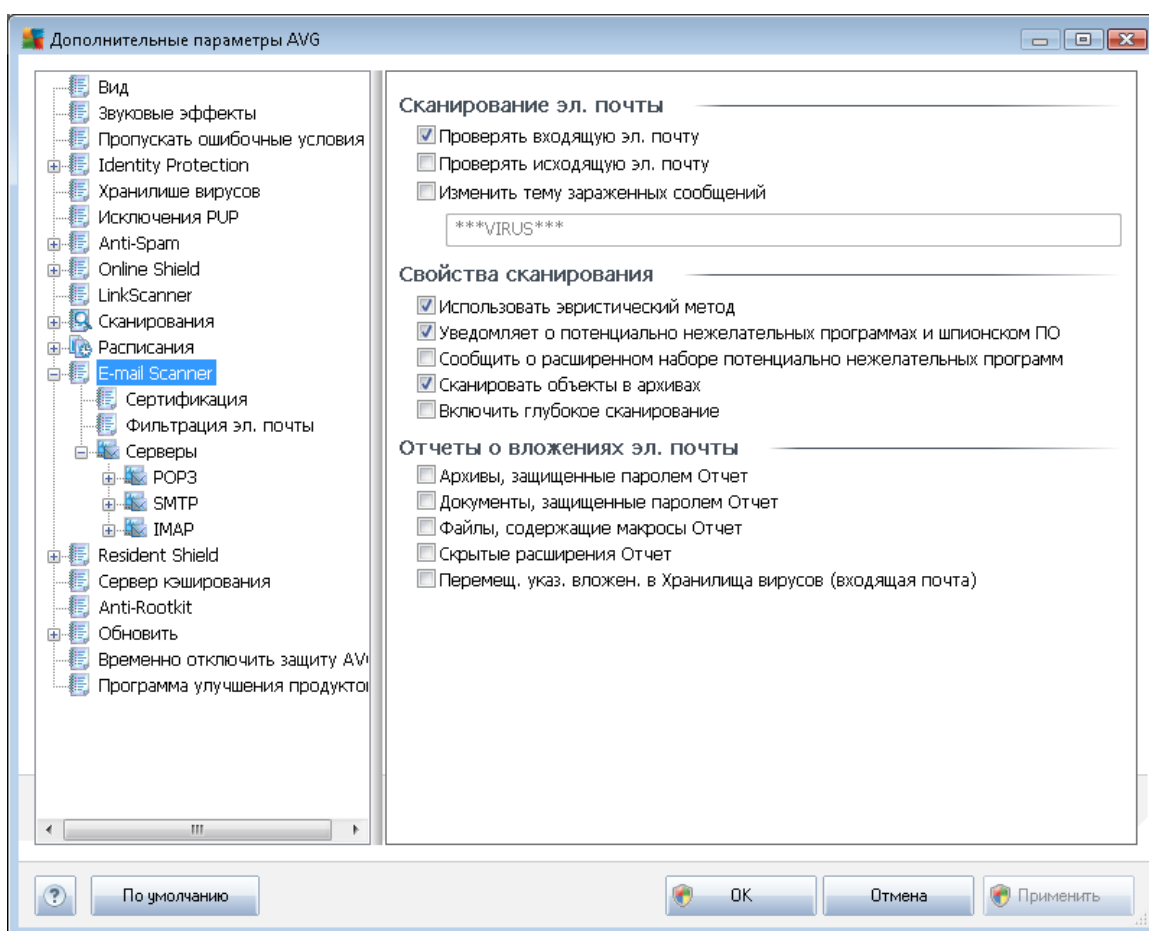
Другие параметры обновления

Установите флажок **Возобновлять обновление при восстановлении подключения к Интернету**, чтобы в случае разрыва соединения с Интернетом и сбое процесса обновления компонента **Anti-Spam** обновление выполнялось сразу же после восстановления подключения к Интернету.

После запуска запланированного обновления появится всплывающее окно с уведомлением о данном событии над **значком AVG в панели задач** (при условии, что параметры диалогового окна по умолчанию **Дополнительные параметры/Внешний вид** не были изменены).

9.12. 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 эл. почты.

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

- **Использовать эвристический анализ** (выбрано по умолчанию). Установите данный флажок, чтобы использовать [эвристический метод обнаружения](#) при сканировании сообщений эл. 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** (не установлено 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 законные 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.

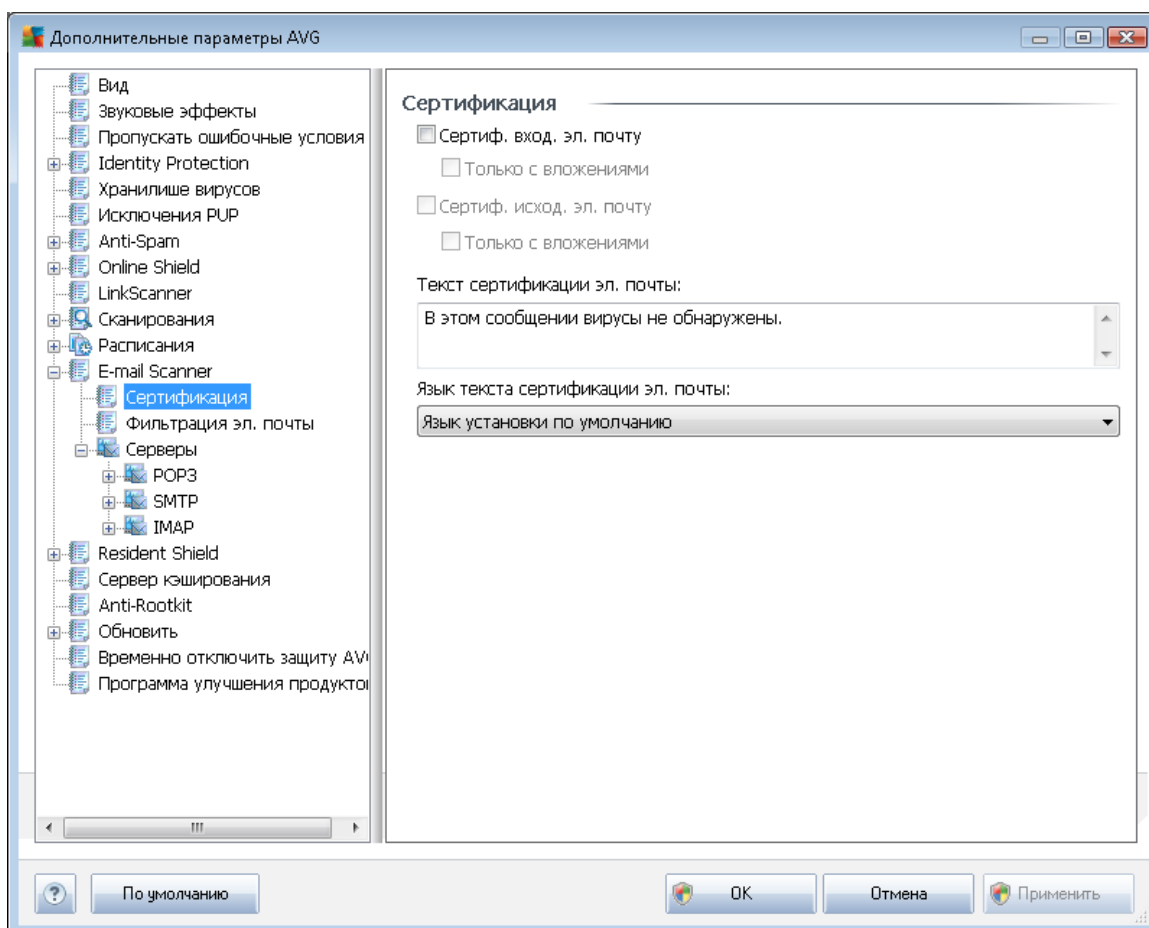
Отчеты о вложениях эл. почты

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 эл. 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.** Скрытое расширение может способствовать отображению, например, подозрительного исполняемого файла something.txt.exe, как безопасного обычного текстового файла 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 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](#).

9.12.1. Сертификация

В диалоговом окне **Сертификация** можно указать текст и язык сертификации для входящих и исходящих сообщений.



Текст сертификации состоит из двух частей: пользовательская часть и системная часть (см. следующий пример): первая строка — это пользовательская часть, остальные строки генерируются автоматически:

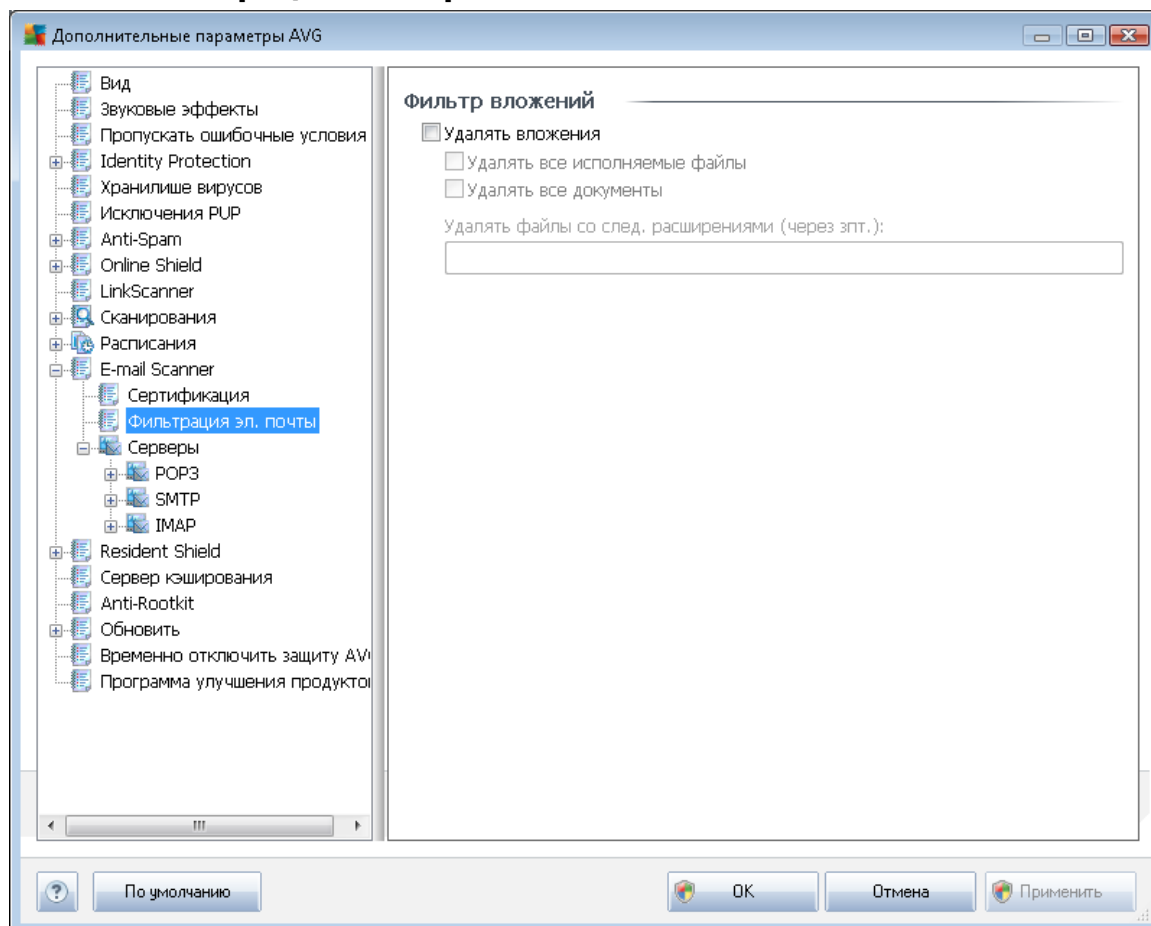
В этом сообщении вирусы не обнаружены.

Проверено AVG.

Версия: x.y.zz /Вирусная база данных : xx.y.z — Дата выпуска: 12/9/2010

Если требуется использовать сертификацию входящих или исходящих сообщений электронной почты, в данном диалоговом окне можно указать текст пользовательской части сертификации (**Текст сертификации эл. почты**) и выбрать язык для системной части сертификации, которая генерируется автоматически (**Язык текста сертификации эл. почты**).

9.12.2. Фильтрация электронной почты

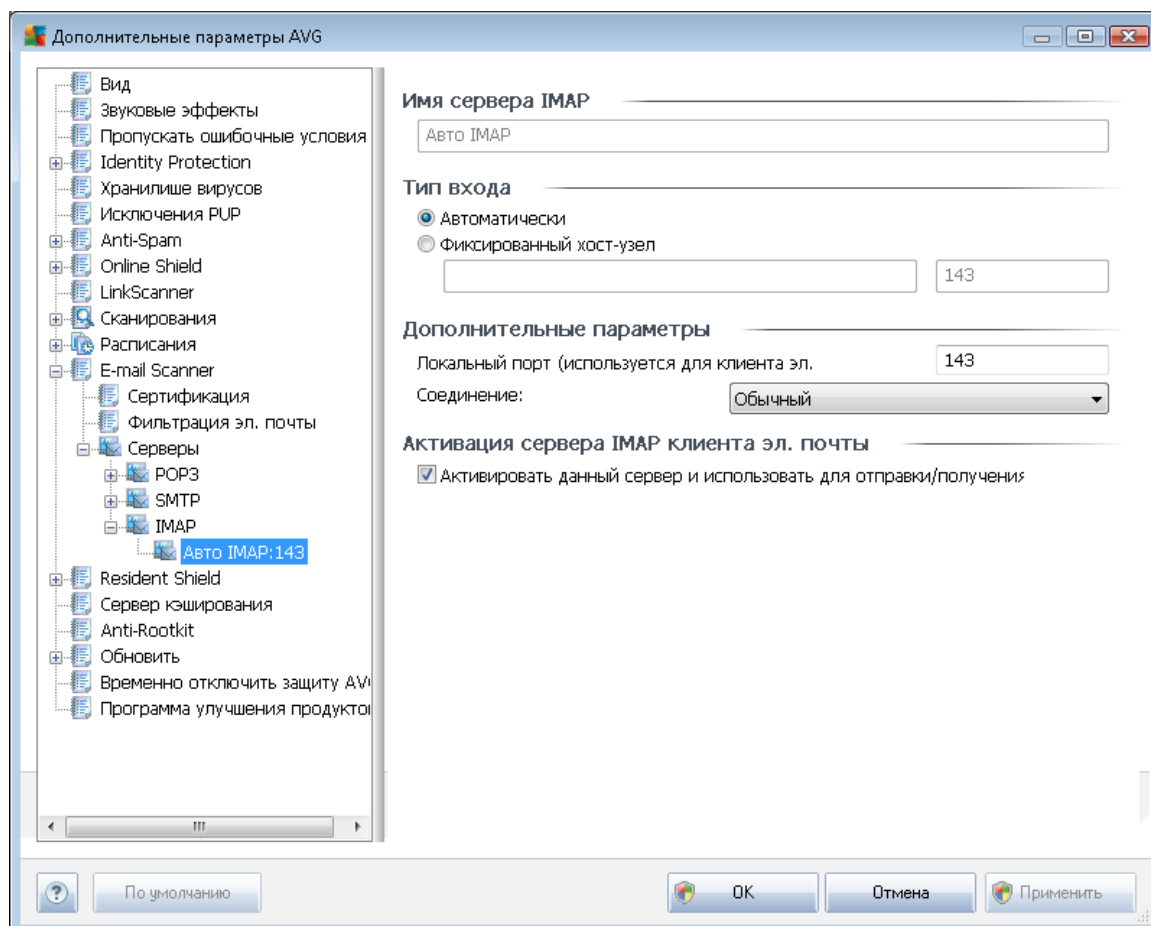


Диалоговое окно **Фильтр вложений** позволяет настроить параметры сканирования вложений в сообщениях электронной почты. По умолчанию параметр **Удалять вложения** отключен. При его установке все обнаруженные зараженные вложения в сообщениях электронной почты или потенциально опасные вложения будут автоматически 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.

9.12.3. Серверы

В разделе **Серверы** можно изменить параметры серверов компонента **E-mail Scanner** или установить новый сервер, нажав кнопку **Добавить новый сервер**.

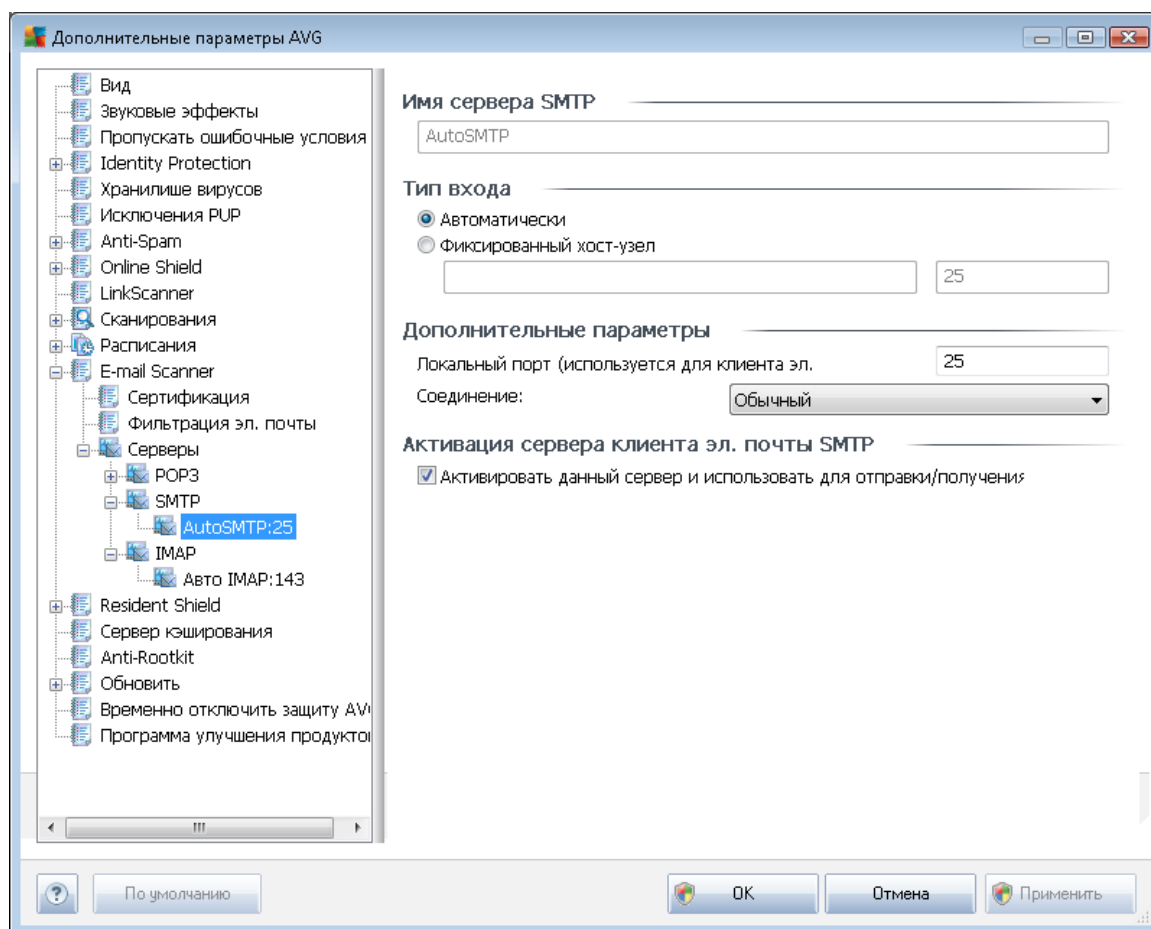


В данном диалоговом окне (открытом при выборе **Серверы/POP3**) можно установить новый сервер для компонента **E-mail Scanner** с помощью протокола POP3 для входящей почты.

- **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.
 - о **Автоматически.** Автоматическое выполнение входа в соответствии с параметрами электронной почты клиента.
 - о **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.aste.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.asme.com:8200*). Стандартным портом соединения POP3 является порт 110.

- **Дополнительные параметры.** Определение более подробных параметров.
 - о **Локальный порт.** Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом приложении необходимо указать данный порт в качестве порта соединения POP3.
 - о **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 эл. почты.** Установите или снимите флажок напротив этого элемента, чтобы активировать или деактивировать указанный сервер POP3.

