



AVG 9 Anti-Virus + Firewall

Руководство пользователя

Версия документа 90.21 (3.2.2010)

© 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 использован код из библиотеки C-SaCzech, (с) Яромир Долечек (Jaromir Dolecek) (dolecek@ics.muni.cz), 1996-2001.

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

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

Содержание

1. Введение	7
2. Требования для установки AVG	8
2.1 Поддерживаемые операционные системы	8
2.2 Минимальные требования и рекомендуемое оборудование	8
3. Варианты установки AVG	10
4. Диспетчер загрузки AVG	11
4.1 Выбор языка	11
4.2 Проверка подключения	12
4.3 Параметры прокси-сервера	13
4.4 Загрузка файлов для установки	14
5. Процесс установки AVG	15
5.1 Запуск установки	15
5.2 Лицензионное соглашение	16
5.3 Проверка состояния системы	16
5.4 Выбор типа установки	17
5.5 Активация лицензии AVG	17
5.6 Выборочная установка — Папка назначения	19
5.7 Выборочная установка — Выбор компонентов	20
5.8 AVG Security Toolbar	21
5.9 Завершение работы открытых приложений	22
5.10 Установка AVG	23
5.11 Планирование регулярных сканирований и обновлений	24
5.12 Выбор типа используемого компьютера	25
5.13 Используемый тип подключения к Интернету	26
5.14 Настройка защиты AVG завершена	27
6. После установки	28
6.1 Оптимизация сканирования	28
6.2 Регистрация продукта	28
6.3 Доступ к интерфейсу пользователя	28
6.4 Сканирование всего компьютера	29
6.5 Тестирование EICAR	29

6.6 Настройки AVG по умолчанию	30
7. Интерфейс пользователя AVG	31
7.1 Системное меню	32
7.1.1 Файл	32
7.1.2 Компоненты	32
7.1.3 История	32
7.1.4 Инструменты	32
7.1.5 Справка	32
7.2 Информация о состоянии безопасности	35
7.3 Быстрые ссылки	36
7.4 Обзор компонентов	37
7.5 Статистика	38
7.6 Значок на панели задач	39
8. Компоненты AVG	41
8.1 Anti-Virus	41
8.1.1 Принципы работы Anti-Virus	41
8.1.2 Интерфейс Anti-Virus	41
8.2 Anti-Spyware	43
8.2.1 Принципы работы Anti-Spyware	43
8.2.2 Интерфейс Anti-Spyware	43
8.3 Anti-Rootkit	45
8.4 Firewall	45
8.4.1 Принципы работы Firewall	45
8.4.2 Профили Firewall	45
8.4.3 Интерфейс Firewall	45
8.5 E-mail Scanner	51
8.5.1 Принципы работы E-mail Scanner	51
8.5.2 Интерфейс E-mail Scanner	51
8.5.3 Обнаружение E-mail Scanner	51
8.6 Лицензия	55
8.7 Link Scanner	56
8.7.1 Принципы работы Link Scanner	56
8.7.2 Интерфейс Link Scanner	56
8.7.3 AVG Search-Shield	56
8.7.4 AVG Active Surf-Shield	56
8.8 Online Shield	60

8.8.1 Принципы работы Online Shield	60
8.8.2 Интерфейс Online Shield	60
8.8.3 Обнаружение Online Shield	60
8.9 Resident Shield	67
8.9.1 Принципы работы Resident Shield	67
8.9.2 Интерфейс Resident Shield	67
8.9.3 Обнаружение Resident Shield	67
8.10 Диспетчер обновления	72
8.10.1 Принципы работы диспетчера обновления	72
8.10.2 Интерфейс диспетчера обновления	72
9. AVG Security Toolbar	75
9.1 AVG Security Toolbar Интерфейс	75
9.2 AVG Security Toolbar	77
9.2.1 Вкладка Общее	77
9.2.2 Вкладка Полезные кнопки	77
9.2.3 Вкладка Безопасность	77
9.2.4 Вкладка Дополнительные параметры	77
10. Расширенные настройки AVG	82
10.1 Внешний вид	82
10.2 Звуки	85
10.3 Игнорирование ошибочных условий	86
10.4 Хранилище вирусов	87
10.5 Исключения PUP	88
10.6 Online Shield	91
10.6.1 Интернет-защита	91
10.6.2 Обмен мгновенными сообщениями	91
10.7 Link Scanner	95
10.8 Сканирование	96
10.8.1 Сканирование всего компьютера	96
10.8.2 Сканирование расширения оболочки	96
10.8.3 Сканирование отдельных файлов или папок	96
10.8.4 Сканирование съемного устройства	96
10.9 Расписания	103
10.9.1 Запланированное сканирование	103
10.9.2 Расписание обновления вирусной базы данных	103
10.10 E-mail Scanner	115

10.10.1 Сертификация	115
10.10.2 Фильтрация электронной почты	115
10.10.3 Журналы и результаты	115
10.10.4 Серверы	115
10.11 Resident Shield	125
10.11.1 Дополнительные параметры	125
10.11.2 Исключаемые каталоги	125
10.11.3 Исключенные файлы	125
10.12 Сервер кэширования	130
10.13 Anti-Rootkit	132
10.14 Обновить	133
10.14.1 Прокси-сервер	133
10.14.2 Подключение по коммутируемой линии	133
10.14.3 URL-адрес	133
10.14.4 Управление	133
10.15 Удаленное администрирование	141
11. Параметры Firewall	143
11.1 Общие	143
11.2 Безопасность	144
11.3 Области и профили адаптеров	145
11.4 Журналы	146
11.5 Профили	148
11.5.1 Сведения о профилях	148
11.5.2 Определенные сети	148
11.5.3 Приложения	148
11.5.4 Системные службы	148
12. Сканирование AVG	160
12.1 Интерфейс сканирования	160
12.2 Предопределенные сканирования	161
12.2.1 Сканирование всего компьютера	161
12.2.2 Сканирование определенных файлов или папок	161
12.3 Сканирование в Проводнике Windows	171
12.4 Сканирование с помощью командной строки	171
12.4.1 Параметры сканирования с помощью командной строки	171
12.5 Расписание сканирования	174
12.5.1 Параметры расписания	174

12.5.2 Способы сканирования	174
12.5.3 Объекты сканирования	174
12.6 Обзор результатов сканирования	185
12.7 Результаты сканирования Сведения	187
12.7.1 Вкладка "Обзор результатов"	187
12.7.2 Вкладка "Заражения"	187
12.7.3 Вкладка "Шпионское ПО"	187
12.7.4 Вкладка "Предупреждения"	187
12.7.5 Вкладка "Средства rootkit"	187
12.7.6 Вкладка "Сведения"	187
12.8 Хранилище вирусов	196
13. Обновления AVG	199
13.1 Уровни обновлений	199
13.2 Типы обновлений	199
13.3 Процесс обновления	200
14. Журнал событий	201
15. Часто задаваемые вопросы и техническая поддержка	203



1. Введение

Руководство пользователя содержит полные сведения о системе **AVG 9 Anti-Virus + Firewall**.

Поздравляем с приобретением AVG 9 Anti-Virus + Firewall!

AVG 9 Anti-Virus + Firewall является одним из представителей линейки продуктов AVG, удостоенных различных наград, который создан для обеспечения вашего спокойствия и полной безопасности компьютера. Как и другие продукты, система **AVG 9 Anti-Virus + Firewall** была полностью переработана для обеспечения традиционно высокой безопасности продуктов AVG, а также имеет новый, более удобный и эффективный интерфейс.

Новый продукт **AVG 9 Anti-Virus + Firewall** 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.



2. Требования для установки AVG

2.1. Поддерживаемые операционные системы

AVG 9 Anti-Virus + Firewall обеспечивает защиту рабочих станций под управлением следующих операционных систем.

- Windows 2000 Professional с пакетом обновлений SP4 + накопительный пакет обновления 1;
- Windows XP Home Edition с пакетом обновлений SP2;
- Windows XP Professional с пакетом обновлений SP2;
- Windows XP Professional x64 Edition с пакетом обновлений SP1;
- Windows Vista (x86 и x64, все версии);
- Windows 7 (x86 и x64, все версии)

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

2.2. Минимальные требования и рекомендуемое оборудование

Минимальные требования к оборудованию для **AVG 9 Anti-Virus + Firewall**.

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

Рекомендуемые требования к оборудованию для **AVG 9 Anti-Virus + Firewall**.

- Процессор Intel Pentium 1,8 ГГц
- 512 МБ памяти ОЗУ



- 510 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 9 Anti-Virus + Firewall.

Рекомендуем воспользоваться нашим новым инструментом [Диспетчер загрузки AVG](#), который поможет настроить файл установки на нужном языке.

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.

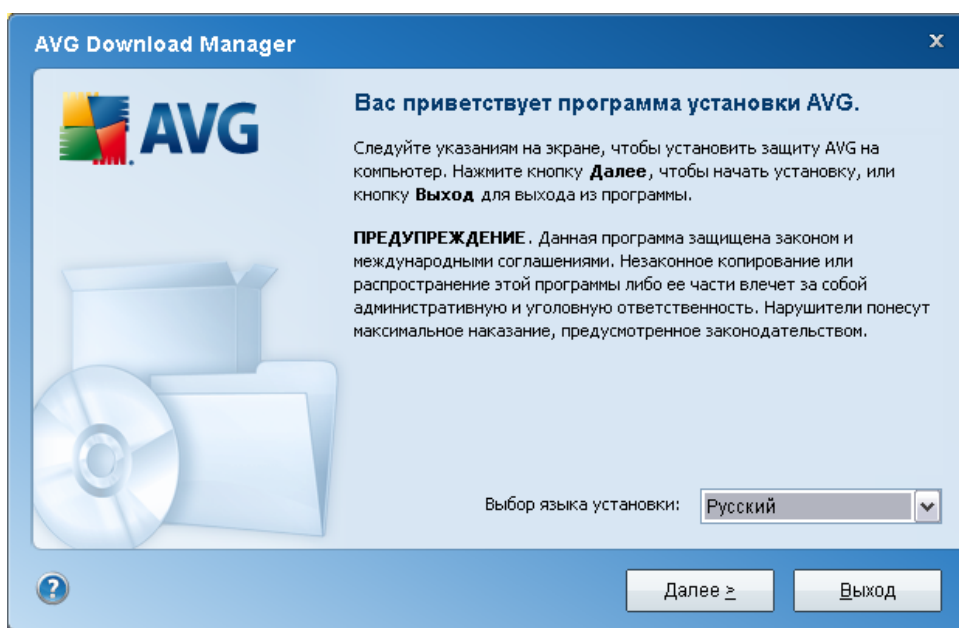
4. Диспетчер загрузки AVG

Диспетчер загрузки AVG — это простой инструмент, помогающий выбрать правильный файл установки для пробной версии продукта AVG. На основании введенных данных диспетчер выберет определенный продукт, тип лицензии, необходимые компоненты и язык. Наконец, **Диспетчер загрузки AVG** загрузит и запустит соответствующий [процесс установки](#).

Предупреждение. Помните, что диспетчер загрузки AVG не предназначен для загрузки сетевых и SBS-версий. Поддерживаются только следующие операционные системы: Windows 2000 (с пакетом обновлений SP4 + накопительный пакет SRP), Windows XP, Windows Vista и Windows 7.

Диспетчер загрузки AVG можно загрузить с веб-сайта AVG (<http://www.avg.com/>). Ниже приведено краткое описание каждого шага, который необходимо выполнить в компоненте **Диспетчер загрузки AVG**.

4.1. Выбор языка

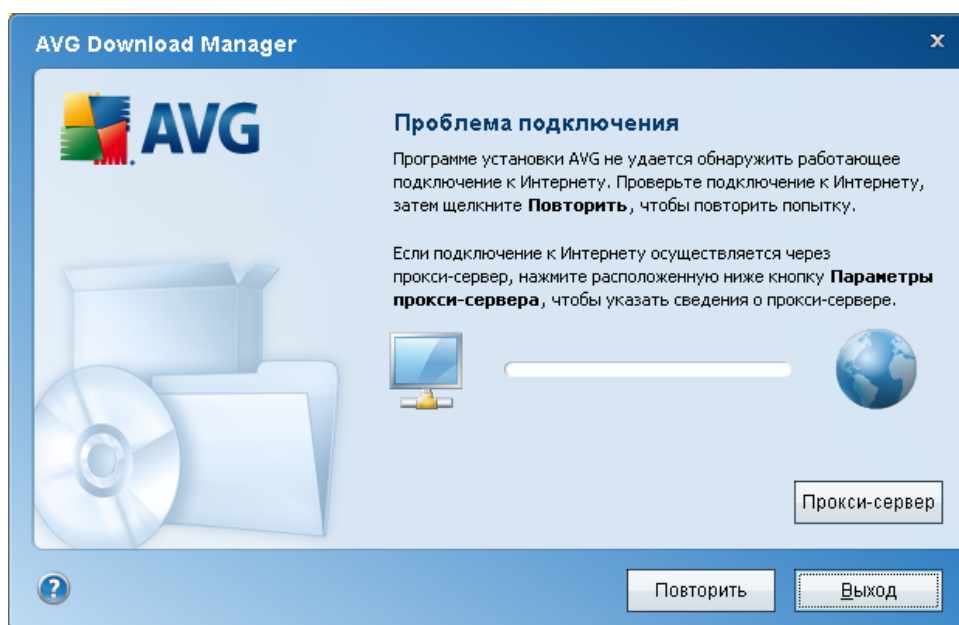


В первом шаге **Диспетчер загрузки AVG** необходимо выбрать язык установки в раскрывающемся меню. Обратите внимание, что выбранный язык используется только в процессе установки. После установки язык можно будет изменить в параметрах программы. Нажмите кнопку **Далее**, чтобы продолжить.

4.2. Проверка подключения

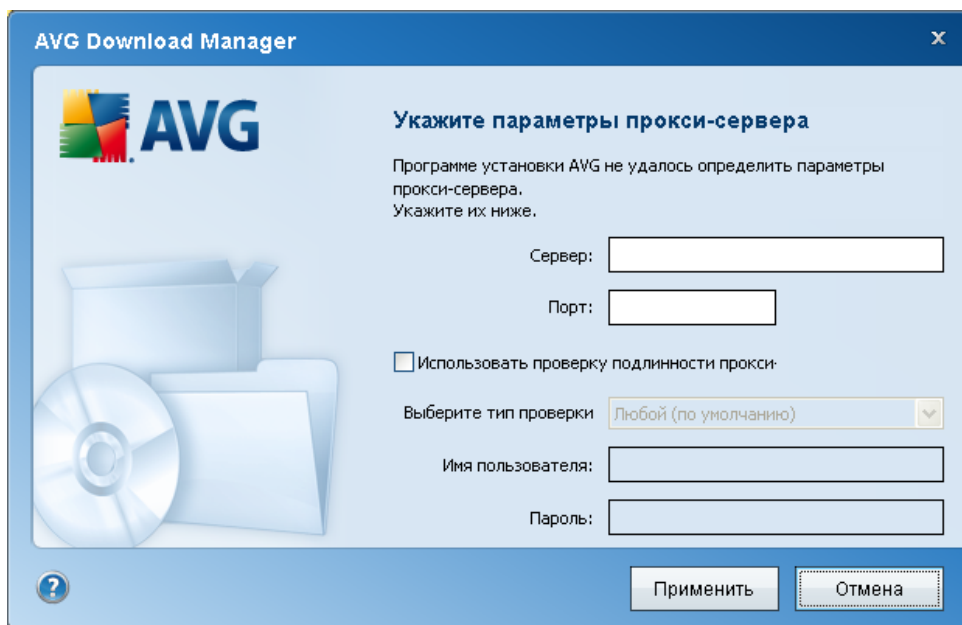
В следующем шаге **Диспетчер загрузки AVG** попытается установить соединение с Интернетом, чтобы обнаружить обновления. Процесс загрузки нельзя будет прервать до тех пор, пока **Диспетчер загрузки AVG** не завершит проверку подключения.

- Если при проверке обнаруживается отсутствие подключения, убедитесь, что компьютер действительно подключен к Интернету. Затем нажмите кнопку **Повторить попытку**.



- При использовании прокси-сервера для подключения к Интернету нажмите кнопку **Параметры прокси-сервера**, чтобы указать [сведения о прокси-сервере](#):
- Если проверка была завершена успешно, нажмите кнопку **Далее**, чтобы продолжить.

4.3. Параметры прокси-сервера



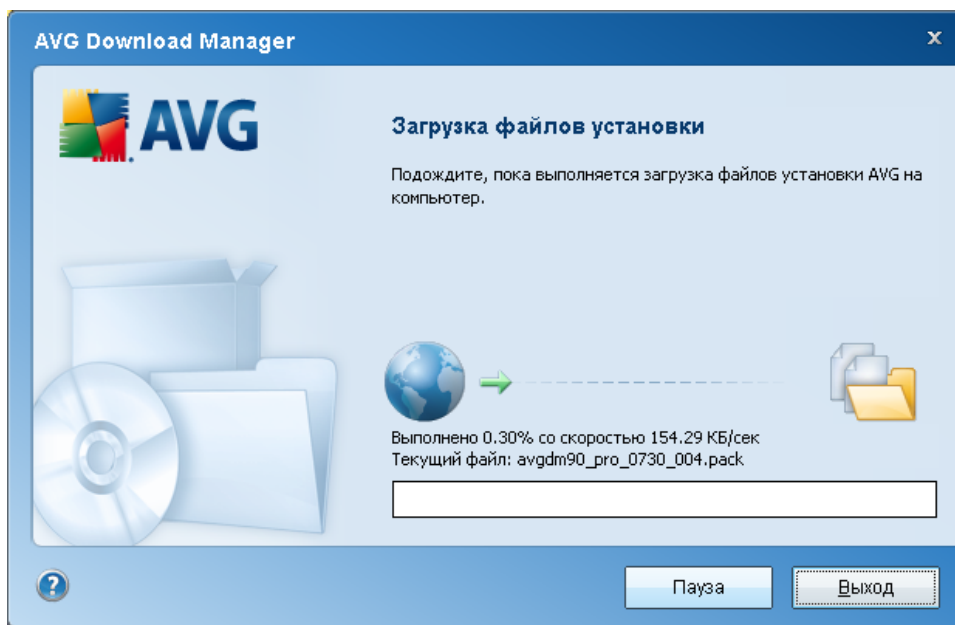
The screenshot shows a window titled "AVG Download Manager" with a close button (X) in the top right corner. On the left is the AVG logo and an illustration of a CD and folders. The main text reads: "Укажите параметры прокси-сервера" (Specify proxy server parameters). Below this, it says: "Программе установки AVG не удалось определить параметры прокси-сервера. Укажите их ниже." (The AVG installation program was unable to determine the proxy server parameters. Specify them below). The form includes: a "Сервер:" (Server) text box; a "Порт:" (Port) text box; a checkbox labeled "Использовать проверку подлинности прокси:" (Use proxy authentication:); a dropdown menu labeled "Выберите тип проверки" (Select check type) with "Любой (по умолчанию)" (Any (default)) selected; a "Имя пользователя:" (Username) text box; and a "Пароль:" (Password) text box. At the bottom right are "Применить" (Apply) and "Отмена" (Cancel) buttons. A help icon (?) is in the bottom left.

Если компоненту **Диспетчер загрузки AVG** не удалось определить параметры прокси-сервера, их необходимо указать вручную. Укажите следующие данные.

- **Сервер** — введите допустимое имя прокси-сервера или IP-адрес
- **Порт** — укажите номер соответствующего порта
- **Использовать проверку подлинности для прокси-сервера** — если прокси-серверу требуется проверка подлинности, установите флажок.
- **Выбор проверки подлинности** — в раскрывающемся меню выберите тип проверки подлинности. Настоятельно рекомендуется сохранить значение по умолчанию (*далее прокси-сервер автоматически сообщит вам требования*). Однако, если вы являетесь опытным пользователем ПК, вы также можете выбрать параметр "Основной" (*необходимый для некоторых серверов*) или NTLM (*необходимый для всех серверов ISA Servers*). Затем введите допустимое **имя пользователя** и **пароль** (при необходимости).

Подтвердите выбор параметров, нажав кнопку **Применить**, для перехода к следующему шагу **Диспетчер загрузки AVG**.

4.4. Загрузка файлов для установки



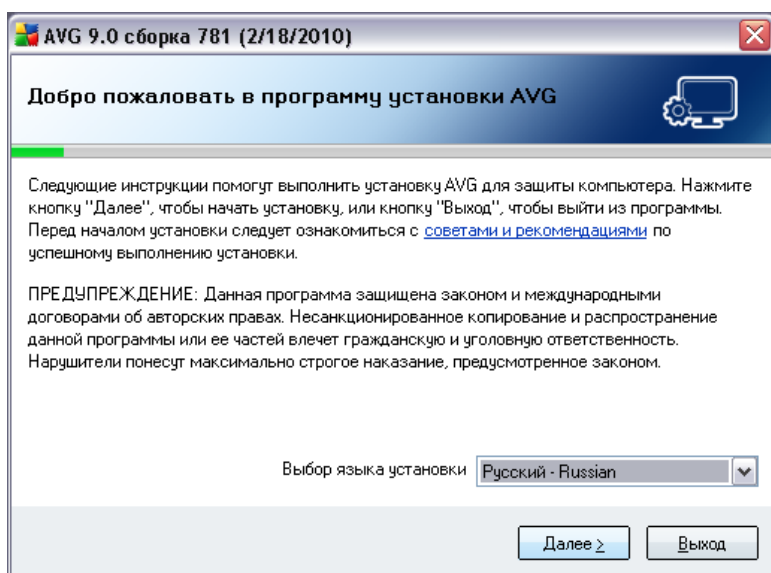
Теперь вы указали все необходимые сведения для загрузки пакета установки **Диспетчер загрузки AVG** и запуска процесса установки. Далее перейдите к пункту [Процесс установки AVG](#).

5. Процесс установки AVG

Для установки **AVG 9 Anti-Virus + Firewall** 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](#). Также можно воспользоваться новым инструментом [Диспетчер загрузки AVG](#), который поможет создать и загрузить необходимый пакет установки и запустить процесс установки.

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

5.1. Запуск установки

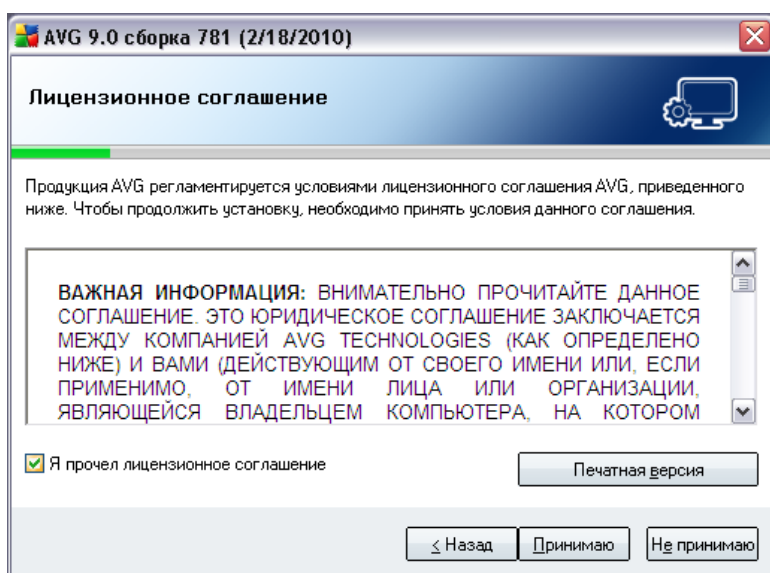


Процесс установки начинается с открытия окна **Вас приветствует программа установки AVG**. В данном окне необходимо выбрать язык, который будет использоваться во время процесса установки. В нижней части диалогового окна найдите элемент **Выбор языка установки** и выберите в раскрывающемся меню необходимый язык. Затем нажмите кнопку **Далее**, чтобы подтвердить выбор и перейти к следующему диалоговому окну.

Обратите внимание: с помощью данного окна выбирается язык только для процесса установки. В данном окне не выбирается язык для приложения AVG. Это

можно сделать позже во время процесса установки.

5.2. Лицензионное соглашение



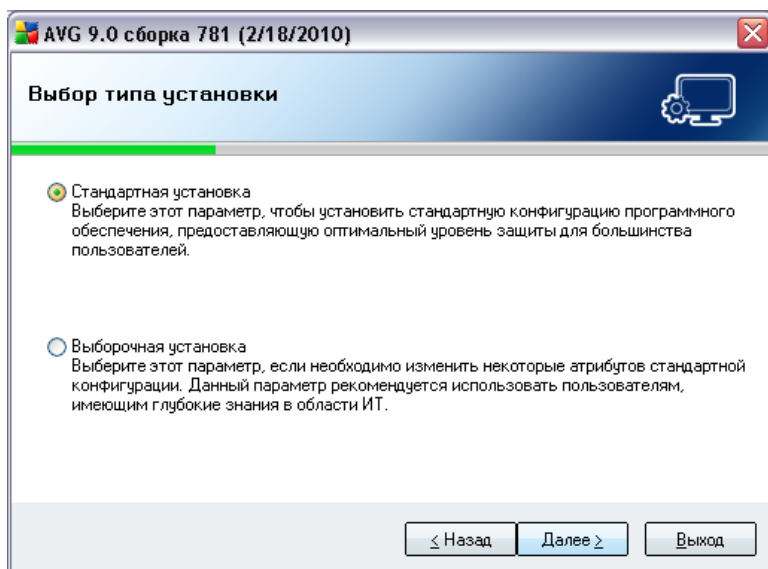
Диалоговое окно **Лицензионное соглашение** содержит полную версию лицензионного соглашения AVG. Прочитайте его внимательно и подтвердите, что вы прочитали, понимаете и принимаете соглашение, установив флажок **Я прочитал лицензионное соглашение** и нажав кнопку **Принять**.

Если вы не согласны с лицензионным соглашением, нажмите кнопку **Не принимать**. Процесс установки будет немедленно прерван.

5.3. Проверка состояния системы

После подтверждения пользовательского соглашения вы будете перенаправлены в диалоговое окно **Проверка состояния системы**. Данное диалоговое окно не требует от пользователя никаких действий. Перед началом установки AVG будет выполнена проверка системы. Дождитесь завершения процесса, после чего вы будете автоматически перенаправлены в следующее диалоговое окно.

5.4. Выбор типа установки



Диалоговое окно **Выбор типа установки** позволяет выбрать один из двух вариантов установки: **стандартная** и **выборочная** установка.

Для большинства пользователей рекомендуется выбирать **стандартную установку**, которая выполняется полностью в автоматическом режиме, устанавливая AVG с настройками, предварительно заданными поставщиком программного обеспечения. Данный вариант установки обеспечивает максимальный уровень защиты наряду с оптимальным уровнем использования ресурсов. Если в дальнейшем потребуются изменить конфигурацию, это всегда можно будет сделать напрямую в приложении AVG.

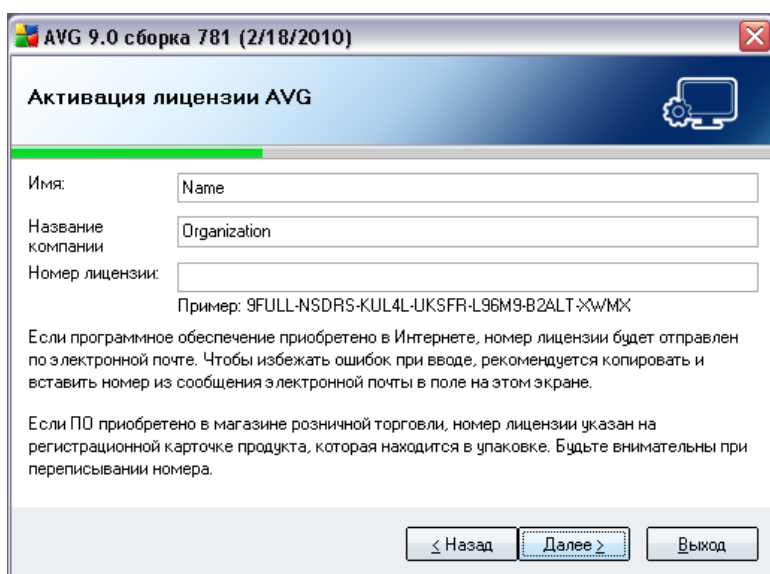
Выборочную установку следует использовать только опытным пользователям, у которых есть значительные основания для установки приложения AVG с параметрами, отличными от стандартных (например, при наличии специальных системных требований).

5.5. Активация лицензии AVG

В диалоговом окне **Активация лицензии AVG** необходимо указать регистрационные сведения. Введите свое имя (в поле **Имя пользователя**) и название организации (в поле **Название компании**).

Затем введите номер лицензии или номер продажи в текстовое поле **Номер**

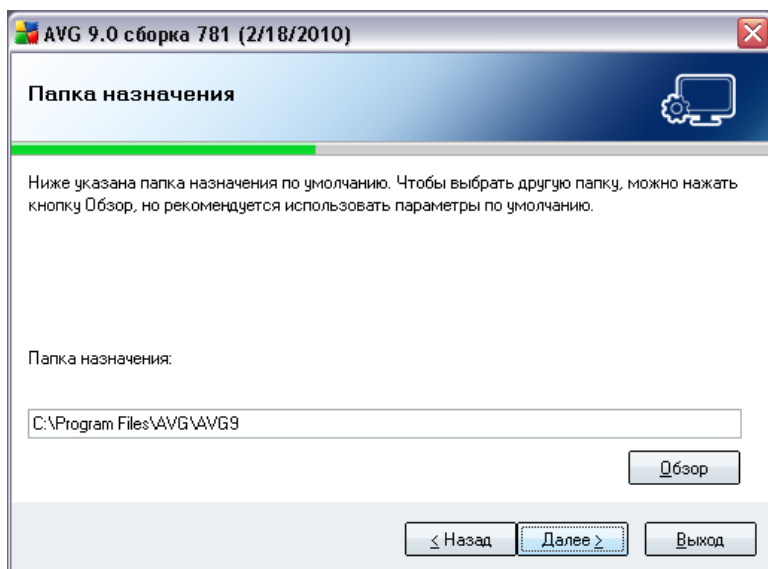
лицензии. Номер продажи указан на футляре компакт-диска в коробке **AVG 9 Anti-Virus + Firewall**. Номер лицензии будет указан в подтверждающем сообщении электронной почты, которое будет получено после оформления покупки **AVG 9 Anti-Virus + Firewall** через Интернет. Необходимо правильно ввести номер. Номер лицензии в цифровом виде (*приведенный в сообщении электронной почты*) можно вставить с использованием стандартного метода копирования и вставки.



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

Если на предыдущем шаге была выбрана стандартная установка, то автоматически произойдет переход в диалоговое окно [AVG Security Toolbar](#). Если была выбрана выборочная установка, откроется диалоговое окно [Папка назначения](#).

5.6. Выборочная установка — Папка назначения

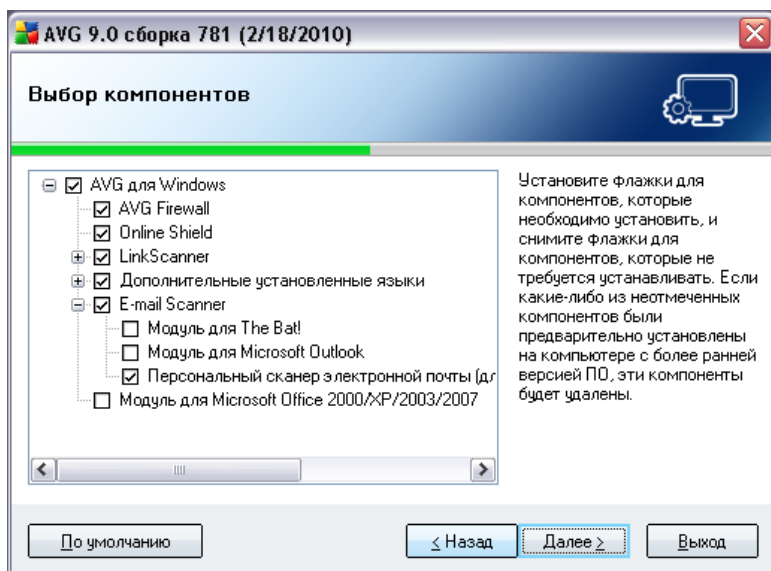


В диалоговом окне **Папка назначения** можно выбрать папку, в которую будет установлена система **AVG 9 Anti-Virus + Firewall**. По умолчанию установка AVG выполняется в папку Program Files, которая расположена на диске C:. Если папка еще не существует, в новом диалоговом окне будет предложено подтвердить создание новой папки для AVG.

Чтобы изменить это местоположение, используйте кнопку **Обзор**, после нажатия которой отобразится структура дисков, в которой можно выбрать соответствующую папку.

Для подтверждения нажмите кнопку **Далее**.

5.7. Выборочная установка — Выбор компонентов



Диалоговое окно **Выбор компонентов** содержит обзор всех компонентов **AVG 9 Anti-Virus + Firewall**, которые могут быть установлены. Если настройки параметров по умолчанию вам не подходят, можно добавить или удалить определенные компоненты.

При этом можно выбирать только компоненты, включенные в купленную версию AVG. Только данные компоненты можно выбрать в диалоговом окне "Выбор компонента".

• Выбор языка

В списке устанавливаемых компонентов можно указать язык (или несколько языков), который будет использоваться при установке AVG. Установите флажок **Дополнительные установленные языки**, а затем выберите необходимые языки в соответствующем меню.

• Модули E-mail Scanner

Щелкните элемент **E-mail Scanner**, чтобы открыть данный компонент и указать, какие модули следует установить для обеспечения безопасности электронной почты. По умолчанию будет установлен **модуль для Microsoft Outlook**. Также можно установить **Модуль для The Bat!**. При использовании других клиентов электронной почты (*MS Exchange, Qualcomm Eudora...*) установите параметр **Персональный сканер электронной почты**, чтобы



автоматически настроить защиту электронной почты независимо от используемой почтовой программы.

Чтобы продолжить, нажмите кнопку **Далее**.

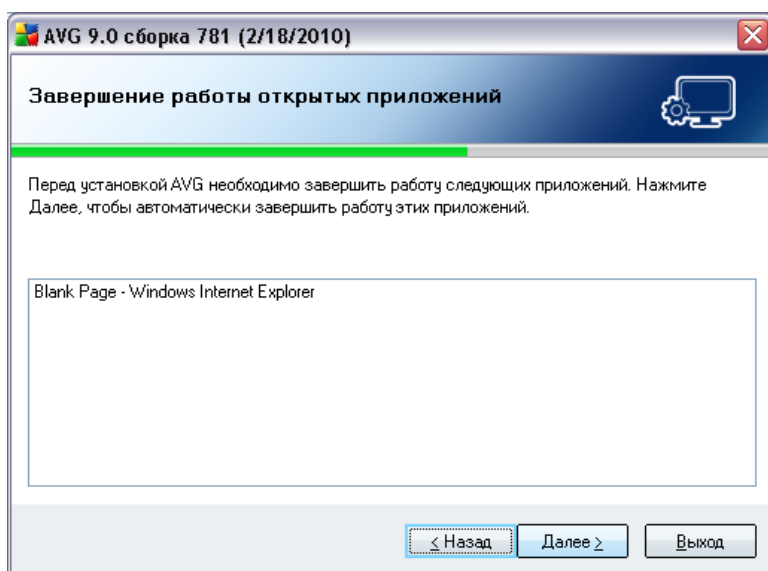
5.8. AVG Security Toolbar



В диалоговом окне **AVG Security Toolbar** укажите, следует ли установить компонент **AVG Security Toolbar** (проверка результатов поиска поддерживаемых поисковых служб в Интернете). 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 2.0 или выше), чтобы обеспечить всестороннюю защиту при работе в Интернете.

Также можно выбрать Yahoo! в качестве службы поиска по умолчанию. Для этого установите соответствующий флажок.

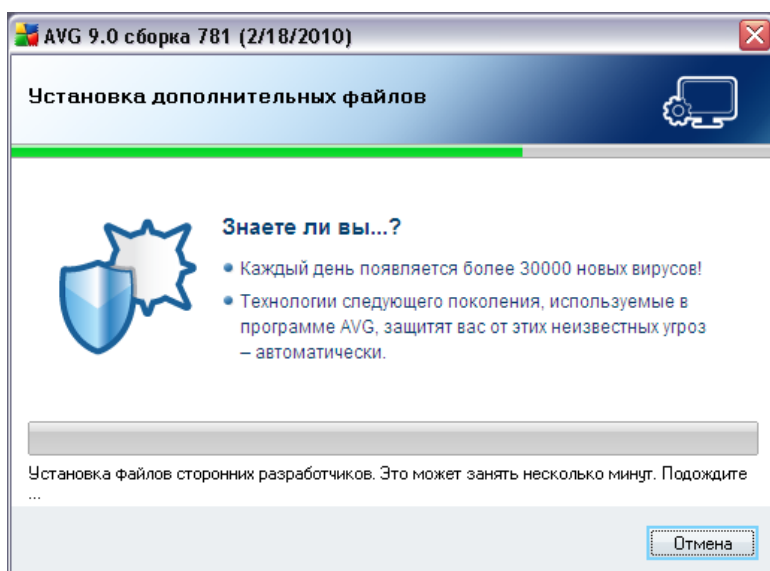
5.9. Завершение работы открытых приложений



Диалоговое окно **Завершение работы открытых приложений** отображается во время установки только в том случае, если на компьютере запущены программы, которые могут помешать установке. В этом случае в нем будет показан список программ, которые требуется завершить для успешной установки. Нажмите кнопку **Далее**, чтобы закрыть соответствующие приложения и перейти к следующему шагу.