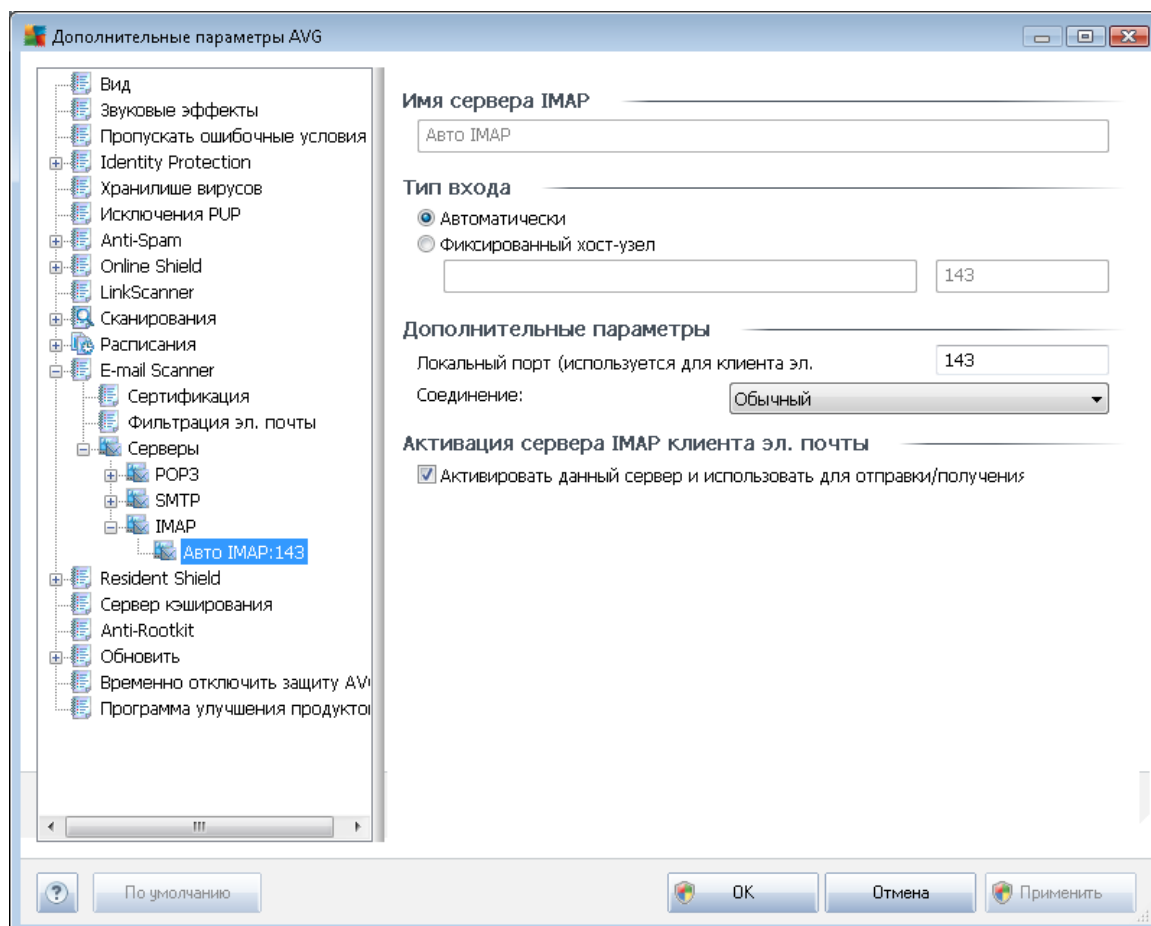


В данном диалоговом окне (открытом через **Серверы/SMTP**) можно настроить новый сервер



[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.
 - о **Автоматически.** Автоматическое выполнение входа в соответствии с параметрами клиента электронной почты.
 - о **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, *pop.acme.com:8200*). Номер стандартного порта соединения SMTP — 25.
- **Дополнительные параметры.** Определение более подробных параметров.
 - о **Локальный порт.** Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом клиенте необходимо указать данный порт в качестве порта соединения SMTP.
 - о **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 эл. 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.
 - о **Автоматически.** Автоматическое выполнение входа в соответствии с параметрами клиента электронной почты.
 - о **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, *pop.acme.com:8200*).

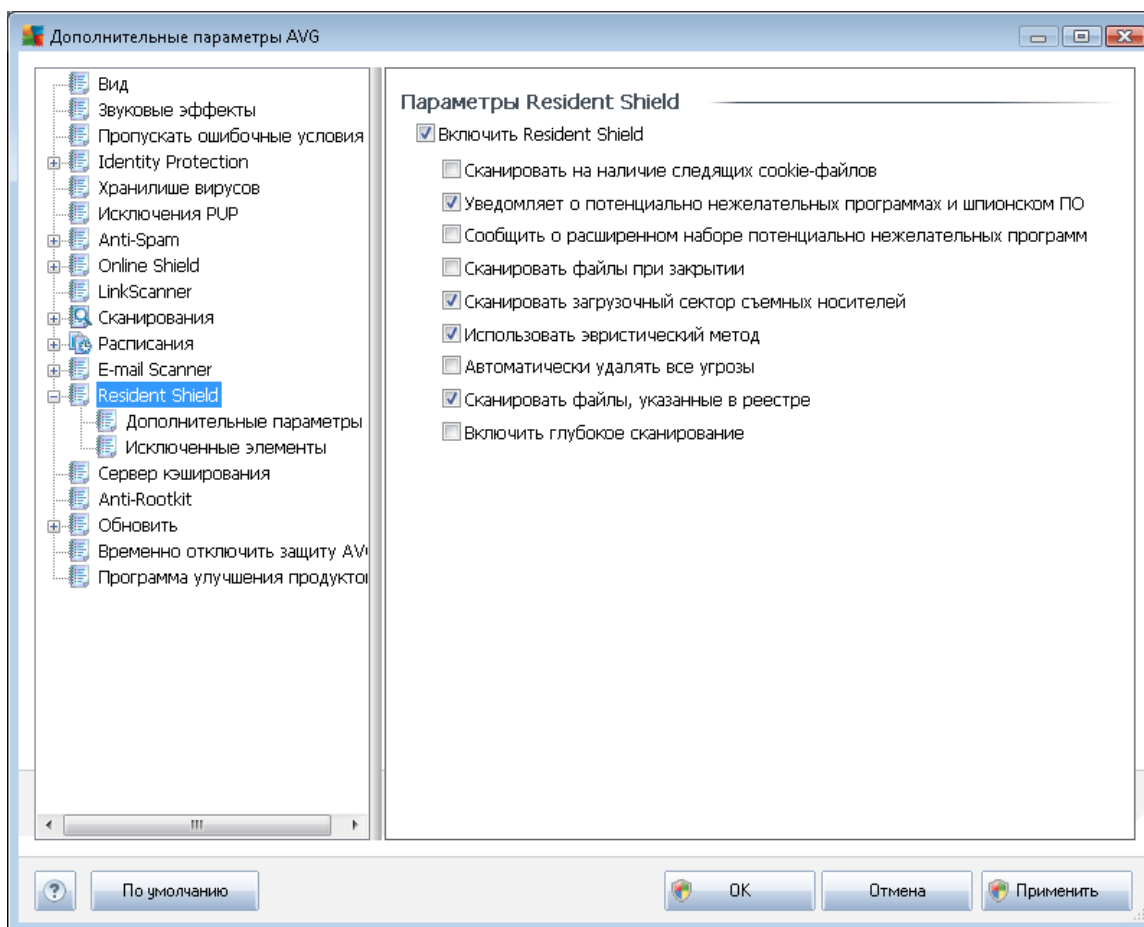


Стандартным портом соединения IMAP является порт 143.

- **Дополнительные параметры.** Определение более подробных параметров.
 - о **Локальный порт.** Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом клиенте необходимо указать данный порт в качестве порта соединения IMAP.
 - о **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 эл. почты.** Установите или снимите этот флажок, чтобы активировать или деактивировать указанный выше сервер SMTP.

9.13. Resident Shield

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





В диалоговом окне **Параметры Resident Shield** можно включить или отключить защиту, осуществляемую компонентом **Resident Shield**, установив или сняв флажок с параметра **Включить Resident Shield** (выбрано по умолчанию). Также можно выбрать функции компонента **Resident Shield**, которые необходимо активировать.

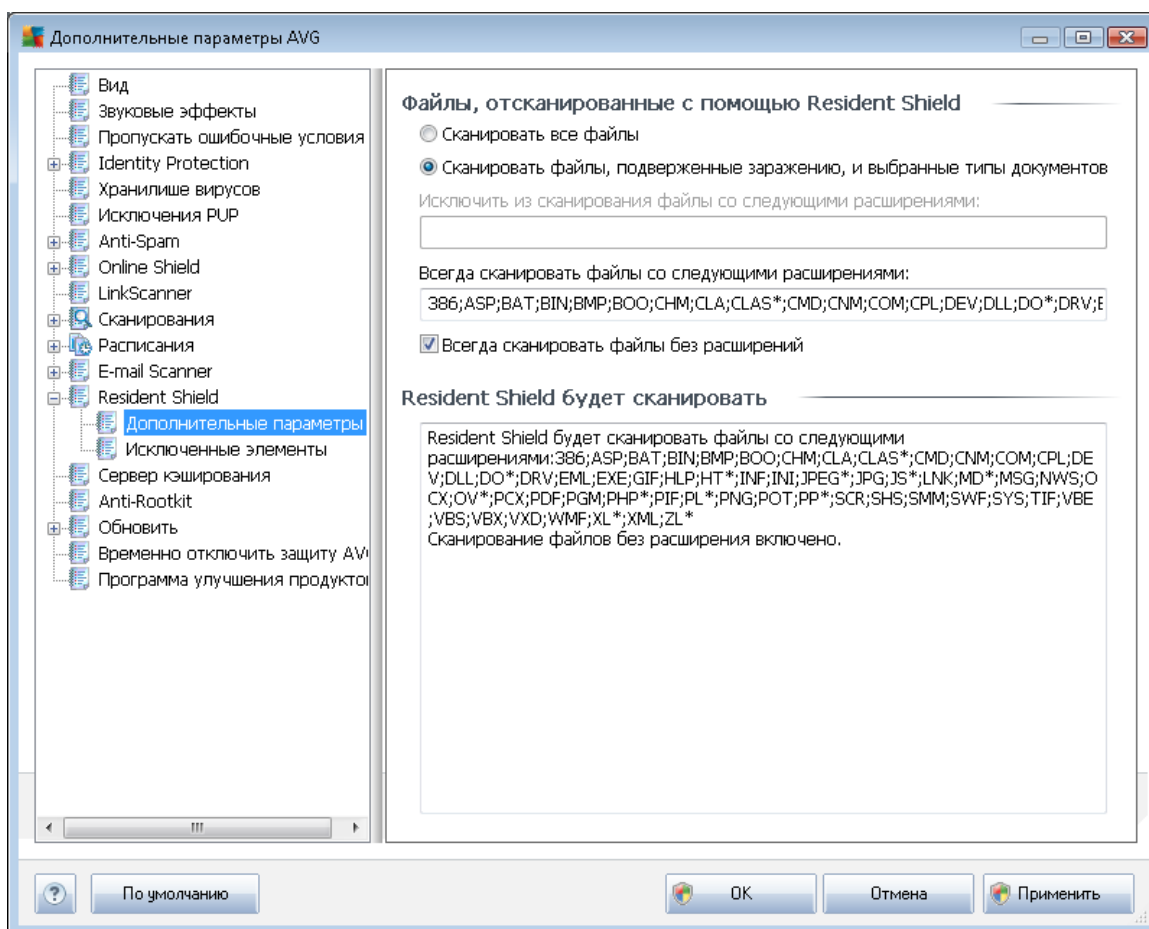
- **Сканировать на наличие следящих файлов cookie** (не выбрано по умолчанию). Данный параметр определяет обнаружение cookie-файлов при сканировании. (Файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержанием корзины для покупок в Интернете).
- **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 увеличить 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 законные программы, поэтому по умолчанию параметр отключен.
- **Сканировать файлы при закрытии** (не выбрано по умолчанию). Сканирование программой AVG активных объектов (например, приложений, документов...) при открытии, а также при закрытии. Данная функция помогает защитить компьютер от некоторых разновидностей самых опасных вирусов.
- **Сканировать загрузочный сектор съемных носителей** (выбрано по умолчанию)
- **Использовать эвристический анализ** (выбрано по умолчанию). **Эвристический анализ** будет использован для обнаружения (динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде).
- **Автоматически удалять все угрозы** (не выбрано по умолчанию). Любое обнаруженное заражение будет вылечено автоматически, если лечение возможно. Угрозы, которые невозможно вылечить, будут удалены.
- **Сканировать файлы, указанные в реестре** (выбрано по умолчанию). Данный параметр определяет, что программа AVG будет выполнять сканирование всех исполняемых файлов, добавляемых в реестр запуска, во избежание выполнения известных заражений при следующем запуске компьютера.
- **Включить глубокое сканирование** (не выбрано по умолчанию). В определенных случаях (в случае крайней необходимости) установите данный флажок, чтобы



активировать самые тщательные алгоритмы сканирования, которые будут максимально глубоко сканировать систему. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

9.13.1. Дополнительные параметры

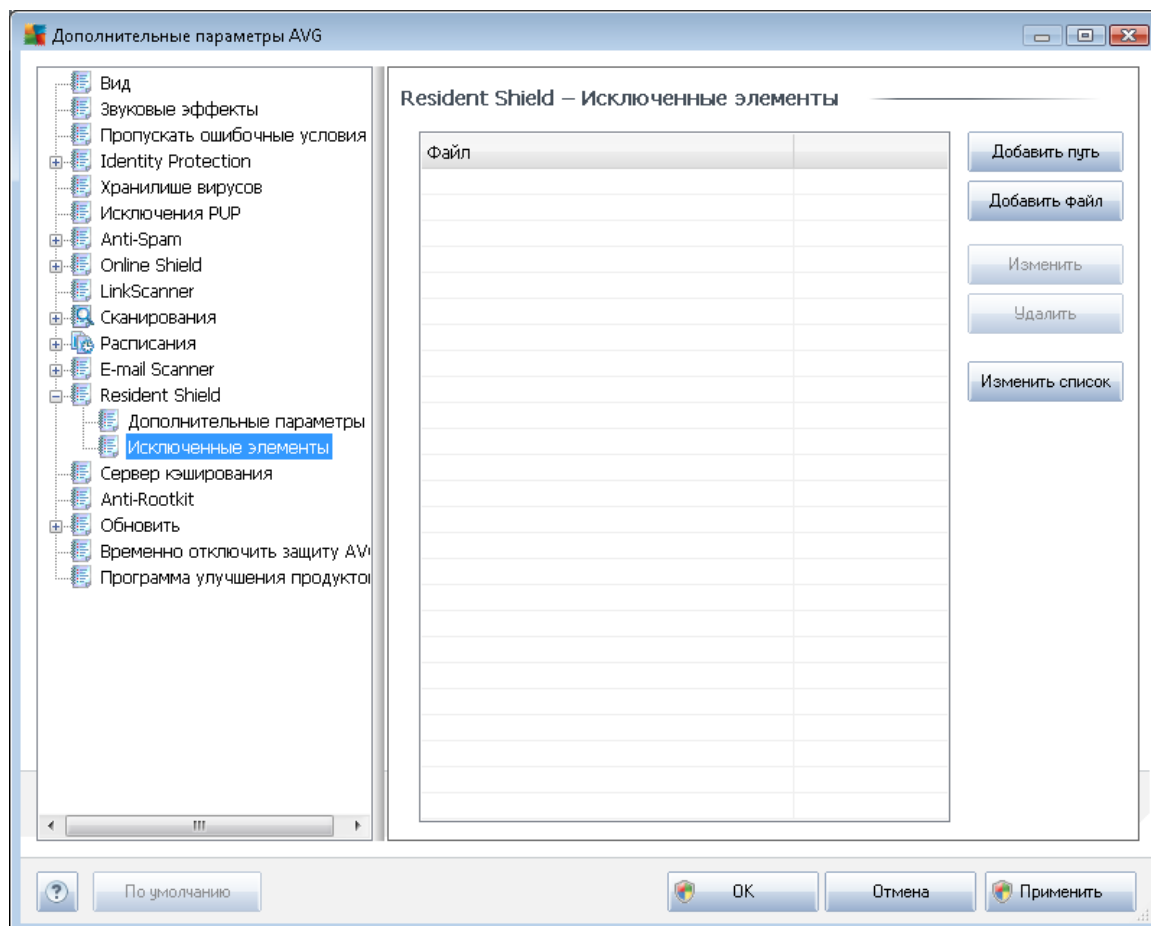
В диалоговом окне **Файлы, сканируемые с помощью Resident Shield** можно указать файлы, которые необходимо сканировать (по определенным расширениям).



Определение необходимости сканировать все файлы или только файлы, подверженные заражению. В данном случае далее можно указать список расширений, определяющих файлы, которые сканировать не нужно, а также список расширений файлов, которые необходимо сканировать в любом случае.

В разделе **Resident Shield просканируем** приводится сводка по текущим параметрам и отображаются подробные сведения об объектах, которые будут сканированы компонентом **Resident Shield**.

9.13.2. Исключенные элементы



В диалоговом окне **Resident Shield — исключенные элементы** можно определить файлы и/или папки, которые необходимо исключить из сканирования [Resident Shield](#).

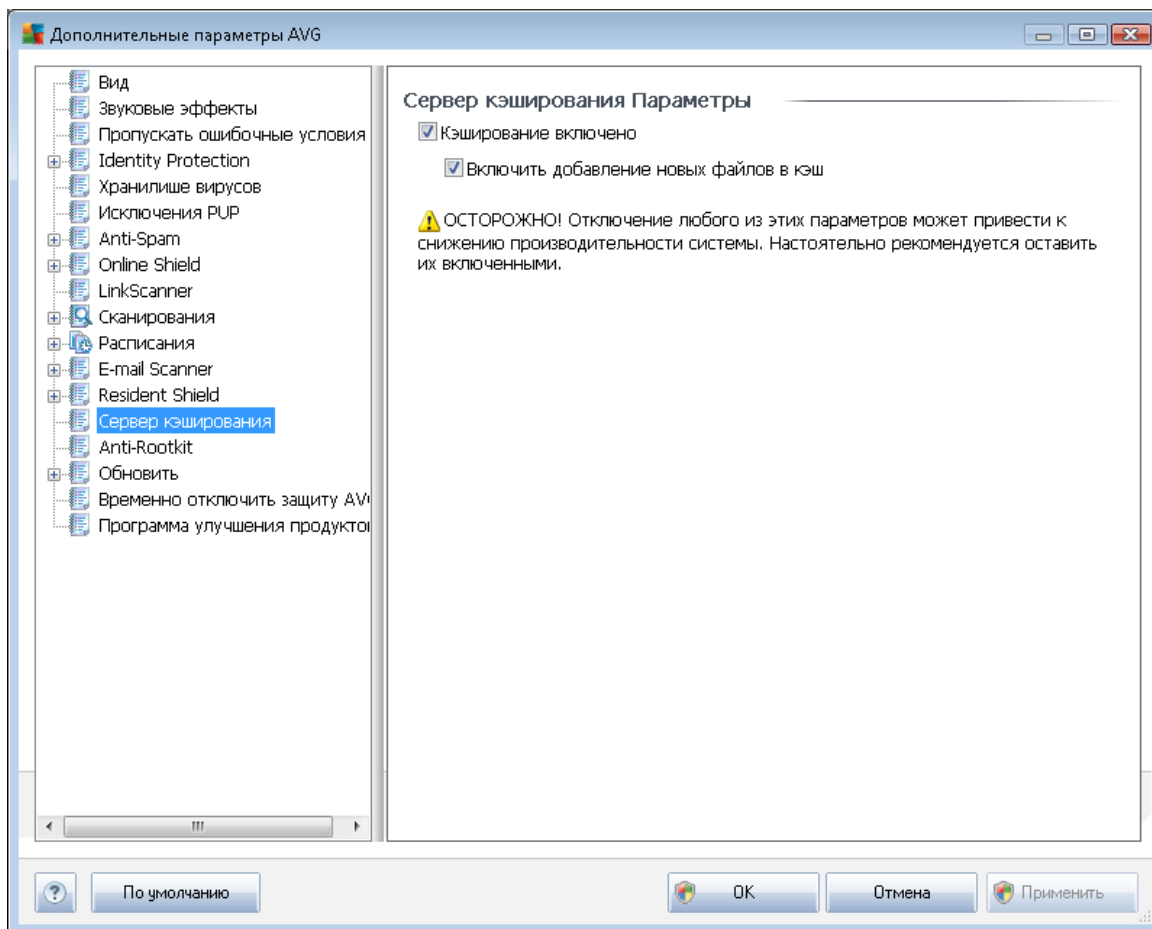
Настоятельно рекомендуется не исключать какие-либо элементы без необходимости.

В диалоговом окне содержатся следующие кнопки управления:

- **Добавить путь.** Укажите каталоги, которые должны быть исключены из сканирования, выбрав их последовательно в 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.

9.14. Сервер кэширования

Сервер кэширования — это процесс, позволяющий более быстро выполнять операции сканирования (*сканирование по требованию, запланированное сканирование всего компьютера, сканирование с помощью [Resident Shield](#)*). Он собирает и хранит информацию о надежных файлах (*системные файлы с цифровой подписью и т. д.*): затем эти файлы определяются как безопасные и пропускаются во время сканирования.