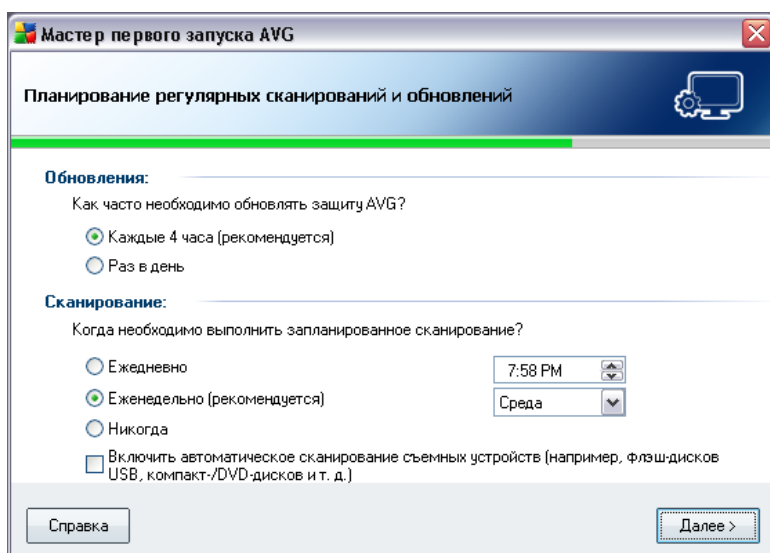
5.10. Установка AVG

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



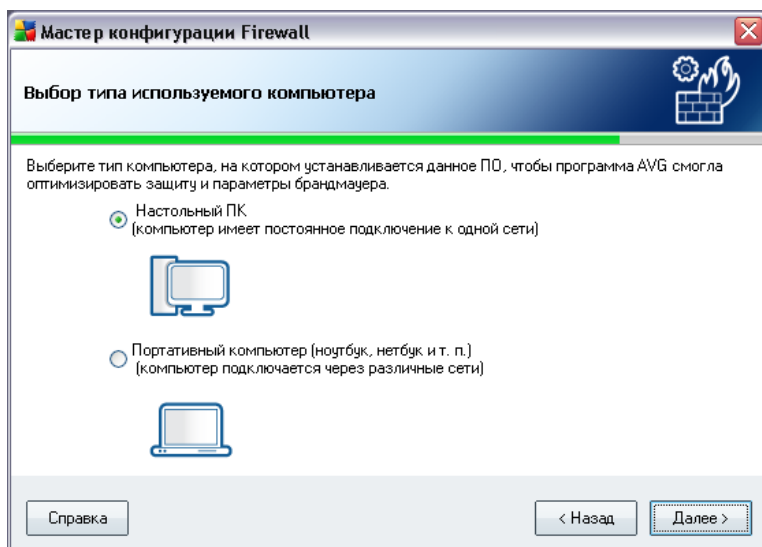
После завершения процесса установки переход к следующему диалоговому окну будет произведен автоматически.

5.1.1. Планирование регулярных сканирований и обновлений



В диалоговом окне **Планирование регулярных сканирований и обновлений** необходимо установить временной интервал проверки доступности новых файлов обновлений, а также определить время запуска [запланированного сканирования](#). Рекомендуется оставить значения по умолчанию. Нажмите кнопку **Далее**, чтобы продолжить.

5.12. Выбор типа используемого компьютера



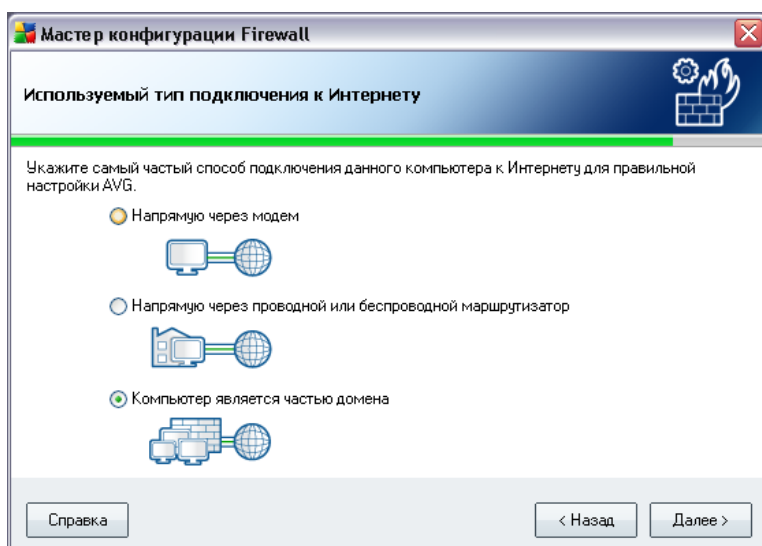
В этом диалоговом окне **Мастер настройки Firewall** запрашивает тип используемого компьютера. Например, для ноутбука, подключаемого к Интернету в различных местонахождениях (*аэропорты, гостиничные номера и т. п.*) требуется наличие более строгих правил безопасности, чем для компьютеров, принадлежащих определенному домену (*корпоративная сеть и т. п.*). В зависимости от типа используемого компьютера будут определены правила компонента **Firewall** по умолчанию с различными уровнями безопасности.

Можно выбрать один из двух вариантов:

- **Настольный компьютер**
- **Портативный компьютер**

Подтвердите свой выбор, нажав кнопку **Далее**. Нажатие данной кнопки приведет к открытию следующего диалогового окна.

5.13. Используемый тип подключения к Интернету



В данном диалоговом окне **Мастер настройки Firewall** запрашивает способ подключения компьютера к Интернету. На основе выбранного типа подключения определяются правила компонента **Firewall** по умолчанию с различными уровнями безопасности.

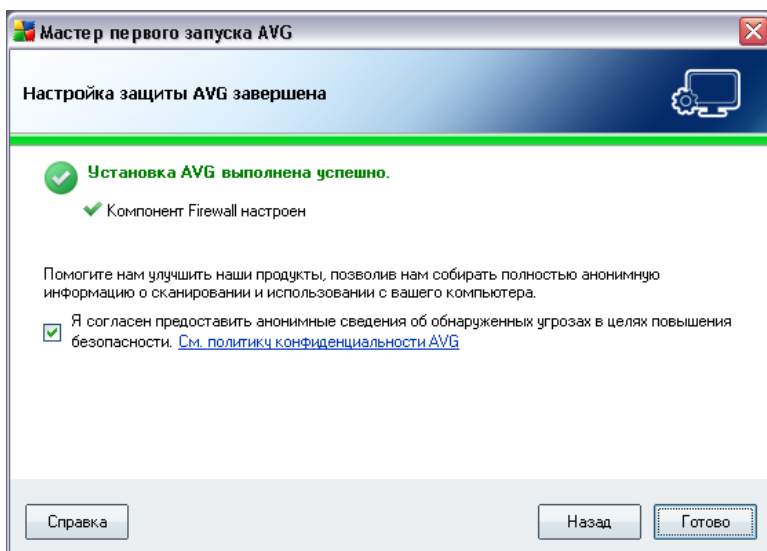
Доступно четыре параметра:

- **Напрямую через модем**
- **Напрямую через проводной или беспроводной маршрутизатор**
- **Компьютер является частью домена**

Выберите тип подключения, соответствующий используемому подключению к Интернету.

Подтвердите свой выбор, нажав кнопку **Далее**. Нажатие данной кнопки приведет к открытию следующего диалогового окна.

5.14. Настройка защиты AVG завершена



Теперь система **AVG 9 Anti-Virus + Firewall** настроена.

В данном окне можно включить или отключить функцию анонимного предоставления отчетов об эксплойтах и вредоносных сайтах в вирусную лабораторию AVG. Чтобы включить функцию, установите флажок **Я согласен предоставлять АНОНИМНЫЕ сведения об обнаруженных угрозах с целью повышения безопасности.**

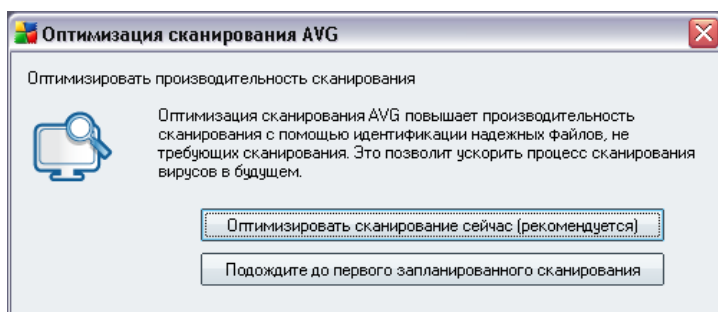
Затем нажмите кнопку **Готово**. Для начала работы с AVG необходимо перезагрузить компьютер.

6. После установки

6.1. Оптимизация сканирования

Функция оптимизации сканирования выполняет поиск в папках *Windows* и *Program files*. Она определяет соответствующие файлы в этих папках (*в данный момент такие файлы имеют расширения *.exe, *.dll и *.sys*) и сохраняет сведения о них. В следующий раз такие файлы не будут сканироваться, что значительно уменьшит время выполнения процедуры сканирования.

После завершения процесса установки в новом окне отобразится приглашение на оптимизацию сканирования.



Рекомендуется использовать эту функцию и запустить процесс оптимизации сканирования с помощью кнопки **Оптимизировать сканирование сейчас**.

6.2. Регистрация продукта

После завершения установки **AVG 9 Anti-Virus + Firewall** выполните регистрацию продукта через Интернет на веб-сайте 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.

6.3. Доступ к интерфейсу пользователя

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

- с помощью двойного щелчка значка AVG на панели задач



- с помощью двойного щелчка значка AVG на рабочем столе
- с помощью меню **Пуск/Все программы/AVG 9.0/Интерфейс пользователя AVG**

6.4. Сканирование всего компьютера

Существует потенциальная опасность того, что до установки **AVG 9 Anti-Virus + Firewall** компьютер был заражен вирусом. Поэтому необходимо запустить [сканирование всего компьютера](#), чтобы убедиться, что компьютер не заражен.

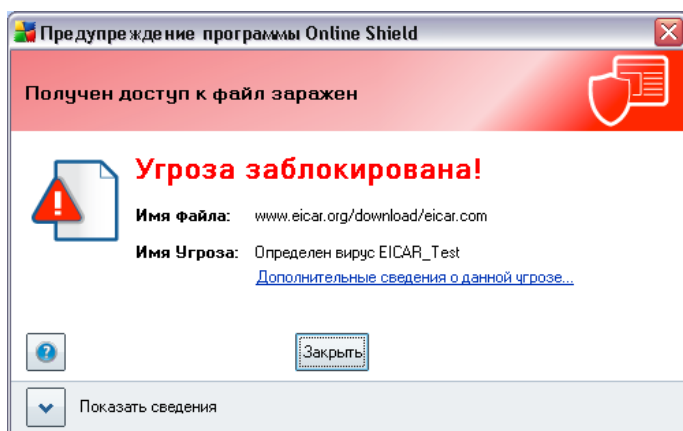
Инструкции по запуску [сканирования всего компьютера](#) см. в главе [Сканирование AVG](#).

6.5. Тестирование EICAR

Чтобы проверить правильность установки **AVG 9 Anti-Virus + Firewall**, можно выполнить тест EICAR.

Тестирование EICAR — стандартный и абсолютно безопасный метод для тестирования работы антивирусных систем. Оно безопасно, так как не является настоящим вирусом и не включает в себя фрагментов 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.



С веб-сайта <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.**

6.6. Настройки AVG по умолчанию

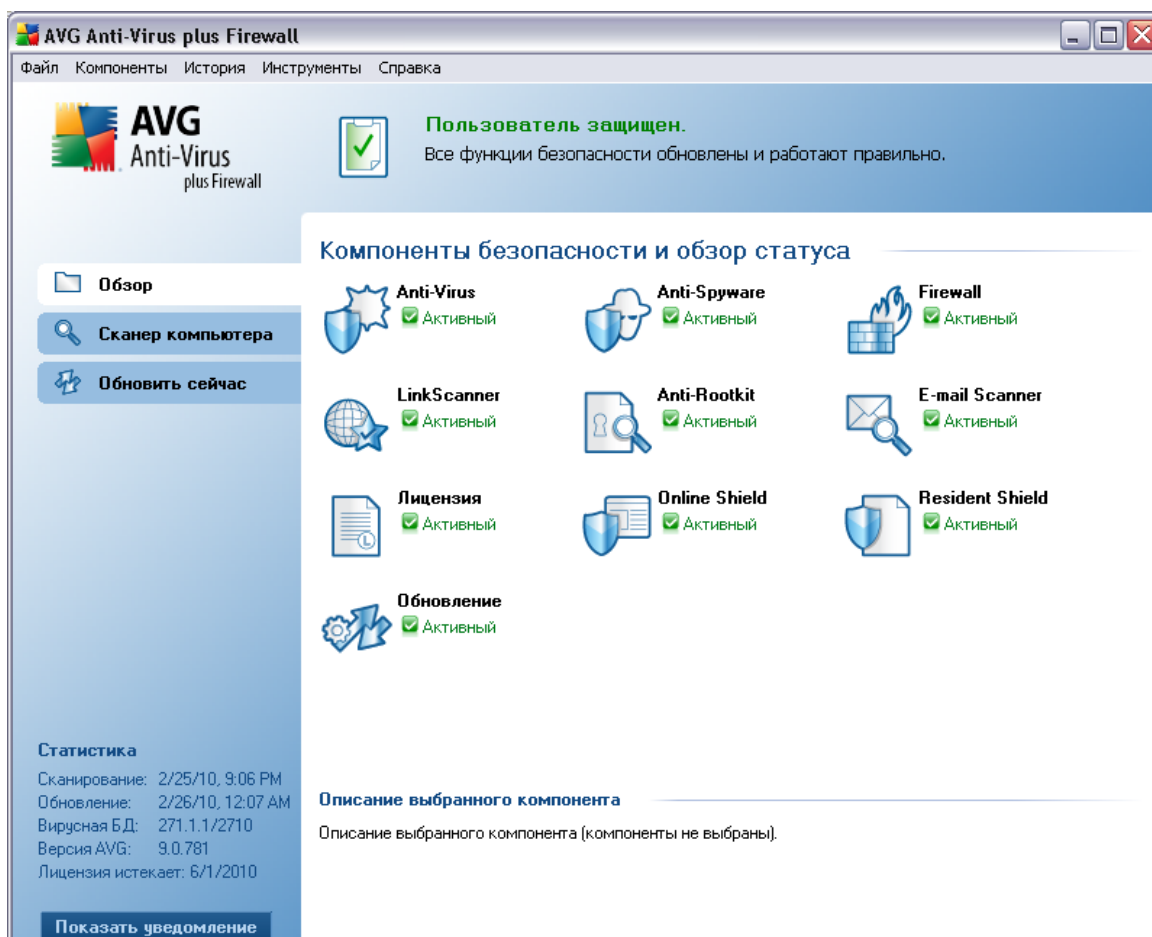
Параметры по умолчанию (параметры приложения после установки) **AVG 9 Anti-Virus + Firewall** настроены поставщиком ПО таким образом, чтобы все компоненты и функции обеспечивали оптимальную производительность.

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](#).

7. Интерфейс пользователя AVG

AVG 9 Anti-Virus + Firewall открывается в главном окне.



Главное окно состоит из нескольких разделов.

- **Системное меню** (системная область в верхней части окна) — это стандартное средство навигации, с помощью которого можно получить доступ ко всем компонентам, службам и функциям. [Подробнее сведения >>](#)
- **Информация о состоянии безопасности** (верхняя часть окна). Информация о текущем состоянии программы AVG. [Подробнее сведения >>](#)
- **Быстрые ссылки** (левая часть окна). Позволяет получить быстрый доступ

к наиболее важным и часто используемым задачам AVG. [Подробнее сведения >>](#)

- **Обзор компонентов** (центральная часть окна). Обзор всех установленных компонентов. [Подробнее сведения >>](#)
- **Статистика** (левая нижняя часть окна). Статистическая информация о работе программы. [Подробнее сведения >>](#)
- **Значок на панели задач** (правая нижняя часть экрана, панель задач). Отображение текущего состояния AVG. [Подробнее сведения >>](#)

7.1. Системное меню

Системное меню — это стандартное средство навигации, которое используется во всех приложениях Windows. Оно расположено горизонтально в верхней части главного окна **AVG 9 Anti-Virus + Firewall**. С помощью системного меню можно получить доступ к специальным компонентам, службам и функциям AVG.

Системное меню состоит из двух основных разделов.

7.1.1. Файл

- **Выход**. Закрывание интерфейса **AVG 9 Anti-Virus + Firewall** пользователя. При нажатии данной кнопки приложение AVG продолжит свою работу в фоновом режиме, а компьютер будет находиться под защитой!

7.1.2. 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**. Открытие стандартной страницы компонента [Anti-Virus](#).
- **Anti-Rootkit**. Открытие стандартной страницы компонента [Anti-Rootkit](#).
- **Anti-Spyware** — открытие стандартной страницы компонента [Anti-Spyware](#).
- **Firewall**. Открытие стандартной страницы компонента [Firewall](#).

- **Link Scanner.** Открытие стандартной страницы компонента [Link Scanner](#).
- **E-mail Scanner** — открытие стандартной страницы компонента [E-mail Scanner](#).
- **License.** Открытие стандартной страницы компонента [Лицензия](#).
- **Online Shield.** Открытие стандартной страницы компонента [Online Shield](#).
- **Resident Shield.** Открытие стандартной страницы компонента [Resident Shield](#).
- **Диспетчер обновления.** Открытие стандартной страницы компонента [Диспетчер обновления](#).

7.1.3. История

- [Результаты сканирования](#). Переход в интерфейс проверки AVG в диалоговое окно [Обзор результатов сканирования](#).
- [Обнаружение Resident Shield](#) . Отображение диалогового окна с обзором 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 с обзором всех зарегистрированных в журнале действий **AVG 9 Anti-Virus + Firewall**.
- [Firewall](#). Открытие интерфейса параметров компонента Firewall на вкладке [Журналы](#), содержащей подробный обзор всех действий компонента Firewall

7.1.4. 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 9 Anti-Virus + Firewall**
- **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 9 Anti-Virus + Firewall**. В основном, рекомендуется не изменять стандартные параметры приложения, определенные производителем.
- **Параметры Firewall**. Открытие отдельного диалогового окна, содержащего дополнительные параметры компонента **Firewall**.

7.1.5. 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 9 Anti-Virus + Firewall** вместо последних двух элементов будут отображаться пункты **Купить** и **Активировать**, которые позволяют сразу приобрести полную версию программы. Для программы **AVG 9 Anti-Virus + Firewall**, 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 базе данных, системная информация, лицензионное соглашение, а также контактная информация **AVG Technologies CZ**.

7.2. 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 9 Anti-Virus + Firewall**. 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.



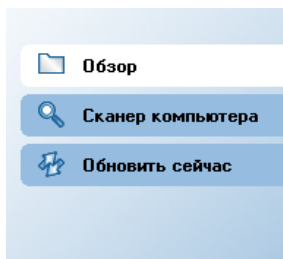
Красный значок означает критическое состояние AVG. Один или несколько компонентов работают неправильно, программа AVG не может защитить компьютер. Необходимо немедленно устранить указанные проблемы. Если проблему не удастся устранить самостоятельно, обратитесь в [службу технической поддержки AVG](#).

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](#).

7.3. 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. главу [Обзор компонентов >>](#)
- **Сканер компьютера**. Используйте данную ссылку для открытия интерфейса сканирования AVG, с помощью которого можно напрямую запускать проверки, запланированные сканирования или изменять их параметры — см. [Сканирование AVG >>](#)
- **Обновить сейчас**. Данная ссылка открывает интерфейс обновления и немедленно запускает процесс обновления 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.

7.4. 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 9 Anti-Virus + Firewall** раздел **Обзор компонентов** содержит сведения о следующих компонентах.

- **Anti-Virus**. Обеспечивает защиту от вирусов, проникающих на компьютер. [Подробные сведения >>](#)
- **Anti-Spyware**. Выполняет сканирование приложений в фоновом режиме при их запуске. [Подробные сведения >>](#)
- **Firewall**. Осуществляет контроль за обменом 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 >>](#)

- **Anti-Rootkit.** Предназначен для обнаружения программ и средств, пытающихся замаскировать вредоносное ПО. [Подробные сведения >>](#)
- **E-mail Scanner.** Проверяет входящие и исходящие сообщения электронной почты на наличие вирусов. [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 >>](#)
- **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 >>](#)

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](#).

7.5. Статистика

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

- **Последнее сканирование** — дата последнего выполненного сканирования.
- **Последнее обновление** — дата последнего запуска обновления.
- **Вирусная БД** — сведения о версии установленной вирусной базы данных.



- **Версия AVG** — сведения о версии установленной программы AVG (номер отображается в формате 9.0.xx, где 9.0 — это версия серии продуктов, а xx — номер сборки).
- **Срок окончания действия лицензии** — дата окончания срока действия лицензии AVG.

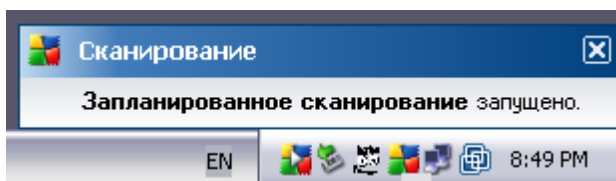
7.6. Значок на панели задач

Значок на панели задач (на панели задач Windows) указывает текущее состояние **AVG 9 Anti-Virus + Firewall**. 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, полноцветный значок AVG на панели задач отображается, 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](#).



- **Обновить** — немедленное [обновление программы](#).

8. Компоненты AVG

8.1. Anti-Virus

8.1.1. 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.

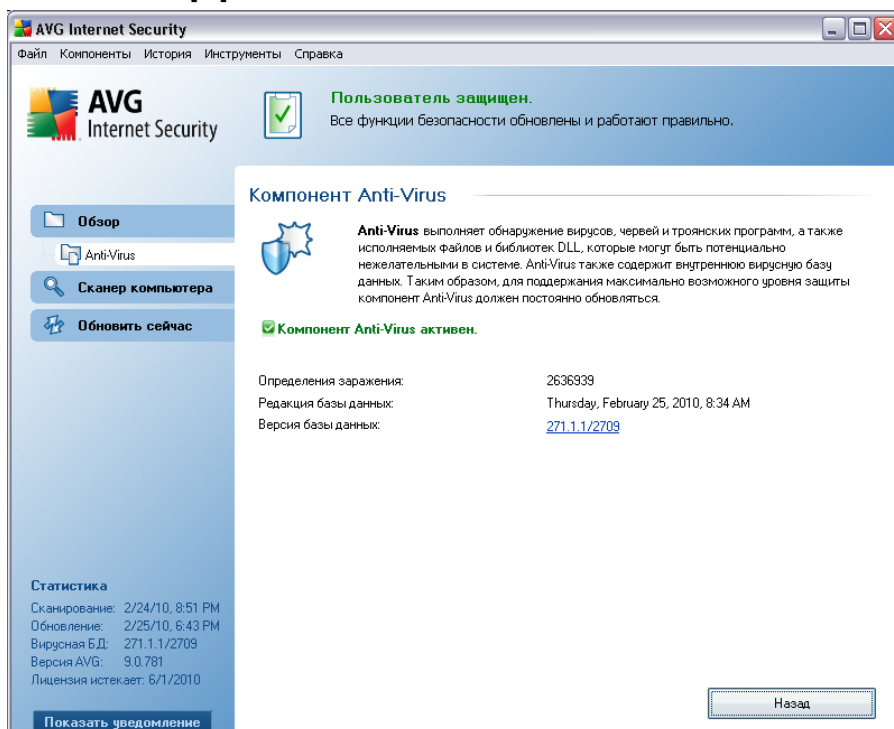
Важной чертой антивирусной защиты является тот факт, что ни один известный вирус не сможет запуститься на компьютере.

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.

8.1.2. 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**.

- **Определения заражений** — количество вирусов, определенных в последней версии вирусной базы данных
- **Последнее обновление базы данных** — дата и время последнего обновления базы данных
- **Версия базы данных** — 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).



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 во вновь открытом диалоговом окне [Расширенные настройки AVG](#).

8.2. Anti-Spyware

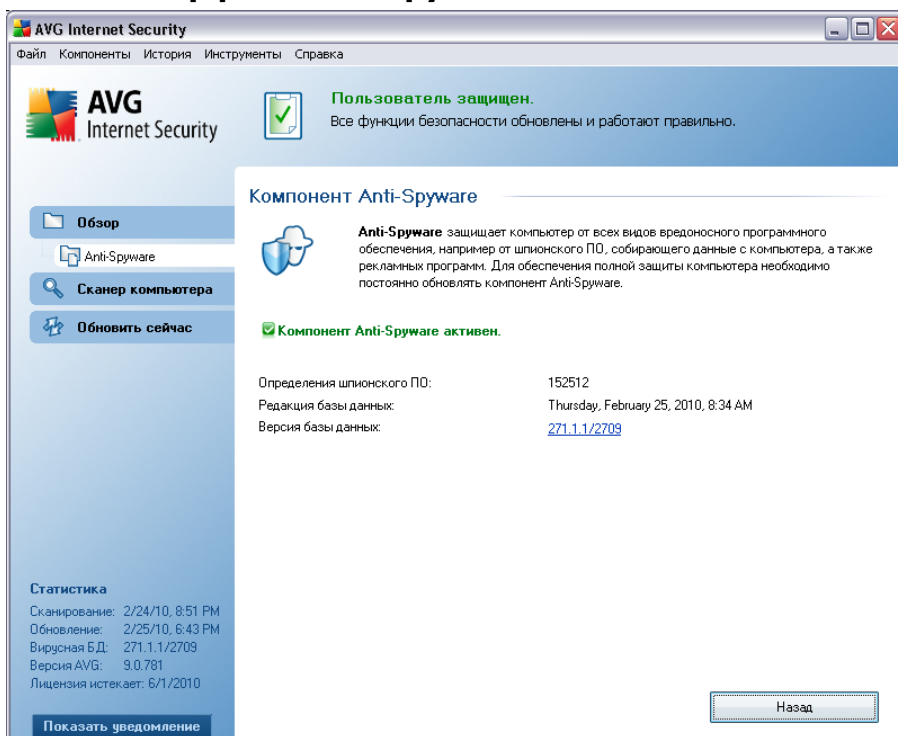
8.2.1. Принципы работы Anti-Spyware

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, аналогичного компоненту resident shield, который сканирует приложения при их запуске.

Также существует потенциальная опасность того, что вредоносное ПО может попасть на компьютер до установки программы AVG, а также если пользователь пренебрег обновлением базы данных **AVG 9 Anti-Virus + Firewall** и загрузкой обновлений программы [***](#). 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.

8.2.2. Интерфейс Anti-Spyware



Интерфейс компонента **Anti-Spyware** содержит краткий обзор функций компонента, сведения о текущем состоянии компонента (компонент *Anti-Spyware* активен.), а также некоторые сведения статистики **Anti-Spyware**:

- **Определение шпионского ПО.** Обеспечивает подсчет образцов шпионского ПО, определенного в последней версии базы данных шпионского ПО.
- **Последнее обновление базы данных** — определяет, когда и в какое время была обновлена база данных шпионского ПО
- **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).

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 во вновь открытом диалоговом окне [Расширенные настройки AVG](#).

8.3. 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 скрывание запущенных процессов от следящих программ, а файлов и системных данных — от операционных систем.

8.4. 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.

8.4.1. 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.

8.4.2. 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 разный 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). Данный системный профиль невозможно копировать или удалить. Его параметры также не могут быть изменены.
- **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. Данный системный профиль невозможно копировать или удалить. Его параметры также не могут быть изменены.
- **Пользовательские профили:**
 - **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.
 - **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.
 - **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.

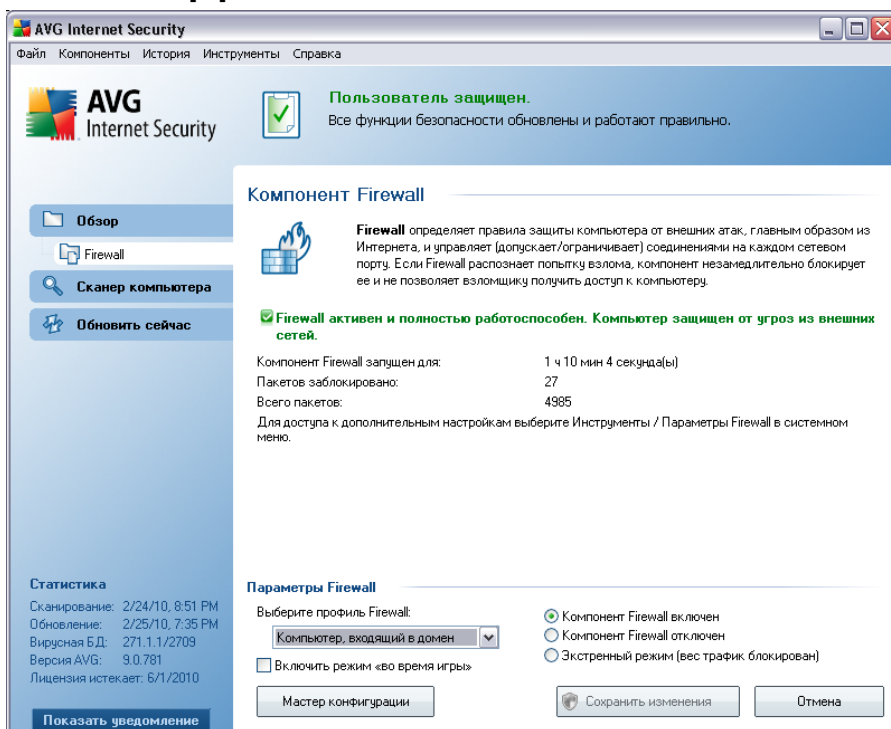
Переключение профиля

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.

8.4.3. Интерфейс Firewall



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

- **Время работы компонента Firewall** — время, прошедшее с последнего запуска компонента Firewall
- **Пакетов заблокировано** — количество заблокированных пакетов из общего числа проверенных пакетов
- **Всего пакетов** — количество пакетов, проверенных компонентом Firewall

Основные настройки компонента

- **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 PowerPoint и др.) компонент **Firewall** не отображал 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.
- **Состояние компонента Firewall.**
 - **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.

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 Firewall выберите элемент системного меню **Инструменты/Параметры Firewall** и исправьте настройки Firewall в новом открытом диалоговом окне **Параметры Firewall**.

Кнопки управления

- **Мастер настройки** — нажмите данную кнопку, чтобы открыть соответствующее диалоговое окно (используемое в процессе установки) **Выбор типа используемого компьютера**, в котором можно указать конфигурацию компонента **Firewall**.
- **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)

8.5. 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.

8.5.1. Принципы работы E-mail Scanner

Компонент **E-mail Scanner** автоматически сканирует входящие и исходящие сообщения электронной почты. Его можно использовать с клиентами электронной почты, которые не имеют модуля в AVG (*например, Outlook Express, Mozilla, Incrimail и т. п.*).

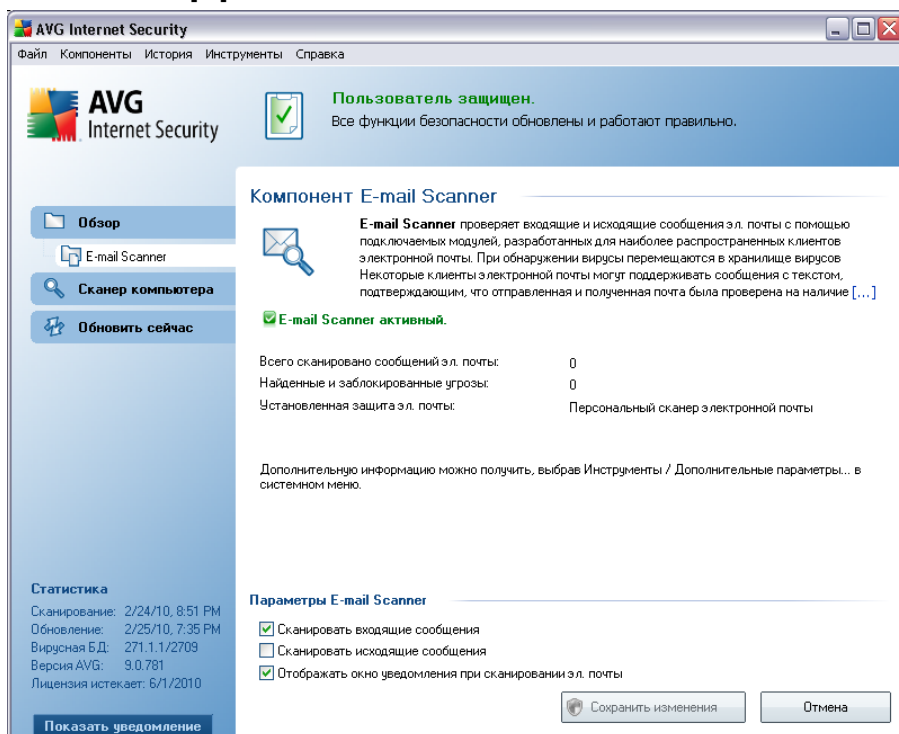
При [установке](#) AVG создаются автоматические серверы для управления электронной почтой: один для проверки входящих сообщений электронной почты, второй для проверки исходящих сообщений. С помощью этих двух серверов сообщения электронной почты автоматически проверяются на портах 110 и 25 (*стандартные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

8.5.2. Интерфейс E-mail Scanner



С помощью диалогового окна компонента **E-mail Scanner** можно получить краткие сведения о работе компонента и информацию о текущем состоянии компонента (*E-mail Scanner активен*), а также 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

Основные настройки компонента

В нижней части диалогового окна расположен раздел **Настройки 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, не рекомендуется изменять значение 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 значок 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.

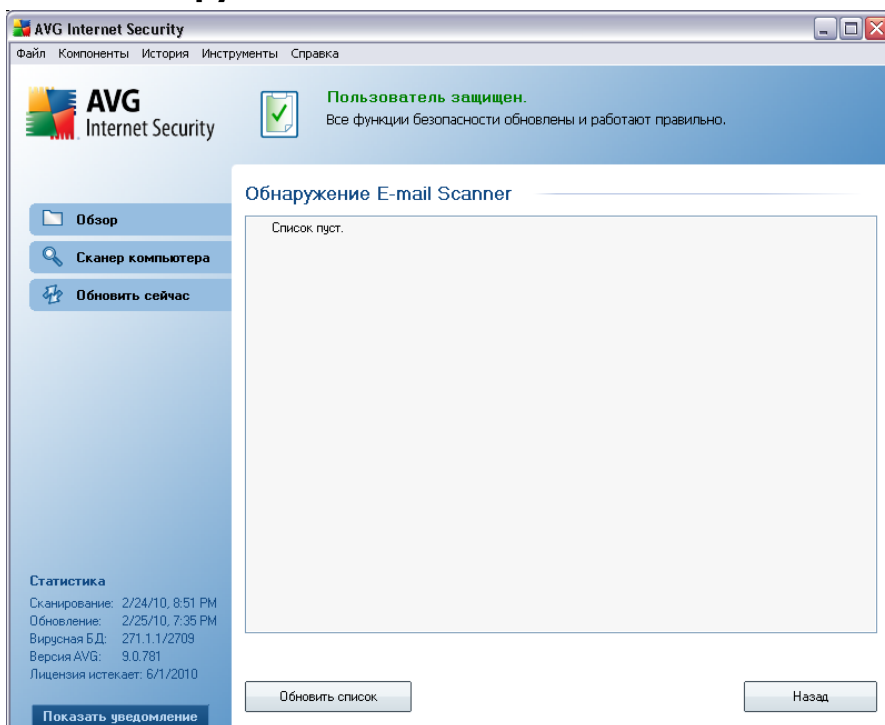
Примечание. Все компоненты AVG настроены поставщиком ПО для обеспечения оптимального качества работы. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться только опытным пользователем. При необходимости изменить настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG во вновь открытом диалоговом окне [Расширенные настройки 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)

8.5.3. Обнаружение E-mail Scanner



Диалоговое окно **Обнаружение E-mail Scanner** (доступное в системном меню "История"/"Обнаружение E-mail Scanner") содержит список всех обнаруженных компонентом **E-mail Scanner** объектов. Для каждого обнаруженного объекта 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



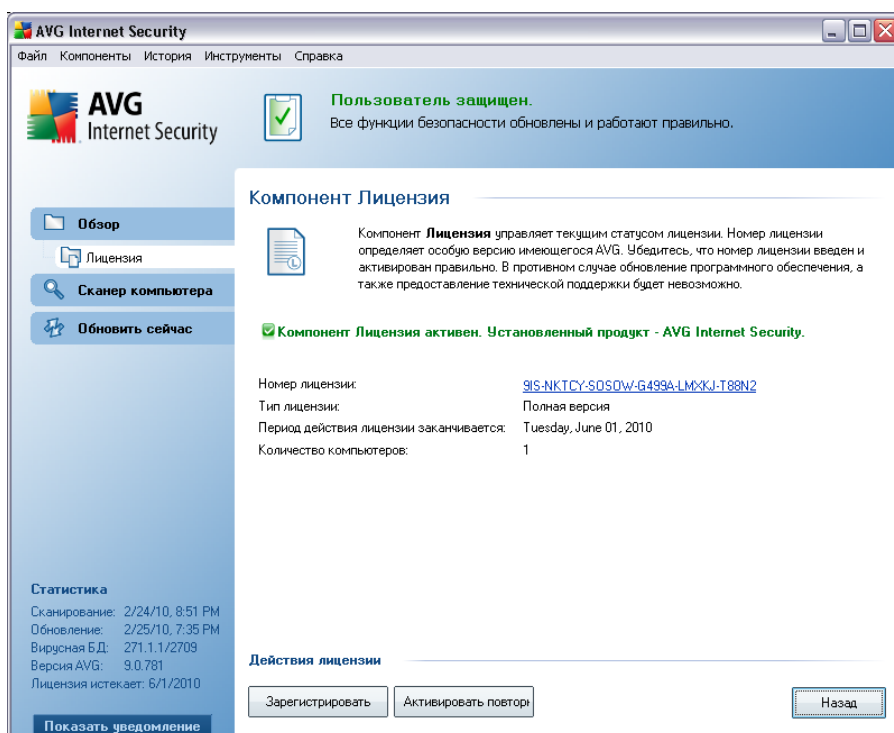
экспортировать весь список обнаруженных объектов в файл (**Экспортировать список в файл**) и удалить все записи об обнаруженных объектах (**Очистить список**).