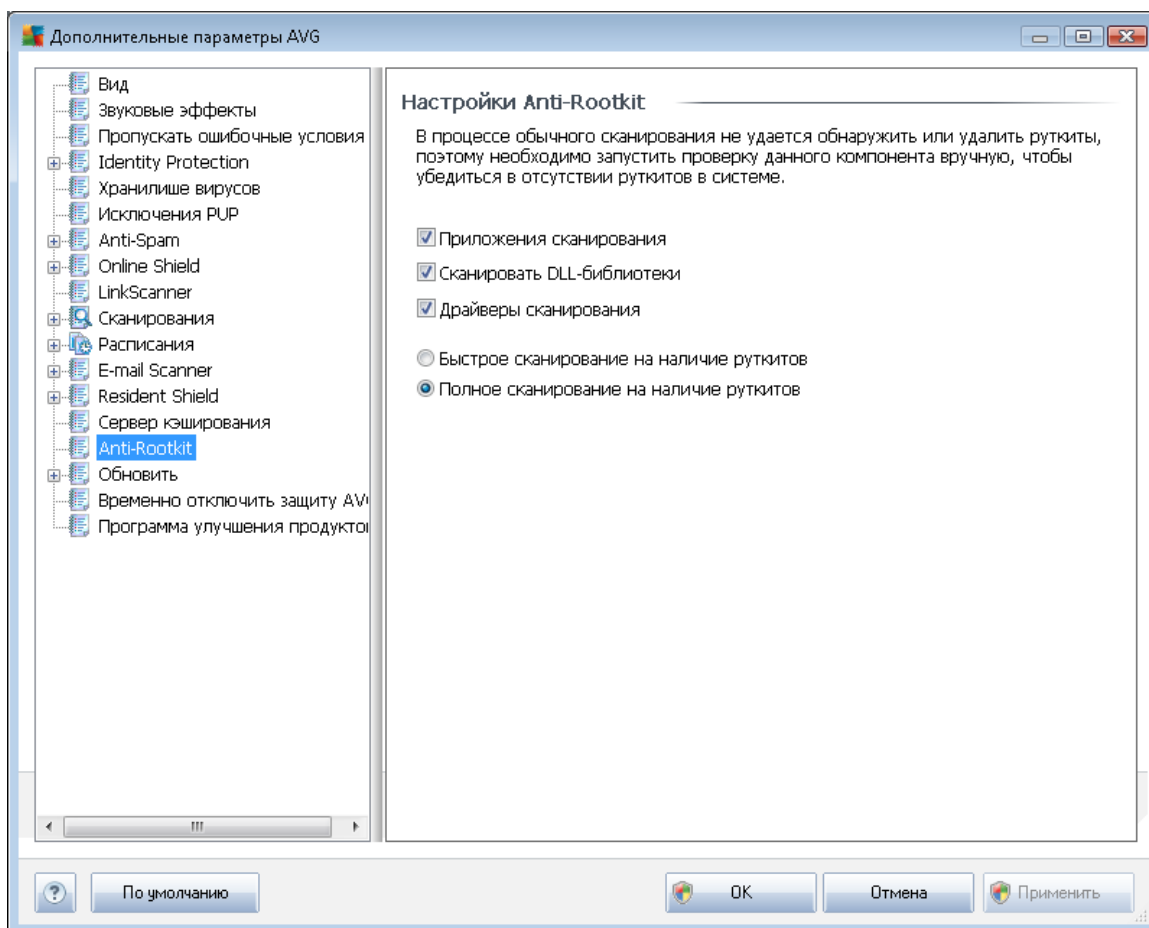
Диалоговое окно настройки содержит два параметра.

- **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.



9.15. Anti-Rootkit

С помощью данного диалогового окна можно изменить параметры компонента [Anti-Rootkit](#).



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

Чтобы указать объекты, которые должны сканироваться, установите соответствующие флажки.

- **Сканировать приложения**
- **Сканировать DLL-библиотеки**
- **Сканировать драйверы**

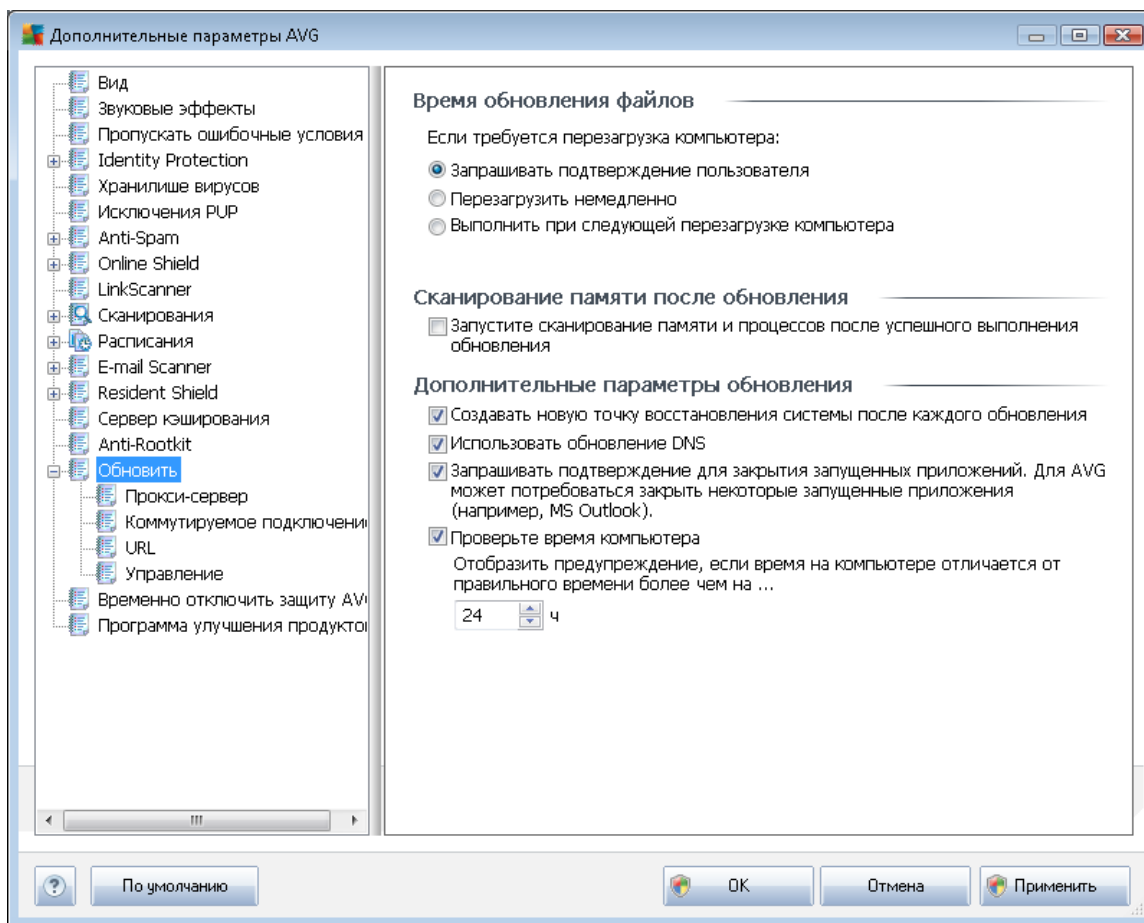
Далее можно включить режим сканирования на наличие средств rootkit.

- **Быстрое сканирование rootkits.** 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 приводов компакт-дисков).

9.16. 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 потребуются 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.** Завершение [процесса обновления](#) будет отложено до следующей перезагрузки. Помните, что данный параметр рекомендуется выбирать, только если компьютер включается регулярно, как минимум раз в день!

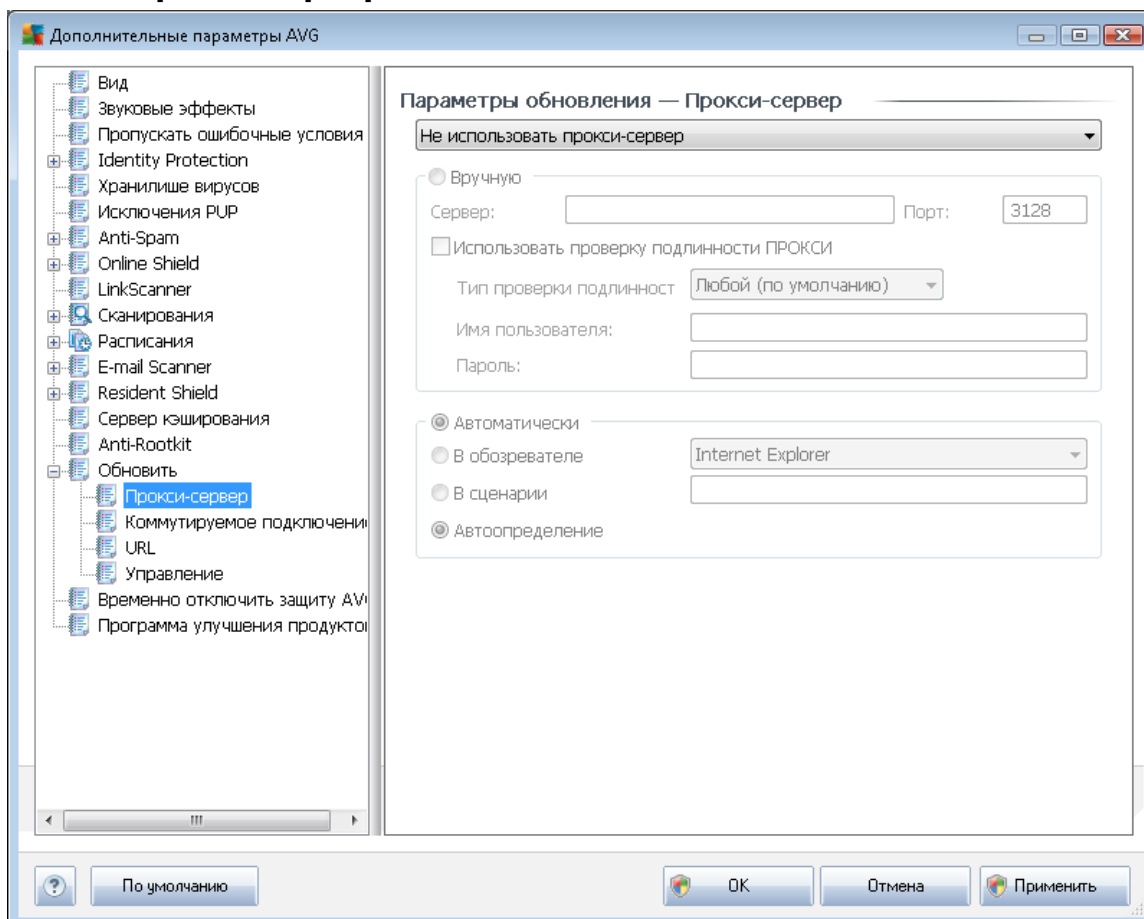
Сканирование памяти после обновления

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 Internet Security 2011** 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 (используется по умолчанию).** 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.

9.16.1. 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.** Параметр 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)

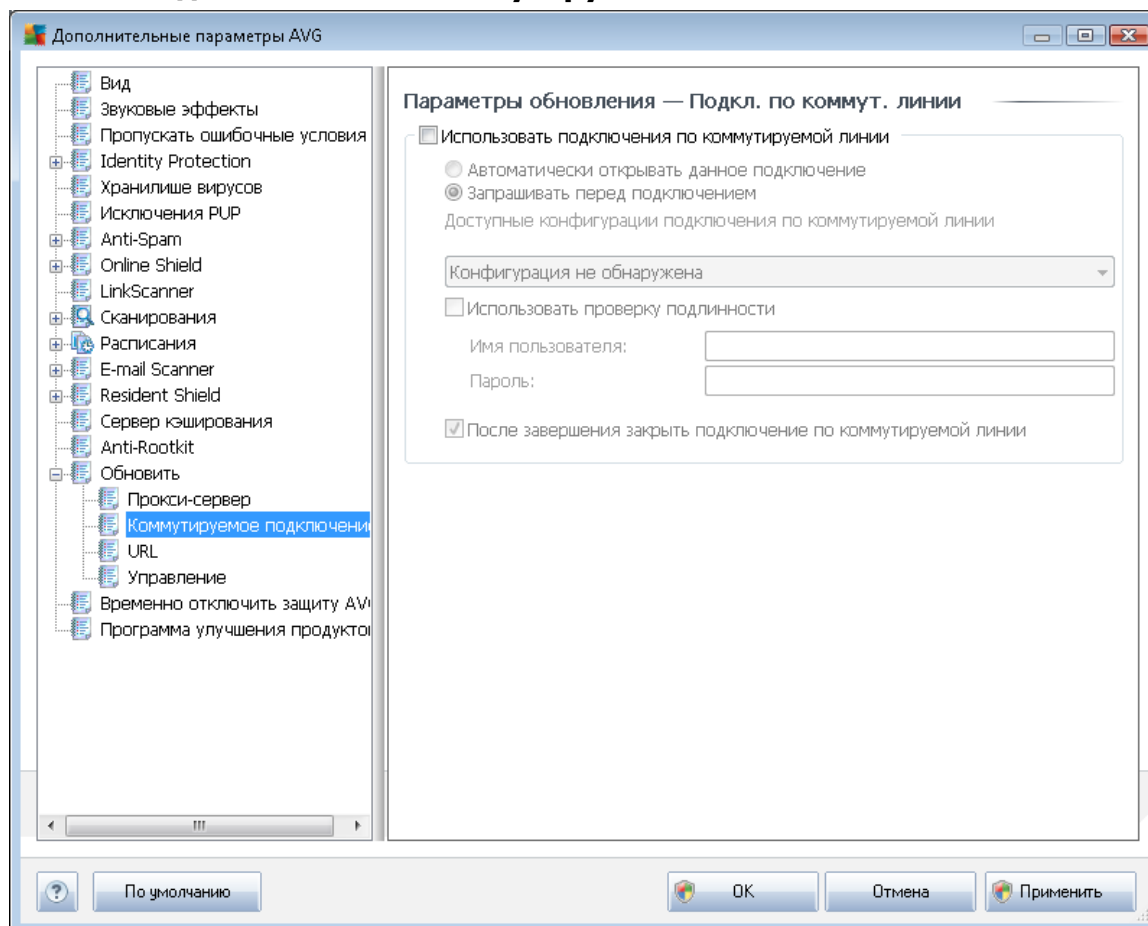
На прокси-сервере также могут быть заданы определенные правила для каждого пользователя. В этом случае установите флажок **Использовать проверку подлинности ПРОКСИ**, чтобы программа выполняла проверку подлинности имени пользователя и пароля перед подключением к Интернету через прокси-сервер.

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

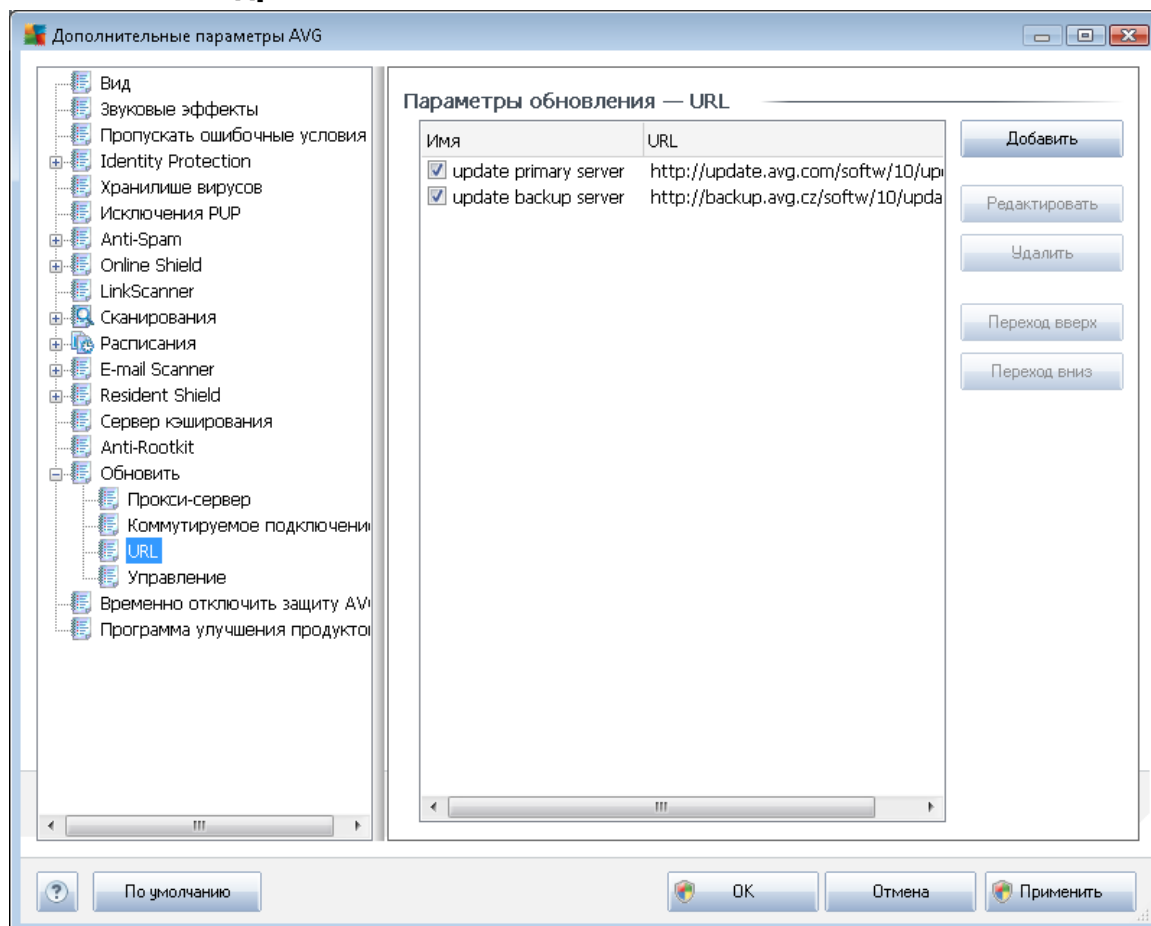
9.16.2. Подключение по коммутируемой линии



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**).

9.16.3. URL-адрес

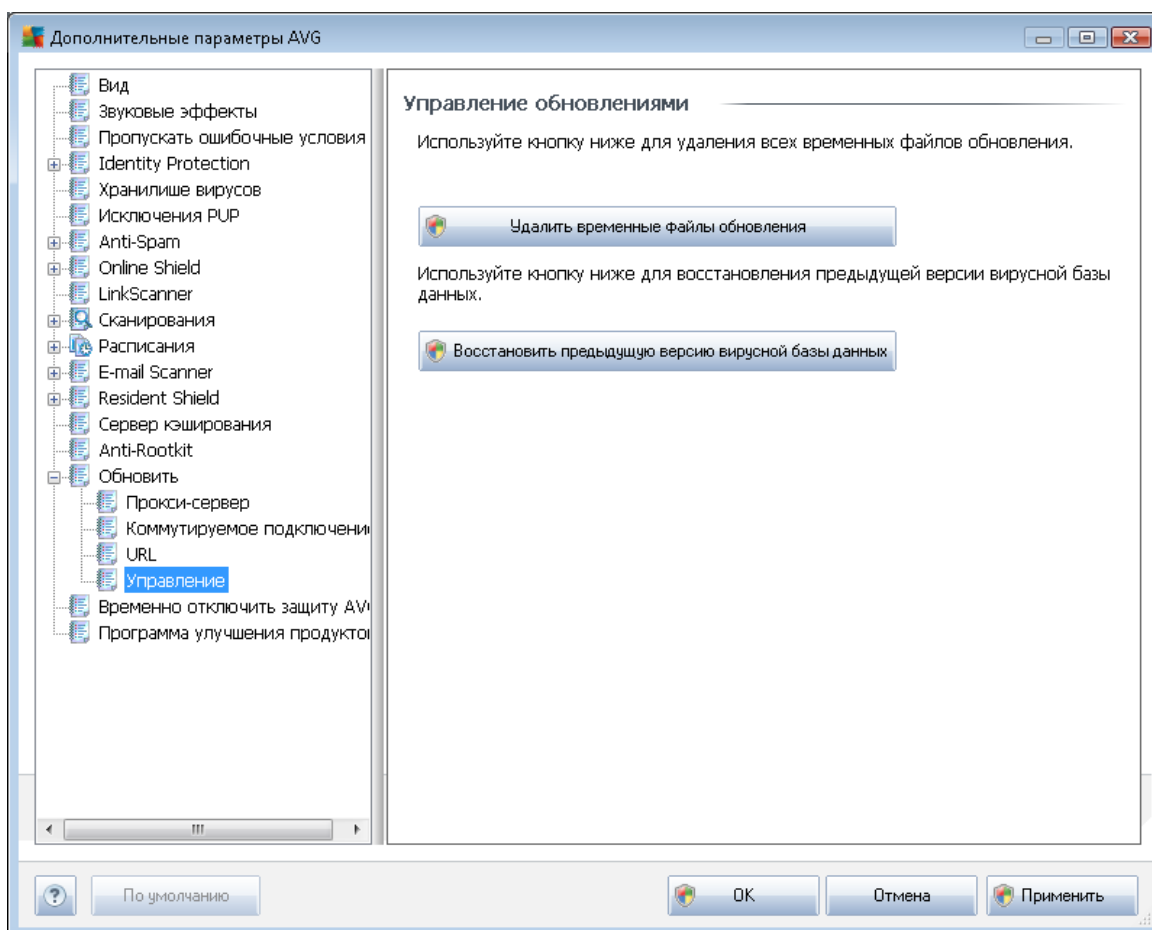


В диалоговом окне **URL-адрес** приведен список интернет-адресов, по которым можно загрузить файлы обновлений. Данный список и его элементы можно изменить с помощью следующих кнопок управления.