Кнопки управления

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

- **Обновить список** — обновление списка обнаруженных угроз
- **Назад** — переход к интерфейсу пользователя AVG по умолчанию (обзор компонентов)

8.6. Лицензия



С помощью интерфейса компонента **Лицензия** можно получить краткие сведения о работе компонента и информацию о текущем состоянии (*компонент "Лицензия" активен.*), а также следующую информацию.

- **Номер лицензии** — номер лицензии вашего продукта. Необходимо правильно ввести номер лицензии. Настоятельно рекомендуется использовать способ "копировать/вставить" для любых операций с номером лицензии.
- **Тип лицензии** — указывает тип устанавливаемого продукта
- **Срок окончания действия лицензии** — данная дата определяет период действия лицензии. Чтобы использовать **AVG 9 Anti-Virus + Firewall** после окончания срока действия лицензии, потребуется выполнить продление срока действия лицензии. Обновление лицензии может быть выполнено в Интернете на веб-сайте AVG (<http://www.avg.com/>).
- **Количество компьютеров** — количество рабочих станций, на которые пользователь может установить приложение **AVG 9 Anti-Virus + Firewall**.

Кнопки управления

- **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.
- **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 9 Anti-Virus + Firewall** кнопки будут называться **Купить** и **Активировать**. С их помощью можно сразу купить полную версию программы. Для программы **AVG 9 Anti-Virus + Firewall**, при установке которой был указан номер продажи, будут отображаться кнопки **Зарегистрировать** и **Активировать**.

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

8.7. Link Scanner

8.7.1. Принципы работы Link Scanner

Компонент **LinkScanner** обеспечивает защиту от веб-сайтов, созданных для установки вредоносного ПО через веб-браузер или его модули. Технология **LinkScanner** включает в себя две функции: [**AVG Search-Shield**](#) и [**AVG Active Surf-Shield**](#):

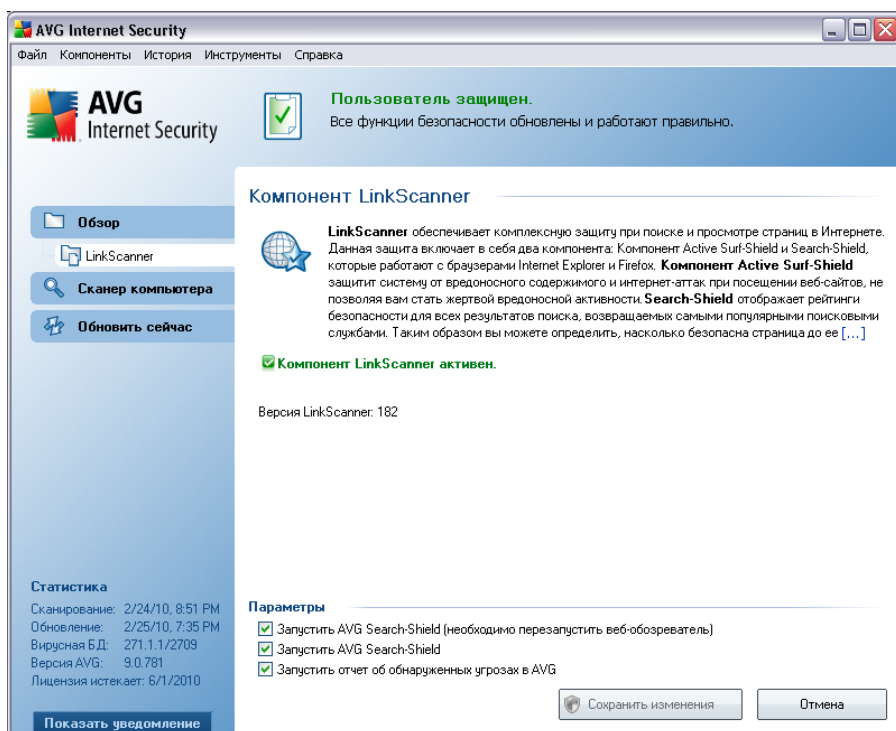
- [**AVG Search-Shield**](#) содержит список известных опасных веб-сайтов (*URL-адресов*). При выполнении поиска в Google, Yahoo!, Bing, Baidu, Altavista или Yandex все результаты поиска проверяются в соответствии с этим списком. После этого отображается значок заключения (для результатов поиска Yahoo! отображаются только значки заключения о наличии эксплойтов на веб-сайтах). Кроме того, когда пользователь вводит адрес в браузер, щелкает ссылку на веб-сайте или, например, в сообщении электронной почты, функция AVG Search-Shield автоматически проверяет объект и блокирует его при необходимости.
- [**AVG Active Surf-Shield**](#) выполняет сканирование содержимого посещаемых веб-сайтов независимо от наличия их адресов в списке. Даже если опасный веб-сайт не обнаружен с помощью [**AVG Search Shield**](#) (например, если он был создан недавно или если ранее безопасный веб-сайт теперь содержит вредоносное ПО), он будет выявлен и заблокирован с помощью [**AVG Active Surf-Shield**](#) при попытке его посещения.

Примечание. AVG Link Scanner не предназначен для использования на серверных платформах.

8.7.2. Интерфейс Link Scanner

Компонент **LinkScanner** состоит из двух частей, которые можно включать и отключать с помощью интерфейса компонента **LinkScanner**.

Интерфейс компонента **LinkScanner** содержит краткое описание функций компонента и сведения о его текущем состоянии (*компонент LinkScanner включен*). Также можно просмотреть сведения о последней версии базы данных **LinkScanner** (*|Версия LinkScanner*).



В нижней части диалогового окна можно изменить некоторые параметры:

- **Включить AVG Search-Shield** (по умолчанию флажок установлен). При выполнении поиска в Google, Yahoo!, Bing, Baidu, Yandex или Altavista будут отображаться информационные значки после проверки содержимого найденных сайтов.
- **Включить AVG Active Surf-Shield** (включен по умолчанию). Активная (в режиме реального 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).
- **Включить отправку отчетов об обнаруженных угрозах в AVG.** Отметьте данный элемент, чтобы включить отправку отчетов об атаках и вредоносных сайтах, обнаруженных пользователями с помощью функций **Safe Surf** или **Safe Search**, для пополнения базы данных информацией о вредоносной активности в Интернете.

8.7.3. AVG Search-Shield

При поиске в Интернете с включенной системой **AVG Search-Shield** все результаты поиска, возвращаемые наиболее популярными поисковыми службами, такими как Yahoo!, Google, Bing, Altavista, Yandex и т. д. 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.

 Связанная страница безопасна (при использовании поисковой службы Yahoo! с компонентом [AVG Security Toolbar](#) данный значок отображаться не будет!).

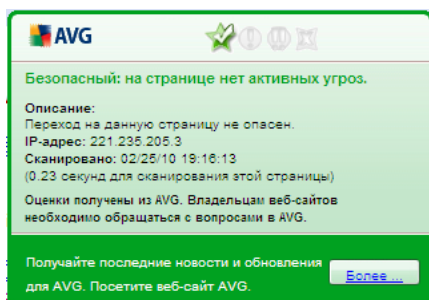
 Связанная страница не содержит угроз, но является подозрительной (из-за своего происхождения или особенностей работы). Поэтому не рекомендуется совершать покупки по данной ссылке и производить другие важные операции.).

 Связанная страница может быть безопасной, но содержать дальнейшие ссылки на зараженные страницы, или иметь подозрительный код, не представляющий угрозы 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. Сведения включают в себя дополнительную информацию об угрозе (если она имеется), IP-адрес и время сканирования страницы программой AVG:



8.7.4. AVG Active 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.

8.8. Online Shield

8.8.1. Принципы работы Online Shield

Online Shield представляет собой 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.

Функция Online Shield предназначена 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.

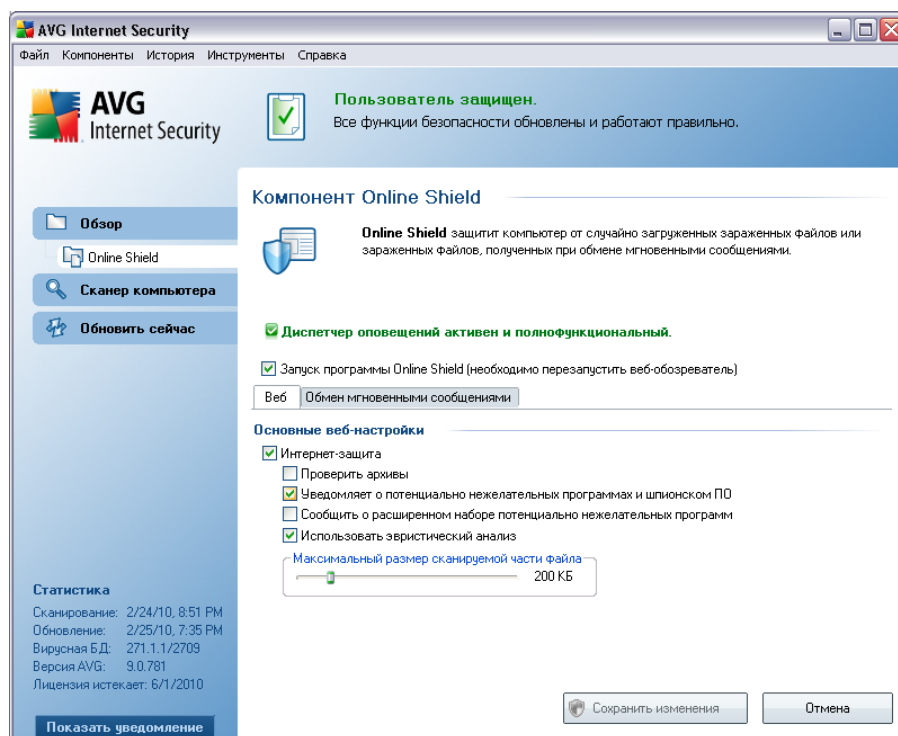
8.8.2. Интерфейс Online Shield

Интерфейс компонента **Online Shield** позволяет определить особенности работы данного типа защиты. Далее находятся сведения о текущем состоянии компонента (*Online Shield активен и полностью функционирует.*). В нижней части диалогового окна находятся начальные параметры функционирования данного компонента.

Основные настройки компонента

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, на двух вкладках можно изменить другие параметры конфигурации.

- **Веб** — изменение параметров компонента, относящихся к сканированию содержимого веб-сайта. Интерфейс редактирования позволяет настроить следующие начальные параметры.



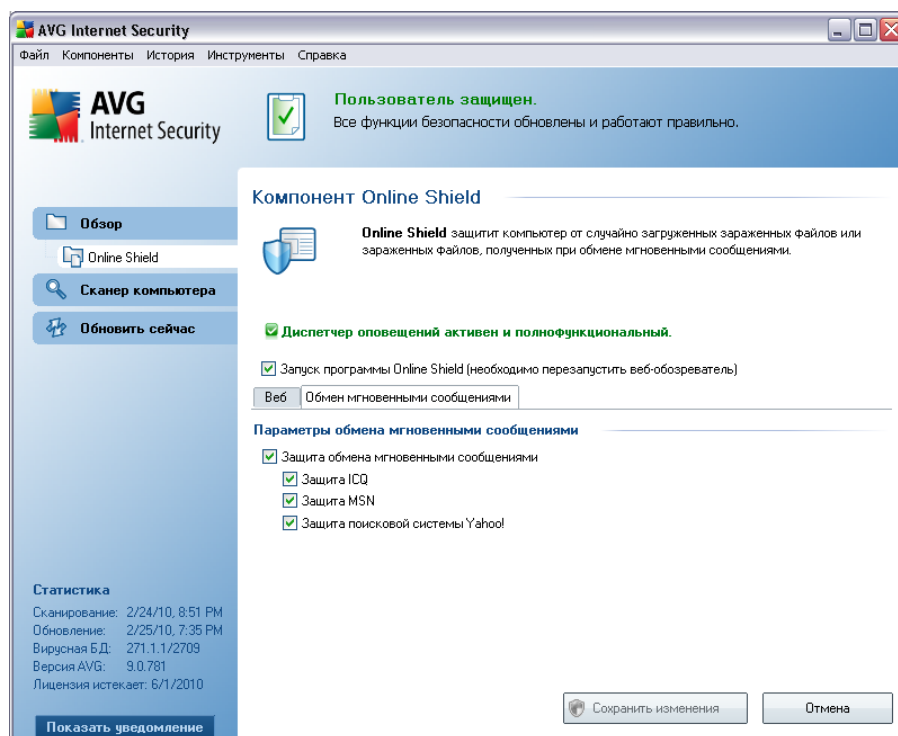
о **Интернет-защита**— данный параметр подтверждает, что компонент **Online Shield** должен сканировать содержимое интернет-станиц. Данный параметр (*включен по умолчанию*) позволяет включать/отключать следующие элементы.

- **Проверка архивов** — сканирование содержимого архивов, которые могут содержаться на отображаемых на интернет-страницах.
- **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО** (флажок установлен по умолчанию). Установите флажок для активации компонента [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. Если предыдущий параметр активирован, можно также выбрать данный параметр для определения расширенного набора [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.

- **Использовать эвристический анализ.** Сканирование содержимого отображаемой страницы с использованием метода эвристического анализа (имитация и оценка команд сканируемых объектов в виртуальной компьютерной среде. Поэтому возможно обнаружение злоумышленного кода, даже не описанного в базе данных вирусов (см. [Принципы работы Anti-Virus](#)).
- **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.

- **Мгновенные сообщения** . Позволяет изменять параметры компонентов, касающихся сканирования мгновенных сообщений (*например, ICQ, MSN Messenger, Yahoo...*).



- о Защита мгновенных сообщений. Установите данный флажок, чтобы компонент Online Shield выполнял проверку мгновенных сообщений на вирусы. После включения данного параметра можно указать, какую прикладную программу для обмена мгновенными сообщениями необходимо контролировать. На данный момент **AVG 9 Anti-Virus + Firewall** поддерживает приложения ICQ, MSN и Yahoo.

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 во вновь открытом диалоговом окне [Расширенные настройки AVG](#).

Кнопки управления

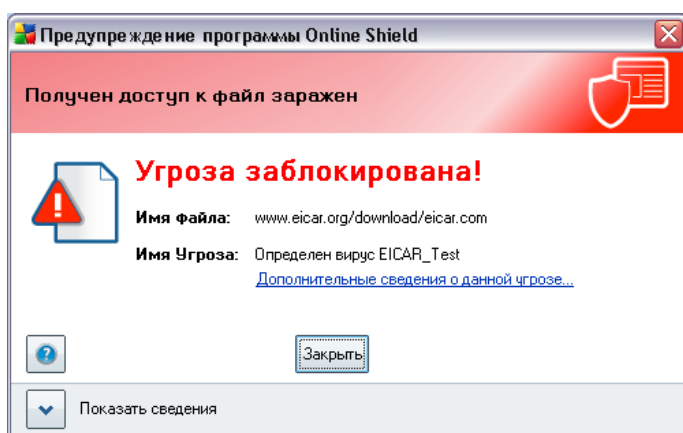
В окне компонента **Online Shield** имеются следующие кнопки управления.

- **Сохранить изменения** — нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне

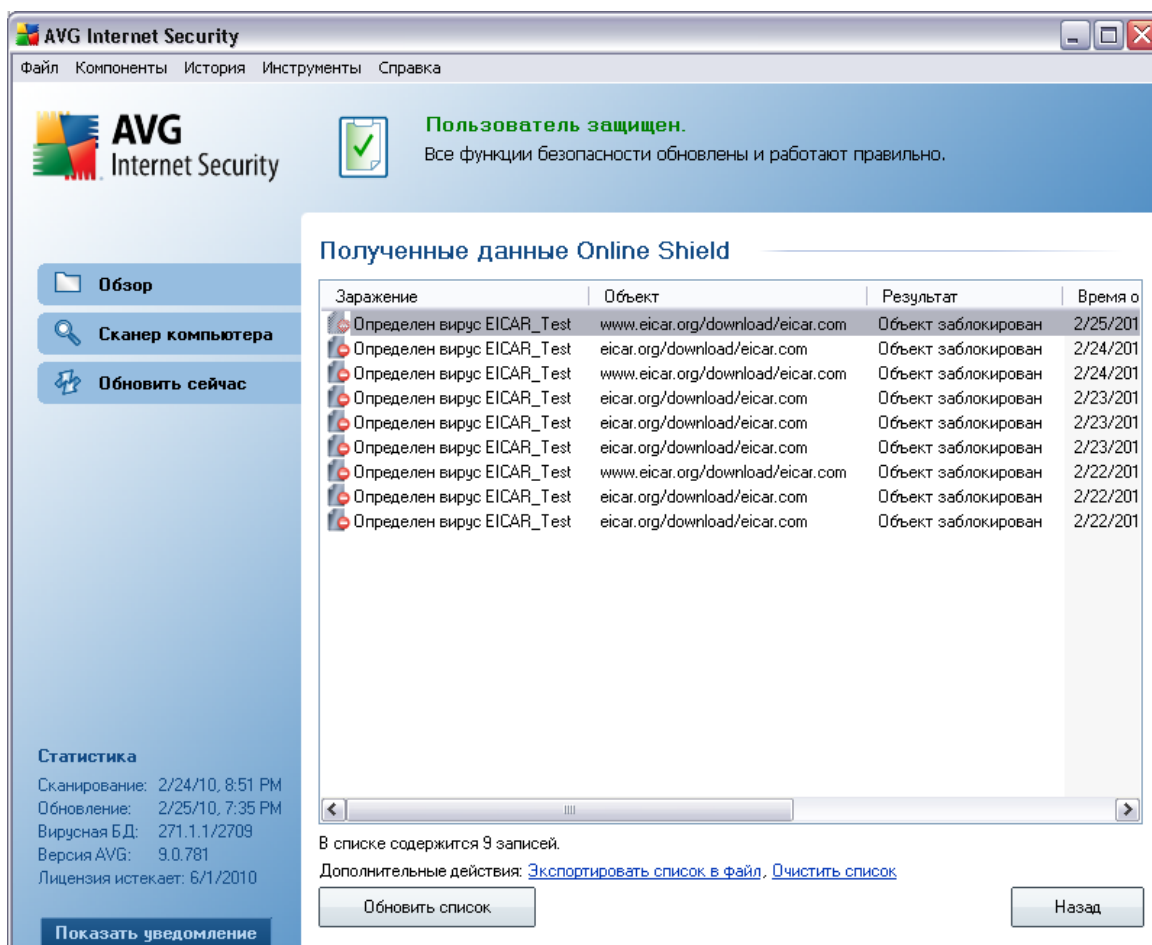
- **Отмена** — нажмите данную кнопку для возврата к установленному по умолчанию [интерфейсу пользователя AVG](#) (*обзор компонентов*)

8.8.3. 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:



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 переключение к [интерфейсу пользователя AVG](#) (по умолчанию обзор компонентов).

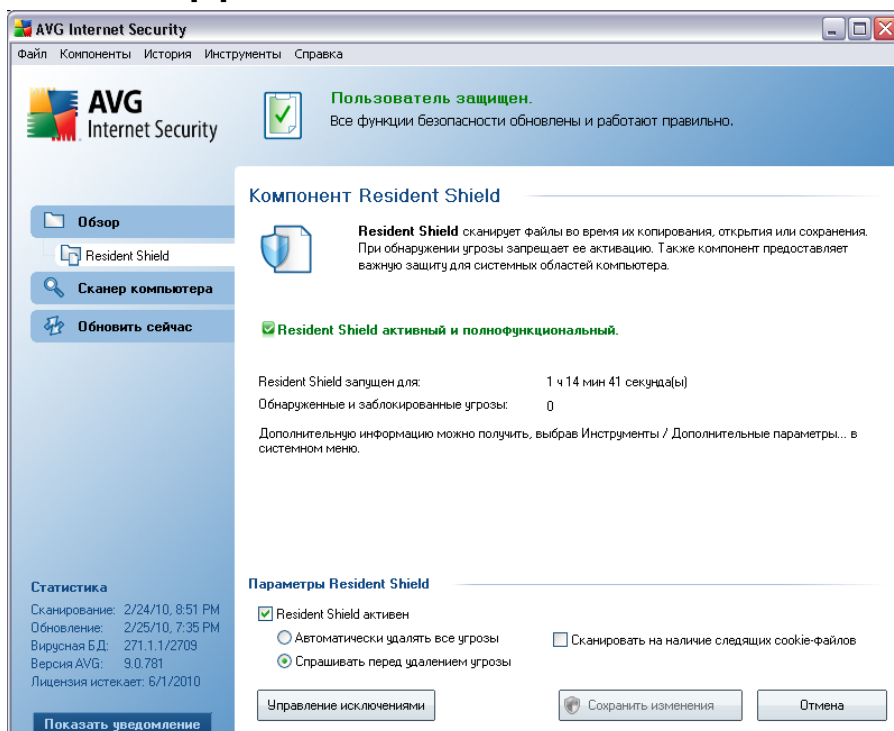
8.9. Resident Shield

8.9.1. 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.

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

8.9.2. Интерфейс Resident Shield



Помимо обзора наиболее важных статистических сведений и информации о текущем состоянии компонента (*Компонент Resident Shield активен и работает правильно*), интерфейс компонента **Resident Shield** также позволяет настроить некоторые основные параметры. В интерфейсе компонента отображается следующая статистическая информация.

- **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")

Основные настройки компонента

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):

- автоматически (**Удалять все угрозы автоматически**);
- 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 cookie-файлов**. В некоторых случаях может потребоваться включение данного параметра, чтобы обеспечить максимальный уровень безопасности. Однако по умолчанию параметр отключен. (*cookies* = текстовые пакеты, отправляемые сервером в веб-браузер, а затем веб-браузером обратно на сервер при каждом подключении браузера к серверу. cookie-файлы протокола HTTP используются для аутентификации, 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 только опытным пользователем. При необходимости изменить настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG во вновь открытом диалоговом окне [Расширенные настройки AVG](#).

Кнопки управления

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

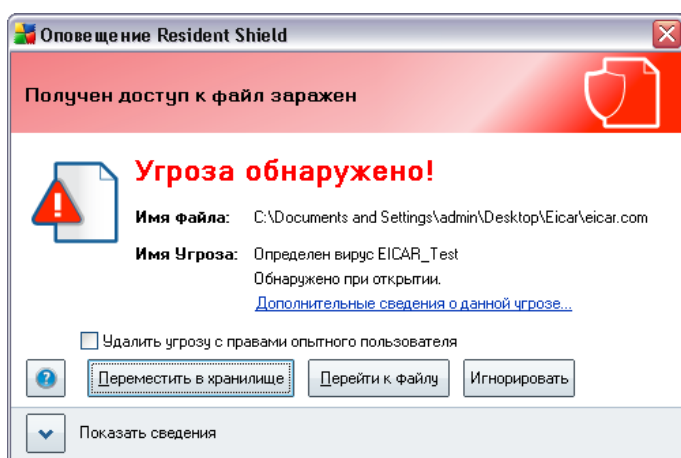
- **Управление исключениями.** Открытие диалогового окна [Resident Shield – Исключения каталогов](#), которое позволяет определить папки, которые не должны сканироваться компонентом [Resident Shield](#).
- **Сохранить изменения.** Нажмите данную кнопку для сохранения и

применения изменений, выполненных в данном диалоговом окне

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

8.9.3. Обнаружение Resident Shield

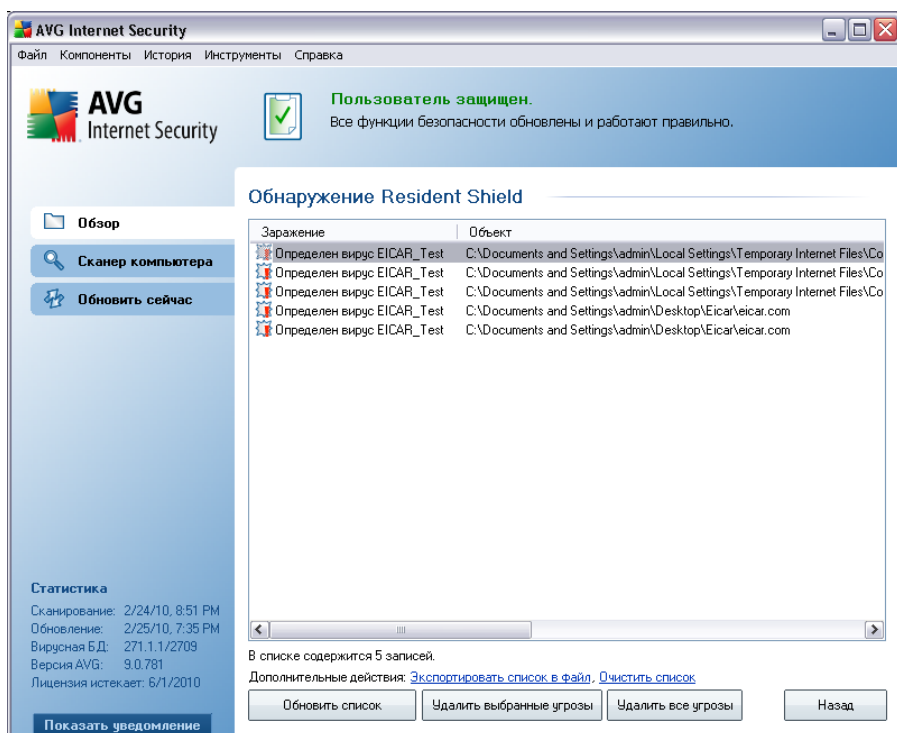
Resident Shield сканирует копируемые, открываемые или сохраняемые файлы. При обнаружении вируса или угрозы сразу же появляется предупреждение в следующем диалоговом окне:



Диалоговое окно предоставляет информацию об обнаруженной угрозе и предлагает возможные действия:

- **Вылечить** — если лечение возможно, AVG вылечит зараженный файл автоматически, рекомендуется именно это действие.
- **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

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**. Для каждого обнаруженного объекта 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 **Resident Shield**. Кнопка **Назад** выполняет переключение к [интерфейсу пользователя AVG](#) (по умолчанию обзор компонентов).

8.10. Диспетчер обновления

8.10.1. Принципы работы диспетчера обновления

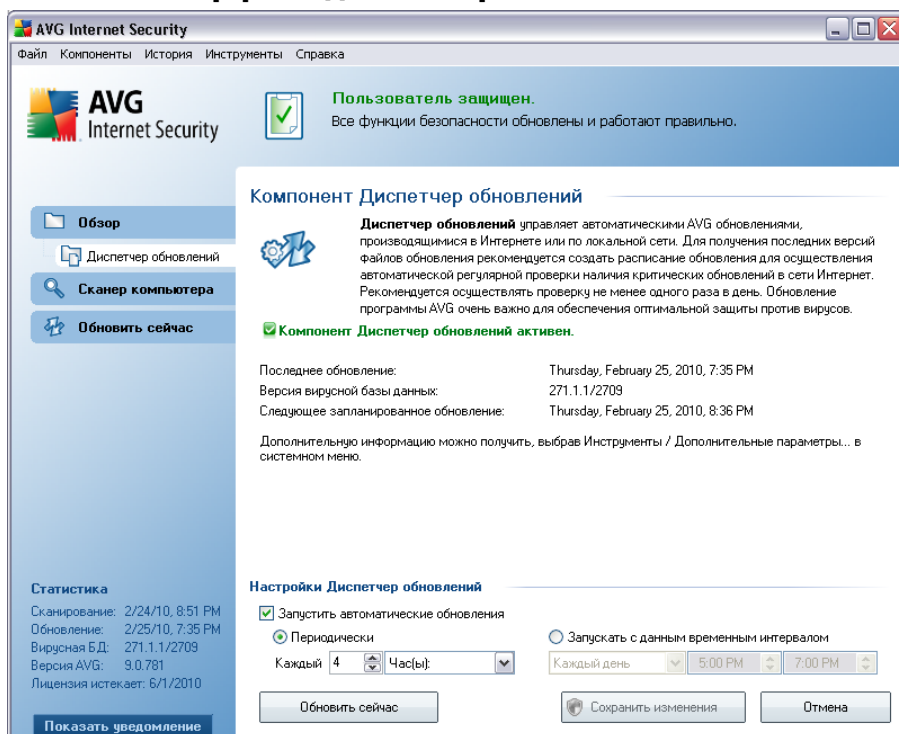
Ни один из программных продуктов по обеспечению безопасности не может гарантировать полноценную защиту от различных типов угроз без регулярного обновления. Создатели вирусов ищут новые уязвимые места для взлома программного обеспечения и операционных систем. Ежедневно совершаются попытки несанкционированного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

8.10.2. Интерфейс диспетчера обновления



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

- **Последнее обновление** — дата и время последнего обновления базы данных
- **Версия вирусной базы данных** — номер последней версии вирусной базы данных; в результате каждого обновления вирусной базы данных номер увеличивается
- **Следующее запланированное обновление** — дата и время следующего запланированного обновления базы данных

Основные настройки компонента

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 файлов обновлений имеет решающее значение для правильной работы ПО по обеспечению безопасности.

Также можно определить время запуска процесса обновления.

- о **Периодически** — позволяет определить временной интервал
- о **В указанное время** — позволяет задать точные дату и время

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 во вновь открытом диалоговом окне [Расширенные настройки 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)



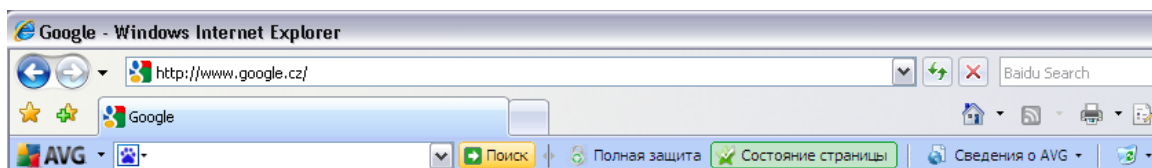
9. AVG Security Toolbar

AVG Security Toolbar — новый инструмент, работающий совместно с компонентом **AVG Link Scanner**, который проверяет результаты поиска поддерживаемых поисковых служб (*Yahoo!, Google, Bing, Altavista, Baidu*). **AVG Security Toolbar** можно использовать для управления функциями и настройки компонента **AVG Link Scanner**.

Если была выбрана установка панели инструментов во время процесса установки **AVG 9 Anti-Virus + Firewall**, она автоматически добавится в веб-браузер. При использовании альтернативного интернет-браузера (*например, Avant*) система может работать неправильно.

9.1. AVG Security Toolbar Интерфейс

Компонент **AVG Security Toolbar** работает вместе с браузерами **MS Internet Explorer** (6.0 или более поздней версии) и **Mozilla Firefox** (2.0 или более поздней версии). Если необходимо установить **AVG Security Toolbar** (при установке AVG пользователю будет предложено выбрать, устанавливать компонент или нет), компонент будет размещен в веб-браузере прямо под адресной строкой:



Примечание. Компонент **AVG Security Toolbar** не предназначен для использования на серверных платформах!

Компонент **AVG Security Toolbar** включает в себя следующие элементы.

- **Логотип AVG.** Обеспечивает доступ к основным элементам панели инструментов. Нажмите кнопку с логотипом, чтобы перейти на веб-сайт AVG (<http://www.avg.com/>). Щелкнув указатель, расположенный рядом со значком AVG, можно открыть следующие элементы.
 - **Сведения о панели инструментов.** Ссылка на домашнюю страницу **AVG Security Toolbar** с подробными сведениями о защите панели инструментов.
 - **Запустить AVG 9 Anti-Virus + Firewall.** Открытие **AVG 9 Anti-Virus + Firewall** интерфейса пользователя.

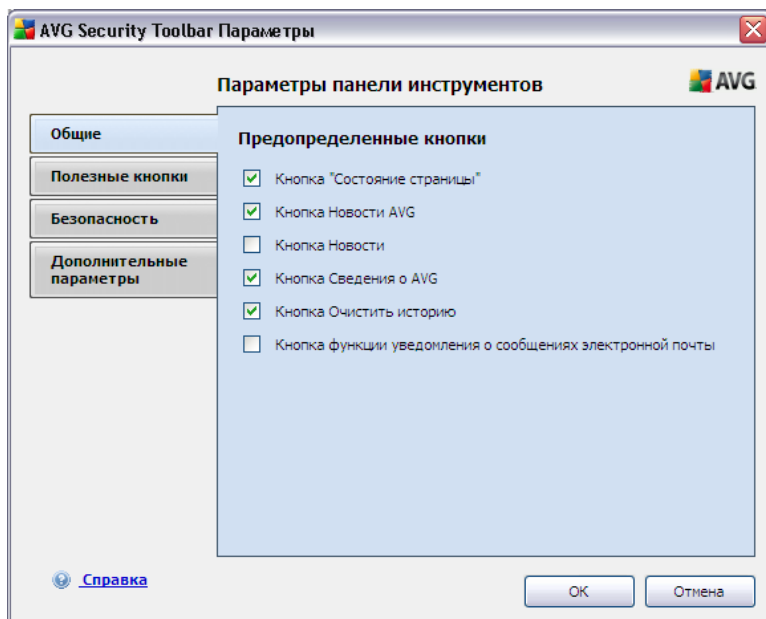
- о **Параметры** — открытие диалогового окна конфигурации, в котором можно настроить параметры **AVG Security Toolbar** в соответствии с требованиями пользователя — см. следующую главу [Параметры AVG Security Toolbar](#)
 - о **Очистить историю** — позволяет полностью очистить историю AVG Security Toolbar или очистить историю поиска, очистить историю браузера, очистить историю загрузок и удалить файлы cookie.
 - о **Обновить** — проверка новых обновлений для компонента **AVG Security Toolbar**
 - о **Справка**. Позволяет открыть файл справки, обратиться в службу технической поддержки AVG, а также просмотреть информацию о текущей версии панели инструментов.
- **Поле поиска**. Введите поле или фразу в поле поиска. Нажмите **Поиск**, чтобы начать поиск с помощью указанной поисковой системы (можно указать необходимую поисковую систему с помощью [дополнительных параметров AVG Security Toolbar](#), можно выбрать Yahoo!, Wikipedia, Baidu, WebHledani или Yandex) с любой веб-страницы. Поле поиска также содержит историю поиска. Операции поиска, выполняемые с помощью поля поиска, анализируются компонентом защиты [AVG Search-Shield](#).
 - **Полная защита**. Эта кнопка может называться **Полная защита**, **Ограниченная защита** или **Нет защиты** в зависимости от **AVG 9 Anti-Virus + Firewall** конфигурации.
 - **Состояние страницы**. Эта кнопка на панели отображает оценку текущей веб-страницы на основе критериев компонента [AVG Search-Shield](#) (страница является безопасной, подозрительной, зараженной, содержит угрозы, не может быть отсканирована). Нажмите эту кнопку, чтобы открыть панель сведений, содержащую подробные данные об указанной веб-странице.
 - **Сведения о программе AVG**. Ссылки на важные сведения о безопасности, расположенные на веб-сайте AVG (<http://www.avg.com/>).
 - о **Сведения о панели инструментов**. Ссылка на домашнюю страницу **AVG Security Toolbar** с подробными сведениями о защите панели инструментов.
 - о **Об угрозах**. Открытие веб-страницы AVG с информацией о текущих вирусах и угрозах в Интернете.

- 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 **Энциклопедия вирусов**. Открытие страницы энциклопедии вирусов, в которой можно осуществить поиск определенных вирусов по имени и получить подробные сведения о каждом из них.

9.2. AVG Security Toolbar

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:

9.2.1. Вкладка Общее

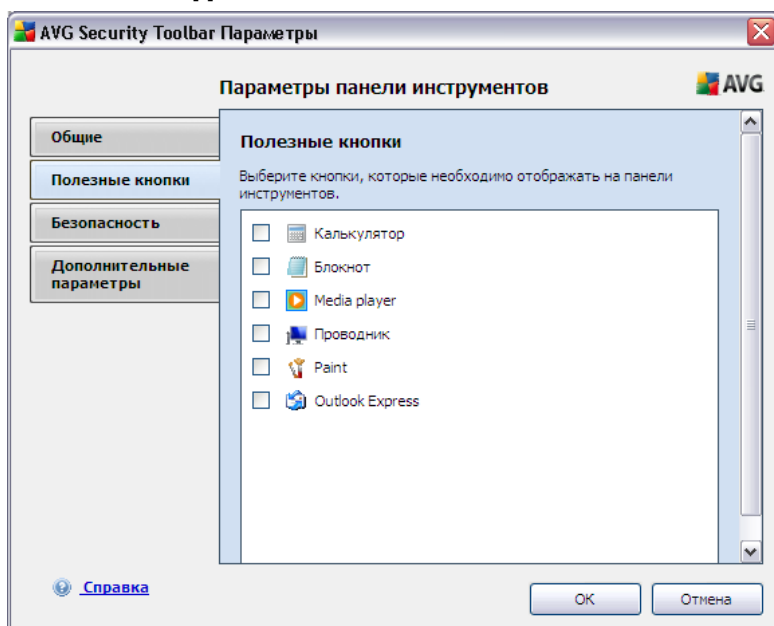


На этой вкладке можно указать кнопки, которые должны быть отображены или скрыты на панели **AVG Security Toolbar**. Пометьте кнопки, которые должны отображаться на панели. Ниже приведено описание каждой кнопки панели

управления.