- **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.

9.16.4. Управление

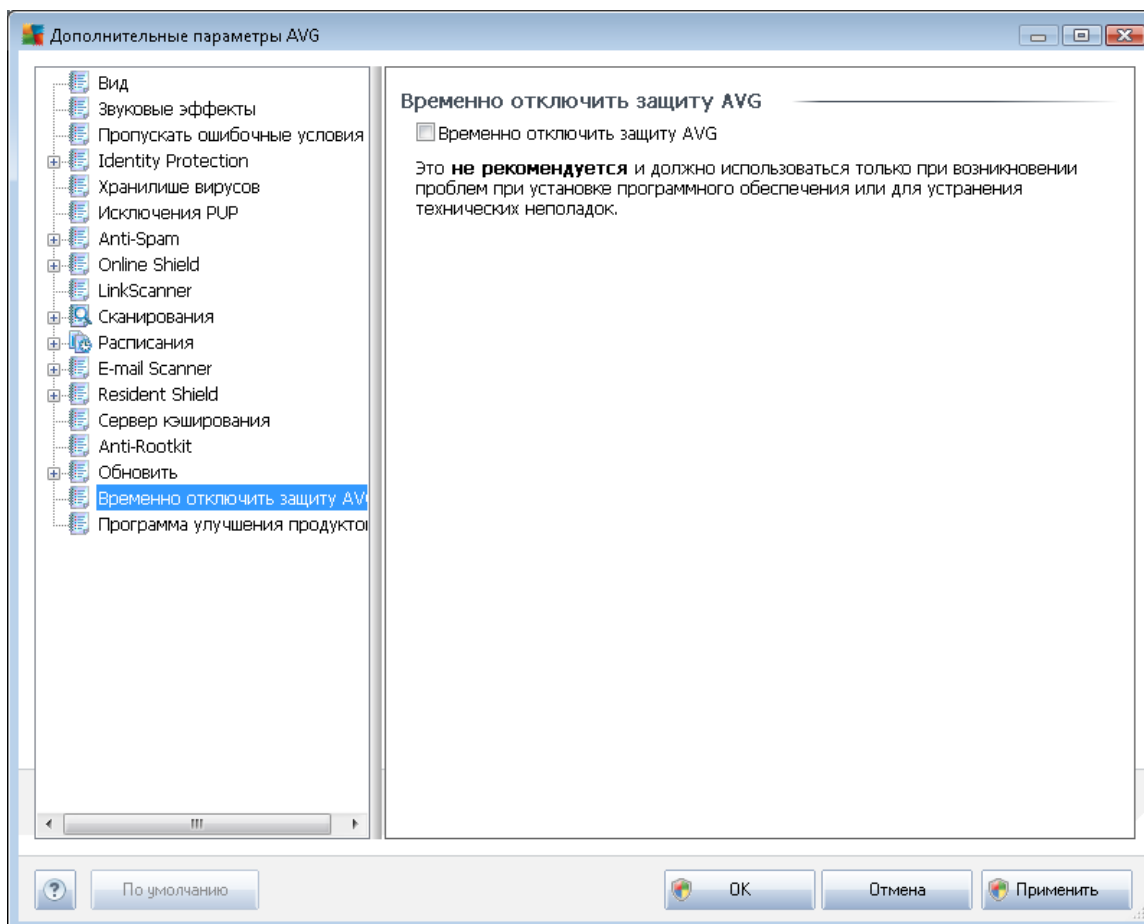
В диалоговом окне **Управление** доступны два параметра, доступ к которым можно получить с помощью двух кнопок.



- **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*).



9.17. Временное отключение защиты AVG



В диалоговом окне **Временное отключение защиты AVG** можно полностью выключить защиту, обеспечиваемую программой **AVG Internet Security 2011**.

Используйте данный параметр только в случае крайней необходимости!

В большинстве случаев программу AVG **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 проблемы, попробуйте сначала отключить компонент **Resident Shield**. Если вам пришлось временно отключить защиту AVG, включите ее, как только завершите установку. Если вы подключены к Интернету или локальной сети, но антивирусная защита выключена, ваш компьютер может подвергнуться атакам.

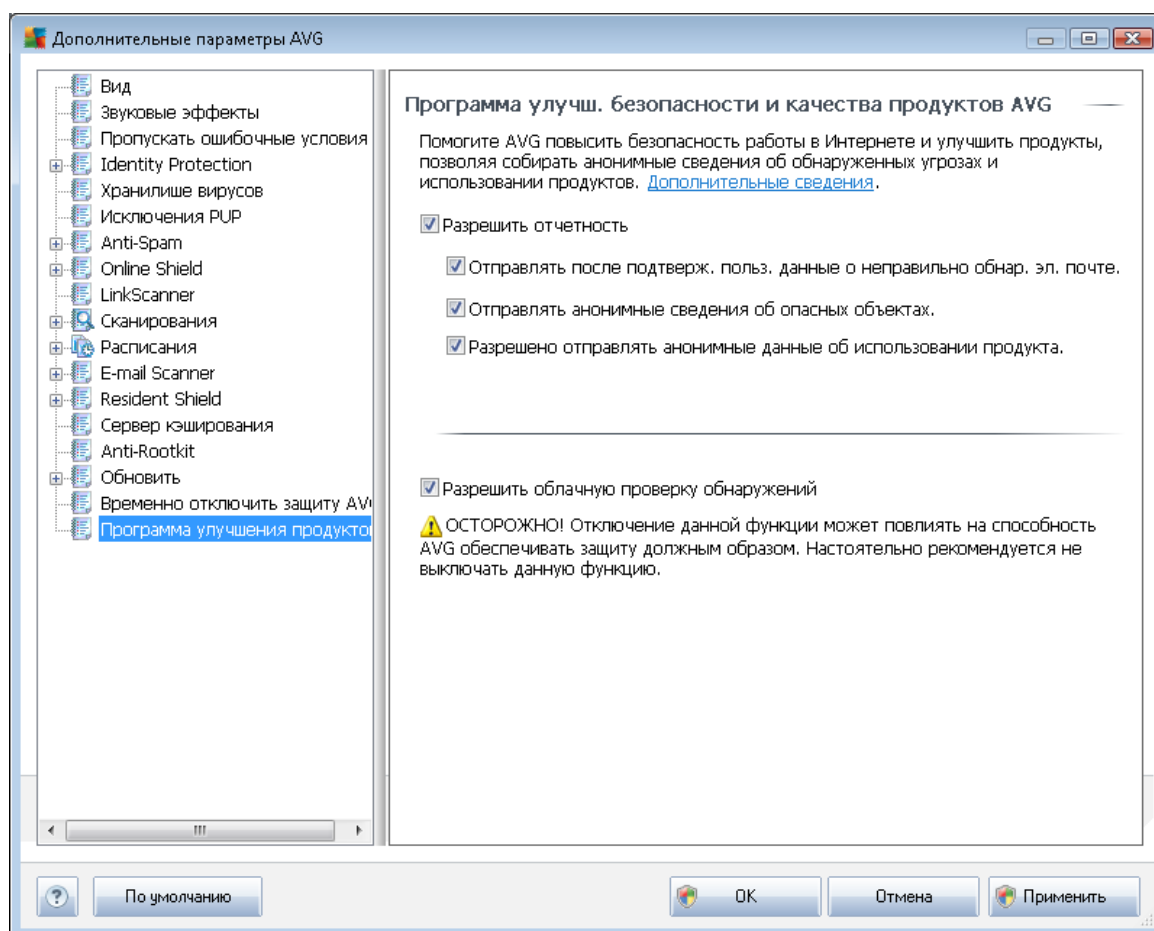
9.18. Программа улучшения продуктов

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



компанию 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. Личные данные не включаются в отчеты. Функция передачи отчетов об обнаруженных угрозах не является обязательной, однако рекомендуется включить данную функцию, так как она помогает совершенствовать защиту всех пользователей AVG.



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 Noax.** Данная угроза представляет собой нежелательное сообщение электронной почты, содержащее опасные, подозрительные или просто бесполезные сведения. Многие из вышеперечисленных угроз распространяются посредством сообщений электронной почты Noax.
- **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 этих видов угроз AVG включает в себя следующие специализированные компоненты:

- **[Anti-Virus](#)** для защиты компьютера от вирусов.
- **[Anti-Spyware](#)** для защиты компьютера от шпионского ПО.



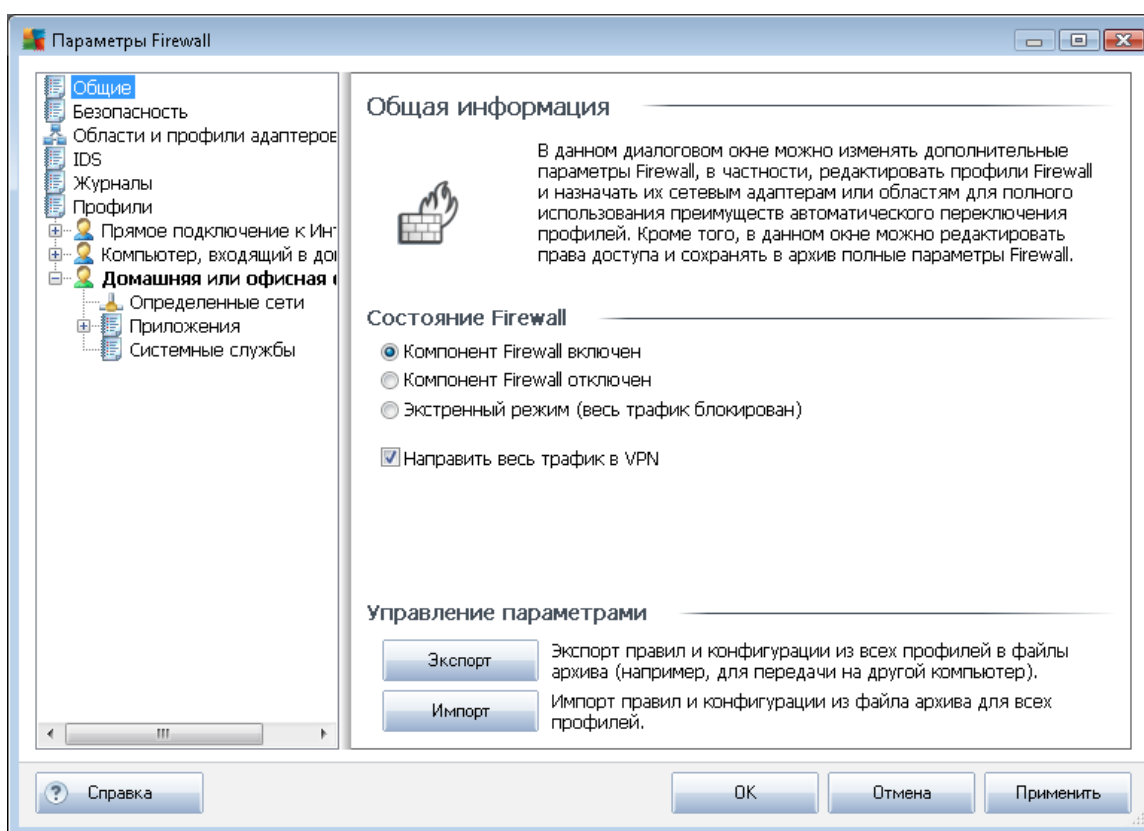
- [Online Shield](#) для защиты компьютера от вирусов и шпионского ПО при работе в Интернете.
- [LinkScanner](#) для защиты от других видов интернет-угроз, описанных в данном разделе.

10. Параметры Firewall

Конфигурация компонента **Firewall** открывается в новом окне, где с помощью нескольких диалоговых окон можно настроить дополнительные параметры компонента. **Настройка дополнительных параметров должна осуществляться только специалистами или опытными пользователями.**

10.1. Общие

Диалоговое окно **Общие сведения** содержит два раздела:



Состояние Firewall

В разделе **Состояние Firewall** можно изменить состояние компонента **Firewall** необходимым образом.

- **Firewall включен.** Выберите этот параметр, чтобы разрешить связь с приложениями, отмеченными как "разрешенные" в наборе правил, определенном в выбранном [профиле Firewall](#).
- **Firewall отключен.** Данный параметр полностью отключает компонент **Firewall**, весь сетевой трафик принимается без проверки.



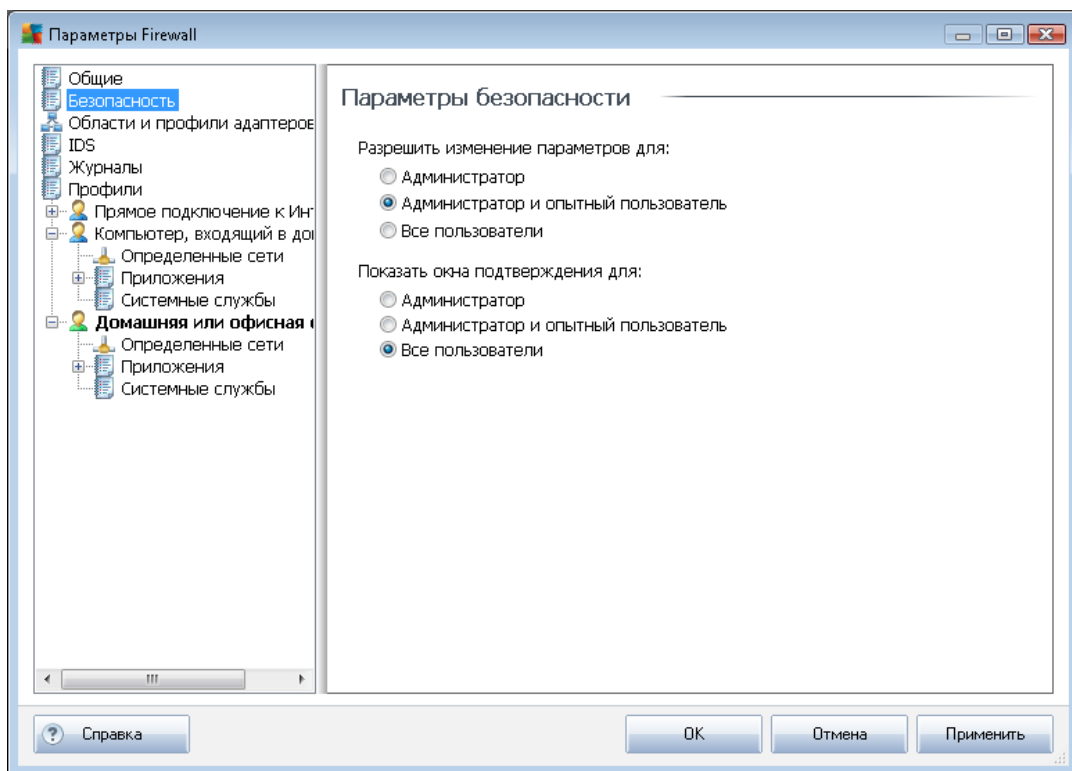
- **Экстренный режим** (блокировка всего интернет-трафика). Выберите данный параметр, чтобы блокировать трафик на всех сетевых портах; **Firewall** будет функционировать, однако прием трафика осуществляться не будет.
- **Направить весь трафик в VPN**. При использовании подключения VPN (виртуальная частная сеть), например, для подключения к офисному компьютеру с домашнего, рекомендуется установить данный флажок. **Компонент AVG Firewall** автоматически выполнит поиск среди сетевых адаптеров, найдет адаптеры, используемые для подключения VPN, и разрешит всем приложениям подключаться к целевой сети (применимо только к приложениям, которым не назначены определенные правила Firewall). В стандартной системе со стандартными сетевыми адаптерами этот простой шаг позволит избежать необходимости в настройке подробного правила для каждого приложения, которое необходимо использовать через VPN.

Примечание. Для полного включения VPN необходимо разрешить обмен данными следующим системным протоколам: GRE, ESP, L2TP, PPTP. Данную операцию можно выполнить в диалоговом окне Системные службы.

Управление параметрами

В разделе **Управление параметрами** можно выполнить **экспорт** или **импорт** конфигурации компонента **Firewall**, т. е. экспортировать определенные правила и параметры компонента **Firewall** в файл резервного копирования или импортировать целый файл резервного копирования.

10.2. Безопасность



Диалоговое окно **Параметры безопасности** позволяет определить общие правила поведения компонента **Firewall**, которые не зависят от выбранного профиля.

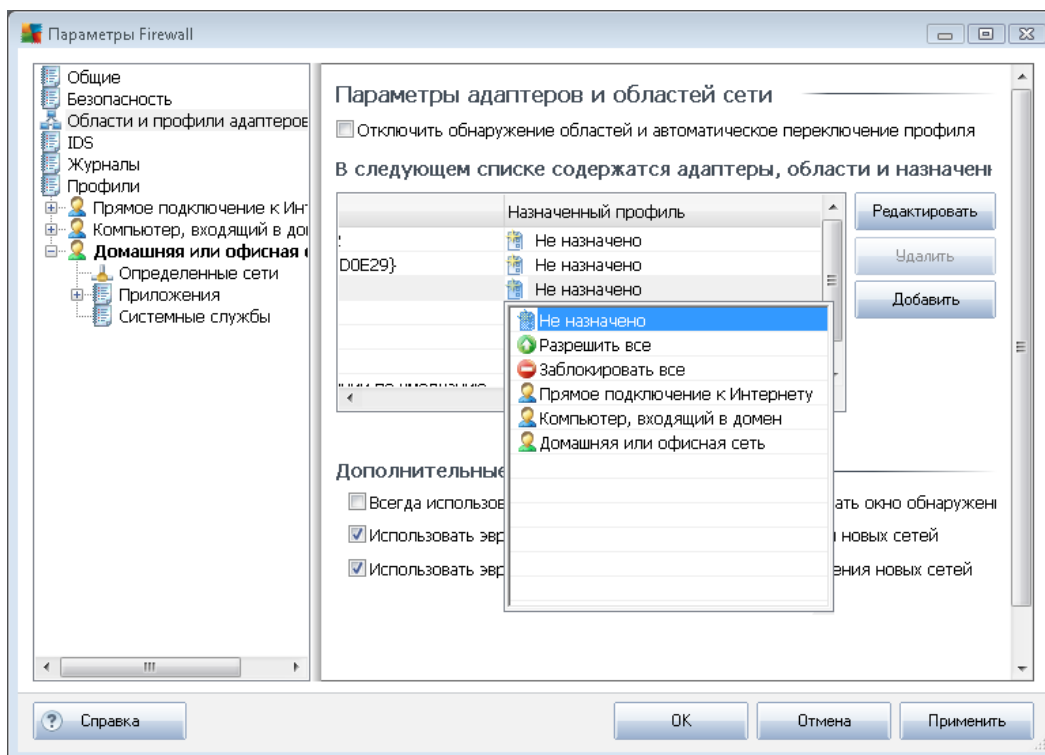
- **Разрешить изменение параметров** — позволяет определить лиц, которым разрешено изменять конфигурацию компонента **Firewall**
- **Показывать окно подтверждения** — позволяет определить лиц, для которых следует отображать диалоговые окна подтверждения (*диалоговые окна с вопросом о действии в ситуации, которая не определена в правиле компонента **Firewall***).

В обоих случаях одной из следующих групп пользователей может быть назначено специальное право.

- **Администратор** — полностью управляет ПК и имеет право назначать каждому пользователю в группах специально определенные права.
- **Администратор и опытный пользователь** — администратор может закрепить каждого пользователя за специальной группой (*Опытный пользователь*) и определить права всех членов группы.
- **Все пользователи** — другие пользователи, не закрепленные за какой-либо специальной группой.

10.3. Области и профили адаптеров

Диалоговые окна **Параметры адаптеров и областей сети** позволяют изменять параметры, относящиеся к определенным профилям конкретных адаптеров и соответствующих сетей.



- **Отключить обнаружение областей и автоматическое переключение профилей.** Один из определенных профилей может быть назначен каждому типу сетевого интерфейса, а также каждой области. В противном случае будет использоваться один общий профиль. Однако, если вы решили разделить профили и назначить их определенным адаптерам и областям, а затем по какой-либо причине хотите временно отключить данную настройку, установите флажок **Отключить обнаружение областей и автоматическое переключение профилей**.
- **Список адаптеров, областей и назначенных профилей.** В данном списке содержится обзор обнаруженных адаптеров и областей. Каждому из них можно назначить специальный профиль из меню определенных профилей. Чтобы открыть данное меню, щелкните соответствующий элемент в списке адаптеров и выберите профиль.

Дополнительные параметры

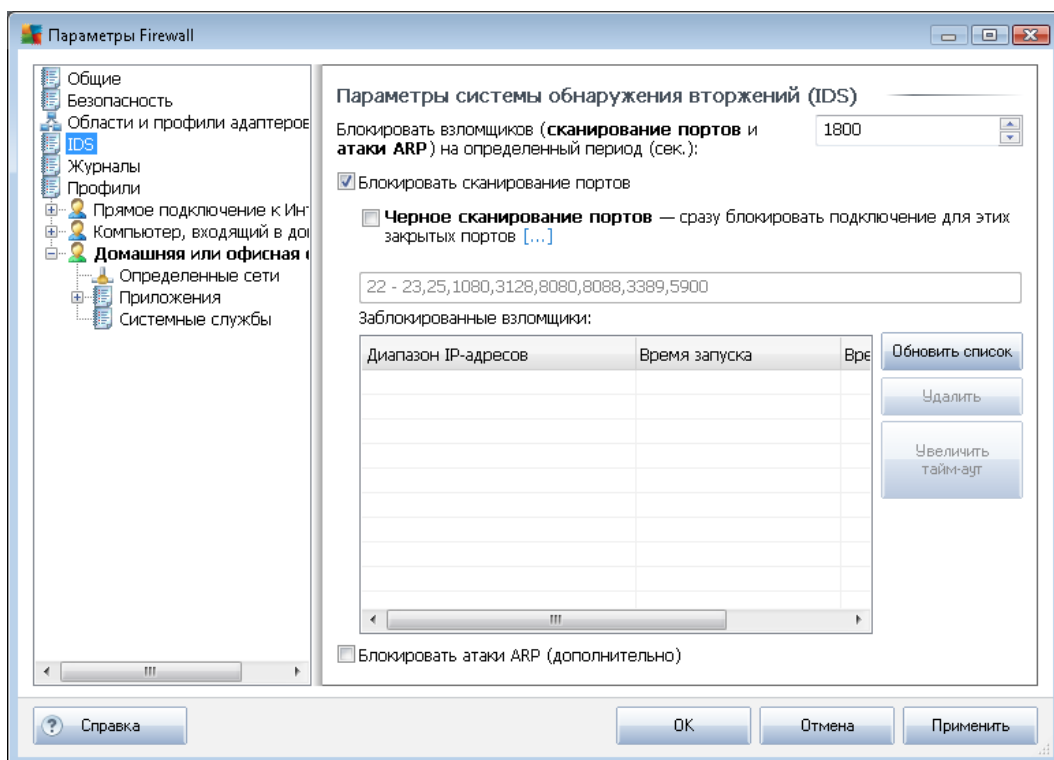
- о **Всегда использовать профиль по умолчанию и не отображать диалоговое окно обнаружения новой сети.** При подключении компьютера к новой сети [Firewall](#) оповестит вас об этом, после чего отобразится диалоговое

окно с запросом на выбор типа сетевого подключения и назначение [профиля Firewall](#). Чтобы данное диалоговое окно не отображалось, установите данный флажок.

- o **Использовать эвристический анализ AVG для обнаружения новых сетей**. Позволяет получать информацию о новых обнаруженных сетях с помощью специального механизма компании AVG (однако данный параметр доступен только при использовании ОС Vista или более поздней версии операционной системы).
- o **Использовать эвристический анализ Microsoft для обнаружения новых сетей**. Позволяет получать информацию о новых обнаруженных сетях из службы Windows (данный параметр доступен только при использовании ОС Windows Vista или более поздней версии операционной системы).

10.4. IDS

Система обнаружения вторжений — это специальная функция анализа поведения, предназначенная для определения и блокировки подозрительных попыток подключения через определенные порты компьютера. В следующем интерфейсе можно настроить параметры IDS.



В диалоговом окне **Параметры системы обнаружения вторжений (IDS)** доступны следующие параметры:

- **Блокировать взломщиков на определенный период**. Данный параметр позволяет установить количество времени в секундах, в течение которого будет блокироваться

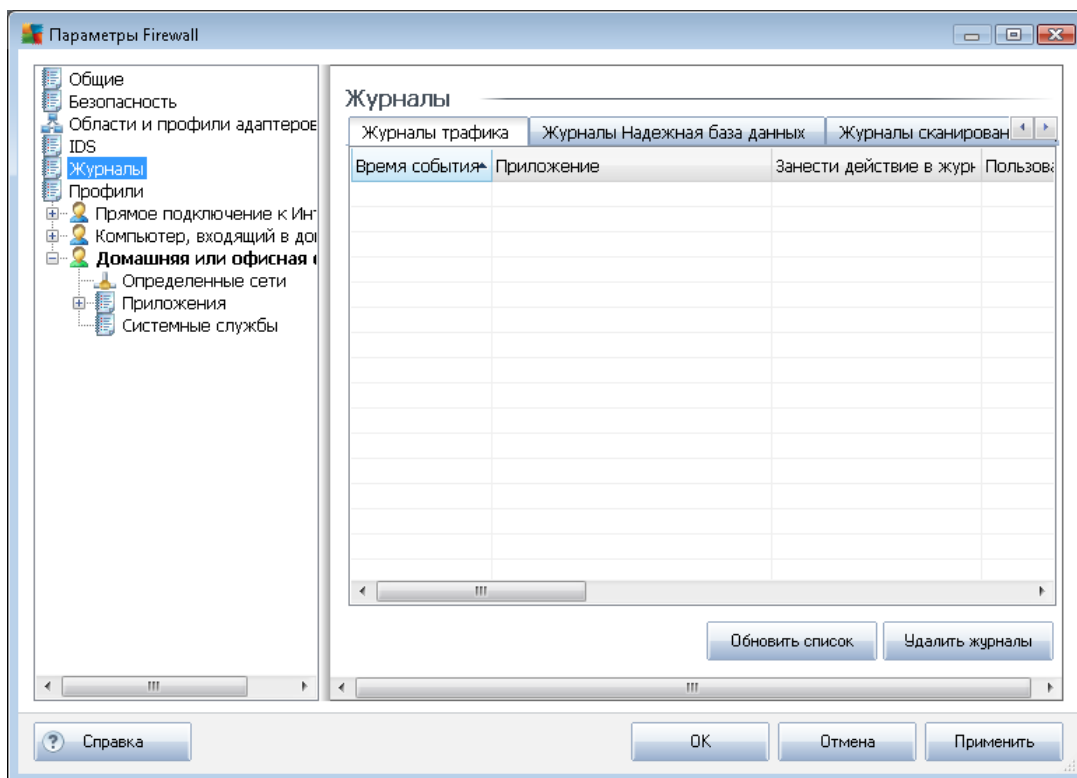
порт при обнаружении подозрительных попыток подключения. По умолчанию установлен интервал 1800 секунд (30 минут).

- **Блокировать сканирование портов.** Установите данный флажок, чтобы блокировать попытки подключения через все порты TCP и UDP, исходящие из внешних сетей. В случае подобных подключений допускается пять попыток, а на шестую приходится блокировка.
 - о **Сканирование черных портов.** Установите данный флажок, чтобы немедленно блокировать любые попытки подключения через порты, указанные в текстовом поле ниже. Отдельные порты или диапазоны портов необходимо указывать через запятую. При использовании данной функции можно воспользоваться списком рекомендуемых портов.
 - о **Заблокированные взломщики.** В данном разделе перечислены попытки подключения, которые были заблокированы компонентом [Firewall](#). Полную историю заблокированных попыток подключения см. в диалоговом окне [Журналы](#) (на вкладке Журналы сканирования портов).
- **Блокировать атаки ARP.** Активация блокировки специальных подключений в локальной сети, определенных **IDS** как потенциально опасные. Будет применено значение времени, установленное для параметра **Блокировать взломщиков на определенный период**. Данную функцию рекомендуется использовать только опытным пользователям, знакомым с типом и уровнем риска их локальной сети.

Кнопки управления

- **Обновить список.** Нажмите данную кнопку, чтобы обновить список (внести записи о последних событиях).
- **Отменить.** Нажмите данную кнопку, чтобы отменить блокировку выбранных элементов.
- **Увеличить тайм-аут.** Нажмите данную кнопку, чтобы продлить период времени, в течение которого будет блокироваться выбранная попытка подключения. Откроется новое диалоговое окно дополнительных параметров, в котором можно установить определенные дату и время или убрать ограничение блокировки по времени.

10.5. Журналы



В диалоговом окне **Журналы** можно просмотреть список всех действий и событий компонента **Firewall**, занесенных в журнал, с подробным описанием соответствующих параметров (*время события, имя приложения, соответствующее действие журнала, имя пользователя, идентификатор процесса, направление трафика, тип протокола, номера удаленных и локальных портов и т. п.*) на четырех вкладках.

- **Журналы трафика.** Сведения об активности всех приложений, которые выполняли попытки подключиться к сети.
- **Журналы надежных баз данных.** *Надежная база данных* — это внутренняя база данных AVG, содержащая сведения о сертифицированных и надежных приложениях, которым всегда разрешен доступ в Интернет. Когда новое приложение первый раз пытается подключиться к сети (*т. е. для него еще не создано правило брандмауэра*), необходимо разрешить или запретить возможность доступа к сети для этого приложения. Сначала AVG выполняет поиск в *надежной базе данных* и, если приложение присутствует в списке, доступ к сети будет предоставлен автоматически. Если в базе данных отсутствуют сведения о данном приложении, отобразится запрос в отдельном окне, в котором необходимо определить, разрешить ли доступ в сеть для данного приложения.
- **Журналы сканирования портов.** Сведения обо всех событиях **системы обнаружения вторжений**.
- **Журналы ARP.** Сведения о случаях блокировки определенных типов попыток

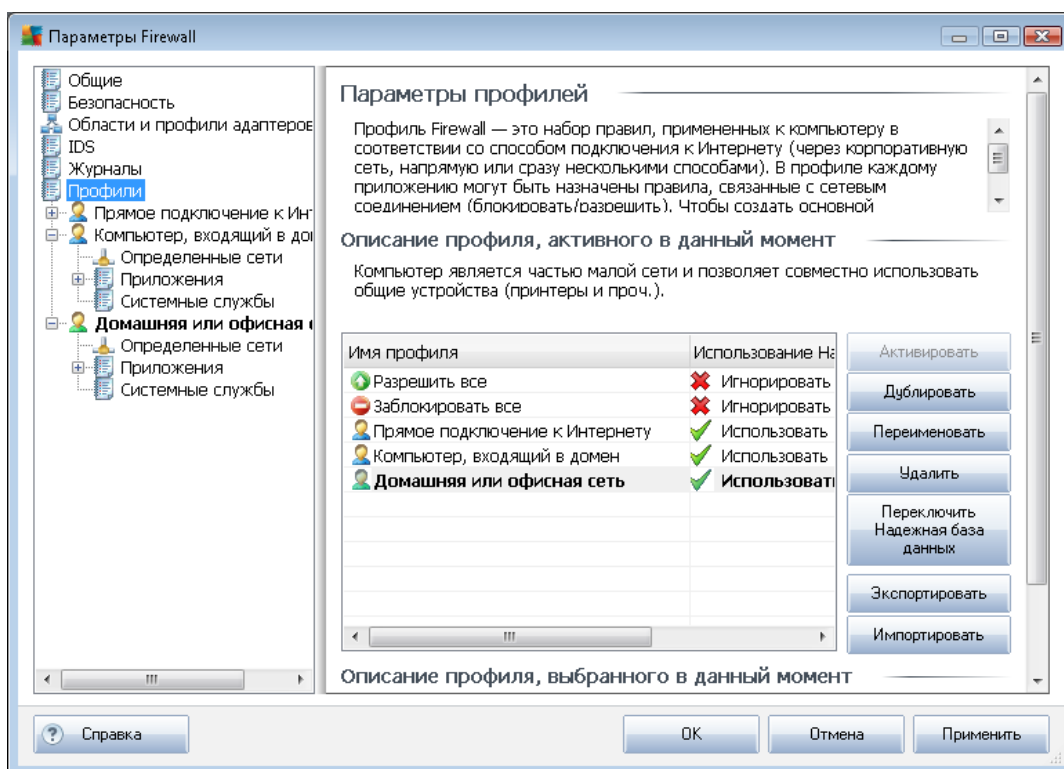
подключения в локальной сети (параметр [Блокировать атаку ARP](#)), обнаруженных и определенных [системой обнаружения вторжений](#) как потенциально опасные.

Кнопки управления

- **Обновить список** . Все записанные в журнале параметры можно упорядочить по выбранному атрибуту: хронологически (*по дате*) или в алфавитном порядке (*другие столбцы*) — просто щелкните заголовок соответствующего столбца. Используйте кнопку **Обновить список**, чтобы обновить отображаемую информацию.
- **Очистить список**. Удаление всех записей в таблице.

10.6. Профили

В диалоговом окне **Параметры профиля** находится список всех доступных профилей.



[Профили](#), отличные от системных, можно редактировать непосредственно в этом диалоговом окне с помощью следующих кнопок управления.

- **Активировать профиль** Данная кнопка активирует выбранный профиль, что означает, что компонент [Firewall](#) будет использовать выбранную конфигурацию профиля для контроля интернет-трафика.
- **Дублировать профиль**. Создание идентичной копии выбранного профиля; в дальнейшем копию можно изменить и переименовать для создания нового профиля на



основе дублированного.

- **Переименовать профиль.** Позволяет определить новое имя для выбранного профиля.
- **Удалить профиль.** Позволяет удалить выбранный профиль из списка.
- **Переключить надежную базу данных.** Использование сведений из *надежной базы данных* для указанного профиля (*Надежная база данных — это внутренняя база данных AVG, содержащая сведения о сертифицированных и надежных приложениях, которым всегда разрешен доступ в Интернет.*).
- **Экспортировать профиль.** Запись конфигурации выбранного профиля в файл, который будет сохранен для использования в дальнейшем.
- **Импортировать профиль.** Настройка параметров выбранного профиля на основе данных, экспортированных из резервного файла настройки.

В нижнем разделе диалогового окна расположено описание профиля, выбранного в настоящее время в списке выше.

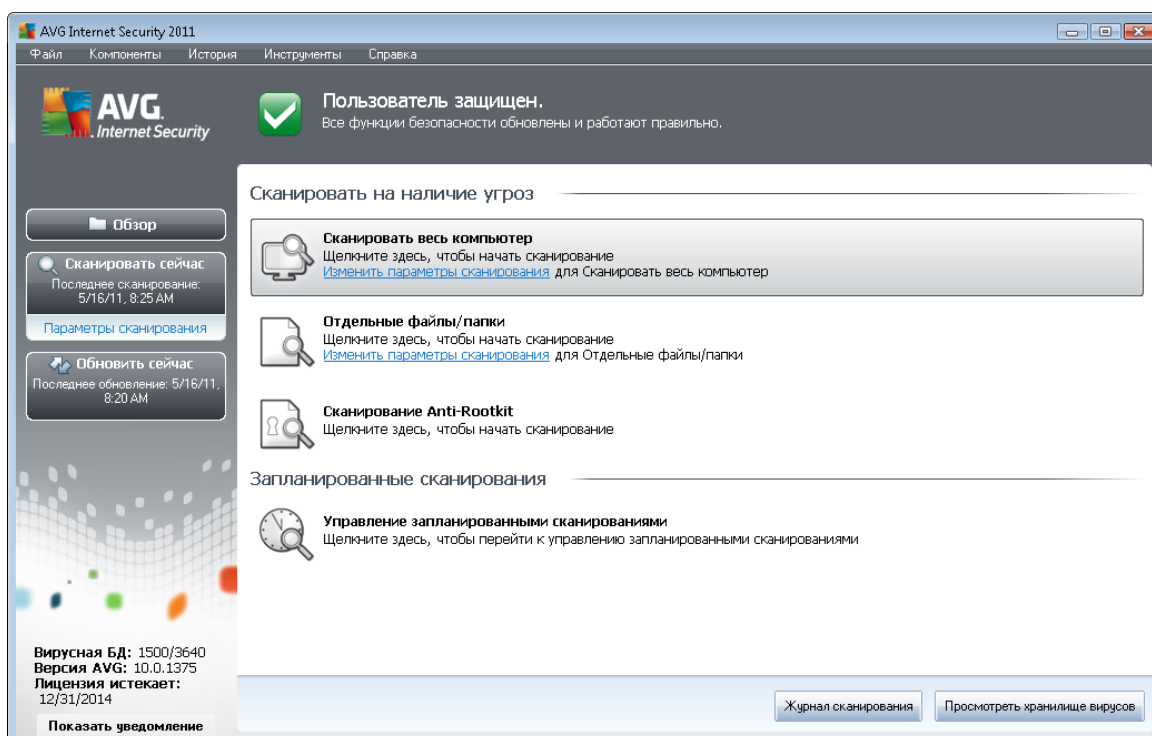
В зависимости от количества определенных профилей, содержащихся в списке диалогового окна **Профиль**, меню навигации слева изменится соответствующим образом. Каждый определенный профиль создает отдельную ветвь под элементом **Профиль**. Определенные профили затем можно редактировать в следующих диалоговых окнах (*идентичны для всех профилей*).



11. Сканирование AVG

Сканирование — это одна из важнейших функций **AVG Internet Security 2011**. Можно выполнять проверки по требованию или [планировать их периодический запуск](#) в удобное для вас время.

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:
 - о [Сканирование всего компьютера](#)
 - о [Сканировать отдельные файлы или папки](#)
 - о [Сканирование Anti-Rootkit](#)
- [Раздел Расписание сканирования](#). В данном разделе можно настроить новые проверки и создать новые расписания 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 Internet Security 2011** — 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.

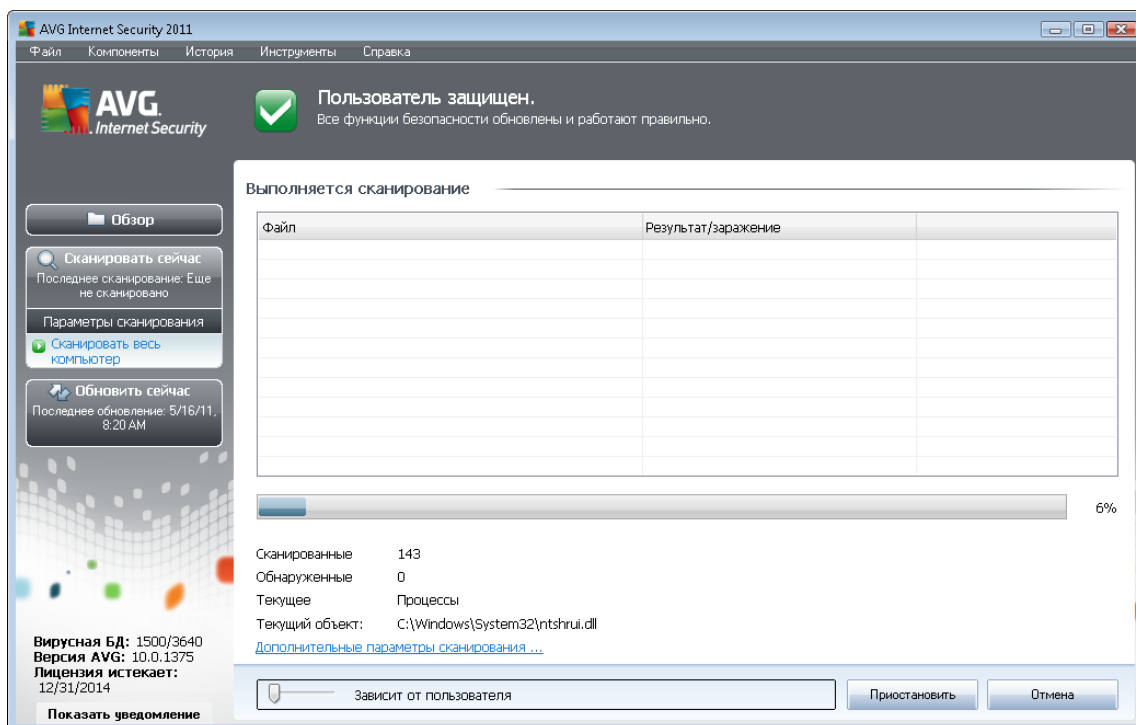
В системе **AVG Internet Security 2011** доступны следующие типы сканирования, настроенные поставщиком программного обеспечения.

11.2.1. Сканирование всего компьютера

Сканировать весь компьютер. 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.