- **Новости AVG.** Эта кнопка открывает веб-страницу, содержащую последние пресс-релизы компании AVG.
- **Новости.** Эта кнопка обеспечивает структурированный обзор текущих новостей из прессы.
- **Сведения об AVG.** Эта кнопка предоставляет сведения о панели инструментов AVG, о текущих угрозах и уровне угроз в Интернете, открывает энциклопедию вирусов, а также позволяет просмотреть новости о продуктах AVG.
- **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 AVG Security Toolbar.

9.2.2. 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.

9.2.3. Вкладка Безопасность

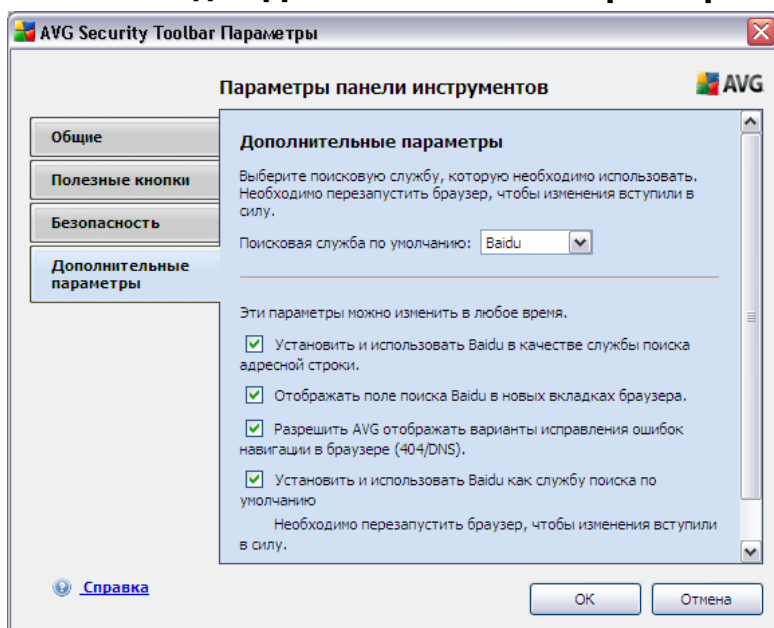


Вкладка **Безопасность** состоит из двух разделов: **Безопасность браузера AVG** и **Оценки**. На вкладке можно установить определенные флажки, чтобы назначить компоненту **AVG Security Toolbar** ряд необходимых функций:

- **Безопасность браузера AVG.** Установите этот флажок, чтобы активировать или отключить **AVG Search-Shield** и/или службу **AVG Active Surf-Shield**.
- **Оценки.** Выберите графические символы, используемые компонентом **AVG 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.**

9.2.4. Вкладка Дополнительные параметры



На вкладке **Дополнительные параметры** сначала выберите поисковую систему, которую требуется использовать по умолчанию. Можно выбрать *Yahoo!*, *Baidu*, *WebHledani* или *Yandex*. После изменения поисковой системы, используемой по умолчанию, перезапустите интернет-браузер, чтобы изменение вступило в силу.

Также можно включить или отключить определенные параметры панели **AVG Security Toolbar**.

- **Установить и использовать Yahoo! в качестве службы поиска адресной строки** — (включен по умолчанию) — данный параметр позволяет вводить ключевые слова поиска непосредственно в адресной строке интернет-браузера, а служба Yahoo! будет автоматически производить поиск соответствующих веб-сайтов.
- **Разрешить AVG отображать варианты исправления ошибок**

навигации в браузере (404/DNS) (по умолчанию флажок установлен). 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.

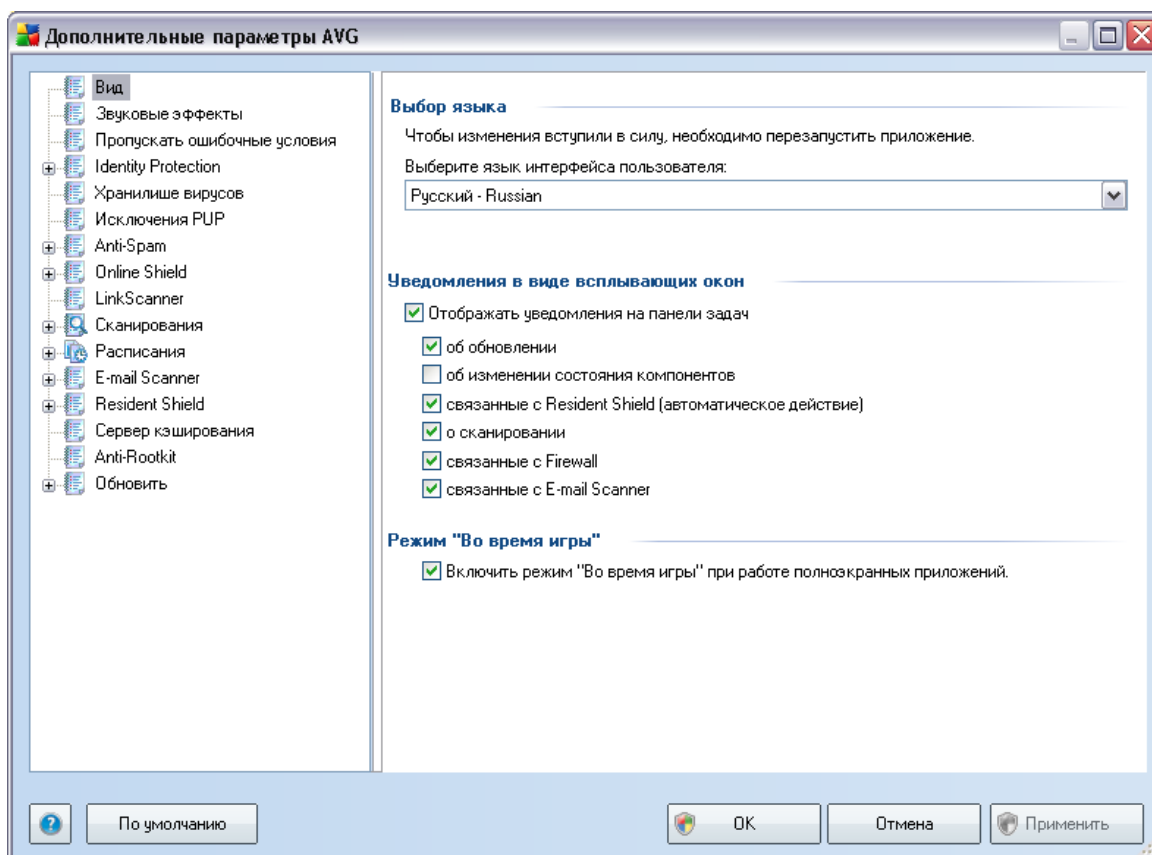
- **Установить и использовать Yahoo! в качестве службы поиска в браузере** — (выключен по умолчанию) — Yahoo! по умолчанию является службой поиска в AVG Security Toolbar. При активации данного параметра она также может по умолчанию стать службой поиска веб-браузера.
- **Отображать AVG Security Toolbar, если скрыта (еженедельно)** — (включен по умолчанию) — данный параметр активен по умолчанию. Если панель **AVG Security Toolbar** будет случайно скрыта, с помощью данного параметра она отобразится вновь через одну неделю.

10. Расширенные настройки AVG

Параметры дополнительной настройки **AVG 9 Anti-Virus + Firewall** откроются в новом диалоговом окне **Дополнительные параметры AVG**. Окно разделено на две части. В левой части расположено навигационное дерево параметров программы. Выберите компонент, параметры которого необходимо изменить (*или часть компонента*), чтобы открыть диалоговое окно редактирования в правой части окна.

10.1. Внешний вид

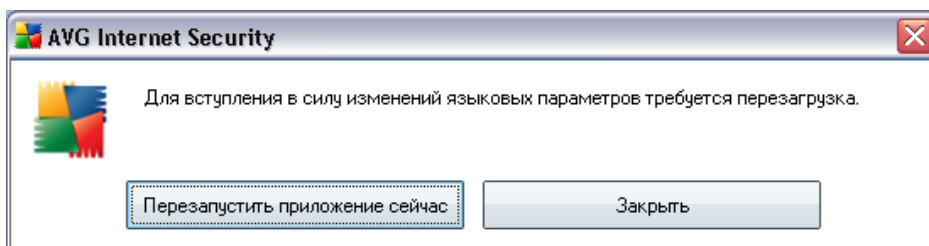
Параметр **Вид**, первый элемент навигационного дерева, относится к общим параметрам [интерфейса пользователя AVG](#) и нескольким начальным параметрам поведения приложения.



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 [Выборочная установка — выбор компонентов](#)). 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 **OK**
- 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.

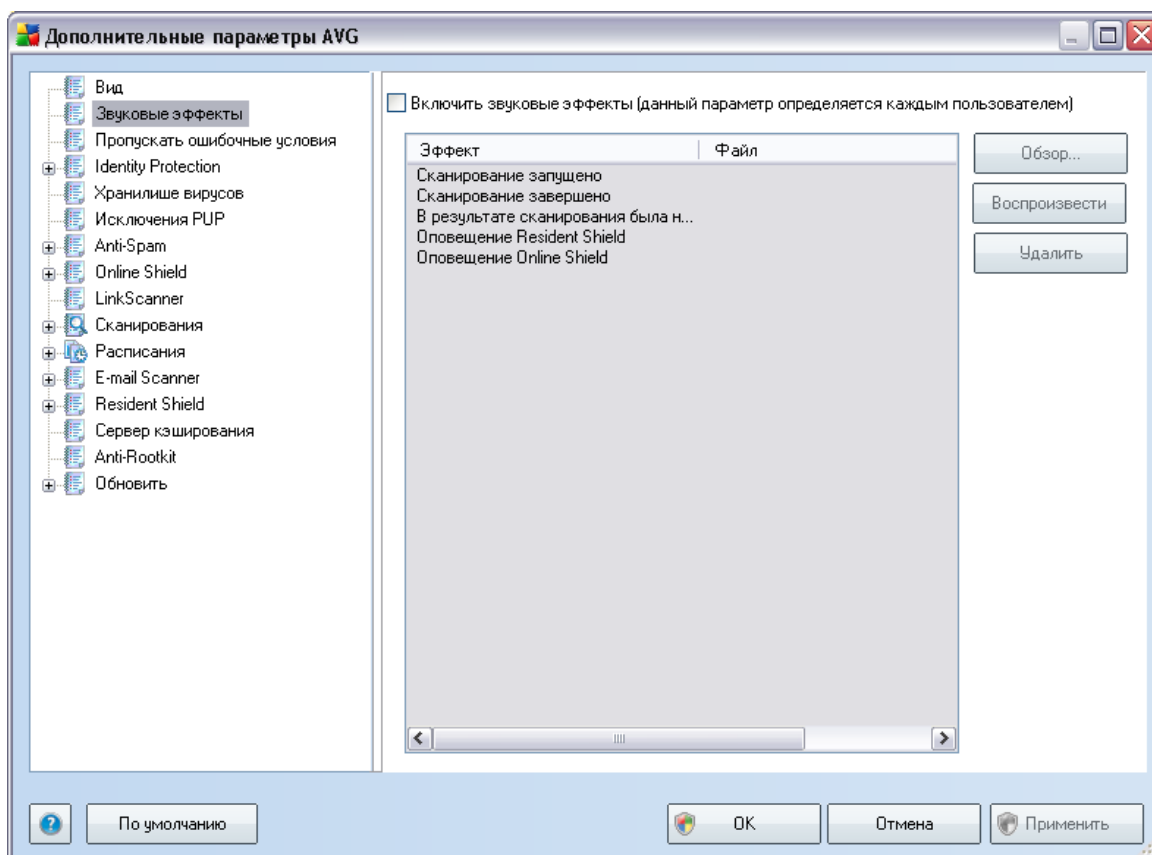
- o **Отображать уведомления об [обновлении](#)** на панели задач — позволяет определить, следует ли отображать информацию о запуске процесса обновления AVG, его состоянии и завершении.
- o **Отображать уведомления об изменении состояния компонентов** — позволяет определить, должна ли отображаться информация 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;
- o **Отображать уведомления компонента [Resident Shield](#) на панели задач**. 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);
- o **Отображать уведомления о [сканировании](#)** на панели задач — позволяет определить, должна ли отображаться информация об автоматическом запуске запланированного сканирования, его состоянии и результатах;
- o **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.
- o **Отображать уведомления компонента [E-mail Scanner](#) на панели задач** — позволяет определить, должна ли отображаться информация о сканировании всех входящих и исходящих сообщений электронной почты.

Режим "Во время игры"

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

10.2. Звуки

В 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:

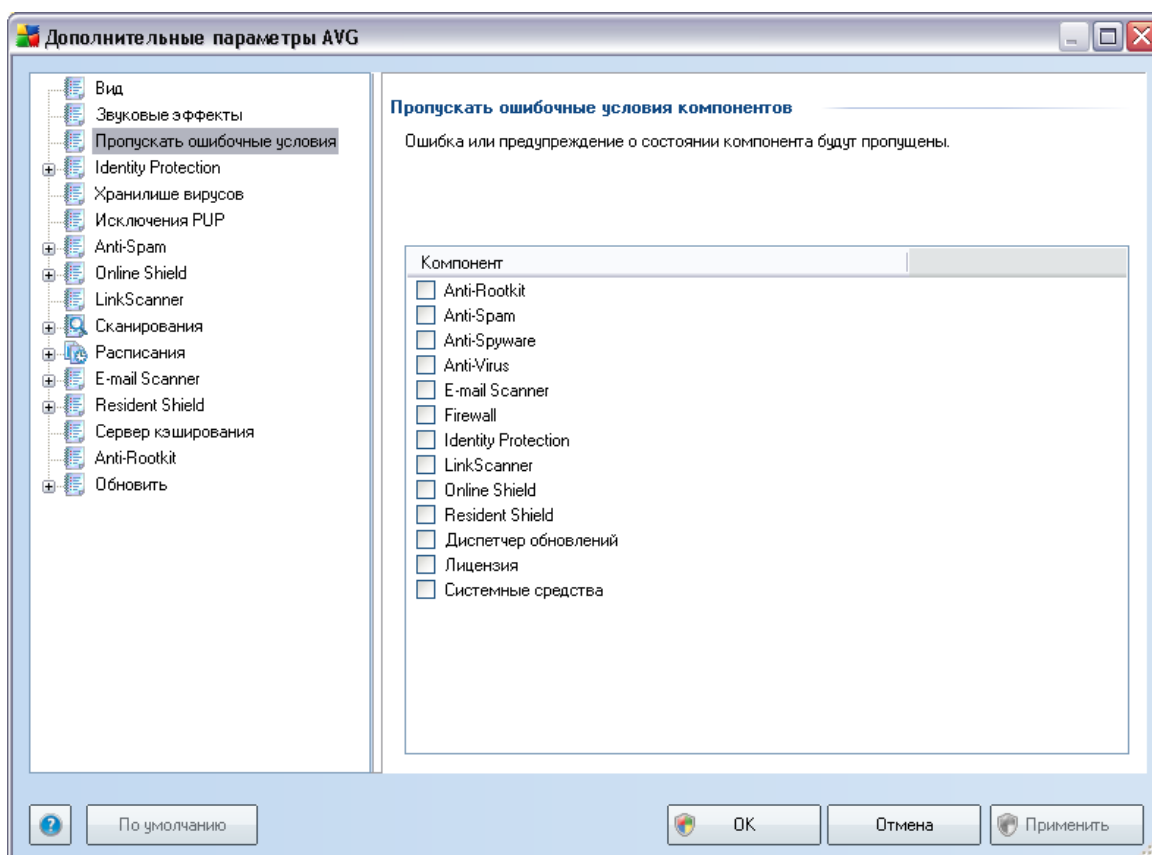


Затем выберите в списке событие и укажите (**Обзор**) на диске аудиофайл, который необходимо назначить для этого события. Чтобы прослушать выбранный аудиофайл, выделите событие в списке и нажмите кнопку **Воспроизвести**. Чтобы удалить звук, назначенный определенному событию, нажмите кнопку **Удалить**.

Примечание. Поддерживаются только файлы в формате *.wav.

10.3. 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.

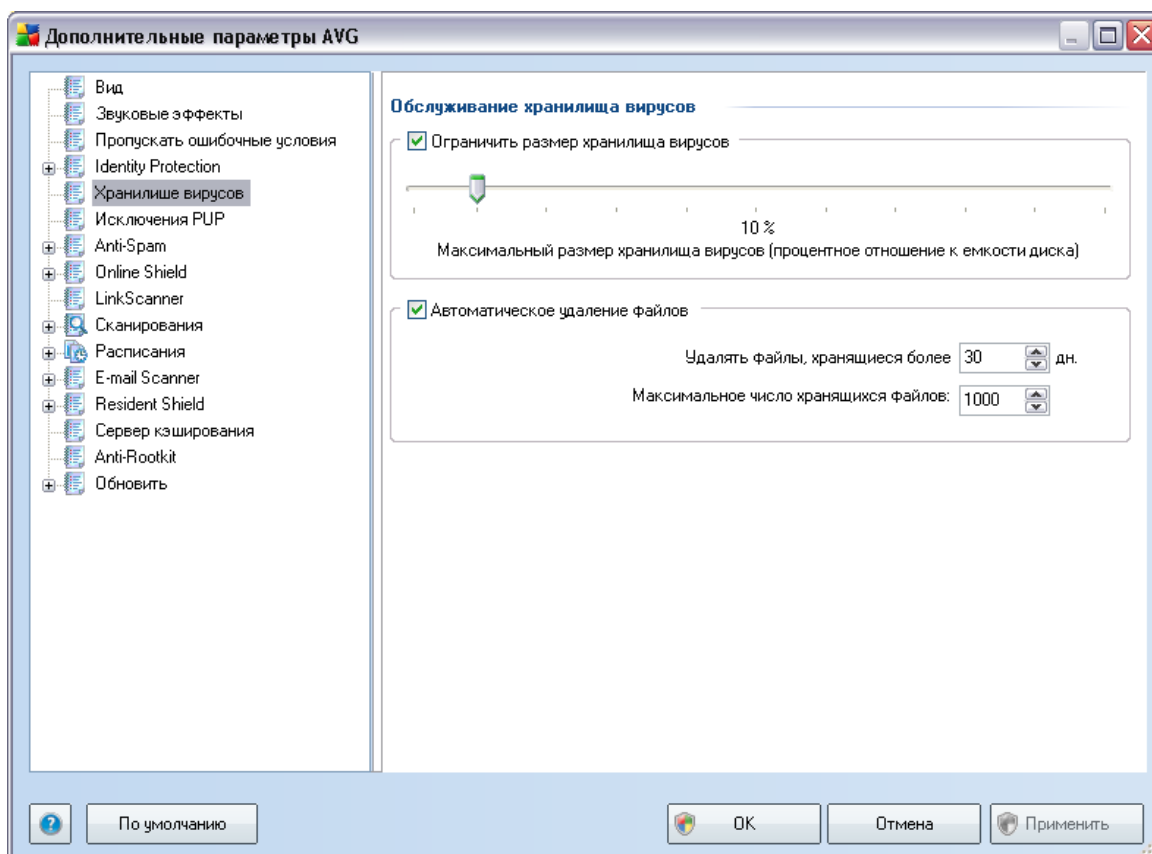
- **Значок на панели задач.** Во время безупречной работы всех компонентов AVG значок отображается четырьмя цветами; при появлении ошибок на значке появляется желтый восклицательный знак.
- Текстовое описание существующей проблемы в разделе **Сведения о состоянии безопасности** в главном окне AVG.

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. Если же значок отобразился серым цветом, он не сможет 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](#).

10.4. Хранилище вирусов

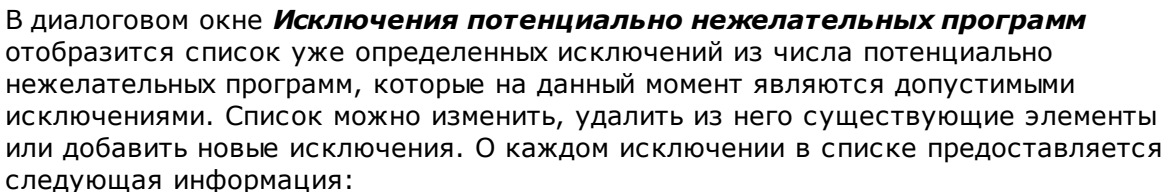


Диалоговое окно **Обслуживание хранилища вирусов** позволяет определить несколько параметров администрирования объектов, находящихся в [хранилище вирусов](#):

- **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**)

10.5. Исключения PUP

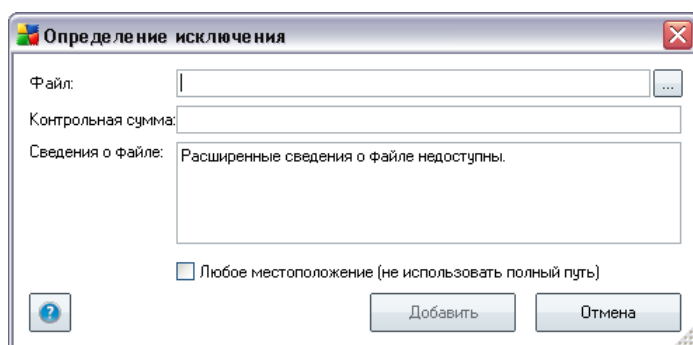
AVG 9 Anti-Virus + Firewall может анализировать и обнаруживать исполняемые приложения или библиотеки DLL, использование которых в системе потенциально нежелательно. В некоторых случаях пользователю может потребоваться сохранить на компьютере некоторые нежелательные программы (*программы, которые были 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:



- AVG 9 Anti-Virus + Firewall © 2010 © AVG Technologies CZ, s.r.o. Все права защищены.

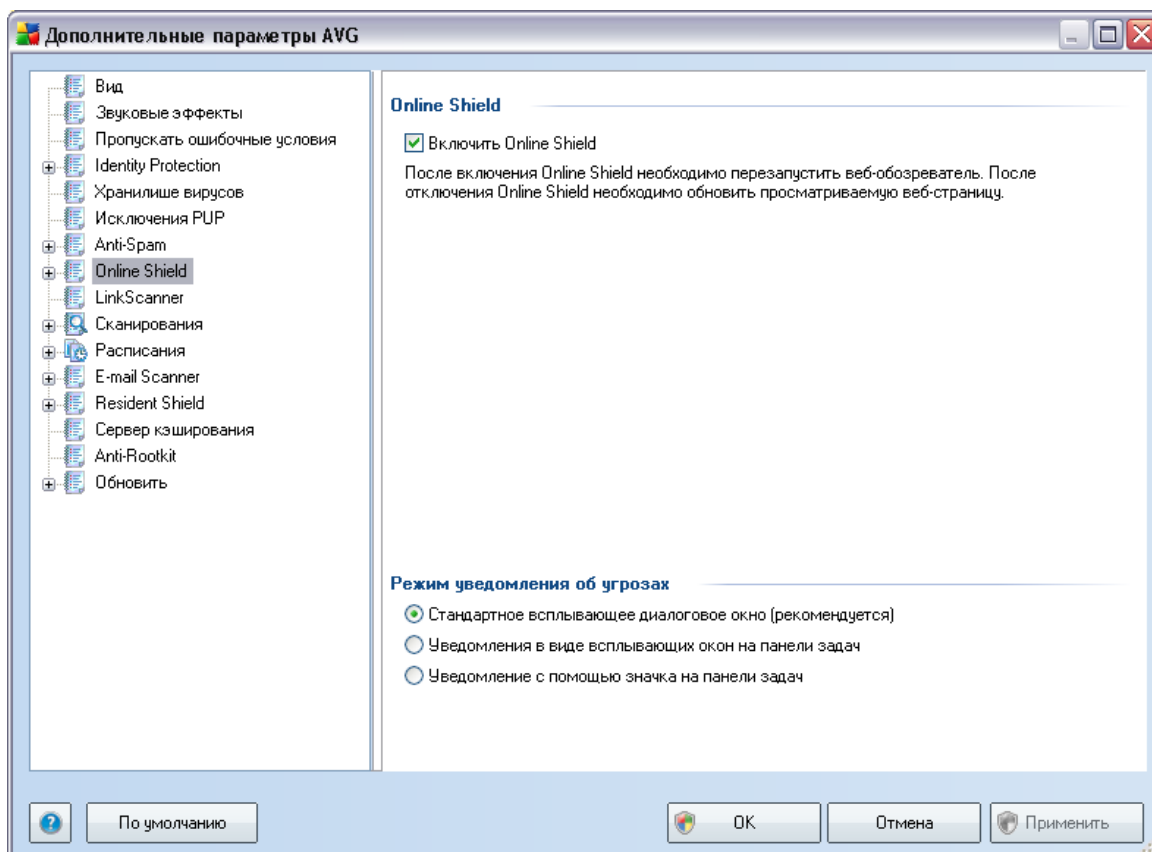
Кнопки управления

- **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

10.6. Online Shield



Диалоговое окно **Интернет-защита** 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.

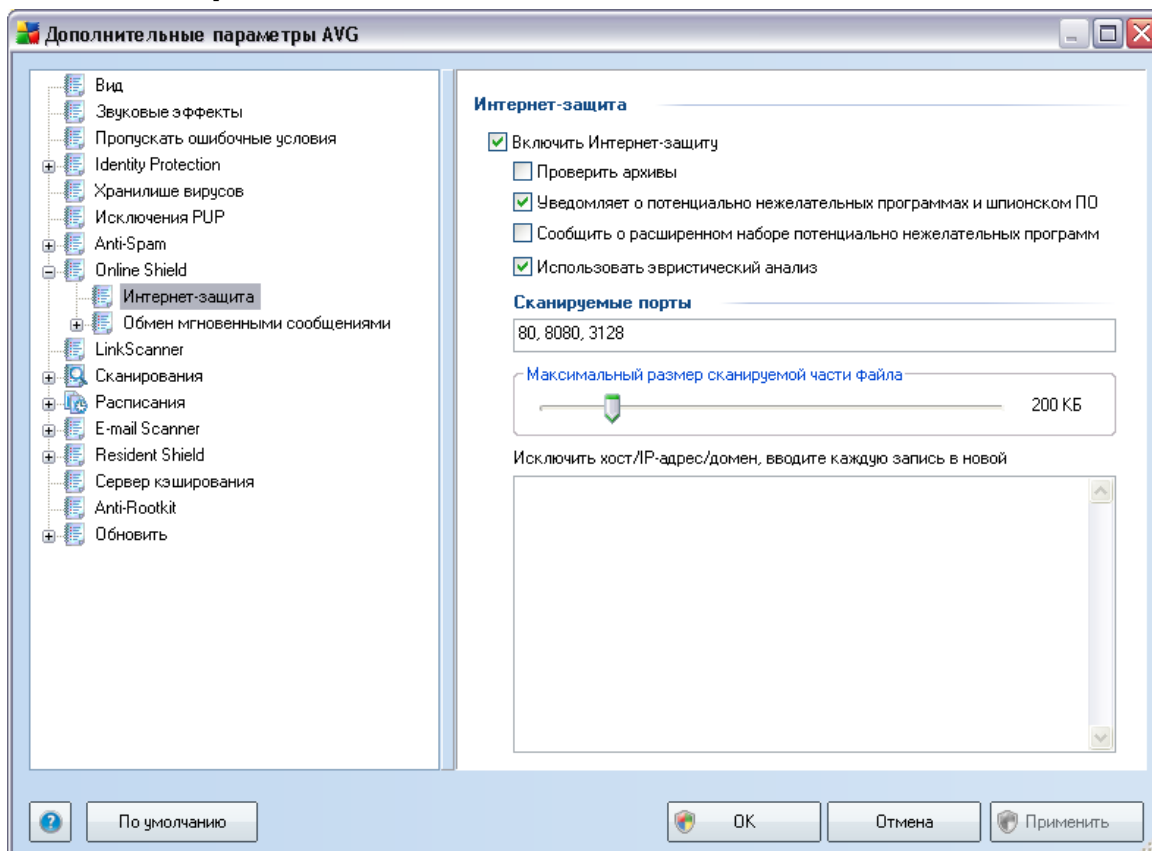
- [**Интернет-защита**](#)
- [**Обмен мгновенными сообщениями**](#)

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.

10.6.1. Интернет-защита



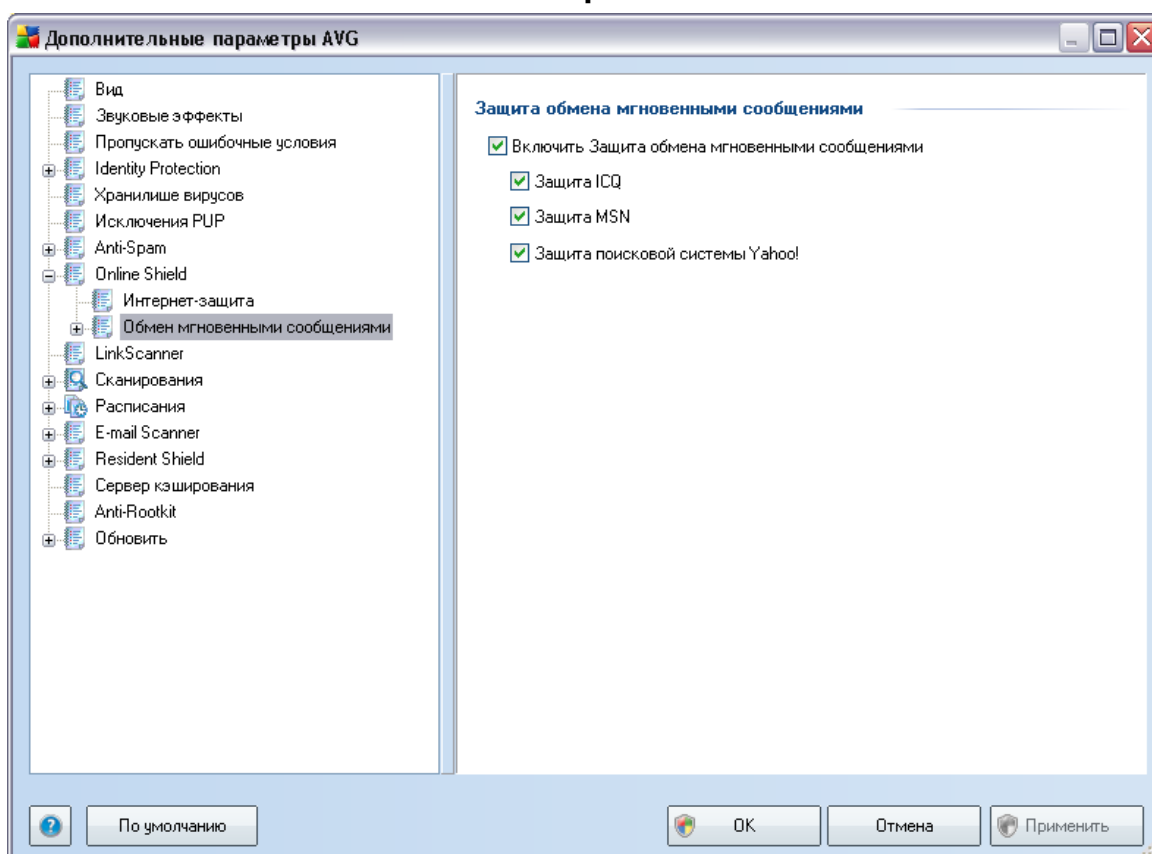
Диалоговое окно **Интернет-защита** позволяет изменять настройки компонента, относящиеся к сканированию содержимого веб-сайта. Интерфейс редактирования позволяет настроить следующие начальные параметры.

- **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.
 - **Проверка архивов.** Сканирование содержимого архивов, которые могут содержаться на отображаемых интернет-страницах.

- o **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО** (флажок установлен по умолчанию). Установите флажок для активации компонента [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.
- o **Уведомлять о расширенном наборе потенциально нежелательных программ.** Если предыдущий параметр активирован, можно также выбрать данный параметр для определения расширенного набора [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.
- o **Использовать эвристический анализ.** Сканирование содержимого отображаемой страницы с использованием метода [эвристического анализа](#) (динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде).
- o **Сканируемые порты** . Данное поле содержит список номеров стандартных коммуникационных портов http. Если конфигурация вашего компьютера отличается, можно изменить номера портов на необходимые.
- o **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.

10.6.2. Обмен мгновенными сообщениями



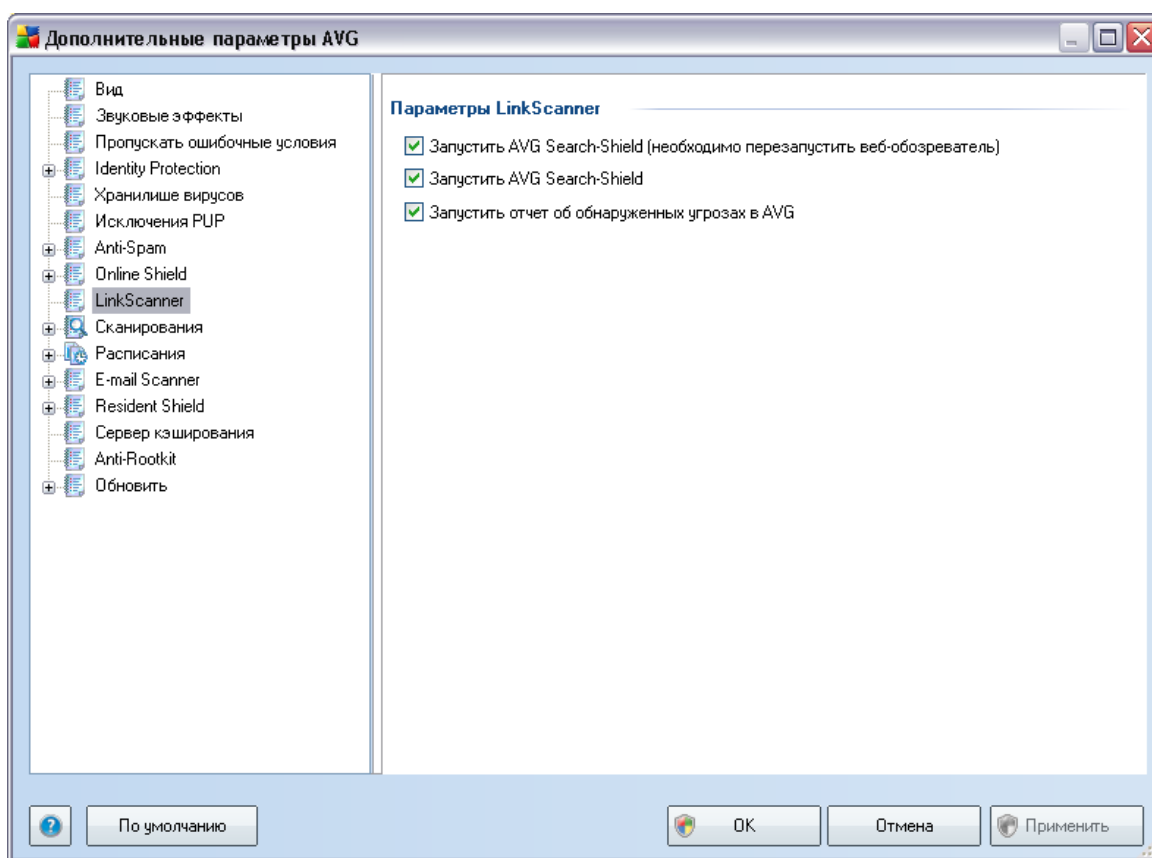
В окне **Защита обмена мгновенными сообщениями** можно изменять параметры компонентов **Online Shield**, относящихся к сканированию мгновенных сообщений. В настоящее время поддерживаются три следующие программы обмена мгновенными сообщениями: **ICQ**, **MSN** и **Yahoo**. Установите флажок в соответствующем 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).

10.7. Link Scanner

Диалоговое окно **Параметры LinkScanner** позволяет включать или отключать основные функции компонента **LinkScanner**.



- **Включить AVG Search-Shield** (по умолчанию флажок установлен). При выполнении поиска в Google, Yahoo, Bing, Yandex, Altavista или Baidu будут отображаться информационные значки, сообщающие о безопасности найденных веб-сайтов.
- **Включить AVG Active Surf-Shield** (включен по умолчанию). Активная (в

режиме реального 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).

- **Включить отправку отчетов об обнаруженных угрозах в AVG** (включено по умолчанию). Выберите данный параметр, чтобы отправлять отчеты об эксплойтах и вредоносных веб-сайтах, обнаруженных пользователями с помощью функций **AVG Active Surf-Shield** или **AVG Search-Shield**, для пополнения базы данных информацией об активности вредоносного ПО в Интернете.