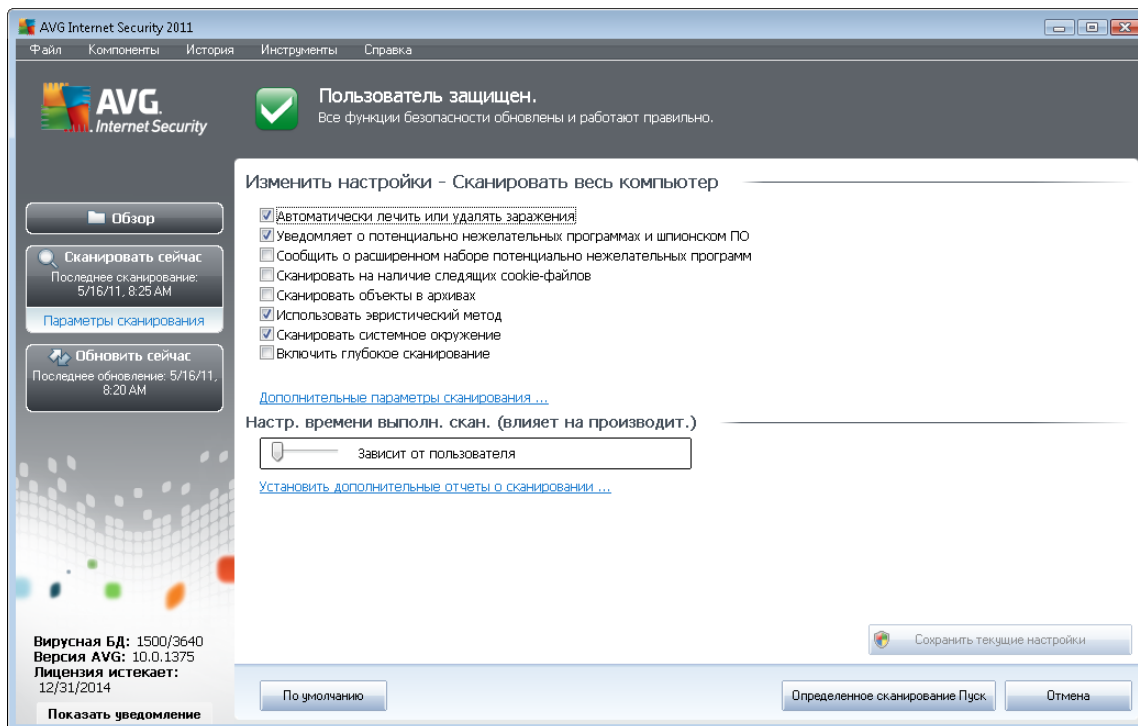
Запуск сканирования

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

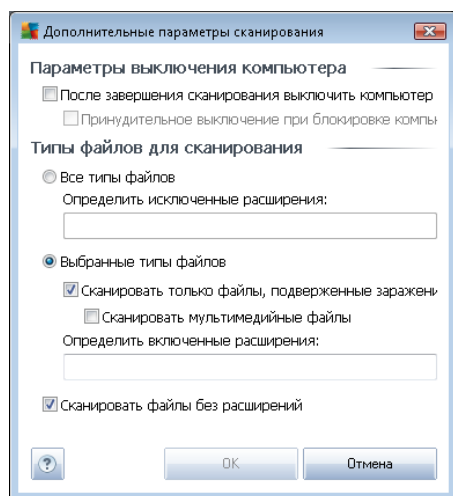
Существует возможность изменения предварительно определенных параметров **сканирования всего компьютера**. Нажмите ссылку **Изменить параметры сканирования** для открытия диалогового окна **Изменение параметров сканирования для сканирования всего компьютера** (доступно через [интерфейс сканирования](#) 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.

- о **Автоматически лечить или удалять заражения** (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](#).
- о **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.
- о **Уведомлять о расширенном наборе потенциально нежелательных программ** (не установлено 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 законные программы, поэтому по умолчанию параметр отключен.

- о **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).
 - о **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.
 - о **Использовать эвристический анализ** (выбрано по умолчанию). Эвристический анализ (динамичная эмуляция команд сканированных объектов в среде виртуального компьютера) является одним из способов, используемых для обнаружения вирусов при сканировании.
 - о **Сканировать системную среду** (не выбрано по умолчанию). При сканировании также будут проверены системные области компьютера.
 - о **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.



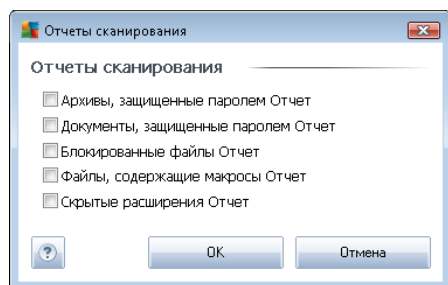
- о **Параметры выключения компьютера.** Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (**Выключить компьютер после завершения сканирования**) становится доступен новый параметр,

позволяющий выключать компьютер, даже если он заблокирован (**Принудительное выключение при блокировке компьютера**).

о **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 потребуется изменить конфигурацию по умолчанию параметра **Сканирование всего компьютера**, можно затем сохранить новые параметры в качестве конфигурации по умолчанию, чтобы они



использовалась каждый раз при сканировании всего компьютера.

11.2.2. Сканирование отдельных файлов или папок

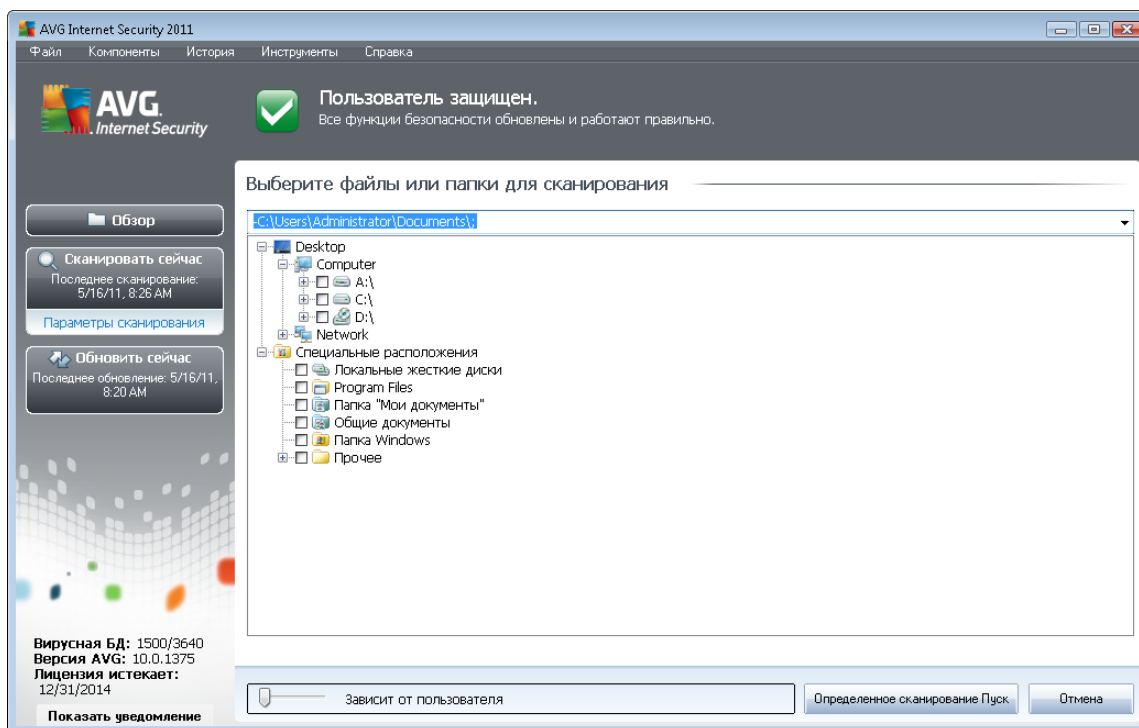
Сканирование отдельных файлов или папок. При данном типе сканирования проверяются только области компьютера, выбранные для сканирования (*выбранные папки, жесткие диски, гибкие диски, компакт-диски и т. п.*). Процессы обнаружения вирусов и лечения зараженных объектов при данном типе сканирования будут 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 отдельных 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.

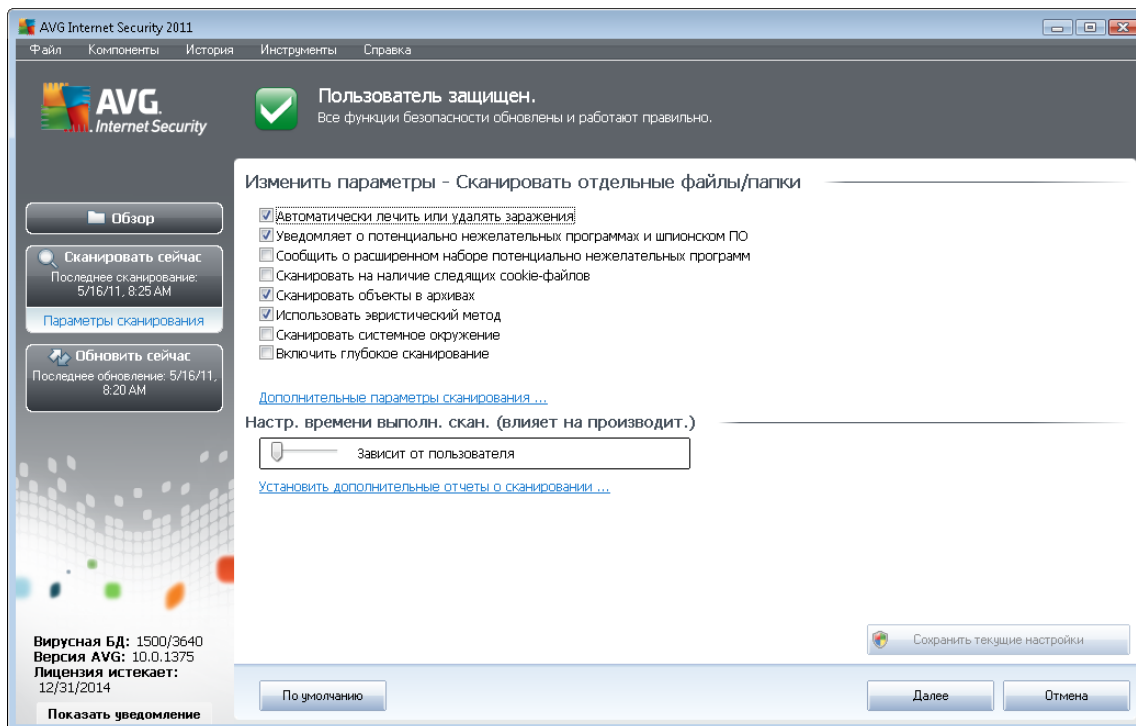
Существует также возможность сканирования определенных папок без сканирования соответствующих подпапок; чтобы выполнить такое сканирование, введите значок минус "-" перед автоматически созданным путем (см. *снимок экрана*). Чтобы исключить всю папку из процесса сканирования, используйте параметр "!".

Наконец, чтобы запустить сканирование, нажмите кнопку **Начать сканирование**; данный процесс сканирования практически идентичен процессу [сканирования всего компьютера](#).



Изменение параметров сканирования

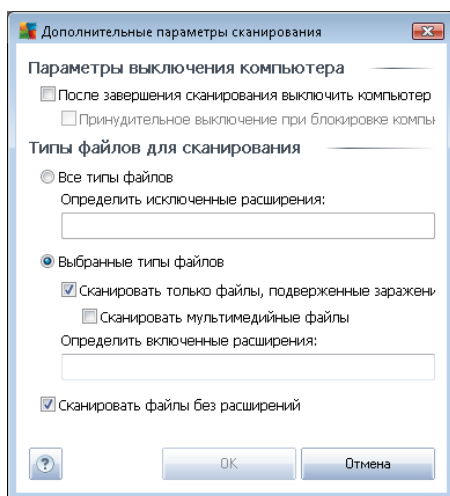
Существует возможность изменения предварительно определенных параметров **сканирования отдельных файлов и папок**. Щелкните ссылку **Изменить параметры сканирования**, чтобы открыть диалоговое окно **Изменение параметров сканирования для сканирования отдельных файлов и папок**. **Рекомендуется сохранять 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.

- о **Автоматически лечить или удалять заражения** (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](#).
- о **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.
- о **Уведомлять о расширенном наборе потенциально нежелательных программ** (не установлено 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 законные программы, поэтому по умолчанию параметр отключен.

- о **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).
 - о **Сканировать объекты в архивах** (выбрано по умолчанию). Благодаря данному параметру при сканировании проверяются все файлы, хранящиеся в архивах, например ZIP, RAR и т. п.
 - о **Использовать эвристический анализ**. (выбрано по умолчанию). Эвристический анализ (динамичная эмуляция команд сканированных объектов в среде виртуального компьютера) является одним из способов, используемых для обнаружения вирусов при сканировании.
 - о **Сканировать системную среду** (не выбрано по умолчанию). При сканировании также будут проверены системные области компьютера.
 - о **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.

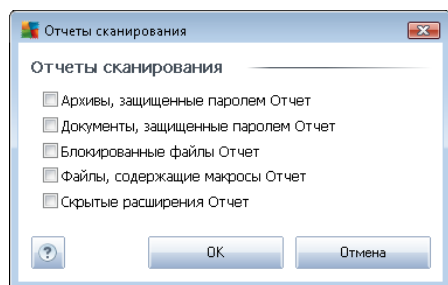


- о **Параметры выключения компьютера**. Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (**Выключить компьютер после завершения сканирования**) становится доступен новый параметр,

позволяющий выключать компьютер, даже если он заблокирован (**Принудительное выключение при блокировке компьютера**).

о **Определение типов файлов для сканирования**. Далее необходимо определить 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



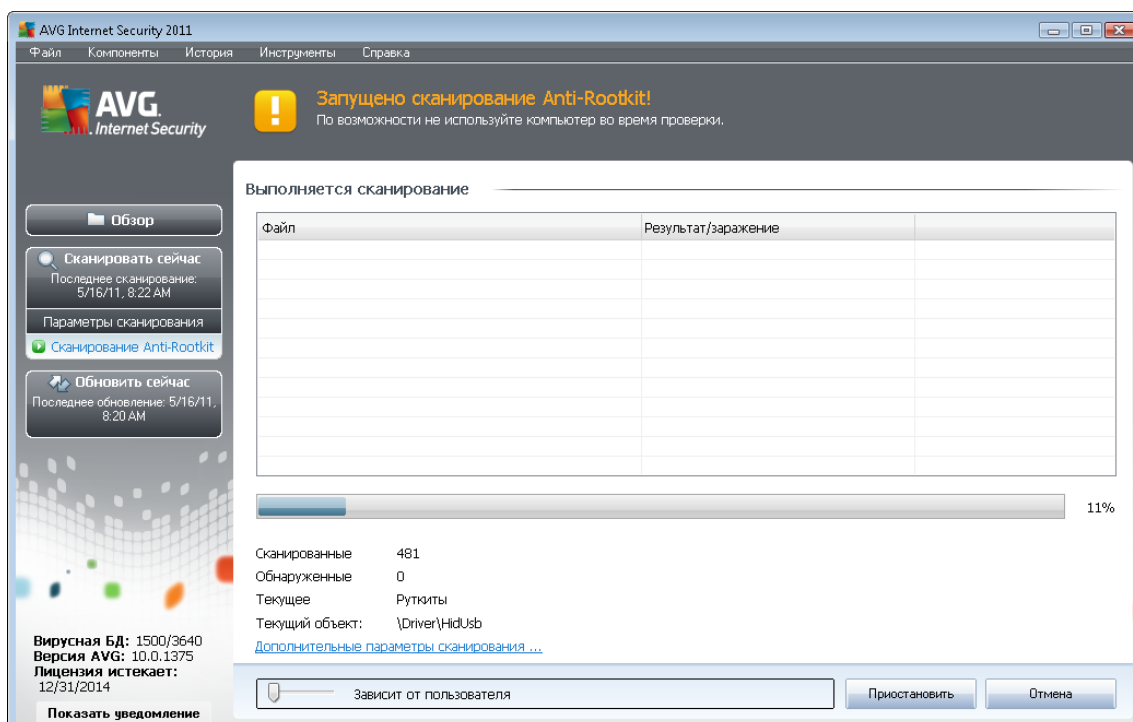
использовалась каждый раз при сканировании отдельных файлов или папок. Кроме того, созданная конфигурация может затем использоваться в качестве шаблона для новых запланированных сканирований ([все пользовательские сканирования основаны на текущей конфигурации сканирования выбранных файлов и папок](#)).

11.2.3. Сканирование Anti-Rootkit

Сканирование Anti-Rootkit исследует компьютер на возможные средства 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.

Запуск сканирования

Сканирование Anti-Rootkit можно запустить непосредственно из [интерфейса 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**).

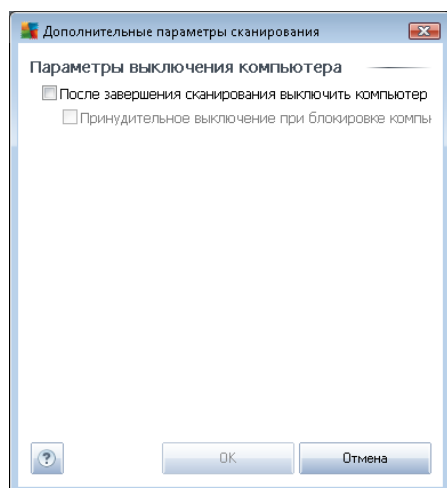


Изменение параметров сканирования

Сканирование Anti-Rootkit всегда запускается по умолчанию, изменение параметров сканирования возможно только в диалоговом окне [Дополнительные параметры AVG/Anti-](#)

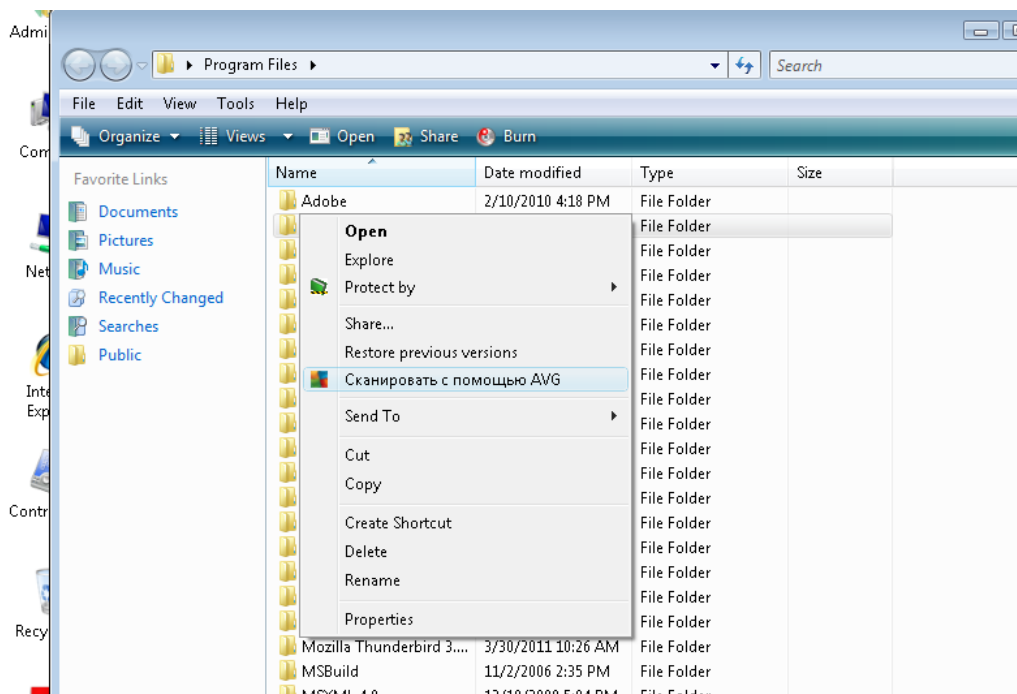
Rootkit. Во время выполнения сканирования в соответствующем интерфейсе доступна следующая конфигурация.

- **Автоматическое сканирование.** 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*).
- **Дополнительные параметры сканирования.** Данная ссылка открывает новое диалоговое окно **Дополнительные параметры сканирования**, в котором можно выбрать возможные условия выключения компьютера, связанные со **сканированием Anti-Rootkit** (**Выключить компьютер по завершении сканирования, также возможно Принудительное выключение при блокировке компьютера**):



11.3. Сканирование в Проводнике Windows

Кроме predetermined сканирований всего компьютера или выбранных областей, программа **AVG Internet Security 2011** 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 программы AVG

11.4. Сканирование с помощью командной строки

В **AVG Internet Security 2011** 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 отдельные 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
- **/MACROW** Сообщать о макросах
- **/PWDW** Сообщать о файлах, защищенных паролем
- **/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](#)"
- **/REG** Сканировать реестр
- **/COO** Сканировать файлы cookie
- **/?** Показать справку по этой теме
- **/HELP** Показать справку по этой теме
- **/PRIORITY** Установить приоритет сканирования /Низкий, Автоматически, 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)
- **/ARCBOMBSW** Сообщать о повторно сжатых архивных файлах

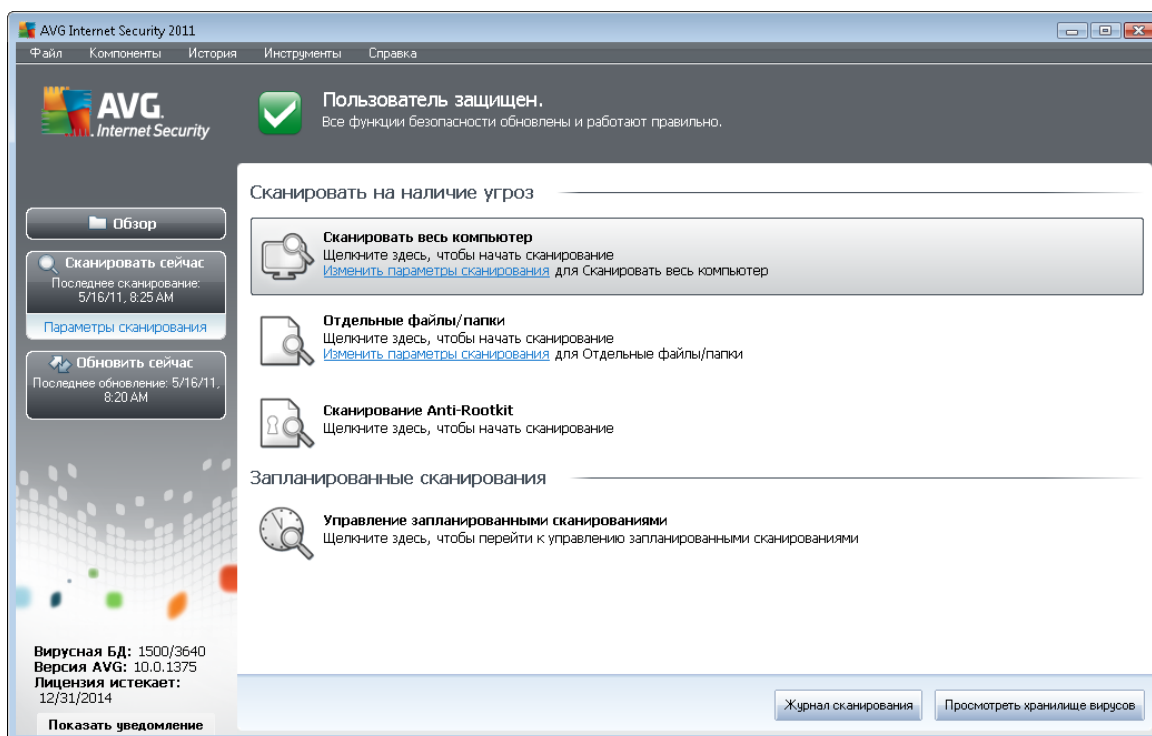


11.5. Расписание сканирования

С помощью **AVG Internet Security 2011** 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.