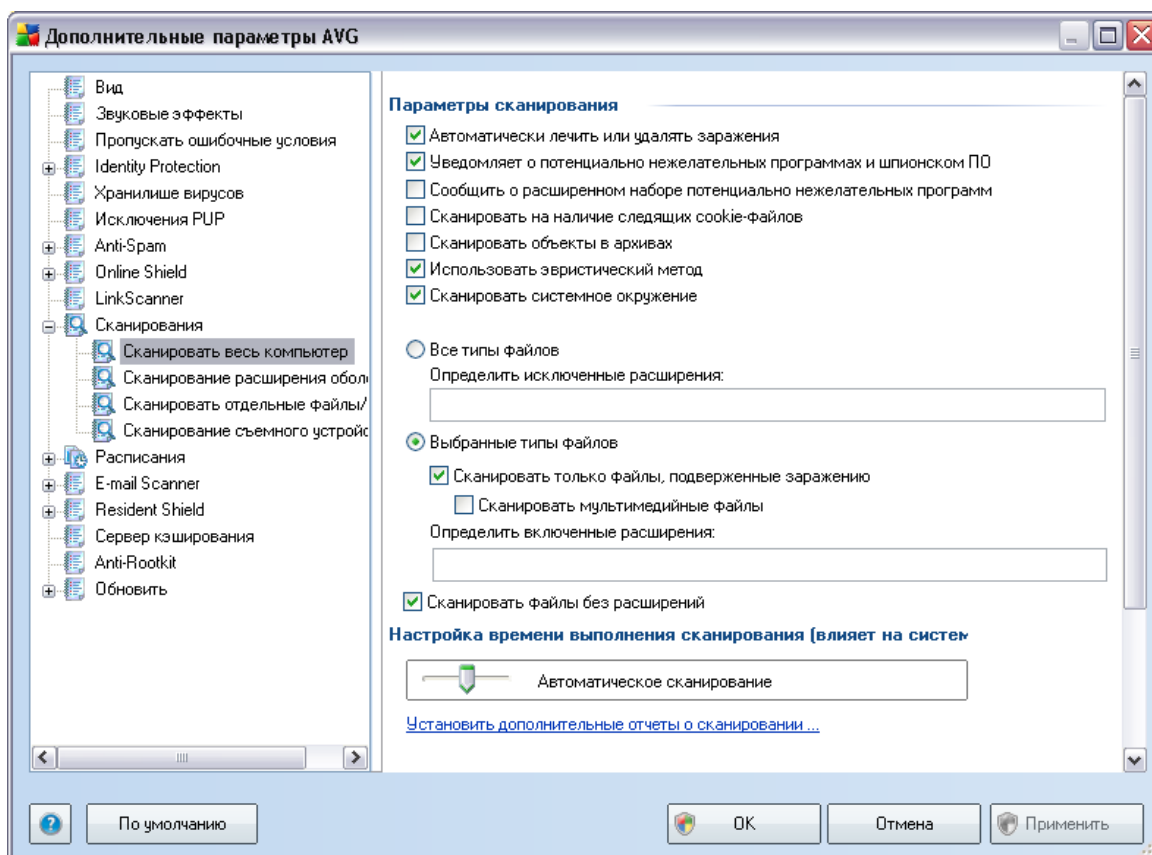
10.8. Сканирование

Дополнительные параметры сканирования разделены на три 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

10.8.1. 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** — 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** (флажок установлен по умолчанию). Установите флажок для активации компонента [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.** Если предыдущий параметр активирован, можно также выбрать данный параметр для определения расширенного набора [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 cookie-файлов.** Данный параметр компонента [Anti-Spyware](#) включает сканирование системы на наличие файлов cookie (файлы cookie протокола HTTP используются для аутентификации, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзины для покупок через Интернет).
- **Сканировать объекты в архивах** — благодаря данному параметру при сканировании проверяются все файлы, включая файлы, хранящиеся в архивах, например ZIP, RAR и т. п.
- **Использовать эвристический анализ** — эвристический анализ (динамичная эмуляция команд сканированных объектов в виртуальной компьютерной среде) является одним из способов, используемых для выявления вирусов при сканировании.
- **Сканировать системную среду** — при сканировании будут также проверяться системные области компьютера.

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 проводится 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.

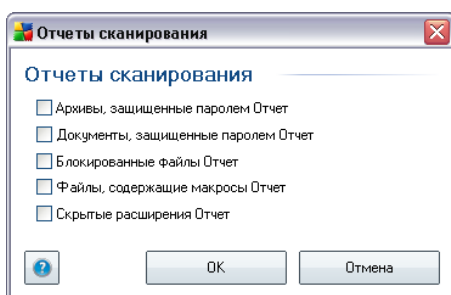
- Дополнительно можно выбрать параметр **Сканировать файлы без расширений** — этот параметр установлен по умолчанию. Рекомендуется не изменять его до появления веской причины. Файлы без расширения являются подозрительными, поэтому необходимо проводить их сканирование каждый раз.

Приоритет процесса сканирования

В разделе **Приоритет процесса сканирования** можно дополнительно выбрать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлено значение среднего уровня 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.

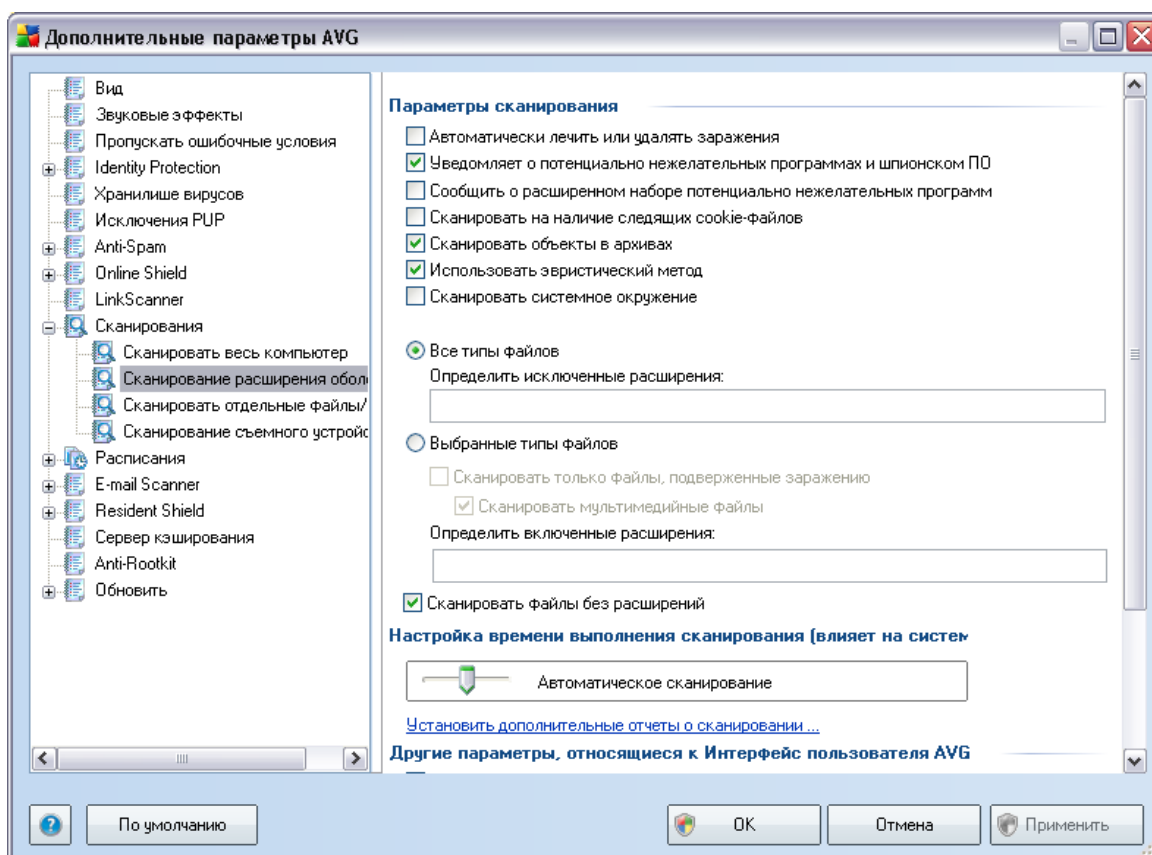
Установить дополнительные отчеты о сканировании ...

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



10.8.2. Сканирование расширения оболочки

Как и предыдущий элемент [Сканировать весь компьютер](#), элемент **Сканирование расширения оболочки** также содержит несколько предварительно установленных поставщиком ПО параметров для настройки сканирования. Данные параметры предназначены для настройки [сканирования определенных объектов, запускаемых непосредственно из Проводника Windows](#) (расширение оболочки), см. главу [Сканирование в Проводнике Windows](#).



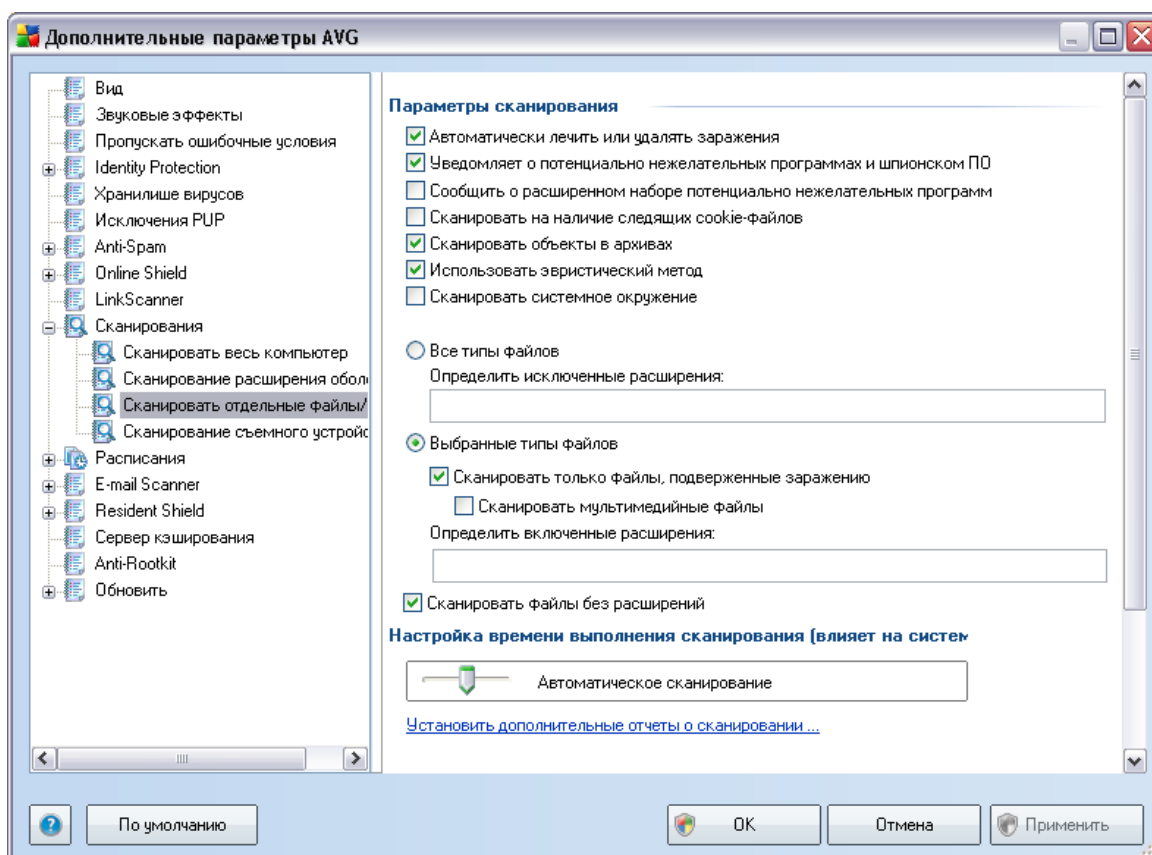
Список параметров соответствует параметрам элемента [Сканирование всего компьютера](#). Однако параметры по умолчанию отличаются. Для элемента **Сканировать весь компьютер** большинство параметров установлено, а для элемента **Сканирование расширения оболочки** ([Сканирование в Проводнике Windows](#)) установлены только подходящие параметры.

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

[компьютера.](#)

10.8.3. Сканирование отдельных файлов или папок

Интерфейс редактирования **Сканировать отдельные файлы или папки** полностью соответствует диалоговому окну редактирования [Сканировать весь компьютер](#). Все параметры конфигурации также не отличаются; однако параметры по умолчанию являются более строгими при [сканировании всего компьютера](#):

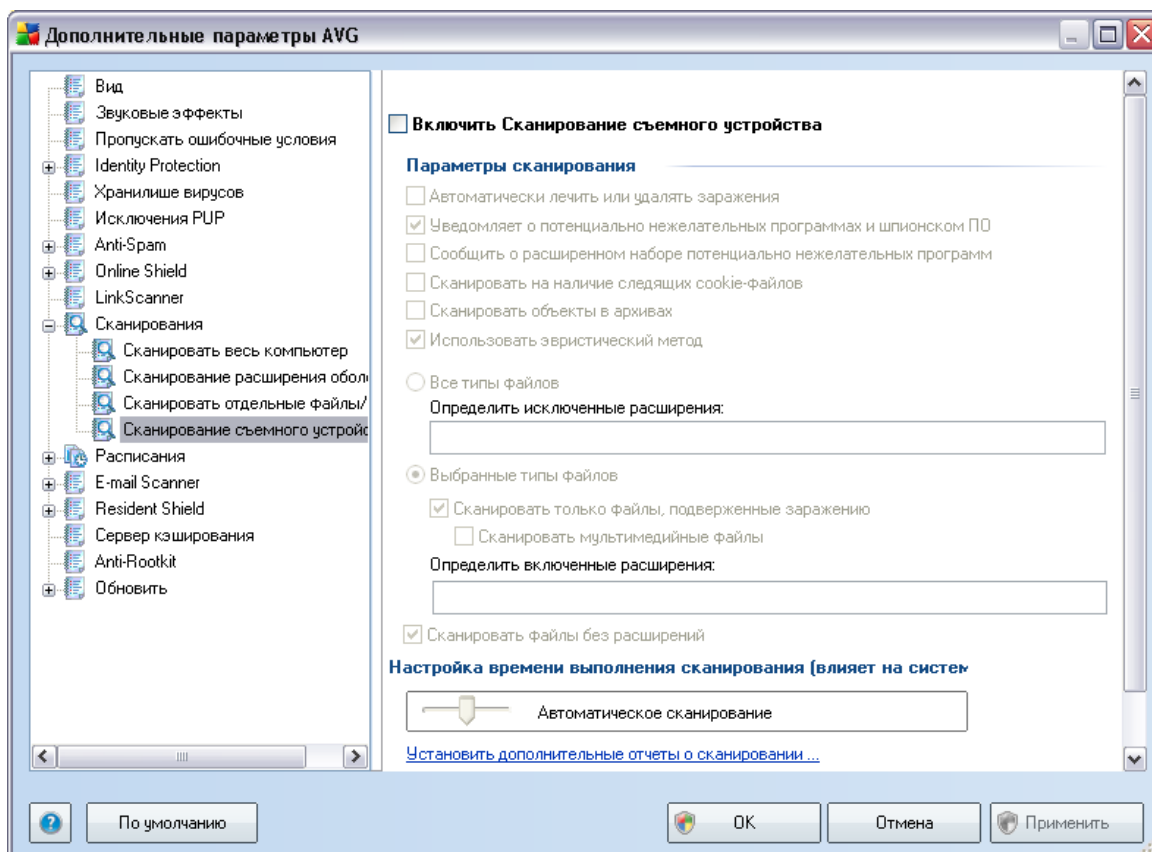


Все параметры, настроенные в этом диалоговом окне конфигурации, применяются только в выбранном для сканирования областях с помощью [Сканирование определенных файлов или папок!](#)

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

10.8.4. Сканирование съемного устройства

Свойства интерфейса редактирования параметров диалогового окна **Сканирование съемного устройства** соответствуют свойствам редактирования параметров диалогового окна [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 специальных параметров приведено в главе [Расширенные настройки AVG/Сканирования/Сканирование всего компьютера](#).

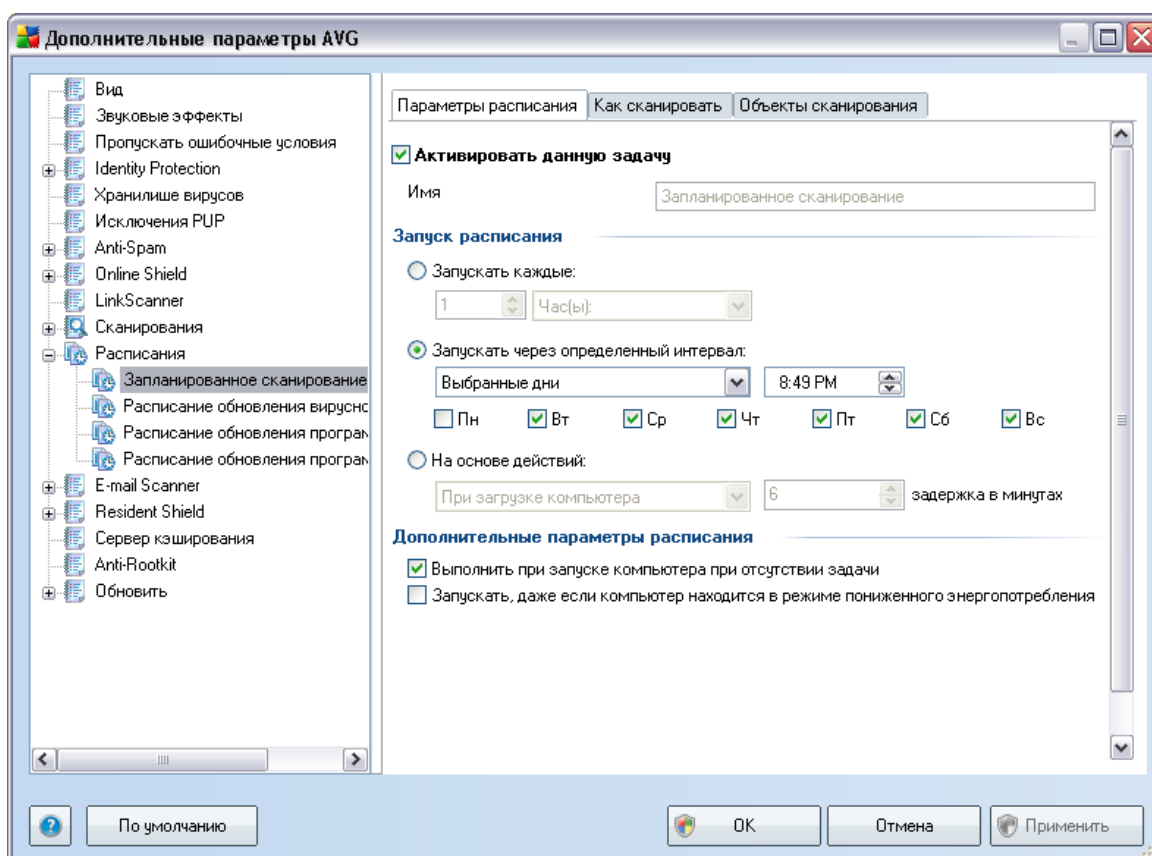
10.9. Расписания

Раздел **Расписания** позволяет изменить стандартные настройки расписания.

- [Расписание сканирования всего компьютера.](#)
- [Расписание обновления вирусной базы данных](#)
- [Расписание обновления программы](#)

10.9.1. Запланированное сканирование

С помощью следующих трех вкладок можно изменить параметры запланированного сканирования (или создать новое расписание).



На вкладке **Параметры расписания** можно сначала установить или снять флажок элемента **Активировать данную задачу**, чтобы временно отключить запланированную проверку и 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 навигационном дереве) 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.

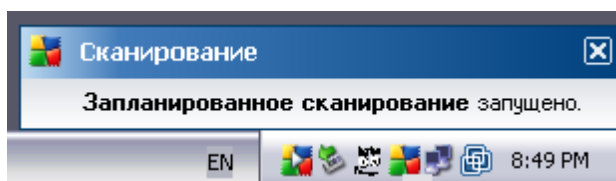
Выполняемое расписание

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**).

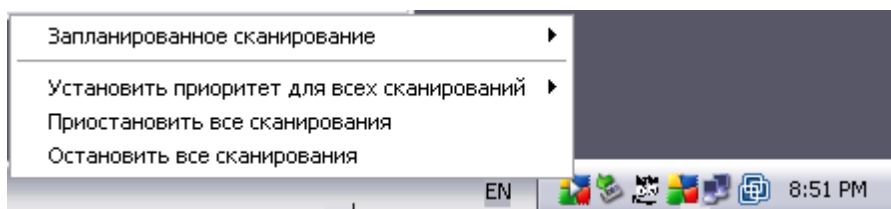
Дополнительные параметры расписания

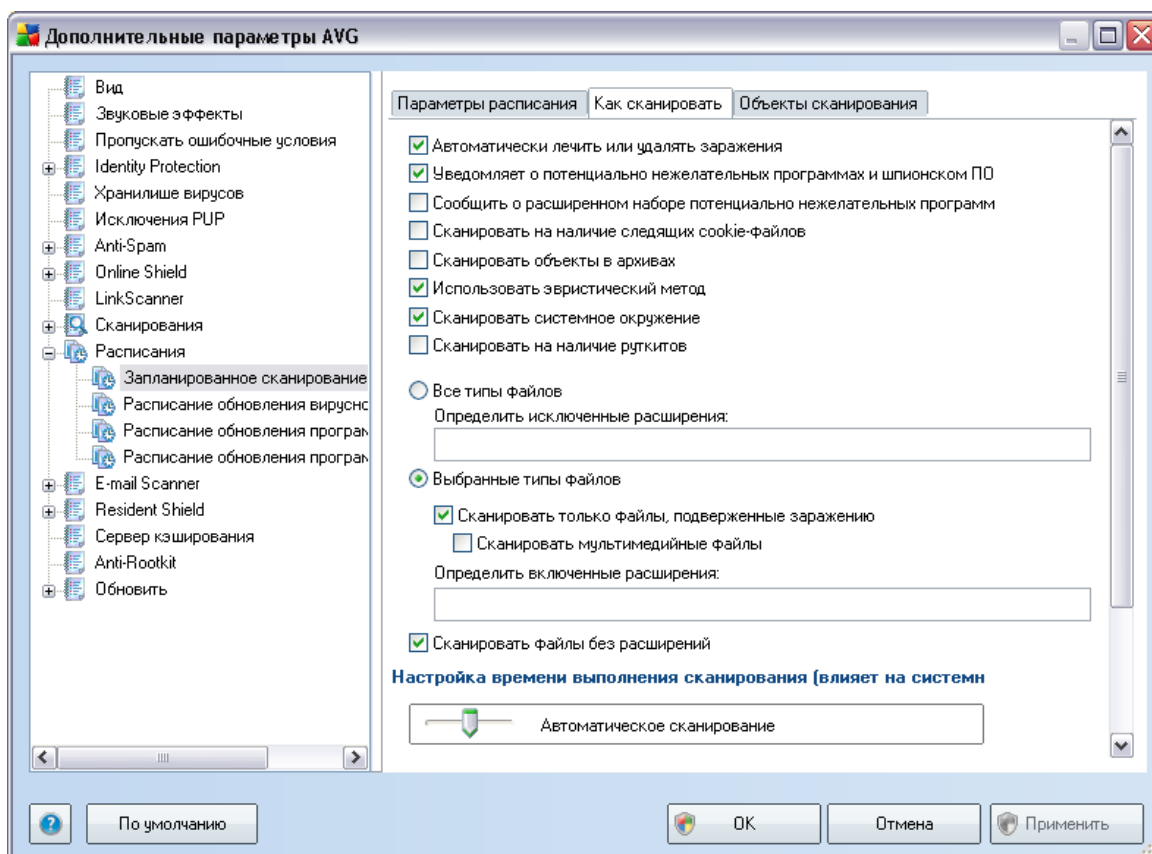
Данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск сканирования, если компьютер работает в энергосберегающем режиме или выключен.

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 — смотрите изображение выше), сообщающий о том, что запланированное сканирование запущено. Щелкните правой кнопкой мыши значок запущенного сканирования AVG, чтобы открыть контекстное меню, с помощью которого можно приостановить или завершить запущенное сканирование.





На вкладке **Способ сканирования** можно найти 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** — 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** (флажок установлен по умолчанию). Установите флажок для активации компонента [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.** Если предыдущий параметр активирован, можно также выбрать данный параметр для определения расширенного набора [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 cookie-файлов** (по умолчанию включено). 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 корзин для покупок через Интернет).
- **Сканировать объекты в архивах** — (включен по умолчанию): в случае выбора данного параметра при сканировании будут проверяться все файлы, включая файлы, хранящиеся в архивах, например ZIP, RAR и т. п.
- **Использовать эвристический анализ** (включен 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** — (включен по умолчанию): при сканировании также будут проверены системные области компьютера.
- **Сканировать на наличие средств rootkit** — отметьте данный элемент, 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

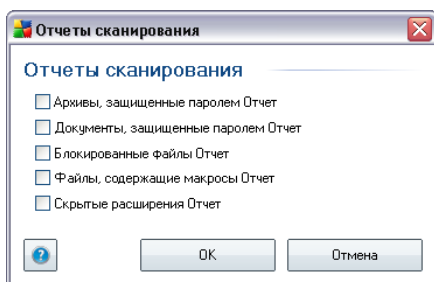
- **Все типы файлов** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми (после сохранения запятые изменяются на точки с запятой), сканирование которых проводиться не будет;

- **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 выбрать параметр **Сканировать файлы без расширений** — этот параметр установлен по умолчанию. Рекомендуется не изменять его до появления веской причины. Файлы без расширения являются подозрительными, поэтому необходимо проводить их сканирование каждый раз.

Приоритет процесса сканирования

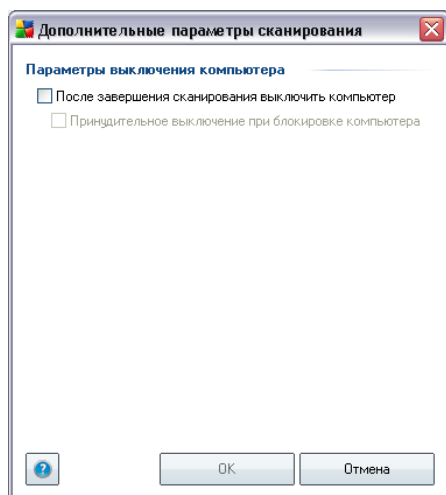
В разделе **Приоритет процесса сканирования** можно дополнительно выбрать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлено значение среднего уровня автоматического использования ресурсов. Если необходимо, чтобы сканирование 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.

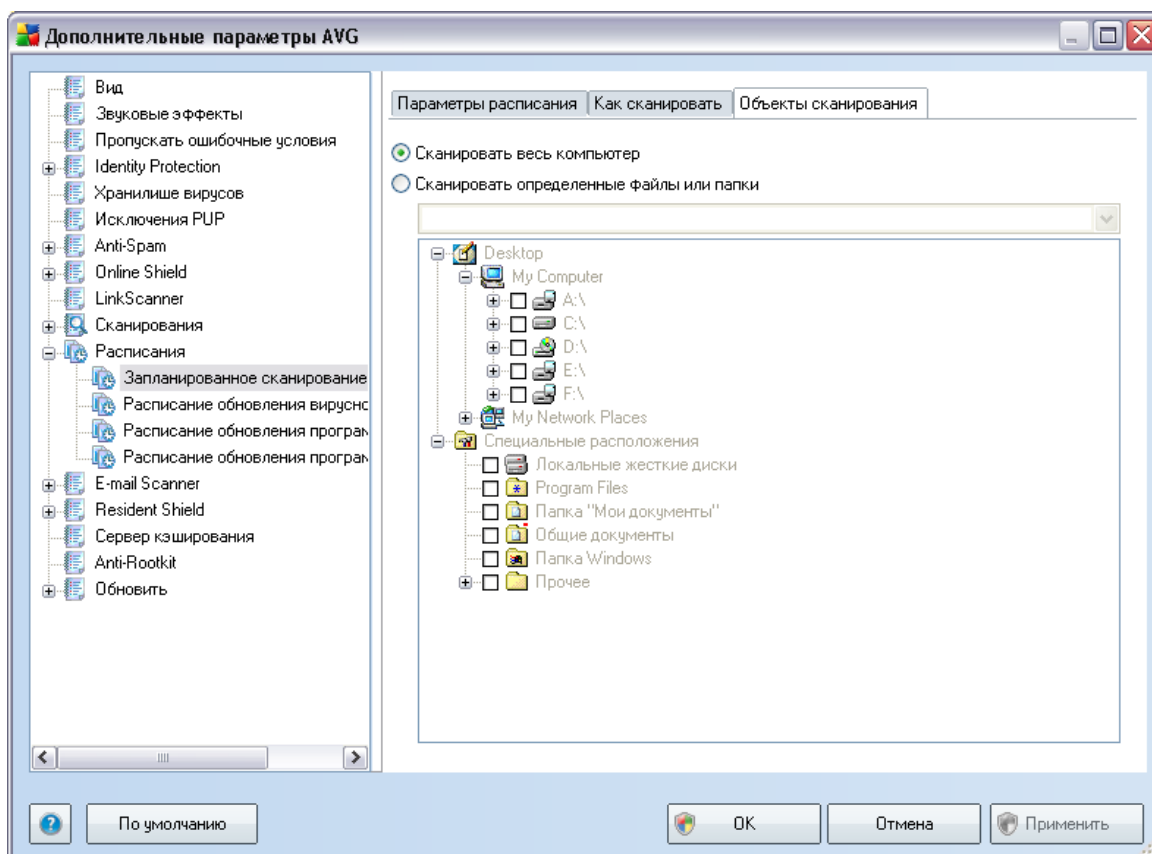
Щелкните ссылку **Настроить дополнительные отчеты сканирования ...**, чтобы открыть диалоговое окно **Отчеты сканирования**, в котором можно выбрать типы объектов, о которых будут выводиться отчеты при сканировании.



Щелкните ссылку **Дополнительные параметры сканирования ...**, чтобы

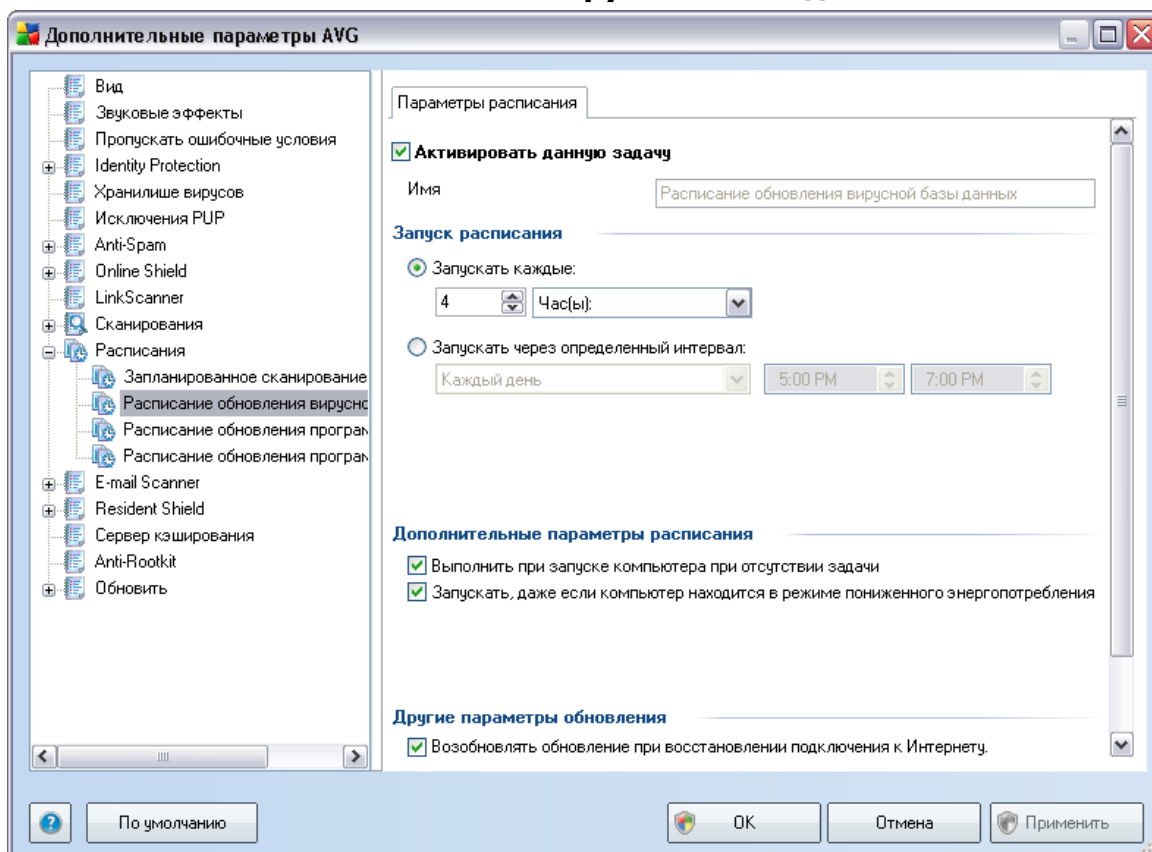
открыть новое диалоговое окно **Параметры выключения компьютера**, с помощью которого можно настроить автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (**Выключить компьютер после завершения сканирования**) становится доступен новый параметр, позволяющий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





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

10.9.2. Расписание обновления вирусной базы данных



На вкладке **Параметры расписания** можно сначала установить или снять флажок напротив элемента **Активировать данную задачу**, чтобы временно отключить запланированное обновление вирусной базы данных, и включить его снова при необходимости. 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...**).

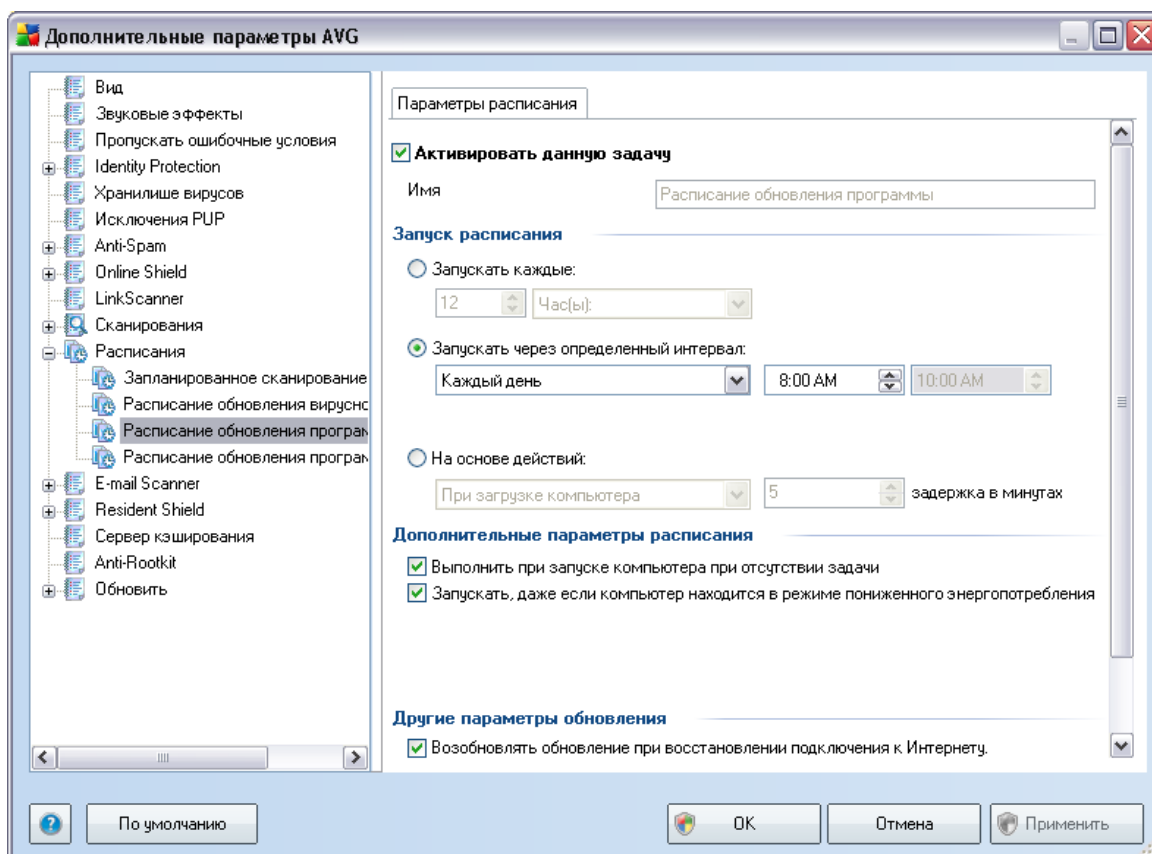
Дополнительные параметры расписания

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).



На вкладке **Параметры расписания** можно сначала установить или снять флажок напротив элемента **Активировать данную задачу** для временного отключения обновления программы или его повторного включения при необходимости. 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.