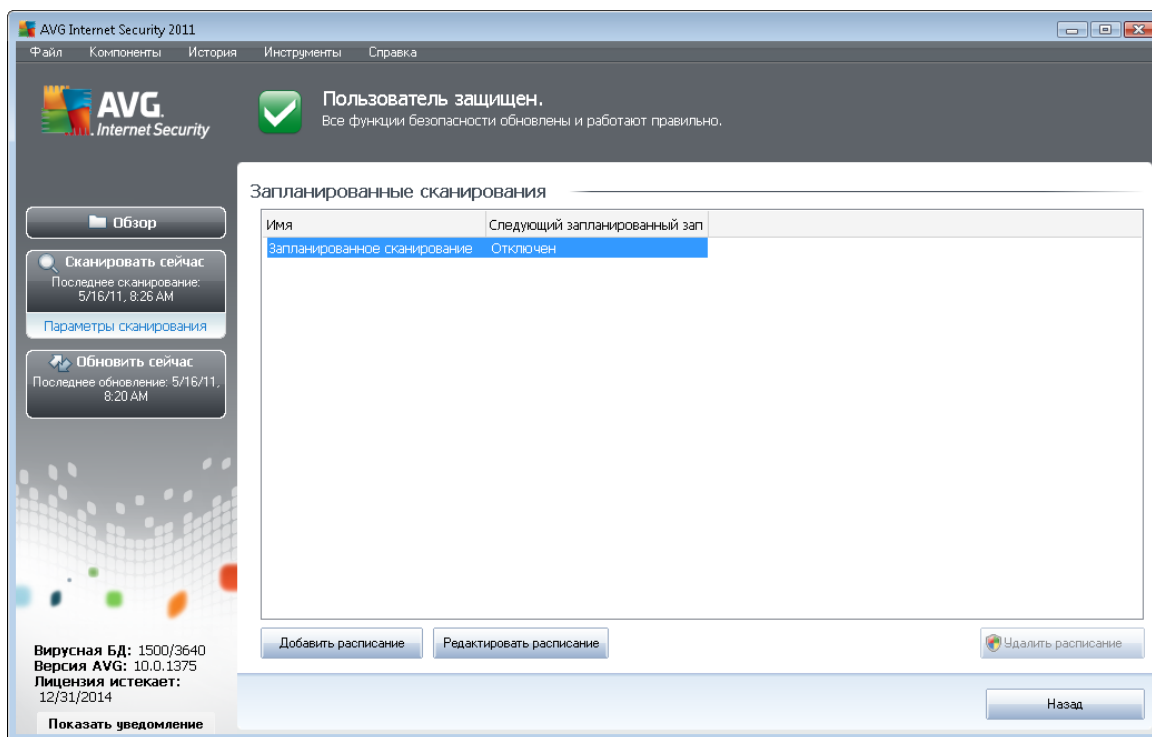
[Сканирование всего компьютера](#) необходимо запускать как минимум раз в неделю. Все же, если это возможно, рекомендуется запускать сканирование всего компьютера ежедневно (как настроено в конфигурации расписания сканирования по умолчанию). Если компьютер всегда включен, можно назначить сканирование 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:

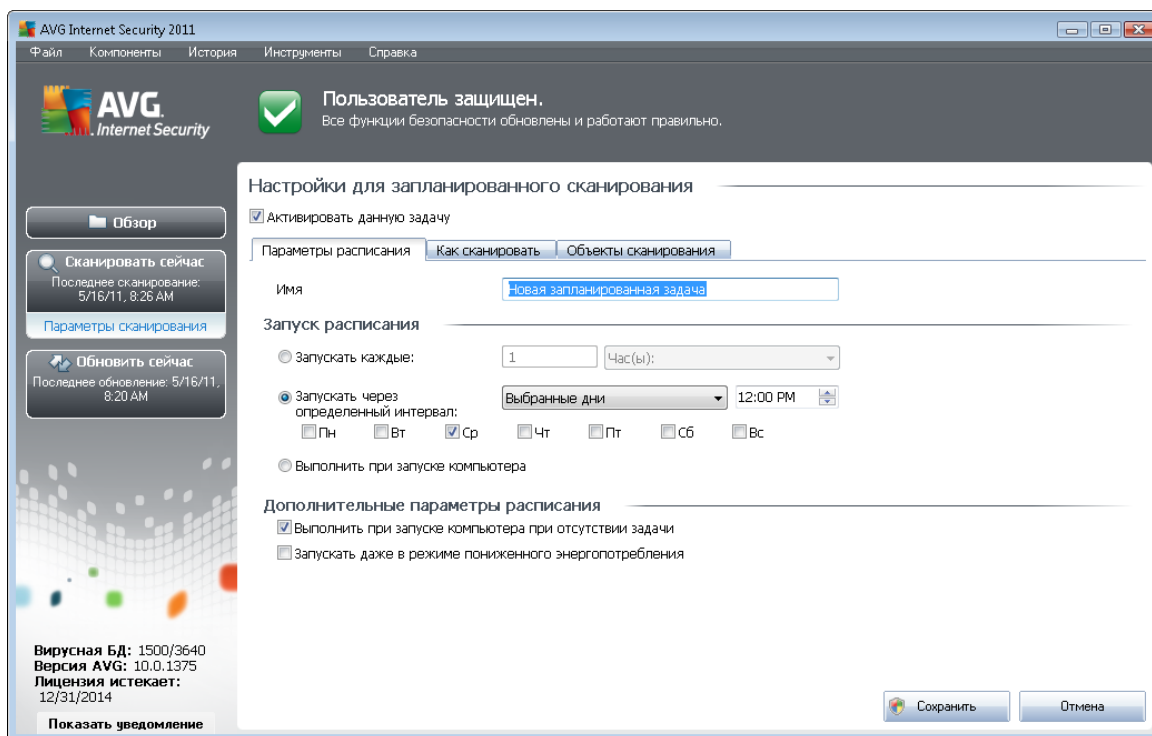
- **Добавить расписание сканирования.** Открытие диалогового окна *Параметры запланированного сканирования*, вкладки [Параметры расписания](#). В данном диалоговом окне можно указать параметры новой созданной проверки.
- **Редактировать расписание сканирования.** Используется, только если текущая проверка 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).

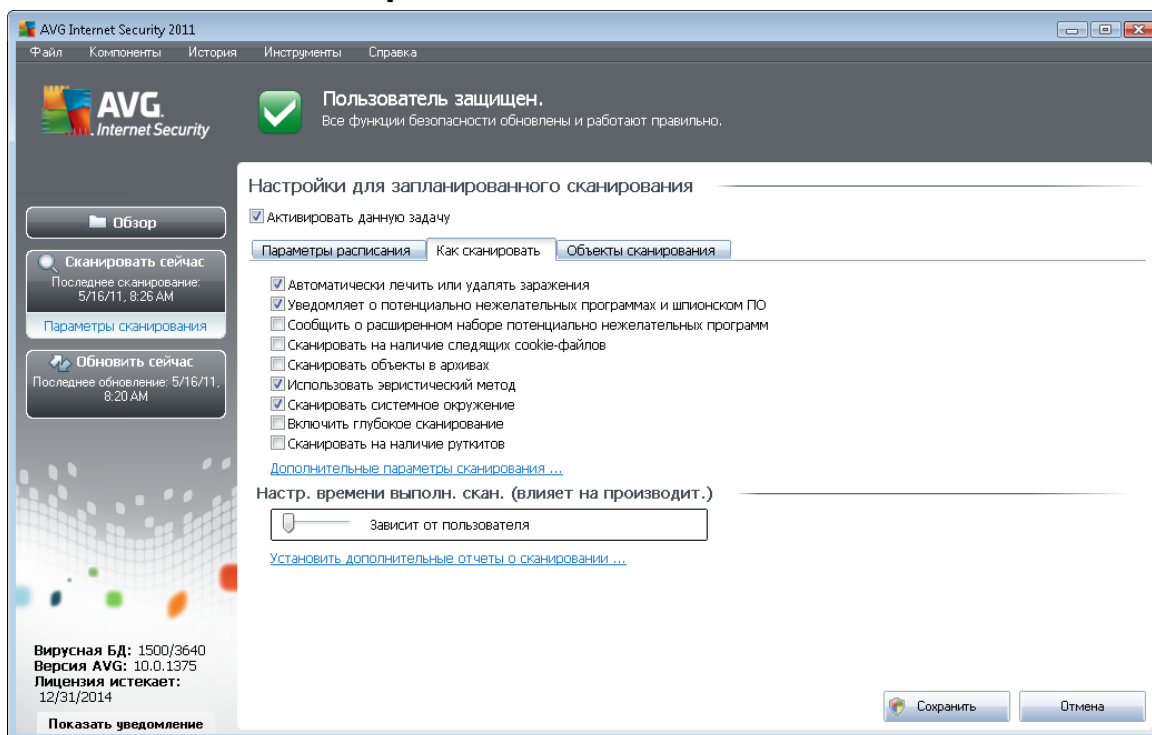
- **Дополнительные параметры расписания** — данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск сканирования, если компьютер работает в энергосберегающем режиме или выключен.

Кнопки управления параметрами диалогового окна запланированного сканирования

На каждой из трех вкладок диалогового окна **Параметры запланированного сканирования** (**Параметры расписания**, **Способы сканирования** и **Объекты 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

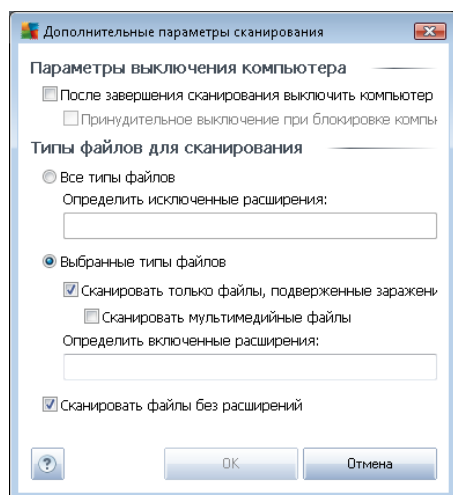
необходимости можно включить или отключить. По умолчанию большинство параметров включены и используются при сканировании. Если нет веских оснований для изменения данных параметров, рекомендуется не изменять стандартные настройки.

- **Автоматически лечить или удалять заражения** (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** (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** (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 законные 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 содержимом 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.

Затем, чтобы изменить параметры сканирования, выполните следующие действия.

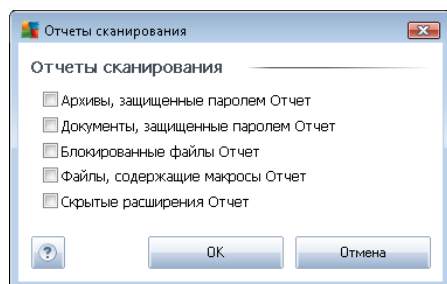
- **Дополнительные параметры сканирования.** Эта ссылка открывает новое диалоговое окно **Дополнительные параметры сканирования**, где можно указывать следующие параметры.



- о **Параметры исключения 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**).
- о **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.



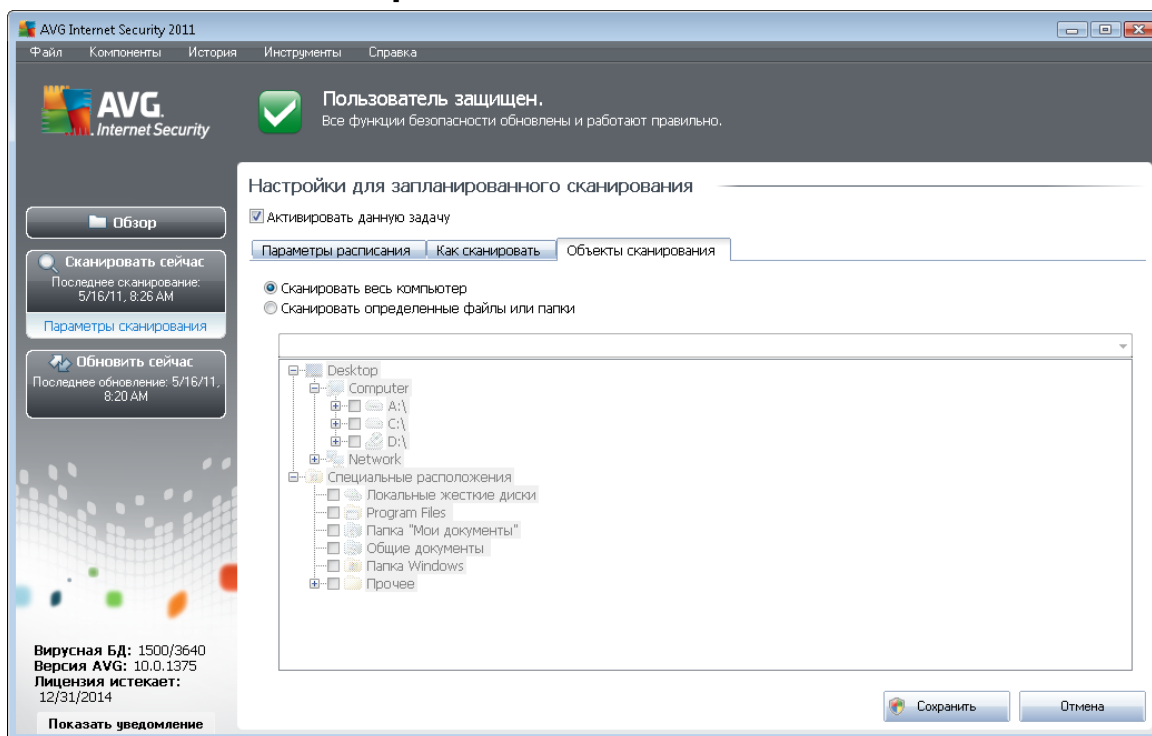
Примечание. По умолчанию установлена конфигурация для достижения оптимальной производительности при сканировании. Не рекомендуется изменять стандартные параметры сканирования без необходимости. Любые изменения параметров должны выполнять только опытные пользователи. Дополнительные параметры конфигурации сканирования находятся в диалоговом окне [Дополнительные параметры](#), доступ к которому можно получить с помощью элементов системного меню **Файл/Дополнительные параметры**.

Кнопки управления

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](#).

11.5.3. 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**
 - o C:\Program Files\
 - o в 64-разрядной версии C:\Program Files (x86)
- **Папка Мои документы**



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

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

- **Общие документы**

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

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

- **Папка Windows** — C:\Windows\

- **Прочее**

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

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

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

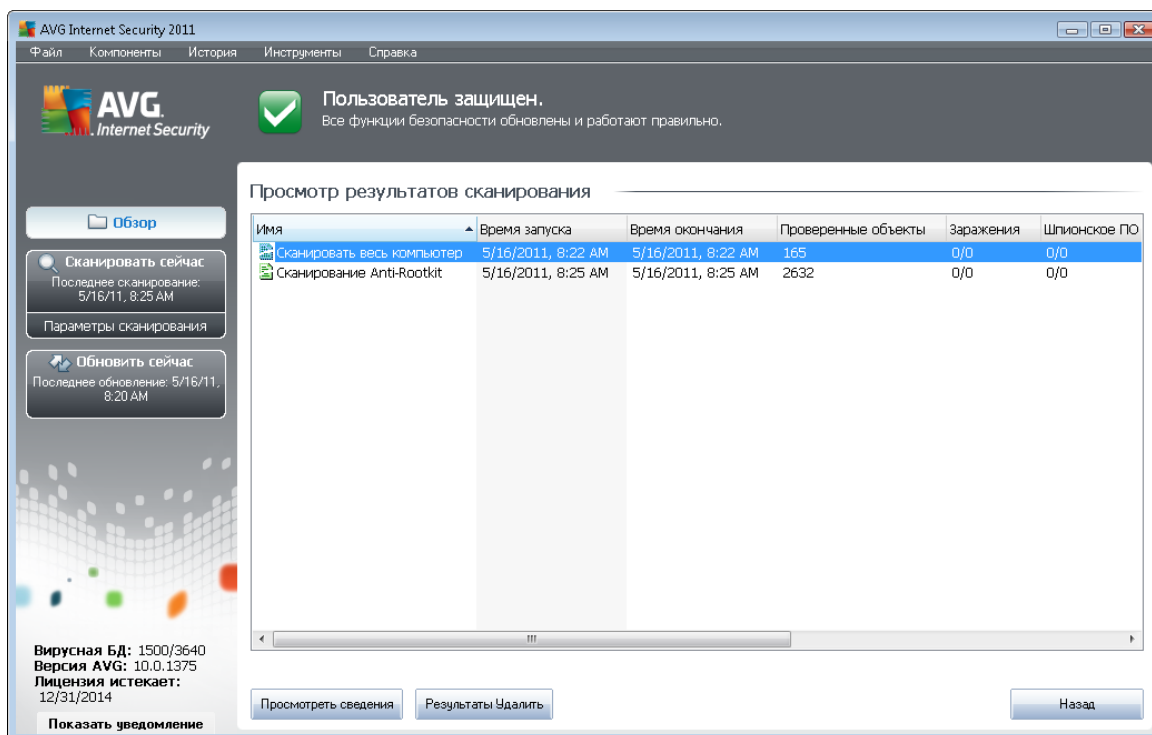
о *Временные файлы Интернета* — C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); или C:\Users\user\AppData\Local\Temp\Microsoft\Windows\Временные файлы Интернета (Windows Vista/7)

Кнопки управления параметрами диалогового окна запланированного сканирования

На каждой из трех вкладок диалогового окна **Параметры запланированного сканирования** (**Параметры расписания**, **Способы сканирования** и **Объекты 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](#).

11.6. 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.