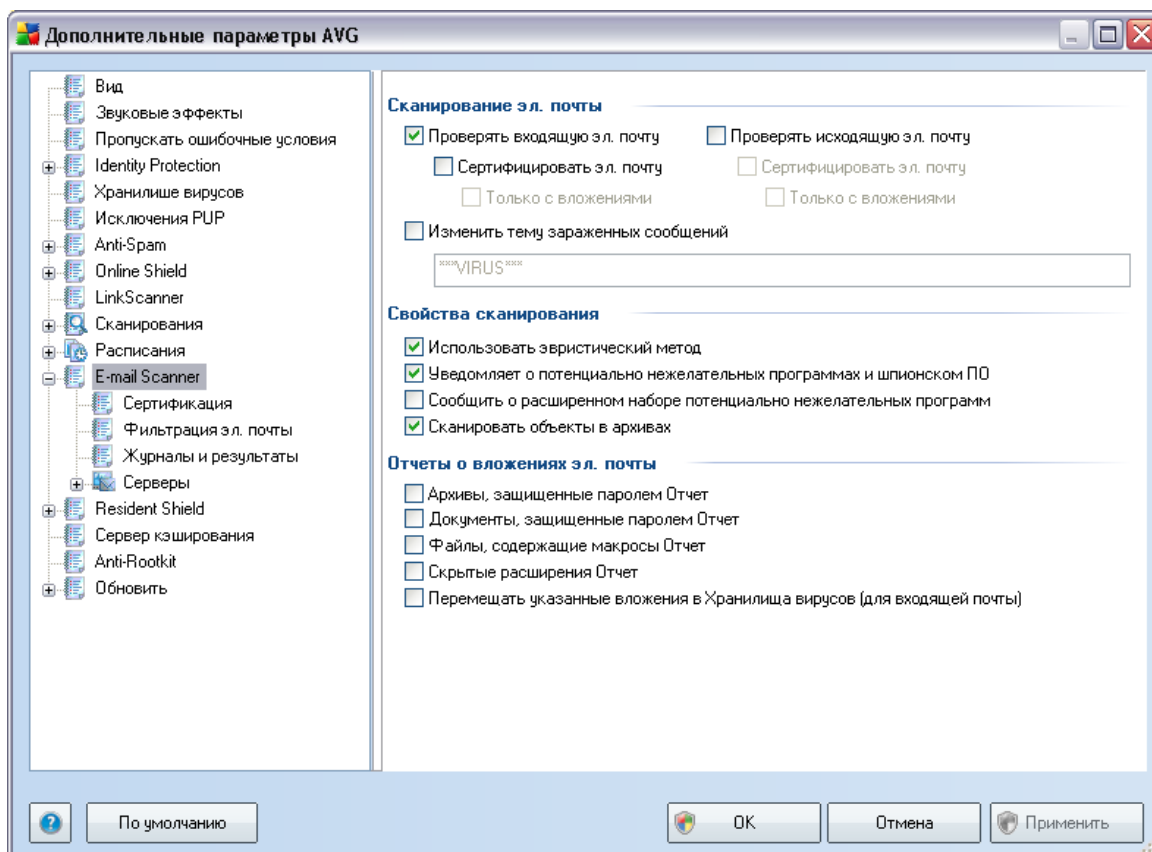
Другие параметры обновления

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.

10.10. E-mail Scanner



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

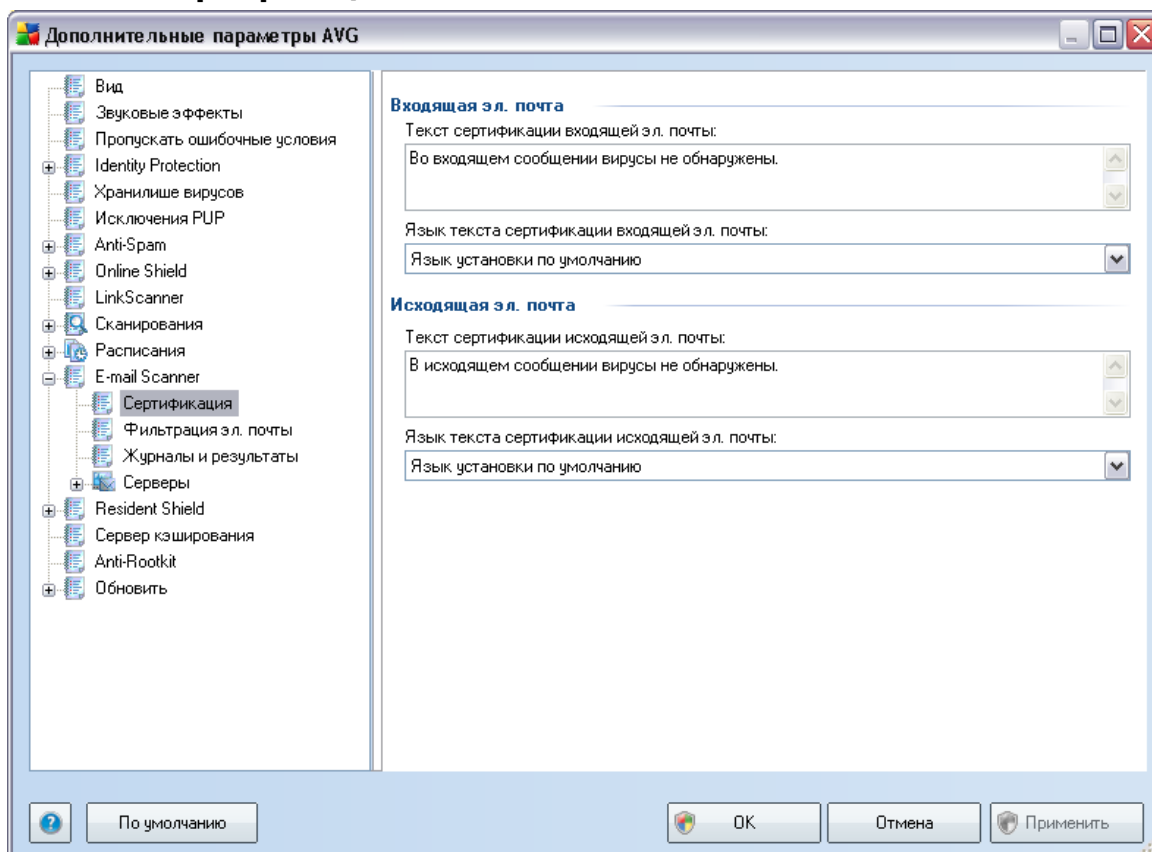
- **Сканирование эл. почты.** В этом разделе можно указать следующие основные требования для входящих и исходящих сообщений электронной почты.
 - о Необходимость проверки сообщений электронной почты на наличие вирусов.
 - о Необходимость добавления в конце каждого сообщения текста сертификации для подтверждения отсутствия вирусов. Текст можно изменить в диалоговом окне [Сертификация](#).
 - о Необходимость добавления текста сертификации только к сообщениям с вложениями.

Чтобы **изменить тему зараженных вирусом сообщений**, установите соответствующий флажок и введите в текстовом поле необходимое значение. В дальнейшем оно будет добавляться в поле темы каждого зараженного сообщения электронной почты, что упростит процесс идентификации и фильтрации. По умолчанию установлено значение *****VIRUS*****, его не рекомендуется менять.

- **Свойства сканирования.** В этом разделе можно указать способ сканирования сообщений электронной почты.
 - **Использовать эвристический анализ.** Установите 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** (флажок установлен 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.** Если предыдущий параметр активирован, можно также выбрать данный параметр для определения расширенного набора [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** – установите флажок, чтобы выполнять сканирование архивов, вложенных в сообщения электронной почты.

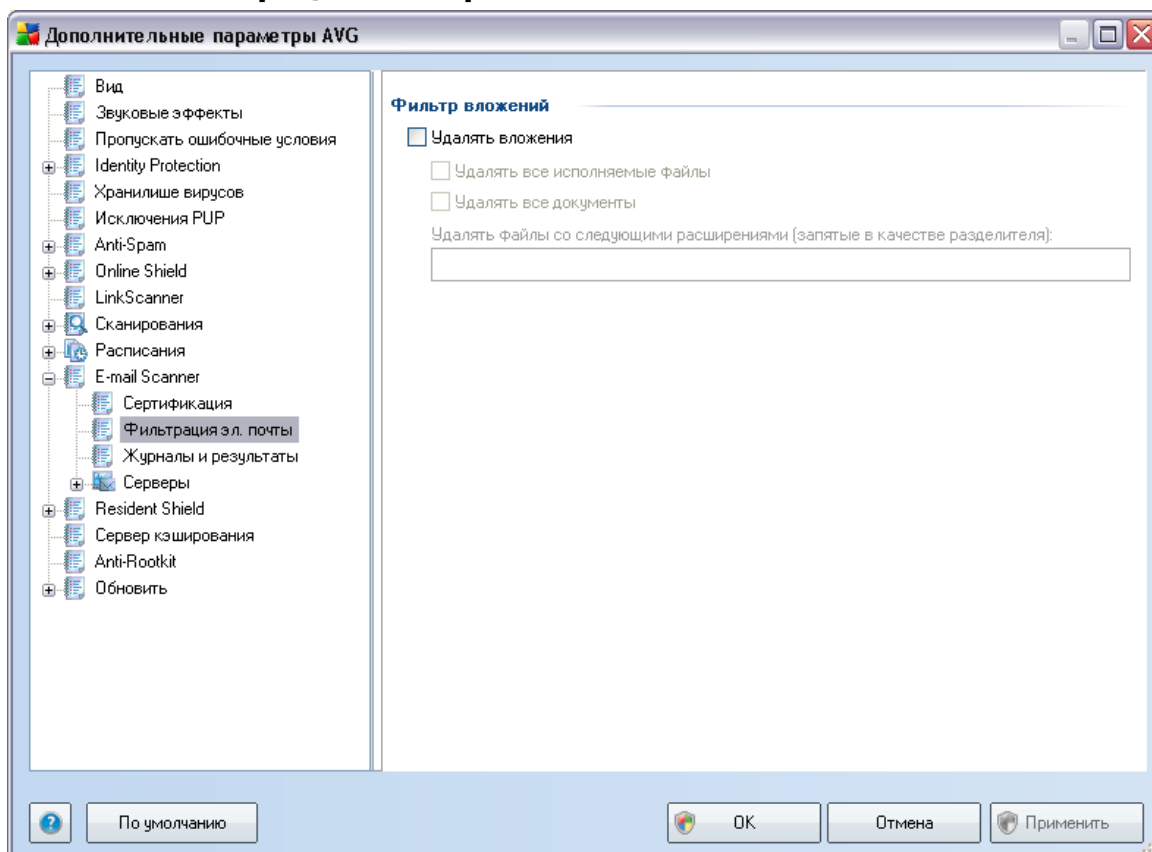
- **Отчеты о вложениях эл. почты.** В этом разделе можно настроить функцию предоставления дополнительных отчетов о потенциально опасных или подозрительных файлах. Обратите внимание, что диалоговое окно с предупреждением отображено не будет. Только текст сертификации будет добавлен в конце сообщения эл.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

10.10.1. Сертификация



В диалоговом окне **Сертификация** можно указать текст, который будет содержаться в сообщении о сертификации, и выбрать язык. Это необходимо сделать отдельно для **входящих** и **исходящих сообщений**.

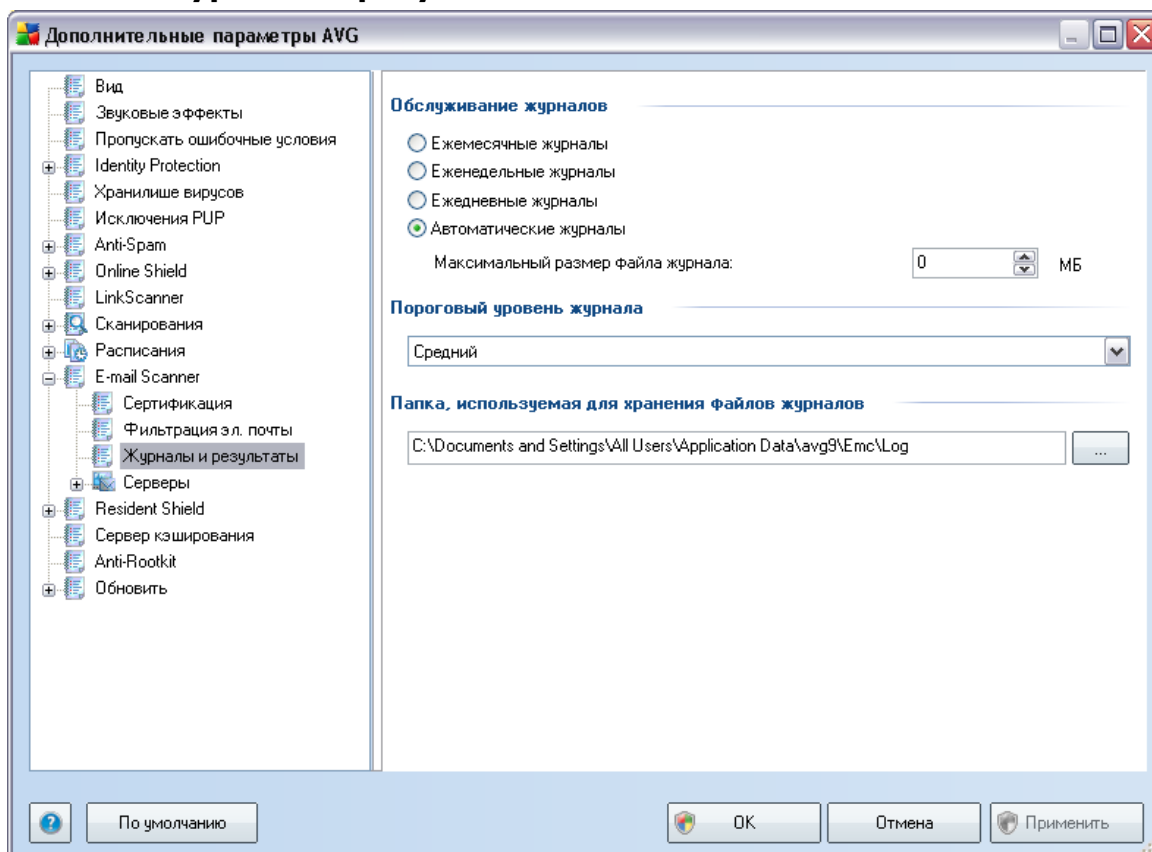
10.10.2. Фильтрация электронной почты



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 с расширениями, разделенными запятыми.** Все файлы с указанными расширениями будут удалены.

10.10.3. Журналы и результаты



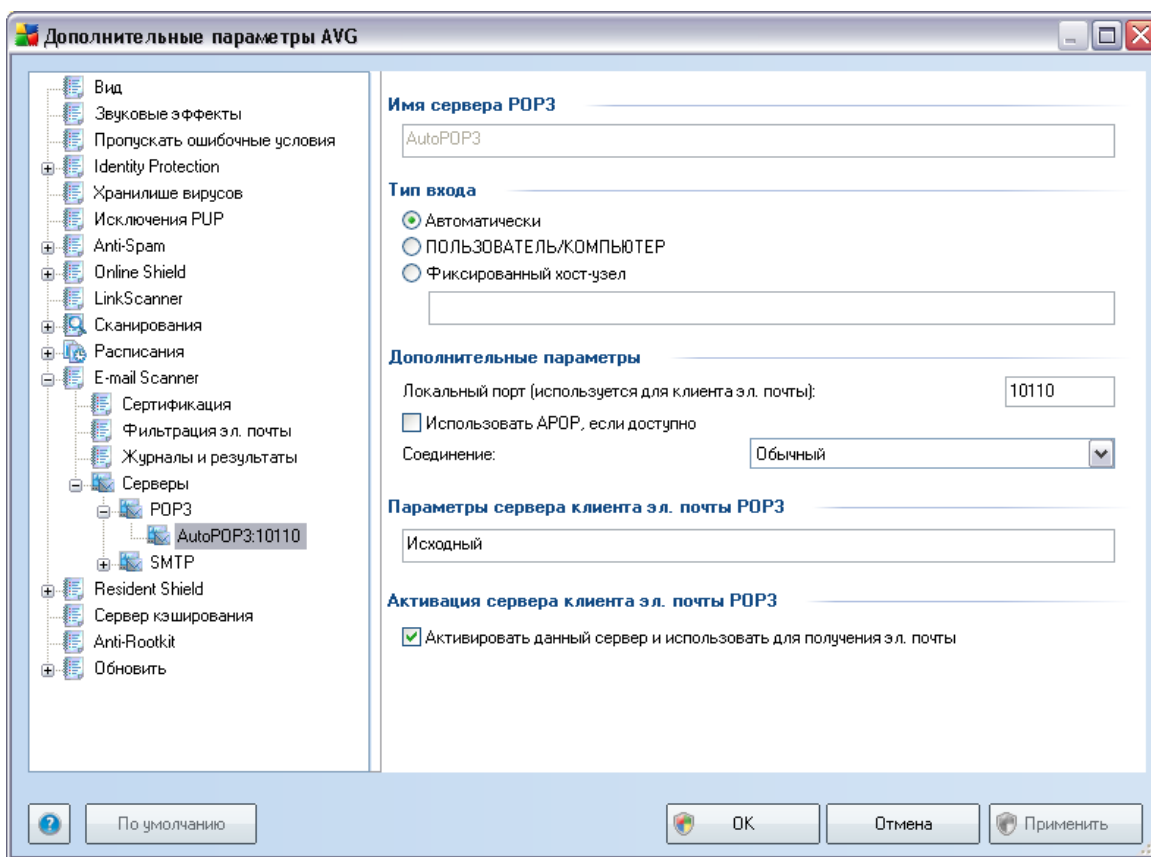
Диалоговое окно, открытое с помощью элемента навигации **Журналы и результаты**, позволяет указать параметры обслуживания результатов сканирования сообщений электронной почты. Диалоговое окно состоит из нескольких разделов.

- **Обслуживание журналов** — определение периодичности занесения в журнал информации о сканировании электронной почты (ежедневно, еженедельно, ежемесячно...). Также можно указать максимальный размер файла журнала (в МБ)
- **Пороговый уровень журнала** — по умолчанию установлен средний уровень. Можно выбрать более низкий уровень (занесение в журнал основных сведений о соединении) или более высокий уровень (занесение в журнал сведений о всем трафике)

- **Папка для хранения файлов журналов** — определите местоположение файла журнала

10.10.4. 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.

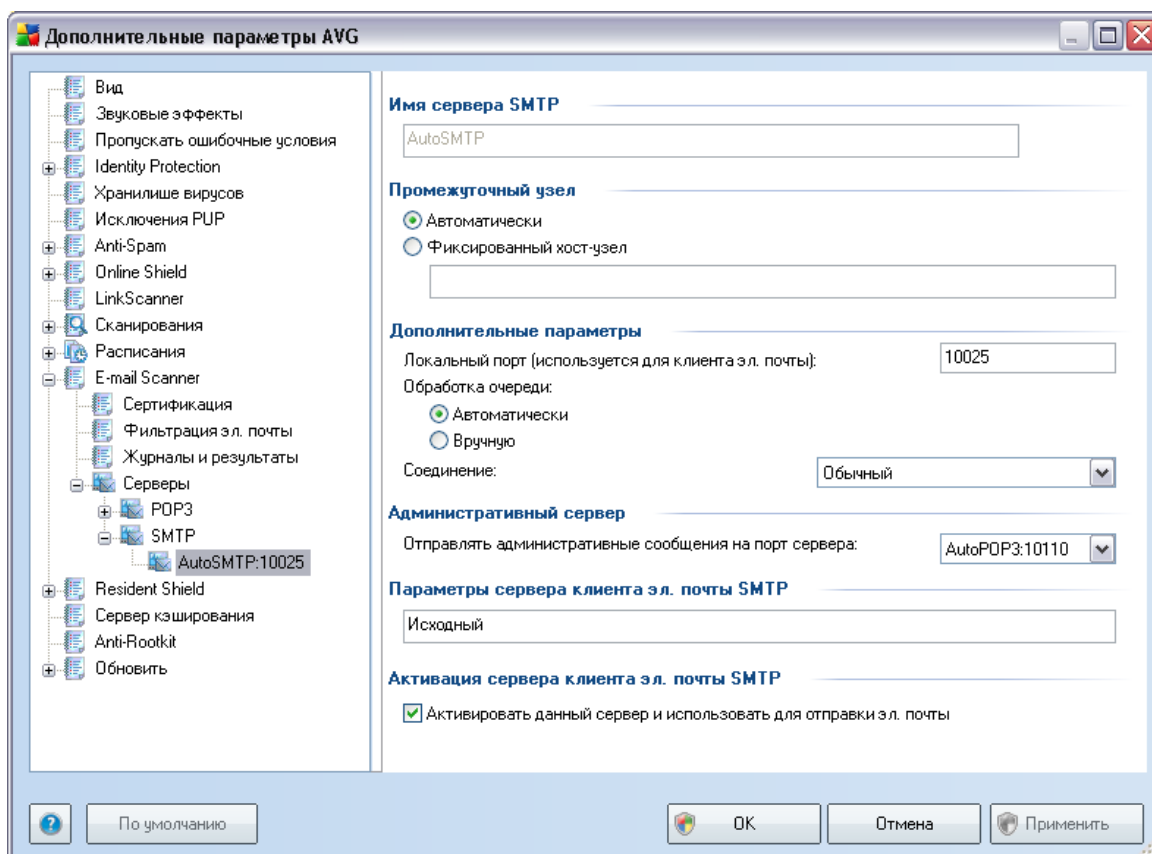
- **Имя сервера POP3** — введите имя сервера или сохраните имя AutoSMTP, установленное по умолчанию.
- **Тип входа** — метод определения почтового сервера, используемого для

входящей почты.

- o **Автоматически** — автоматическое выполнение входа в соответствии с параметрами электронной почты клиента.
- o **ПОЛЬЗОВАТЕЛЬ/КОМПЬЮТЕР** — наиболее простой и часто используемый способ определения почтового сервера назначения — это способ прокси-сервера. Чтобы воспользоваться данным методом, укажите имя или адрес (а также порт) в имени пользователя соответствующего почтового сервера, разделив их символом "/". Например, для учетной записи user1 на сервере pop.asme.com и порта 8200 необходимо ввести следующее имя пользователя: user1/pop.asme.com:8200.
- o **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.asme.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.
 - o **Локальный порт**. Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом приложении необходимо указать данный порт в качестве порта соединения POP3.
 - o **Использовать APOP, если доступно** — данный параметр обеспечивает более безопасный вход на почтовый сервер. При этом компонент **E-mail Scanner** использует альтернативный способ передачи пароля учетной записи пользователя, отправляя пароль на сервер в зашифрованном формате и используя полученную с сервера цепь переменных. Следовательно, данная функция доступна, только если она поддерживается почтовым сервером назначения.
 - o **Подключение** — в раскрывающемся меню можно определить необходимый тип подключения (обычное/SSL/SSL по умолчанию). При выборе подключения 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.

- **Параметры сервера POP3 клиента электронной почты.** Краткие сведения о параметрах конфигурации, необходимых для правильной настройки клиента электронной почты (проверка всех входящих сообщений электронной почты компонентом **E-mail Scanner**). Данное краткое описание основано на соответствующих параметрах, указанных в данном диалоговом окне или других соответствующих диалоговых окнах.
- **Активация сервера POP3 клиента электронной почты.** Установите или снимите флажок напротив этого элемента, чтобы активировать или деактивировать указанный сервер POP3



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

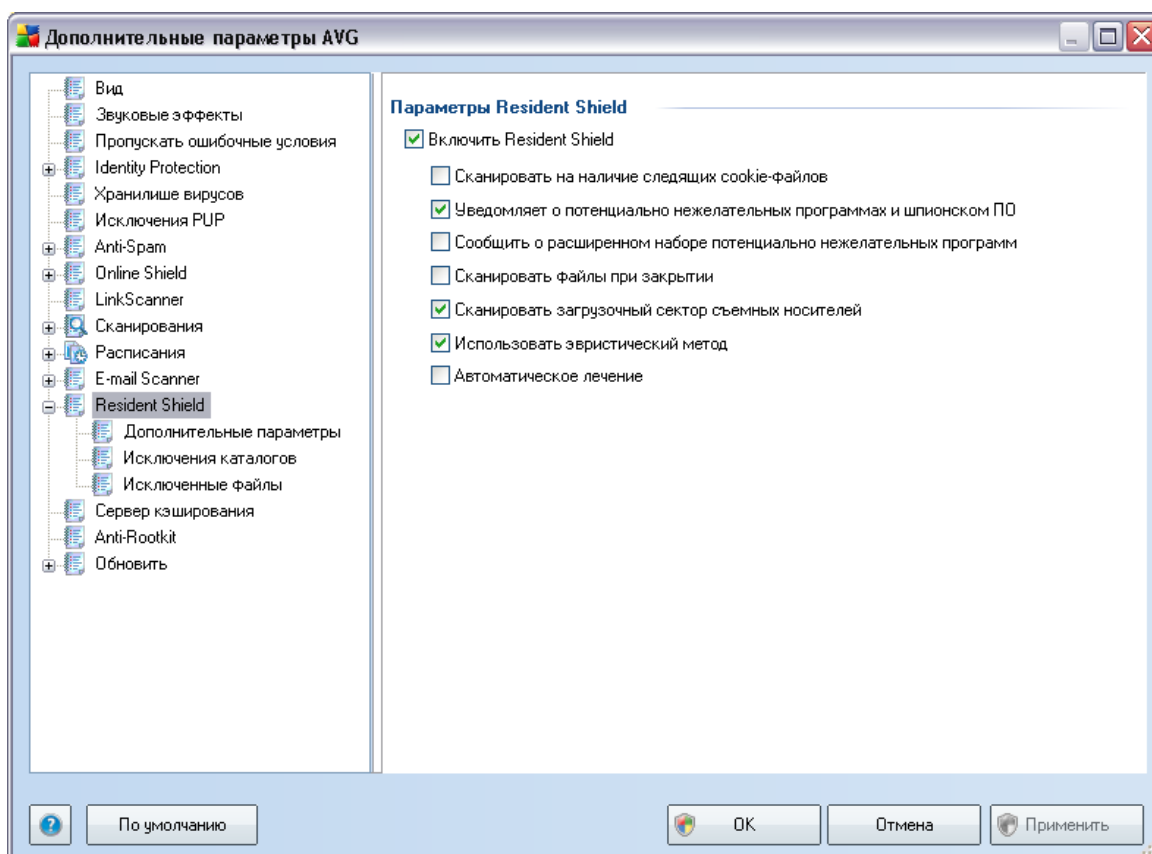
- **Имя сервера SMTP.** Введите имя сервера или оставьте имя AutoSMTP, установленное по умолчанию.
- **Промежуточный хост-узел.** Определяет способ определения сервера электронной почты, используемого для исходящей почты.
 - **Автоматически** — автоматическое выполнение входа в соответствии с параметрами клиента электронной почты
 - **Фиксированный хост-узел** — постоянное использование программой указанного сервера. Укажите адрес или имя используемого почтового сервера. В качестве имени можно указать имя домена (например, smtp.acme.com) или IP-адрес (например, 123.45.67.89). Если почтовый сервер использует нестандартный порт, данный порт можно указать после имени сервера, используя двоеточие в качестве разделителя (например, pop.acme.com:8200). Номер стандартного порта соединения SMTP — 25.
- **Дополнительные параметры** — определение более подробных параметров.
 - **Локальный порт.** Выбор порта, используемого почтовым приложением для соединения. Далее в почтовом клиенте необходимо указать данный порт в качестве порта соединения SMTP.
 - **Обработка очереди** — определение поведения компонента [**E-mail Scanner**](#) при обработке запросов отправки сообщений электронной почты.
 - Автоматически. Исходящие сообщения сразу доставляются (отправляются) на конечный почтовый сервер.
 - Вручную — сообщение помещается в очередь исходящих сообщений и отправляется позже.
 - **Подключение** — раскрывающееся меню, в котором можно указать необходимый тип подключения (обычное/SSL/SSL по умолчанию). При выборе безопасного 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.
- **В разделе** Административный сервер отображается номер порта сервера, который используется для обратной доставки административных отчетов. Например, данные сообщения создаются, если конечный почтовый сервер

недоступен или отклоняет исходящее сообщение.

- **Параметры сервера SMTP клиента электронной почты.** Содержит краткие инструкции по настройке приложения почтового клиента для проверки исходящих сообщений с помощью измененного сервера для проверки исходящих сообщений электронной почты. Данное краткое описание основано на соответствующих параметрах, указанных в данном диалоговом окне или других соответствующих диалоговых окнах.
- **Активация сервера SMTP клиента электронной почты.** Установите или снимите этот флажок, чтобы активировать или деактивировать указанный выше сервер SMTP.

10.11. Resident Shield

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



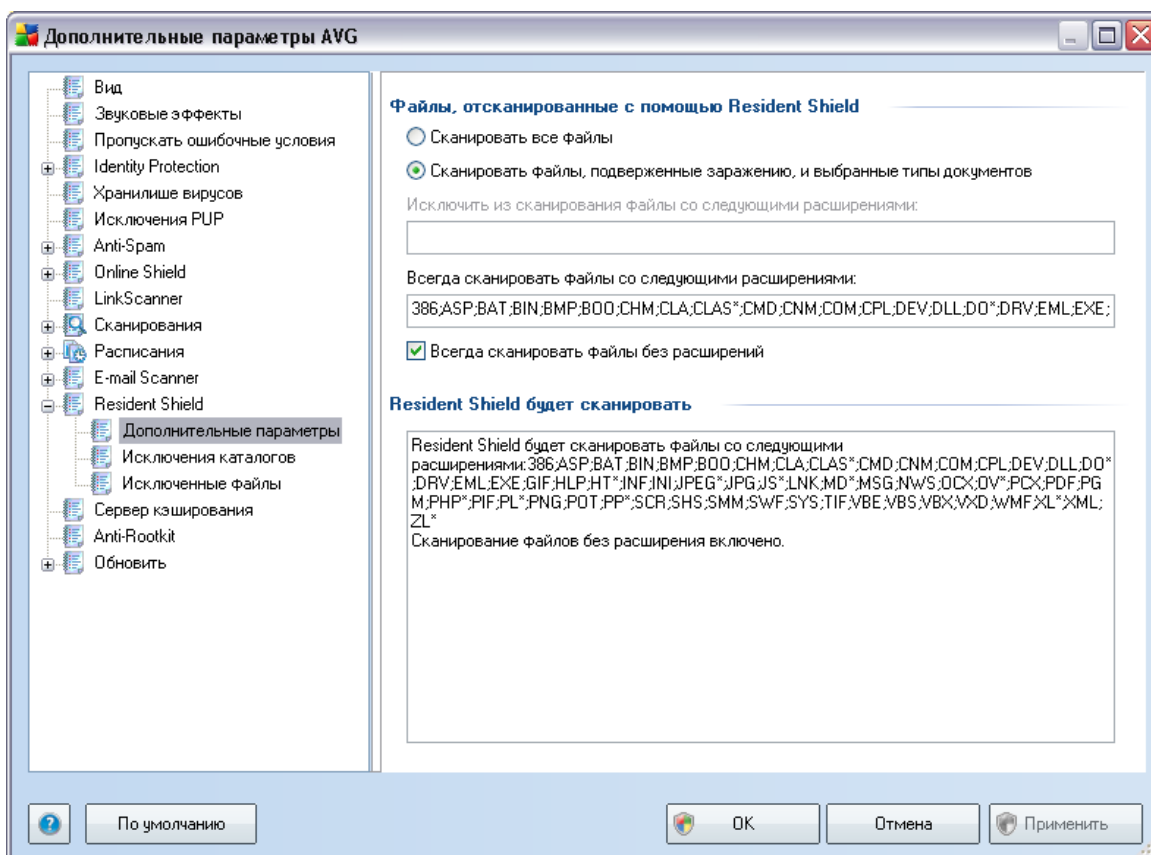
В диалоговом окне **Параметры Resident Shield** можно включить или отключить защиту, осуществляемую компонентом **Resident Shield**, установив или сняв флажок с параметра **Включить Resident Shield** (по умолчанию данный параметр включен). Также можно выбрать функции компонента **Resident Shield**, которые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

- **Сканировать на наличие следящих cookie-файлов** — данный параметр определяет обнаружение cookie-файлов при сканировании. (Файлы cookie протокола HTTP используются для аутентификации, 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** (флажок установлен 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**. Если предыдущий параметр активирован, можно также выбрать данный параметр для определения расширенного набора **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** — сканирование программой AVG активных объектов (например, приложений, документов...) при открытии, а также при закрытии. Данная функция помогает защитить компьютер от некоторых разновидностей современных вирусов.
- **Сканировать загрузочный сектор съемных носителей** — (по умолчанию включен)
- **Использовать эвристический анализ** (по умолчанию включен)
эвристический анализ будет использован для обнаружения (динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде).

- **Автоматическое лечение** — любое обнаруженное заражение будет вылечено автоматически, если лечение возможно.

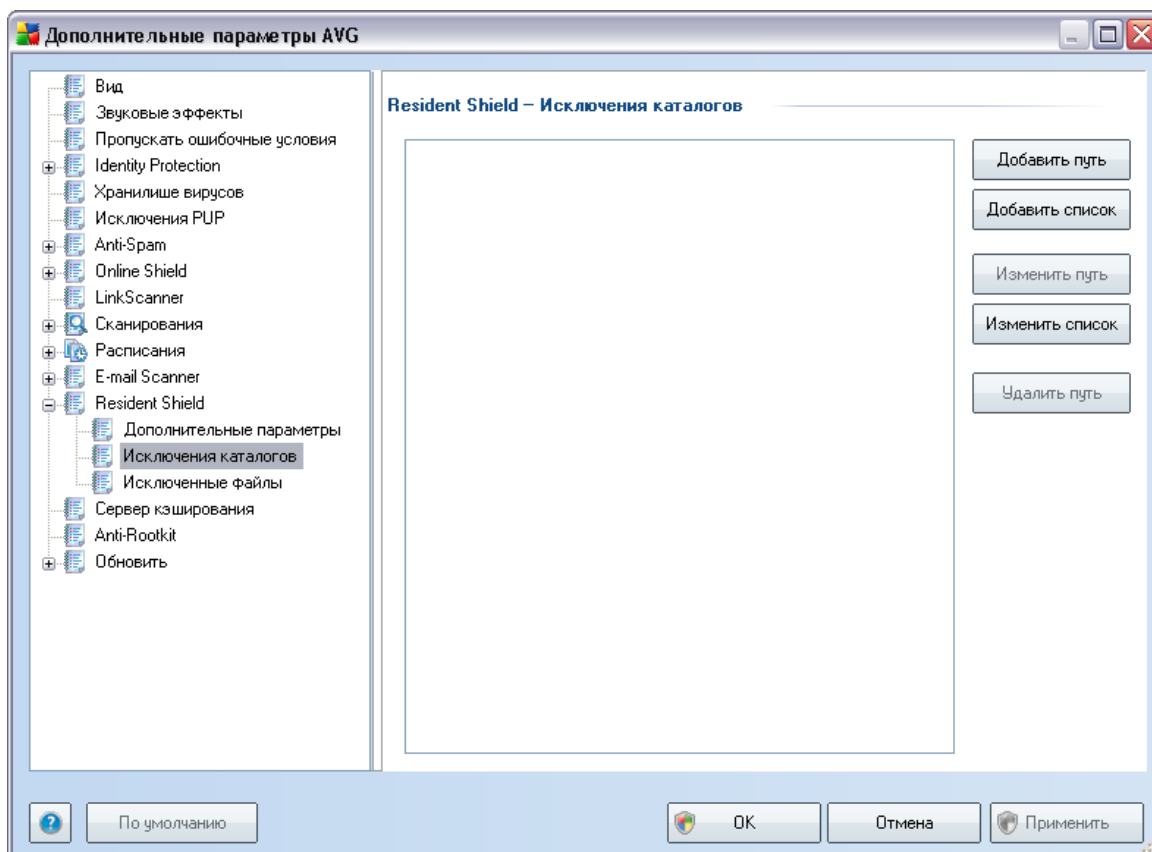
10.11.1. Дополнительные параметры

В диалоговом окне **Файлы, сканируемые с помощью компонента 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.

10.11.2. Исключаемые каталоги



Диалоговое окно **Resident Shield — Исключения каталогов** позволяет определить папки, которые должны быть исключены из сканирования компонентом **Resident Shield**.

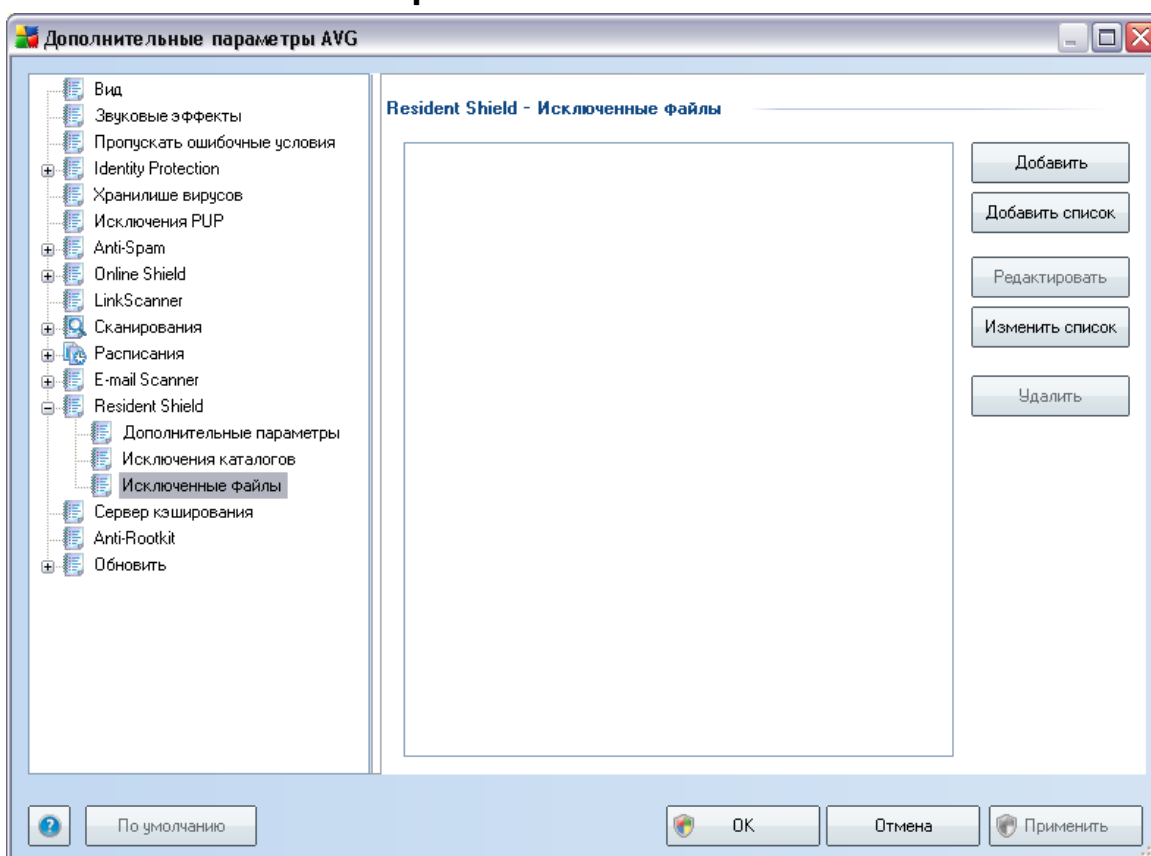
Настоятельно рекомендуется не исключать папки без необходимости.