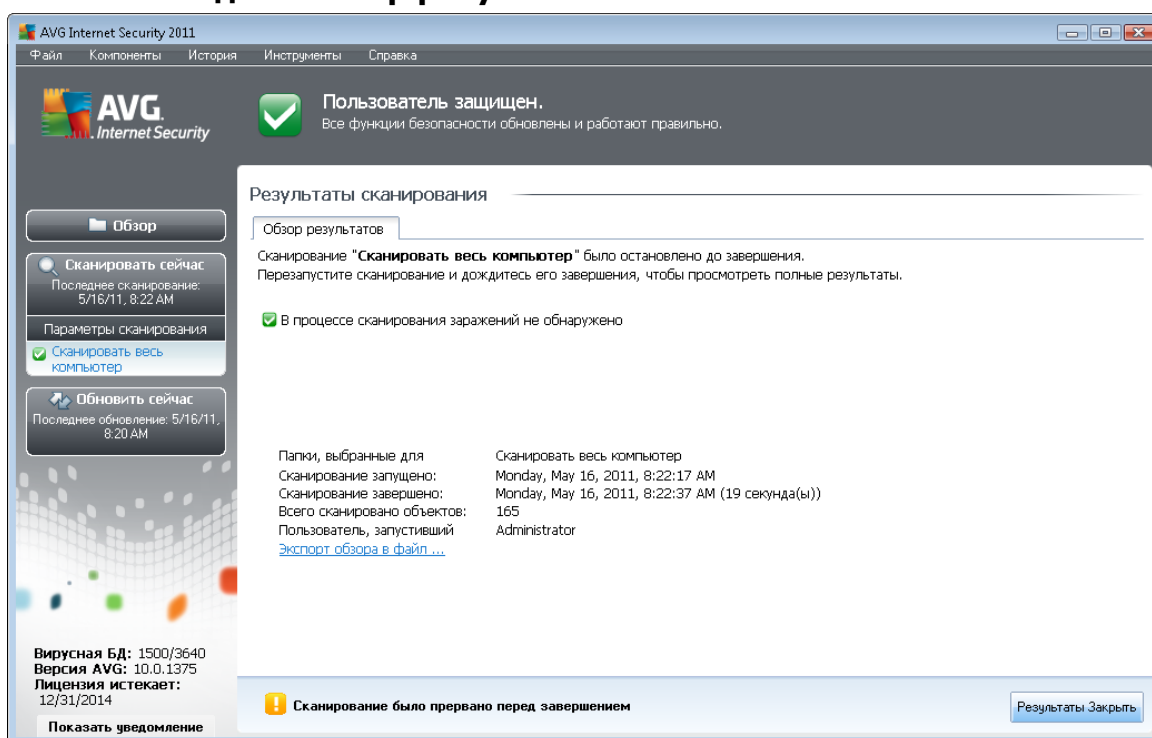
- **Обзор результатов**. Данная вкладка отображается каждый раз при выполнении сканирования и предоставляет статистические данные с описанием процесса сканирования.
- **Заражения**. Данная вкладка отображается только в том случае, если во время



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 подпадающие 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"



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

- обнаруженные [вирусы](#)/[шпионское ПО](#)
- Удаленные [заражения](#)/[шпионское ПО](#).
- количество [вирусов](#)/[объектов шпионского ПО](#), которые не могут быть удалены или вылечены

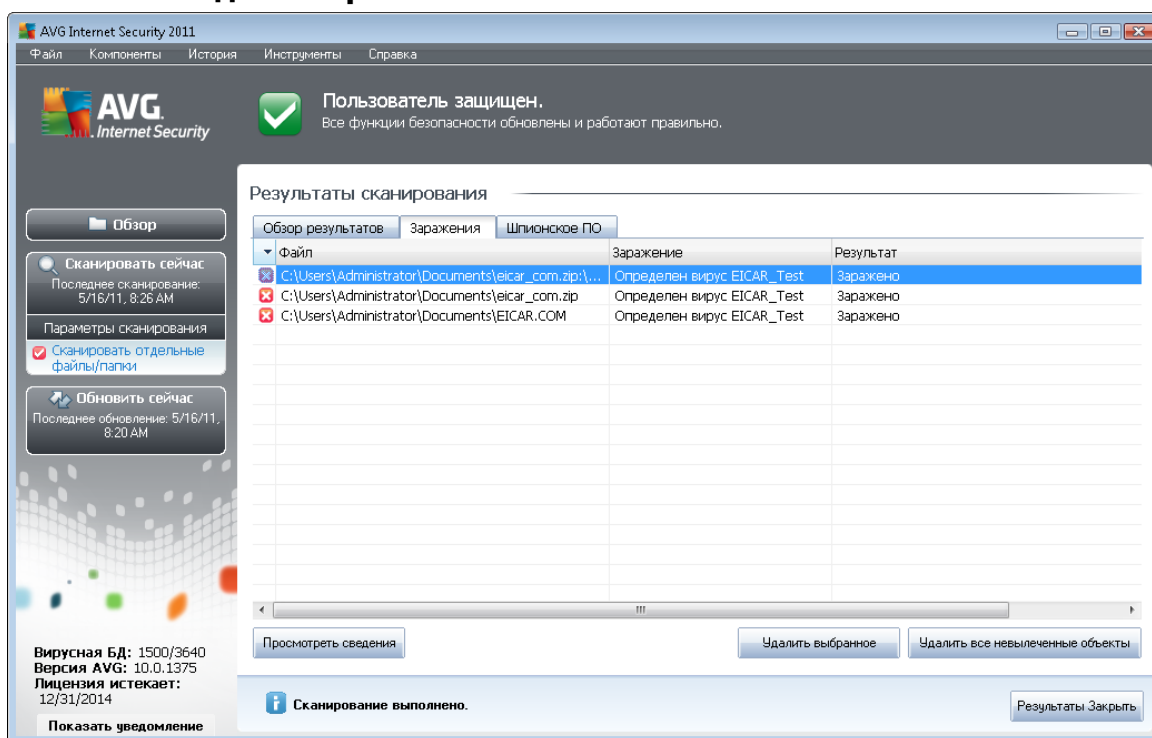


Кроме того, здесь содержится информация о дате и точном времени запуска сканирования, общем количестве сканированных объектов, продолжительности сканирования и количестве ошибок, произошедших при сканировании.

Кнопки управления

В данном диалоговом окне имеется только одна кнопка управления. Кнопка **Заккрыть 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.
 - о **Заражен.** Зараженный объект обнаружен, его начальное местоположение сохранено (например, если в специальных параметрах сканирования [отключен](#)

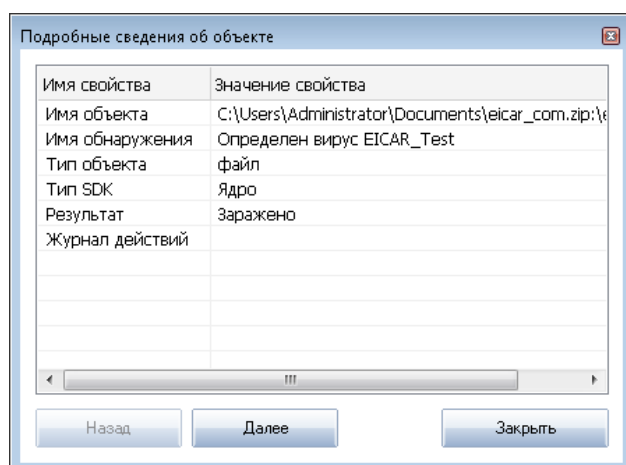
параметр автоматического лечения).

- о **Вылечен**. Зараженный объект вылечен автоматически, его начальное местоположение сохранено.
- о **Перемещен в хранилище вирусов**. Зараженный объект помещен на карантин в [хранилище вирусов](#).
- о **Удален**. Зараженный объект удален.
- о **Добавлен в список исключений PUP**. Обнаруженный объект получил статус исключения и был добавлен в список исключений PUP (настроенный в диалоговом окне [Исключения PUP](#) дополнительных параметров).
- о **Заблокированный файл — не проверен**. Объект заблокирован, поэтому AVG не может выполнить его сканирование.
- о **Потенциально опасный объект**. Объект является потенциально опасным, но не заражен (например, содержит макросы); данная информация имеет лишь предупредительный характер.
- о **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**.



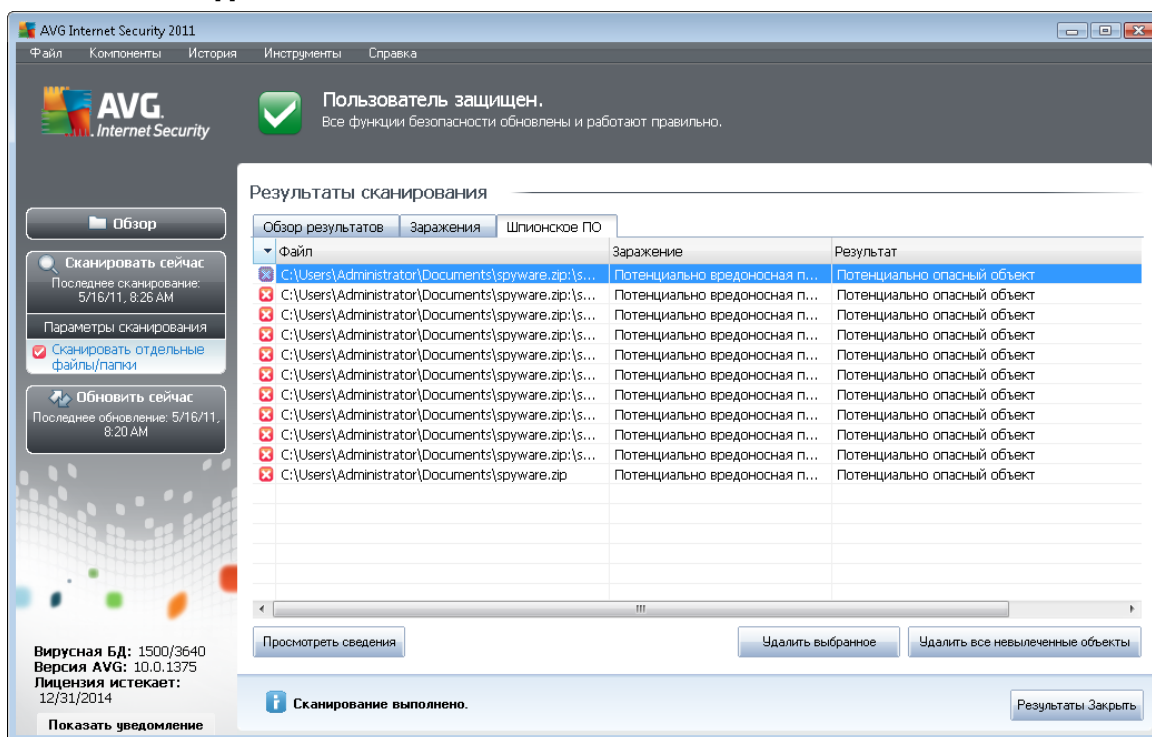
В данном диалоговом окне приведена подробная информация об обнаруженном зараженном объекте (например, имя, местонахождение, тип объекта,



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](#).
- **Заккрыть результаты.** Заккрытие 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.

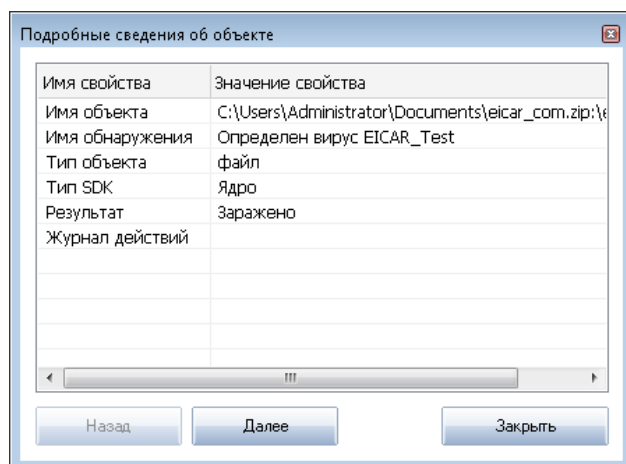


- о **Заражен**. Зараженный объект обнаружен, его начальное местоположение сохранено (например, если в особых настройках сканирования [отключен параметр автоматического лечения](#)).
- о **Вылечен**. Зараженный объект вылечен автоматически, его начальное местоположение сохранено.
- о **Перемещен в хранилище вирусов**. Зараженный объект помещен на карантин в [хранилище вирусов](#).
- о **Удален**. Зараженный объект удален.
- о **Добавлен в список исключений PUP**. Обнаруженный объект получил статус исключения и добавлен в список исключений PUP (*настроенный в диалоговом окне дополнительных параметров [Исключения PUP](#)*).
- о **Заблокированный файл — не проверен**. Объект заблокирован, поэтому AVG не может выполнить его сканирование.
- о **Потенциально опасный объект**. Объект является потенциально опасным, но не заражен (например, содержит макросы); данная информация имеет лишь предупредительный характер.
- о **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](#).
- **Заккрыть результаты.** Заккрытие 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 при проверке AVG выводятся только предупреждения, 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 сообщает об обнаружении скрытого файла, который кажется подозрительным, его можно переместить в [хранилище вирусов AVG](#).
- **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 средствах rootkit, обнаруженных при сканировании, если было запущено [сканирование Anti-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.

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

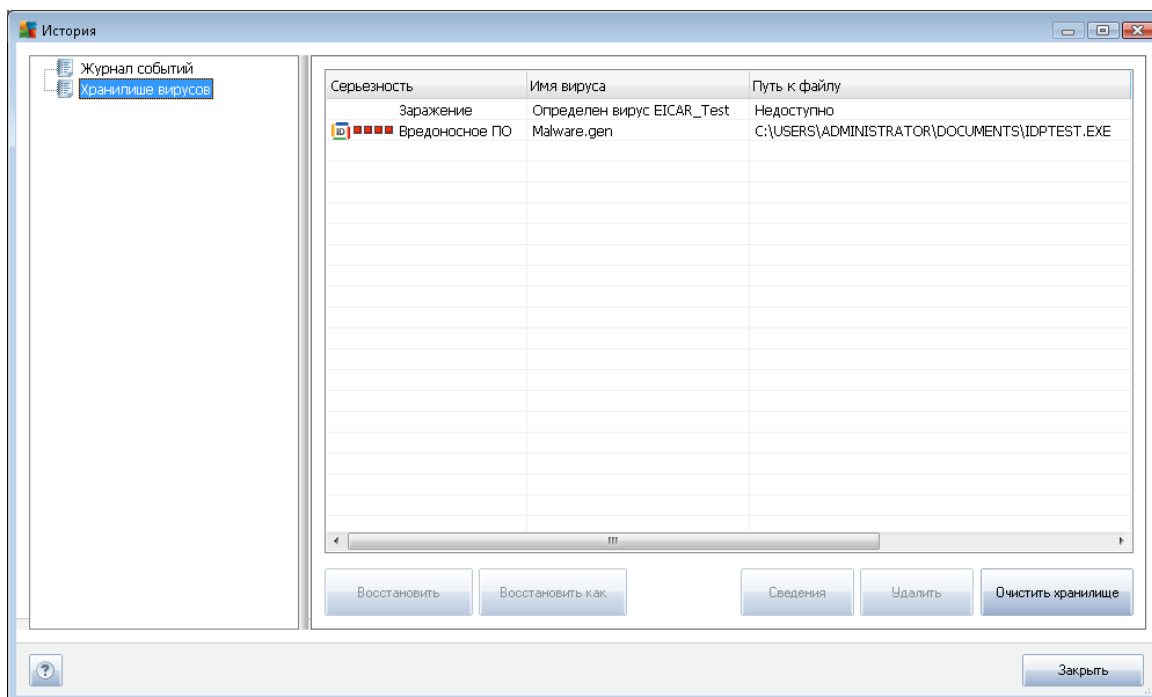
11.7.6. Вкладка "Сведения"

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 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 (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 программа AVG отправляет 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), программа AVG сообщает о таком расхождении. В некоторых случаях вирусы используют имена стандартных системных процессов, чтобы скрыть свое присутствие в системе.
- **Заблокированные файлы** — если файл, о котором было сообщено, заблокирован, программа AVG 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 Internet Security 2011** 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

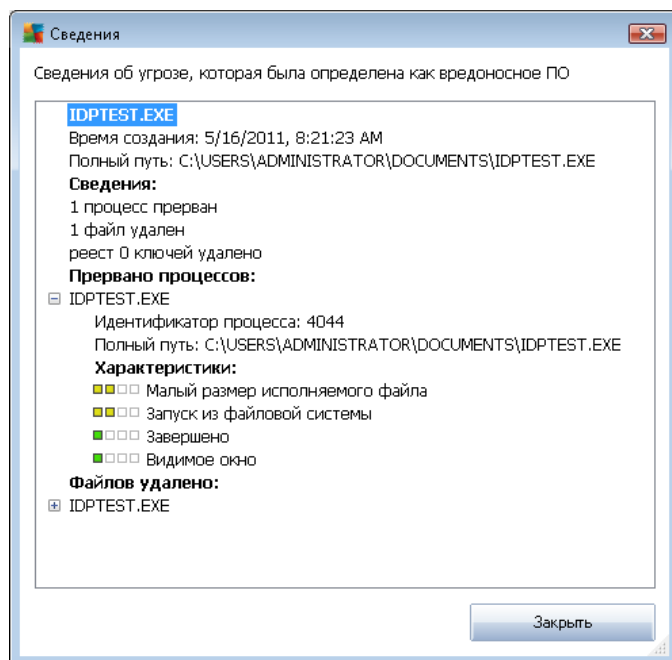
известное исходное имя (например, имя вложения электронной почты, не соответствующее фактическому содержимому вложения), оно отобразится в данном столбце.

- **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

Важно регулярно обновлять приложение AVG, чтобы быть уверенным, что все новые вирусы будут сразу же обнаружены.

Так как обновления AVG не выпускаются согласно какому-либо точному расписанию, а скорее в ответ на количество и опасность появляющихся новых угроз, рекомендуется выполнять проверку на наличие обновлений как минимум раз в день. При проверке каждые 4 часа система **AVG Internet Security 2011** будет находиться в обновленном состоянии в течение всего дня.

12.1. Уровни обновлений

Существует два уровня обновления AVG.

- **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 [определении параметров расписания обновления](#) можно указать уровень приоритета для загрузки и установки обновлений.

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

12.2. Типы обновлений

Существует два типа обновлений.

- **Обновление по запросу.** Представляет собой мгновенное обновление продукта AVG, которое может быть выполнено в любое время.
- **Запланированное обновление.** В AVG также можно [предварительно настраивать план обновления](#). После этого запланированное обновление будет периодически выполняться в соответствии с установленными параметрами. При появлении новых файлов обновления в указанном местоположении они будут загружены напрямую из Интернета или из сетевого каталога. Если обновления недоступны, ничего не будет происходить.

12.3. Процесс обновления

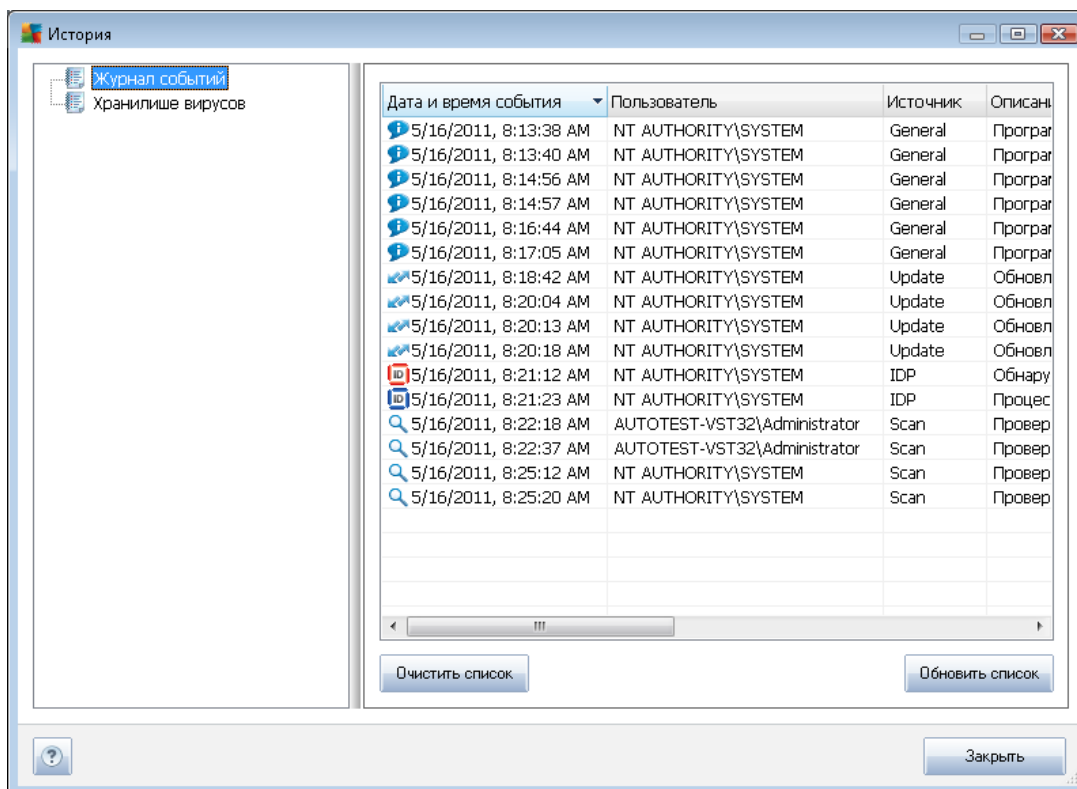
Процесс обновления может быть запущен сразу, как только потребуется, с помощью [быстрой ссылки Обновить сейчас](#). Данная ссылка всегда доступна в диалоговом окне [Интерфейс пользователя AVG](#). Тем не менее, настоятельно рекомендуется регулярно выполнять обновления по расписанию, которое можно изменить с помощью компонента [Диспетчер обновления](#).



После подтверждения начала обновления программа AVG сначала проверит наличие новых доступных файлов обновления. Если файлы имеются, AVG начнет их загрузку и выполнит запуск обновления самостоятельно. В процессе обновления откроется интерфейс **Обновление**, где можно увидеть выполняемый процесс в графическом представлении, а также просмотреть соответствующие статистические параметры (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. Данный параметр доступен в меню Пуск/Все программы/Стандартные /Служебные/ Восстановление системы. Однако любые изменения следует вносить только опытным пользователям.

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 Internet Security 2011**. В журнале **История** регистрируются следующие типы событий.

- Сведения об обновлениях приложения AVG
- Начало, завершение или приостановка процесса сканирования (*включая автоматические тесты*)
- События, связанные 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.** Точная дата и время события
- **Пользователь.** Лицо, запустившее событие
- **Источник.** Исходный компонент или другой элемент системы AVG, запустивший



событие

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

Кнопки управления

- **Очистить список.** Удаление всех записей из списка событий
- **Обновить список.** Обновление всех записей в списке событий



14. Часто задаваемые вопросы и техническая поддержка

При возникновении любых проблем при работе с программой коммерческого или технического характера см. раздел [Часто задаваемые вопросы](http://www.avg.com/) веб-сайта AVG (<http://www.avg.com/>).

Если необходимые справочные сведения не найдены, обратитесь в службу технической поддержки по электронной почте. Используйте контактную форму системного меню, доступную в разделе **Справка/Получить интерактивную справку**.