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 список**— позволяет ввести полный список каталогов, которые должны быть исключены из сканирования компонентом **Resident Shield**

- **Изменить путь**— позволяет изменить указанный путь к выбранной папке.
- **Редактировать список**— позволяет редактировать список папок
- **Удалить путь**— позволяет удалить путь к выбранной папке из списка.

10.11.3. Исключенные файлы



Диалоговое окно **Resident Shield — Исключенные файлы** работает так же, как ранее описанное **Resident Shield — Исключения каталогов**, но вместо папок теперь можно указать определенные файлы, которые не должны сканироваться компонентом **Resident Shield**.

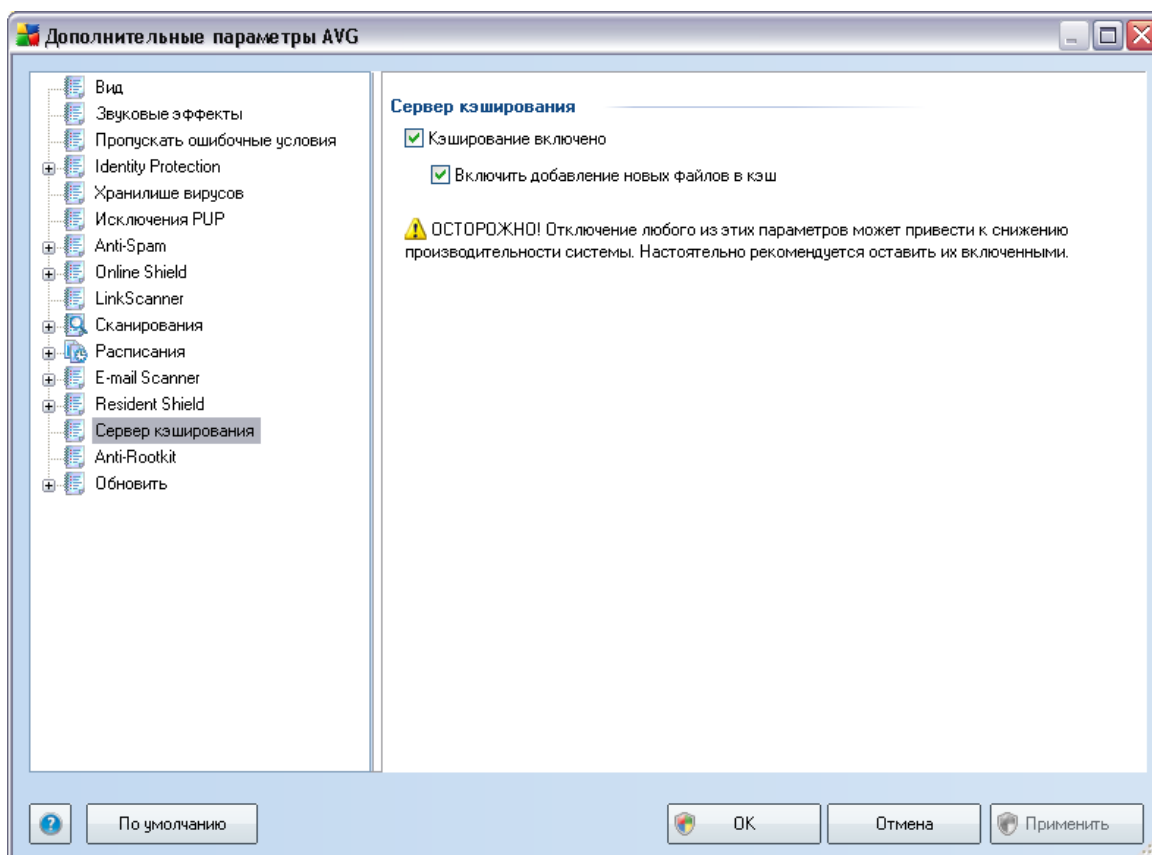
Настоятельно рекомендуется не исключать файлы без необходимости.

В диалоговом окне содержатся следующие кнопки управления:

- **Добавить.** Укажите файлы, которые должны быть исключены из сканирования, выбрав их последовательно в навигационном дереве локального диска.
- **Добавить список.** Позволяет ввести полный список файлов, которые должны быть исключены из сканирования компонентом [Resident Shield](#).
- **Редактировать.** Позволяет редактировать указанный путь к выбранному файлу.
- **Редактировать список.** Позволяет редактировать список файлов.
- **Удалить.** Позволяет удалить путь к выбранному файлу из списка.

10.12. 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.

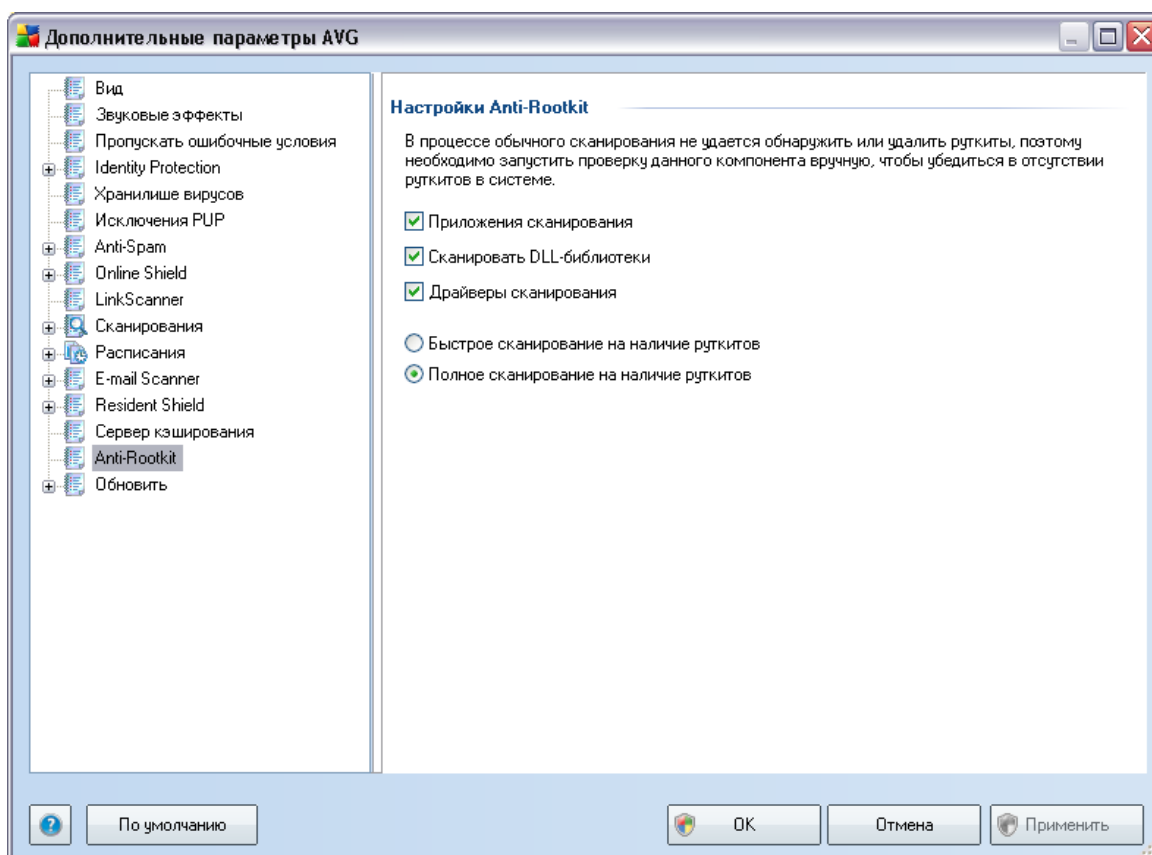


Диалоговое окно настройки содержит два параметра.

- **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.

10.13. 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**.

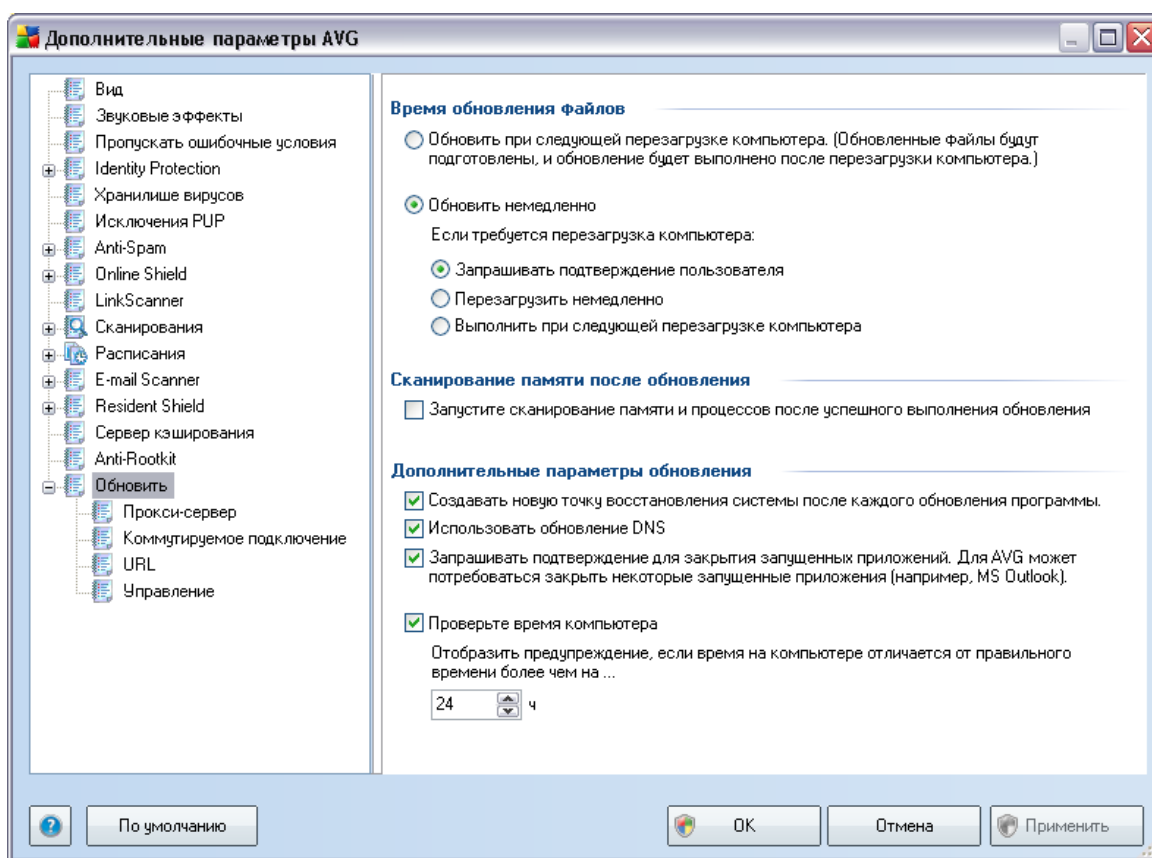
Чтобы указать объекты, которые должны сканироваться, установите соответствующие флажки.

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

Далее можно включить режим сканирования на наличие средств rootkit.

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

10.14. Обновить



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

Время обновления файлов

В этом разделе можно выбрать один из двух вариантов: выполнять [обновление](#) при следующей перезагрузке компьютера или выполнять [обновление](#) немедленно. Для обеспечения максимального уровня безопасности по умолчанию выбран второй вариант (немедленное обновление). Первый вариант (обновление при следующей перезагрузке компьютера) следует выбирать только в том случае, если вы уверены, что перезагрузка компьютера выполняется не реже одного раза в день.

Если вы решили не изменять конфигурацию по умолчанию и немедленно запускать обновление, можно выбрать условия, при которых будет выполнена перезагрузка компьютера.

- **Запрашивать подтверждение пользователя** — появится запрос на подтверждение перезагрузки, 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 компьютера (не забывайте, что этот вариант следует выбирать только в том случае, если вы уверены, что перезагрузка компьютера выполняется не реже одного раза в день)

Сканирование памяти после обновления

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

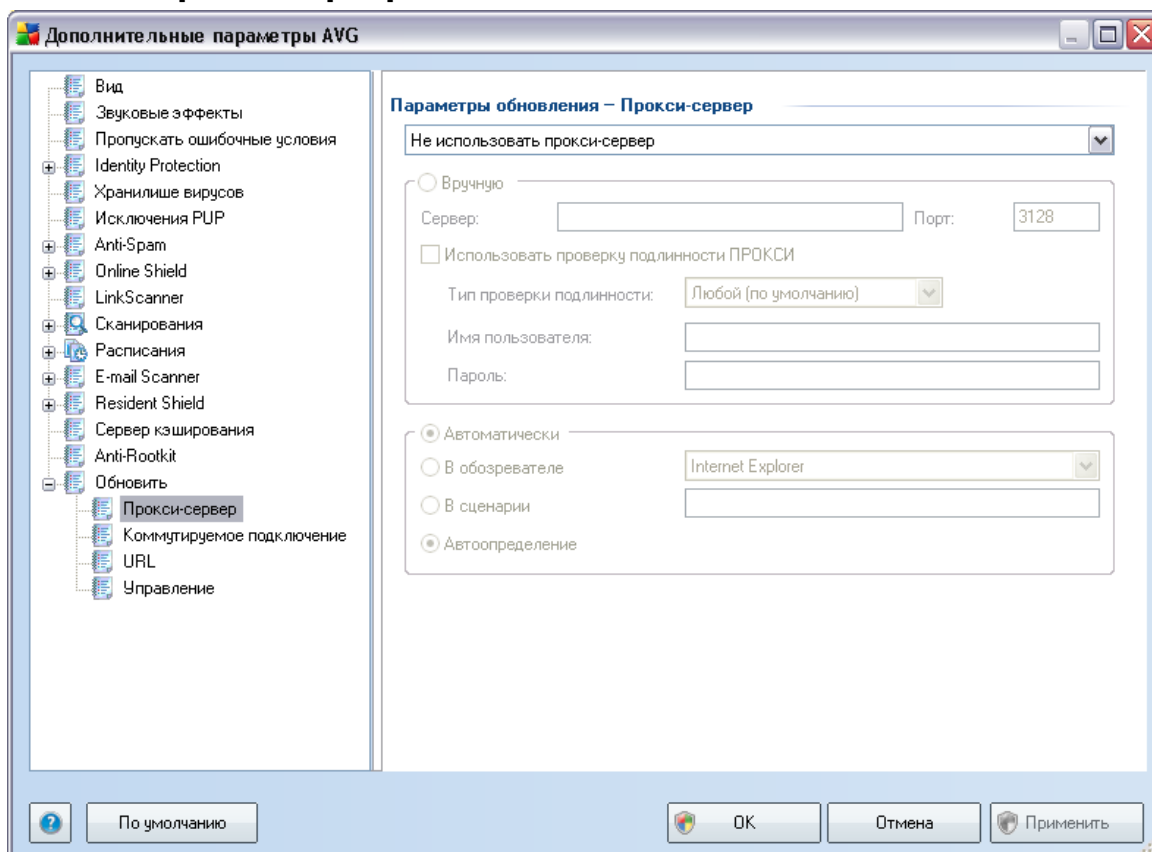
Дополнительные параметры обновления

- **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** — установите этот флажок, чтобы подтвердить необходимость использования способа обнаружения файлов обновлений, что позволит избежать передачи данных между сервером обновлений и клиентом AVG.
- **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.

10.14.1. 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 с помощью прокси-сервера, если не удастся — подключиться напрямую**

При выборе параметров, использующих прокси-сервер, необходимо указать

некоторые дополнительные данные. Параметры сервера можно настроить автоматически или вручную.

Настройка вручную

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

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

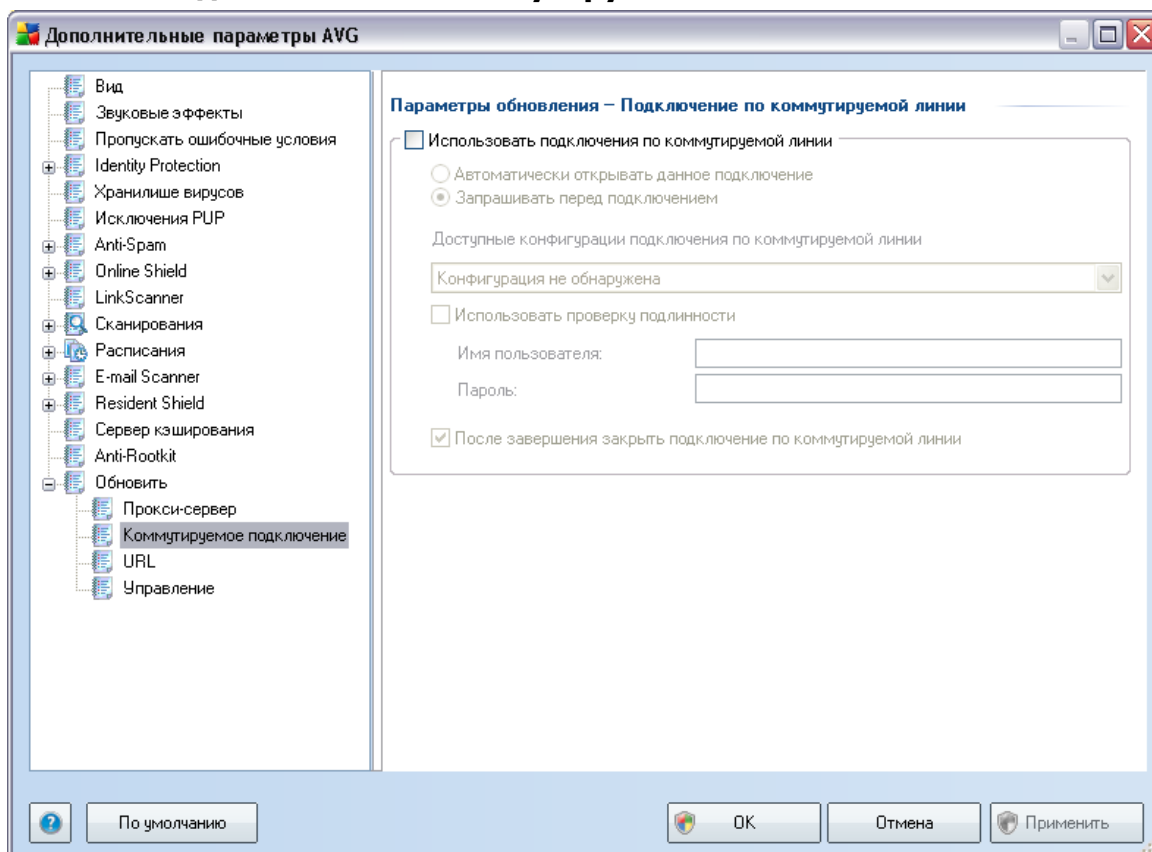
На прокси-сервере также могут быть заданы определенные правила для каждого пользователя. В этом случае установите флажок **Использовать проверку подлинности ПРОКСИ**, чтобы программа выполняла проверку подлинности имени пользователя и пароля перед подключением к Интернету через прокси-сервер.

Автоматическая настройка

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

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

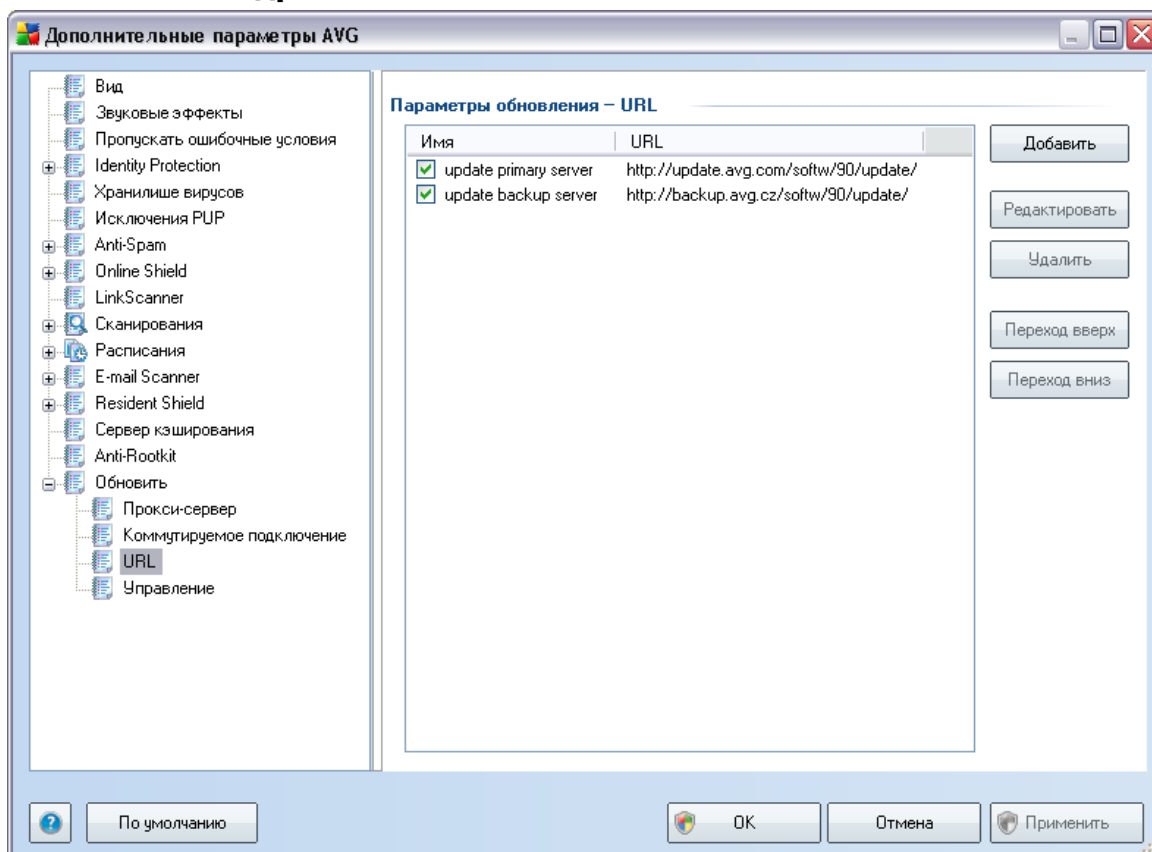
10.14.2. Подключение по коммутируемой линии



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

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

10.14.3. URL-адрес

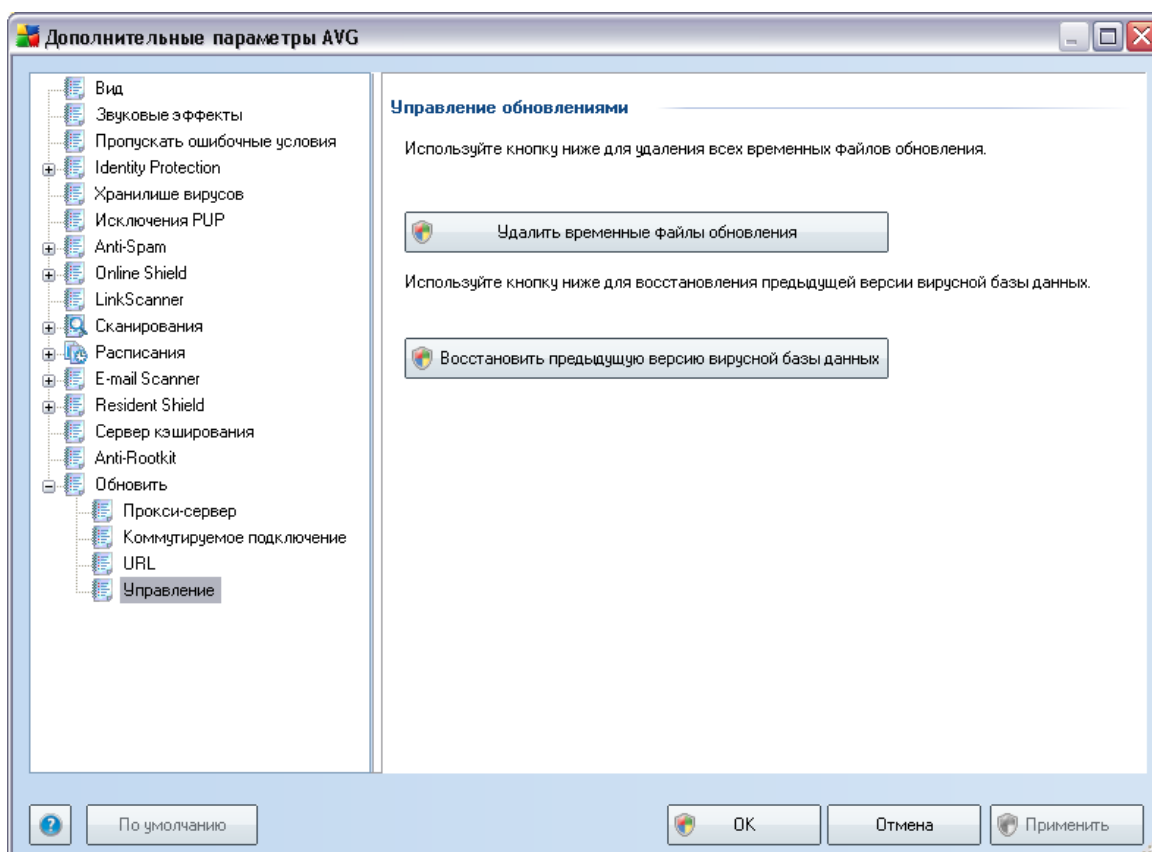


В диалоговом окне **URL-адрес** приведен список интернет-адресов, по которым можно загрузить файлы обновлений. Данный список и его элементы можно изменить с помощью следующих кнопок управления.

- **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.

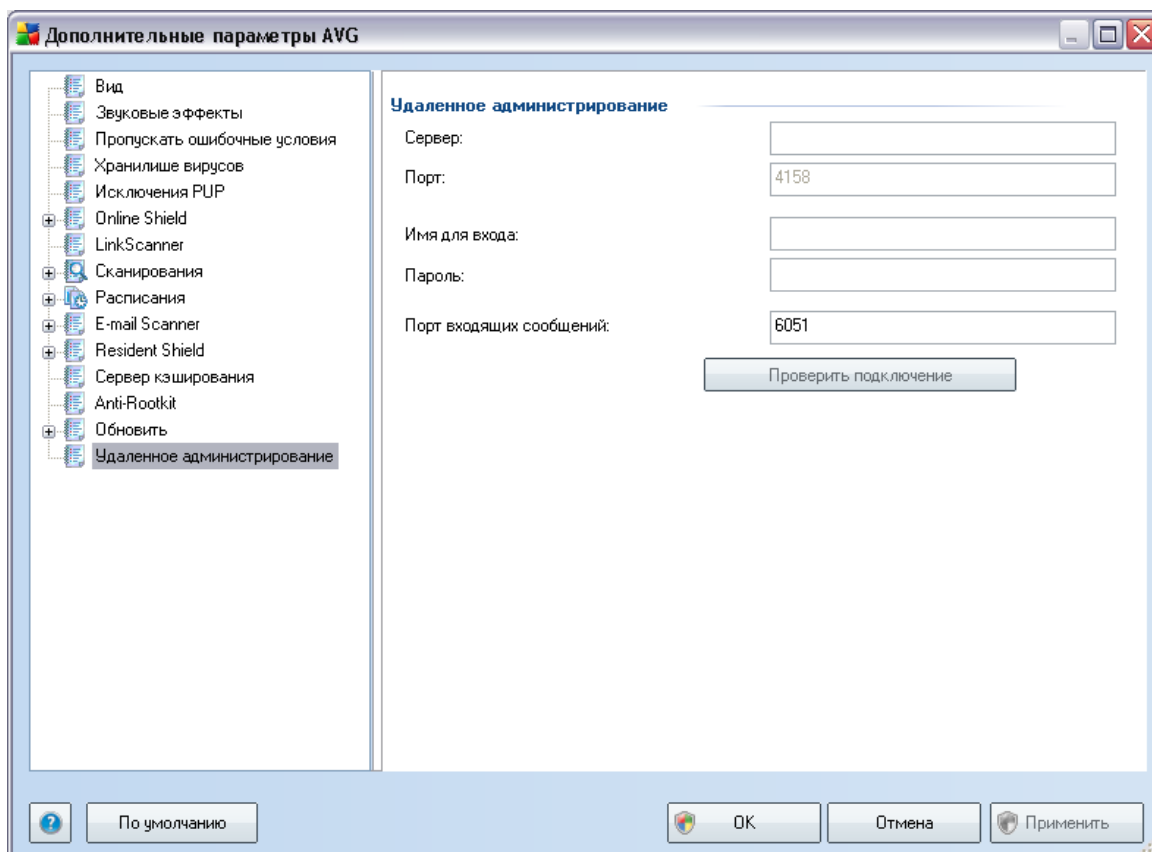
10.14.4. Управление

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*).

10.15. Удаленное администрирование



Параметры **удаленного администрирования** предназначены для настройки подключения клиентской рабочей станции AVG к системе удаленного администрирования. Для подключения соответствующей станции к системе удаленного администрирования необходимо указать следующие параметры.

- **Сервер** — имя сервера (или IP-адрес сервера), на котором установлено приложение AVG Admin Server.
- **Порт** — номер порта, с помощью которого клиент AVG устанавливает соединение с приложением AVG Admin Server (*номер порта 4158 установлен по умолчанию; если используется данный номер порта, нет необходимости его указывать*).
- **Имя пользователя** — если используется безопасное соединение между клиентом AVG и приложением AVG Admin Server, необходимо указать имя



пользователя.

- **Пароль** — ... также необходимо указать пароль.
- **Порт входящих сообщений** — номер порта, через который клиент AVG принимает входящие сообщения от приложения AVG Admin Server.

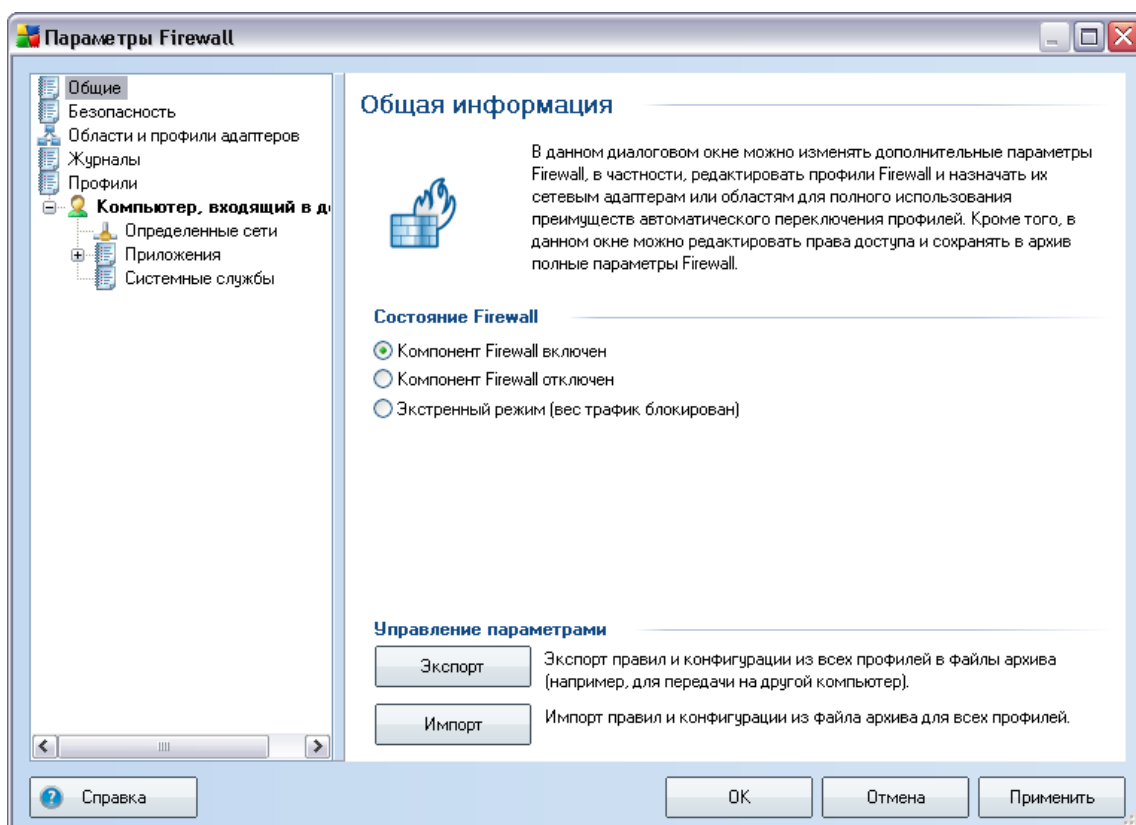
Кнопка **Проверить подключение** позволяет удостовериться, что вся упомянутая выше информация является допустимой и может быть использована для успешного соединения с DataCenter.

Примечание. Подробное описание системы удаленного администрирования смотрите в документации, прилагаемой к сетевой версии AVG.

11. Параметры Firewall

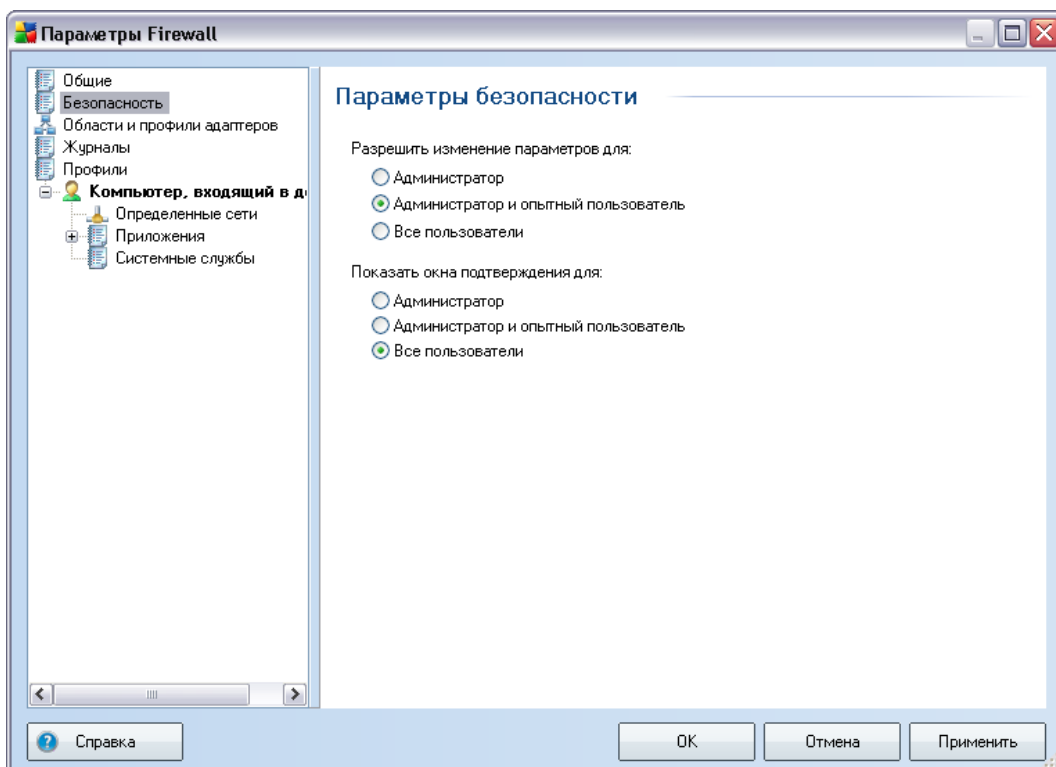
Конфигурация компонента **Firewall** открывается в новом окне, где с помощью нескольких диалоговых окон можно настроить дополнительные параметры компонента. **Настройка дополнительных параметров должна осуществляться только специалистами или опытными пользователями.**

11.1. Общие



В разделе **Общие сведения** можно выполнить **экспорт** или **импорт** конфигурации компонента **Firewall**. То есть экспортировать определенные правила и параметры компонента **Firewall** или импортировать целый файл резервной копии.

11.2. Безопасность



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

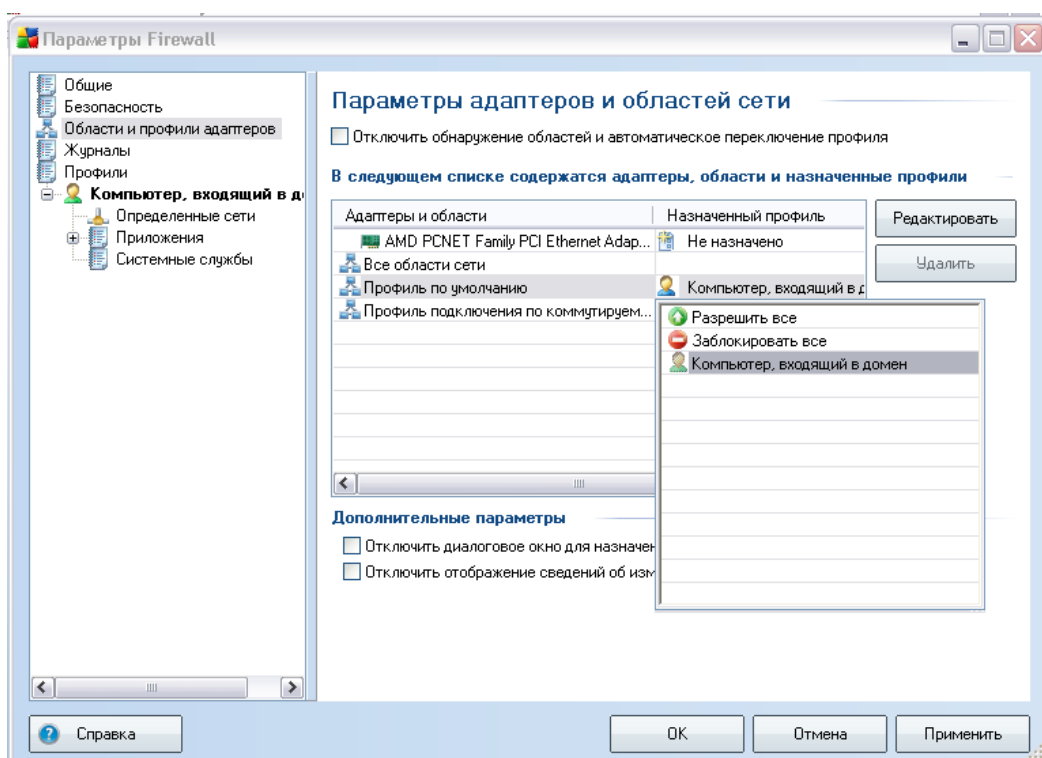
- **Разрешить изменение параметров** — позволяет определить лиц, которым разрешено изменять конфигурацию компонента **Firewall**
- **Показывать окно подтверждения** — позволяет определить лиц, для которых следует отображать диалоговые окна подтверждения (*диалоговые окна с вопросом о действии в ситуации,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

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

- о **Администратор** — полностью управляет ПК и имеет право назначать каждому пользователю в группах специально определенные права.

- о **Администратор и опытный пользователь** — администратор может закрепить каждого пользователя за специальной группой (*Опытный пользователь*) и определить права всех членов группы.
- о **Все пользователи** — другие пользователи, не закрепленные за какой-либо специальной группой.

11.3. Области и профили адаптеров



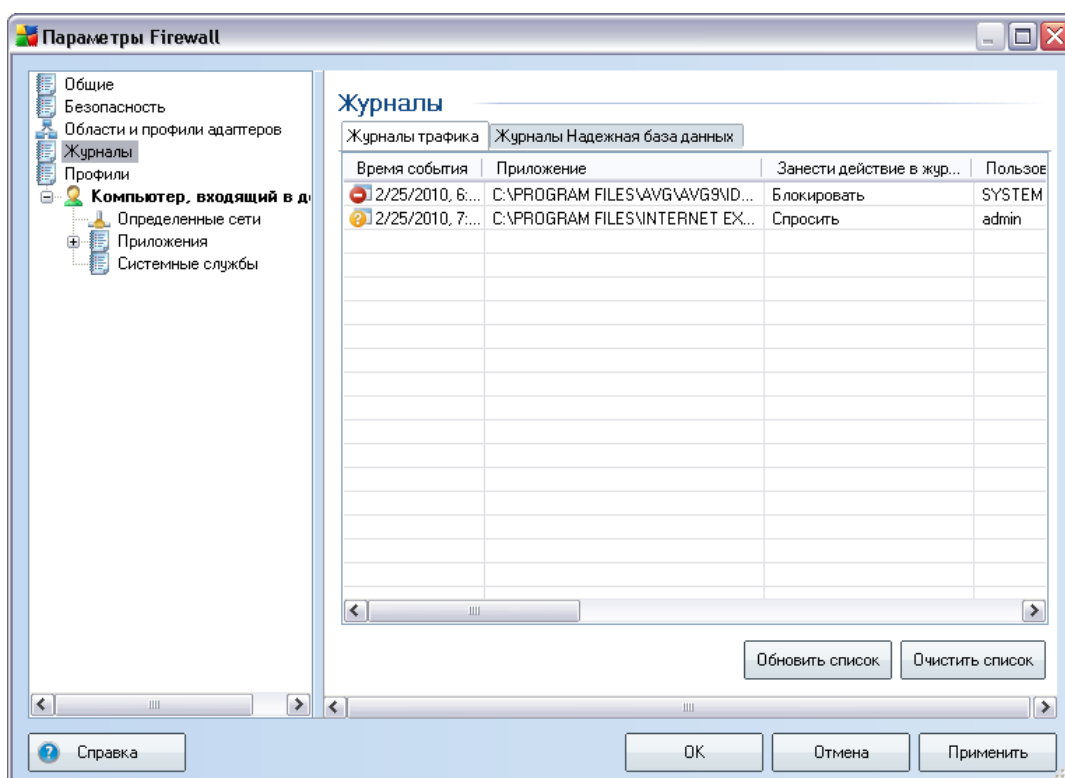
Диалоговые окна **Параметры адаптеров и областей сети** позволяют изменять параметры, относящиеся к определенным профилям конкретных адаптеров и соответствующих сетей.

- **Отключить обнаружение областей и автоматическое переключение профилей** — один из определенных профилей может быть назначен каждому типу сетевого интерфейса, а также каждой области. Если не указаны специальные профили, будет использоваться один общий профиль, определенный на основе выбора [типа используемого компьютера](#) и [проекта сети для используемого компьютера](#) во время [процесса установки](#). 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.** Установка соответствующего флажка приведет к отключению отображения информационного сообщения.

11.4. 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 др.) на двух вкладках:

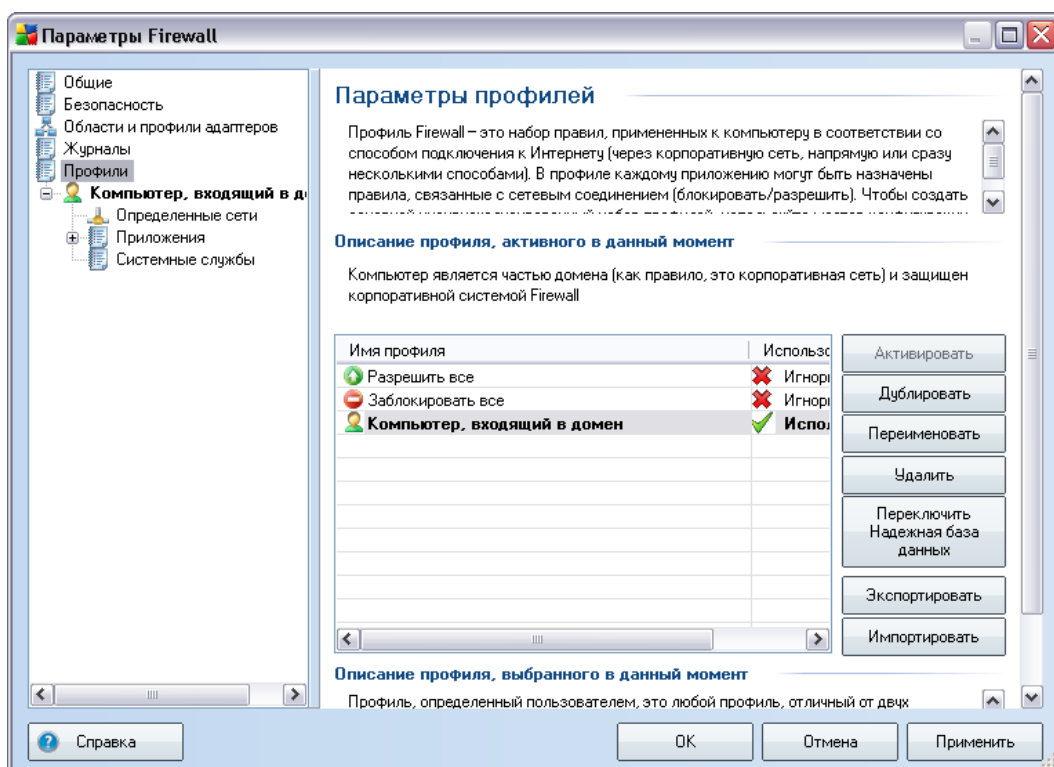
- **Журналы трафика.** Сведения об активности всех приложений, которые выполняли попытки подключиться к сети.
- **Журналы надежных баз данных.** Надежная база данных — это внутренняя база данных AVG, содержащая сведения о сертифицированных и надежных приложениях, которым всегда разрешен доступ в Интернет. 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.

Кнопки управления

- **Справка.** Открытие файла справки для текущего диалогового окна.
- **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.

11.5. 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** — 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
- **Справка** — открытие диалогового окна с файлом справки

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*).

11.5.1. Сведения о профилях



Диалоговое окно **Сведения о профилях** — это первое диалоговое окно раздела, в котором можно редактировать настройки каждого профиля в отдельных диалоговых окнах, относящихся к определенным параметрам профиля.

- **Использовать надежную базу данных для этого профиля** (по умолчанию флажок установлен). Установите флажок, чтобы активировать надежную базу данных для профиля. Например, внутреннюю базу данных AVG, содержащую сведения о надежных и сертифицированных приложениях, передающих данные по Интернету. Если для соответствующего приложения до сих пор не указано правило, необходимо выяснить, может ли приложению быть предоставлен доступ в сеть. Сначала приложением AVG выполняется поиск в надежной базе данных, и если данное приложение имеется в списке, оно будет считаться безопасным и сможет подключиться к сети. В противном случае пользователю будет предложено выбрать, разрешить ли данному приложению подключаться к сети.

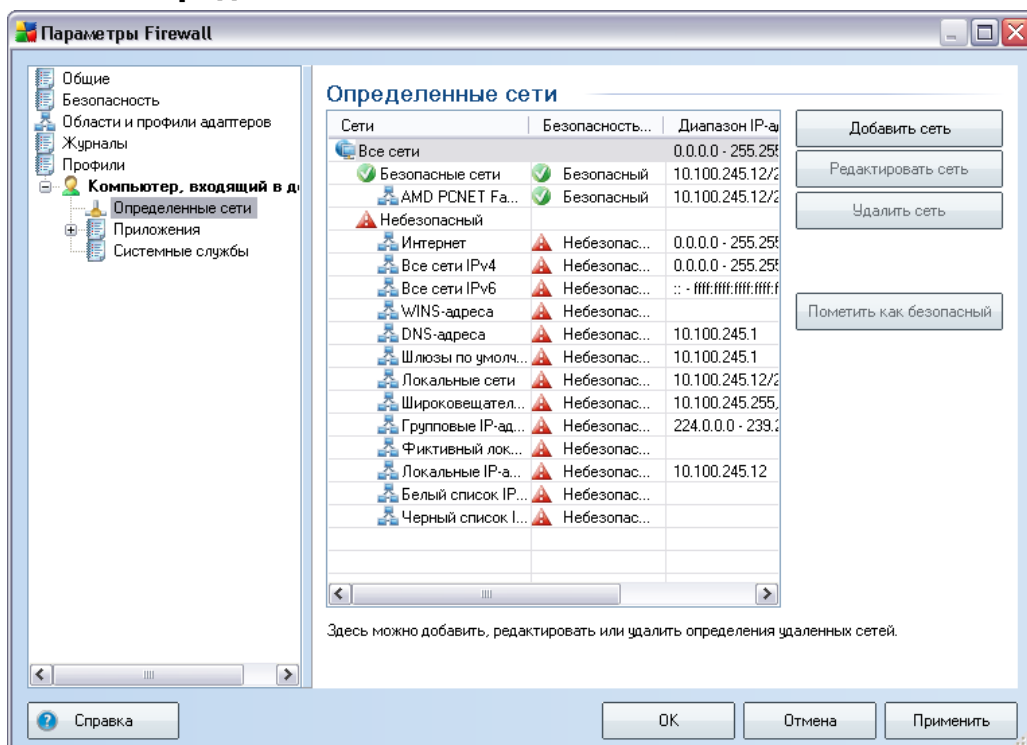
- **Включить мостовое сетевое соединение с виртуальными машинами** (отключен по умолчанию). Установите этот флажок, чтобы разрешить виртуальным машинам в среде VMware выполнять прямое подключение к сети.

Параметры режима «Во время игры»

В разделе **Параметры режима "Во время игры"** можно выбрать и подтвердить, отметив флажком соответствующий элемент, отображение информационных сообщений компонента **Firewall** во время работы полноэкранного приложения на компьютере (как правило, такими приложениями являются игры, но также к ним относятся такие приложения, как презентации PowerPoint). Так как информационные сообщения могут нарушать работу приложения.

При выборе пункта **Отключить уведомления Firewall во время игры** необходимо затем в раскрывающемся меню выбрать действие, которое будет выполнено при попытке нового приложения, для которого не определены правила, установить сетевое подключение (приложения, при открытии которых отображается диалоговое окно с запросом). Сетевое подключение для этих приложений может быть либо разрешено, либо заблокировано.

11.5.2. Определенные сети

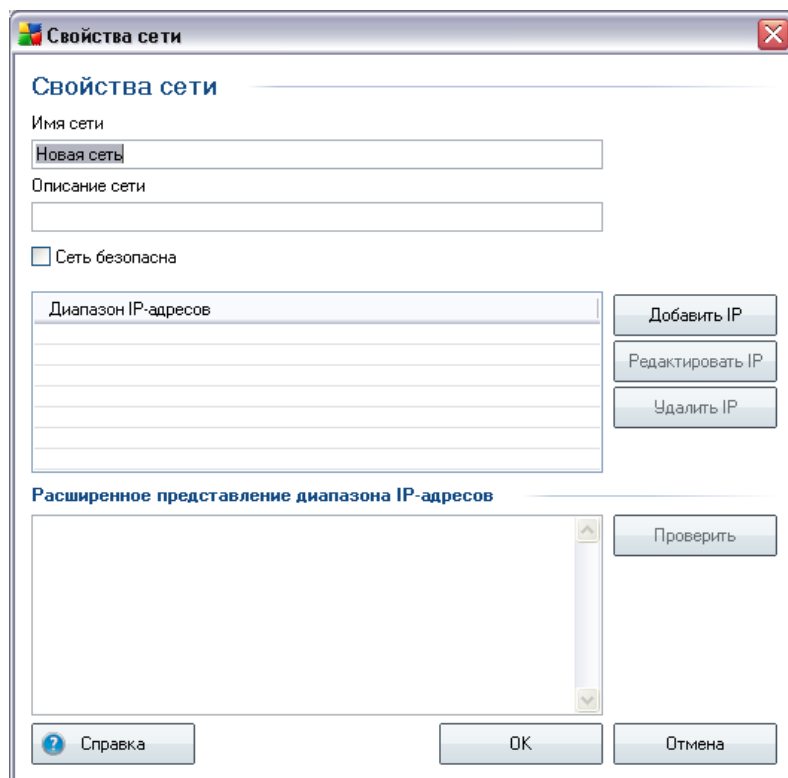


Диалоговое окно **Определенные сети** содержит список всех сетей, к которым подключен компьютер. Следующие сведения приведены для каждой обнаруженной сети.

- **Сети** — список имен всех сетей, к которым подключен компьютер.
- **Безопасность сети.** По умолчанию все сети считаются небезопасными. Если вы уверены, что соответствующая сеть является безопасной, можно определить для нее данное состояние (*щелкните соответствующий сети элемент списка и выберите в контекстном меню пункт "Безопасно"*). В результате все безопасные сети будут включены в группу, с которой приложение может устанавливать соединение с установленным набором правил для приложения "Разрешить для безопасных".
- **Диапазон IP-адресов** — каждая сеть будет обнаружена автоматически и указана в виде диапазона IP-адресов.

Кнопки управления

- **Добавить сеть** — открытие диалогового окна **Свойства сети**, с помощью которого можно изменить параметры только что определенной сети.



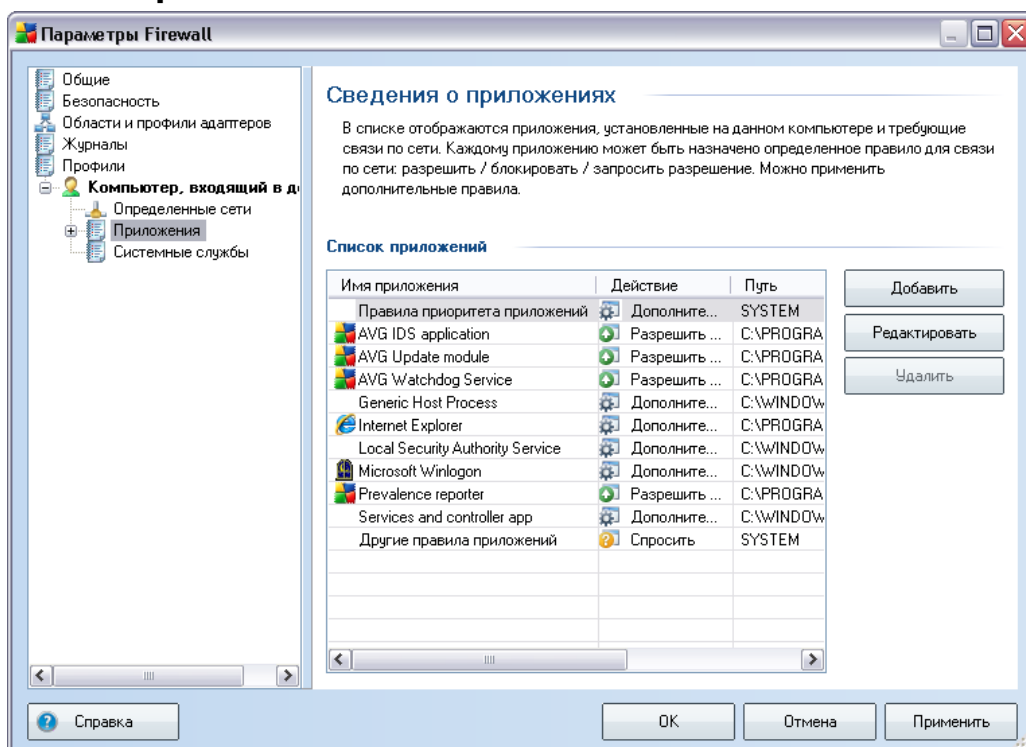
Данное диалоговое окно позволяет определить **Имя сети**, указать **Описание сети**, а также определить для сети состояние "Безопасно". Новая сеть может быть определена вручную с помощью отдельного диалогового окна, открываемого с помощью кнопки **Добавить IP-адрес** (также **Изменить IP-адрес/Удалить IP-адрес**). С помощью данного диалогового окна можно определить сеть, указав диапазон IP-адресов сети или маску.

Для большинства сетей, которые необходимо определить как части вновь созданной сети, можно использовать параметр **Расширенное представление диапазона IP-адресов**. Введите список всех сетей в соответствующее текстовое поле (*поддерживаются все стандартные форматы*) и нажмите кнопку **Проверить**, чтобы убедиться, что формат

может быть распознан. Затем нажмите кнопку **ОК**, чтобы подтвердить и сохранить введенные сведения.

- **Редактировать службу.** Открытие диалогового окна **Свойства сети** (см. выше), с помощью которого можно редактировать параметры уже определенной сети (данное диалоговое окно соответствует диалоговому окну добавления новой сети, см. описание в предыдущем абзаце).
- **Удалить сеть** — удаление сведений о выбранной сети из списка сетей.
- **Отметить как безопасный.** По умолчанию все сети считаются небезопасными, и только если вы уверены, что соответствующая сеть является безопасной, можно отметить ее таким образом с помощью данной кнопки (если сеть помечена в качестве безопасной, название кнопки изменится на "Отметить как небезопасный").
- **Справка** — открытие диалогового окна с файлом справки

11.5.3. Приложения



Диалоговое окно **Сведения о приложениях** содержит список всех

установленных приложений, которым может потребоваться обмен данными по сети и значки назначенных действий.

-  Разрешить обмен данными для всех сетей
-  Разрешить обмен данными только для сетей со статусом "Безопасно"
-  Запретить обмен данными
-  Отобразить диалоговое окно "Спрашивать" (можно разрешить или заблокировать попытку соединения).
-  Определены дополнительные параметры

Приложения, указанные в списке, были обнаружены на компьютере (и назначены соответствующие действия) в процессе поиска [мастером конфигурации Firewall](#) или, в случае неизвестного или недавно установленного приложения, позднее.

Примечание. Обратите внимание, что можно обнаружить только уже установленные приложения. Таким образом, при установке нового приложения необходимо определить для него правила Firewall. По умолчанию при первой попытке подключения по сети со стороны нового приложения компонент Firewall автоматически создаст правило для этого приложения в соответствии с надежной базой данных или обратится с запросом на разрешение или запрет соединения. В последнем случае можно будет сохранять ответ в качестве постоянного правила, которое впоследствии будет внесено в список в этом диалоговом окне.

Также можно сразу определить правила для нового приложения. Для этого необходимо в данном диалоговом окне нажать кнопку **Добавить** и заполнить сведения о приложении.

Кроме приложений, в списке также содержатся два особых элемента.

- **Правила приоритета приложений** (вверху списка) являются предпочтительными и всегда применяются перед правилами других приложений.
- **Другие правила приложений** (внизу списка) используются в последнюю очередь, если не назначено особых правил приложений, например для неизвестного или неопределенного приложения.

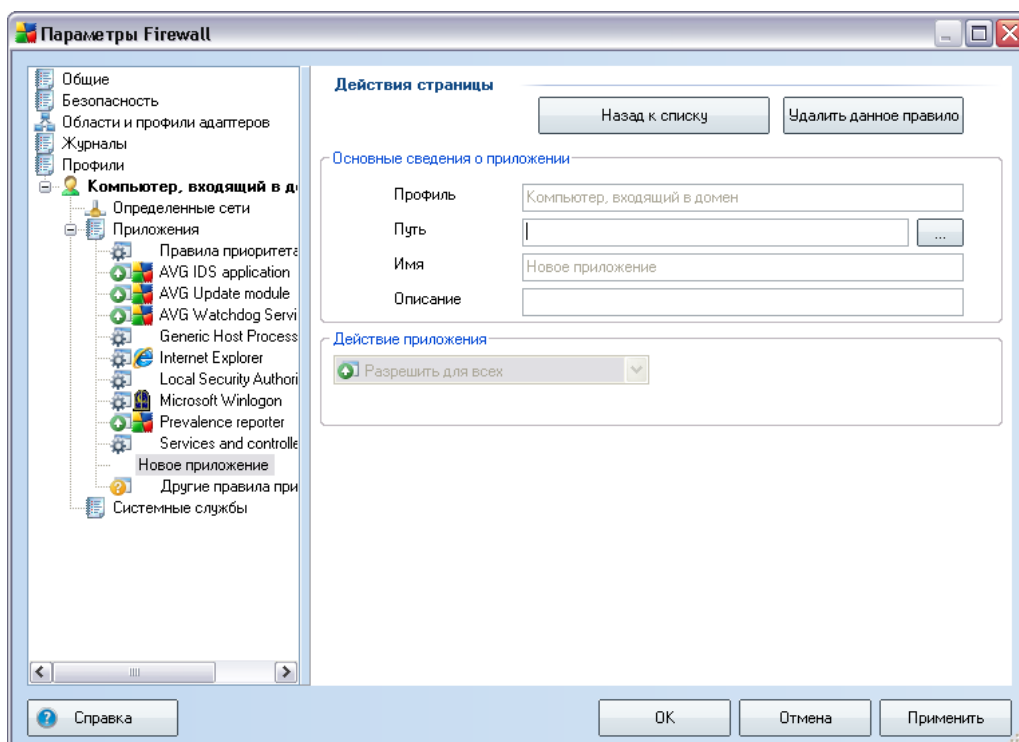
Настройки данных элементов отличаются от настроек обычных

**приложений и предназначены только для опытных пользователей.
Настоятельно рекомендуется не изменять параметры**

Кнопки управления

Данный список можно редактировать с помощью следующих кнопок управления.

- **Добавить** — открытие пустого диалогового окна [Действия страницы](#), в котором можно определить правила для нового приложения.
- **Редактировать** — открытие диалогового окна [Действия страницы](#), содержащего данные для редактирования набора правил существующего приложения.
- **Удалить** — удаление выбранного приложения из списка
- **Справка** — открытие диалогового окна с файлом справки



Данное диалоговое окно позволяет подробно определить параметры

соответствующего приложения.

Действия страницы

- **Вернуться к списку.** Кнопка обеспечивает отображение сводки всех настроенных правил приложений.
- **Удалить это правило.** Кнопка обеспечивает удаление текущего правила приложения. Обратите внимание, что это действие необратимо.

Основные сведения о приложении

В данном разделе заполните поле **Имя** приложения и при необходимости поле **Описание** (краткий комментарий к сведениям). В поле **Путь** укажите полный путь к приложению (исполняемый файл) на диске. Также для указания пути к приложению можно воспользоваться более удобной древовидной структурой, нажав кнопку "...".

Действие приложения

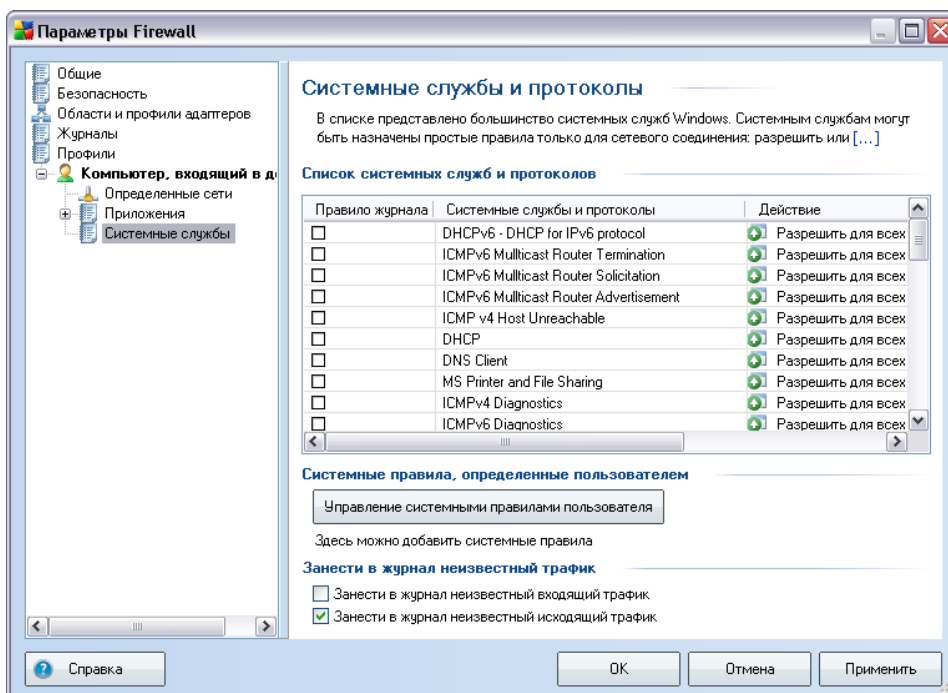
В раскрывающемся меню можно выбрать правило Firewall для приложения, например определить действия компонента Firewall при попытке приложения установить сетевое соединение.

-  **Разрешить для всех.** Позволяет приложению устанавливать соединение со всеми назначенными сетями и адаптерами без ограничений.
-  **Разрешить для безопасных.** Позволяет приложению устанавливать соединение только с безопасными (надежными) сетями.
-  **Блокировать.** Автоматический запрет на обмен данными. Приложению будет запрещено подключаться к любой сети.
-  **Спрашивать.** Отображение диалогового окна, в котором можно разрешить или заблокировать попытку соединения.
-  **Дополнительные параметры.** Отображение дополнительных параметров в нижней части диалогового окна в разделе **Подробные правила приложения**. Сведения будут применены в соответствии с

порядком в списке. Таким образом, правила в списке можно перемещать **вверх** или **вниз**, чтобы установить последовательность выполнения. После выбора в списке определенного правила в нижней части диалогового окна будут отображаться краткие сведения об этом правиле. Любое подчеркнутое значение синего цвета может быть изменено после выбора в соответствующем диалоговом окне параметров. Чтобы удалить выделенное правило, нажмите **Удалить**. Чтобы определить новое правило, нажмите кнопку **Добавить** для открытия диалогового окна **Изменить сведения о правиле**, которое позволяет указывать все необходимые сведения.

11.5.4. Системные службы

Редактирование параметров в диалоговом окне "Системные службы и протоколы" должно выполняться только опытными пользователями.



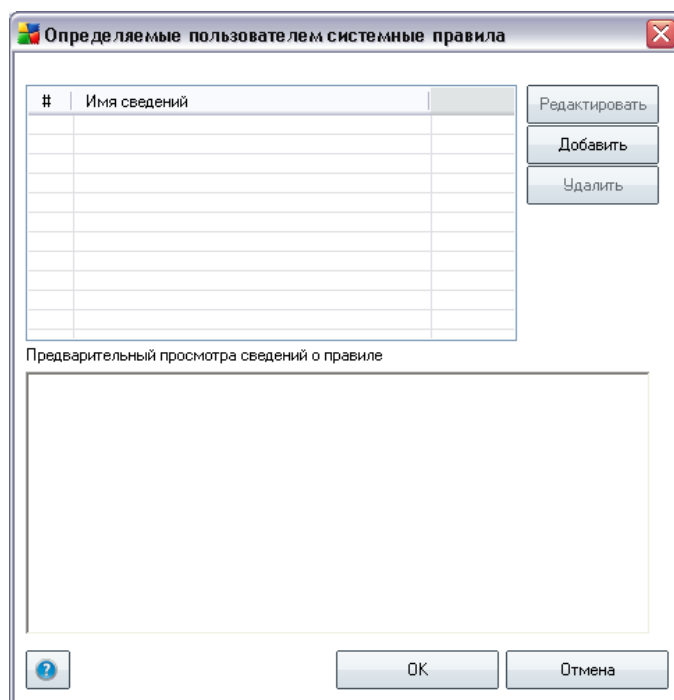
В диалоговом окне **Системные службы и протоколы** перечислены стандартные системные службы Windows и протоколы, необходимые для передачи данных по сети. Таблица содержит следующие столбцы.

- **Записать в журнал применения правила.** Позволяет включить сохранение каждого применения правила в журналах.

- **Системная служба и протоколы.** В этом столбце указано имя соответствующей системной службы.
- **Действие.** В этом столбце отображается значок для назначенного действия.
 -  Разрешить обмен данными для всех сетей
 -  Разрешить обмен данными только для сетей со статусом "Безопасно"
 -  Запретить обмен данными
- **Сети.** В этом столбце указывается сеть, для которой применяется системное правило.

Данный список (в том числе назначенные действия) можно редактировать с помощью следующих кнопок.

- Для редактирования параметров элементов в списке (включая назначенные действия) щелкните правой кнопкой мыши элемент и выберите **Редактировать**.
- Чтобы открыть новое диалоговое окно для определения правила системной службы (см. рисунок ниже), нажмите кнопку **Управление системными правилами пользователя**. В верхней части диалогового окна **Определяемые пользователем системные правила** представлен обзор всех сведений текущего измененного системного правила, в нижней части представлены выбранные сведения. Сведения о правиле, определенном пользователем, можно изменять, добавлять или удалять соответствующей кнопкой; сведения о правиле, определенном производителем, можно только изменять.



Предупреждение. Обратите внимание, что эти параметры подробного правила являются дополнительными и предназначены для сетевых администраторов, которым необходим полный контроль над конфигурацией компонента Firewall. Если вам неизвестны типы протоколов обмена данными, номера сетевых портов, определения IP-адресов и т. д., не изменяйте эти параметры! Если требуется изменить конфигурацию, ознакомьтесь с файлами справки соответствующих диалоговых окон.

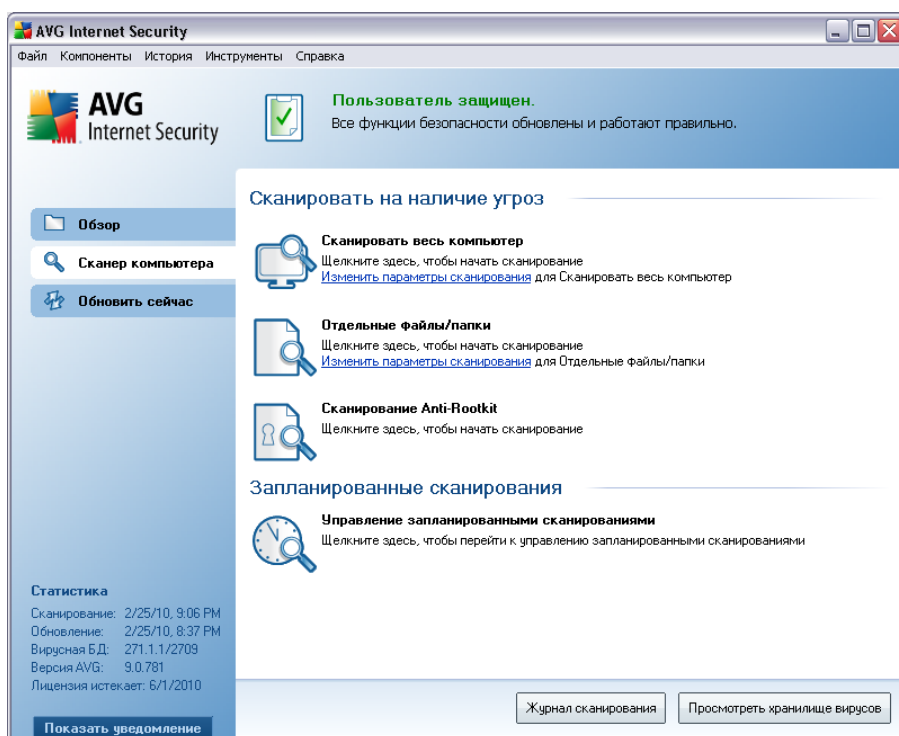
Занести в журнал неизвестный трафик

- **Вести журнал неизвестного входящего трафика** – установите этот флажок для регистрации в Журналах каждой неизвестной попытки подключиться к компьютеру извне.
- **Вести журнал неизвестного исходящего трафика** – установите этот флажок для регистрации в Журналах каждой неизвестной попытки компьютера подключиться к объекту во внешней сети.

12. Сканирование AVG

Сканирование — это одна из важнейших функций **AVG 9 Anti-Virus + Firewall**. Можно выполнять проверки по требованию или [планировать их периодический запуск](#) в удобное для вас время.

12.1. Интерфейс сканирования



Для перехода к интерфейсу сканирования AVG необходимо выбрать [быструю ссылку](#) **Сканер компьютера**. Щелкните эту ссылку, чтобы открыть диалоговое окно **Сканирование на наличие угроз**. Данное диалоговое окно содержит следующие разделы:

- обзор [предопределенных сканирований](#) — три типа сканирований, определенных поставщиком ПО, готовые к использованию по расписанию или при необходимости:
 - [Сканирование всего компьютера](#)
 - [Сканировать отдельные файлы или папки](#)

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

12.2. Предопределенные сканирования

Одна из главных функций **AVG 9 Anti-Virus + Firewall** — 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 9 Anti-Virus + Firewall** доступно два вида сканирования, настроенных поставщиком программного обеспечения:

12.2.1. Сканирование всего компьютера

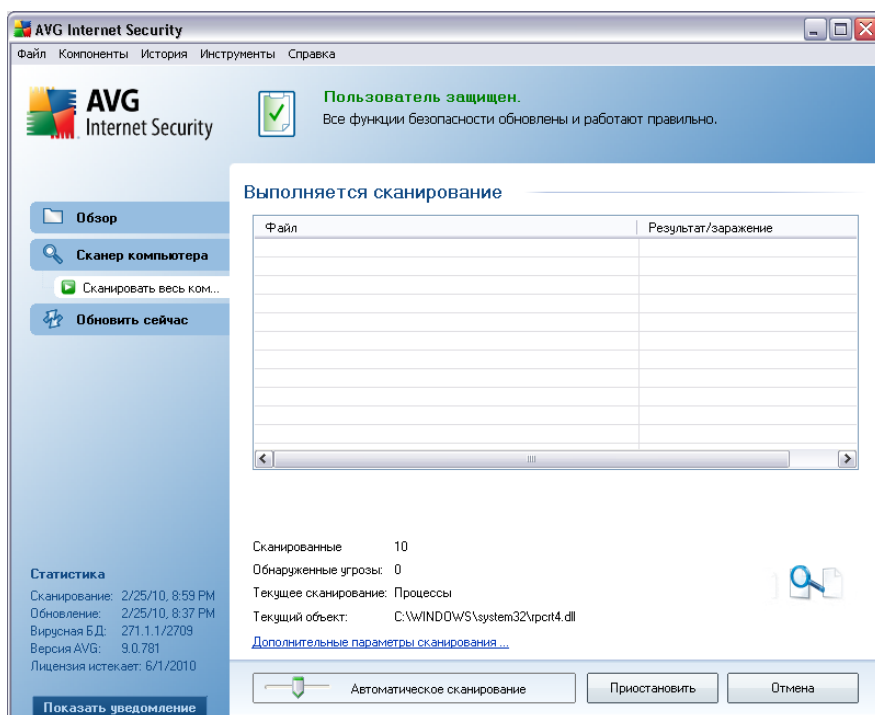
Сканировать весь компьютер — сканирование всего компьютера на наличие заражений и/или потенциально нежелательных программ. При данном типе проверки выполняется сканирование всех жестких дисков компьютера, производится обнаружение и лечение зараженных объектов или перемещение в [хранилище вирусов](#). 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

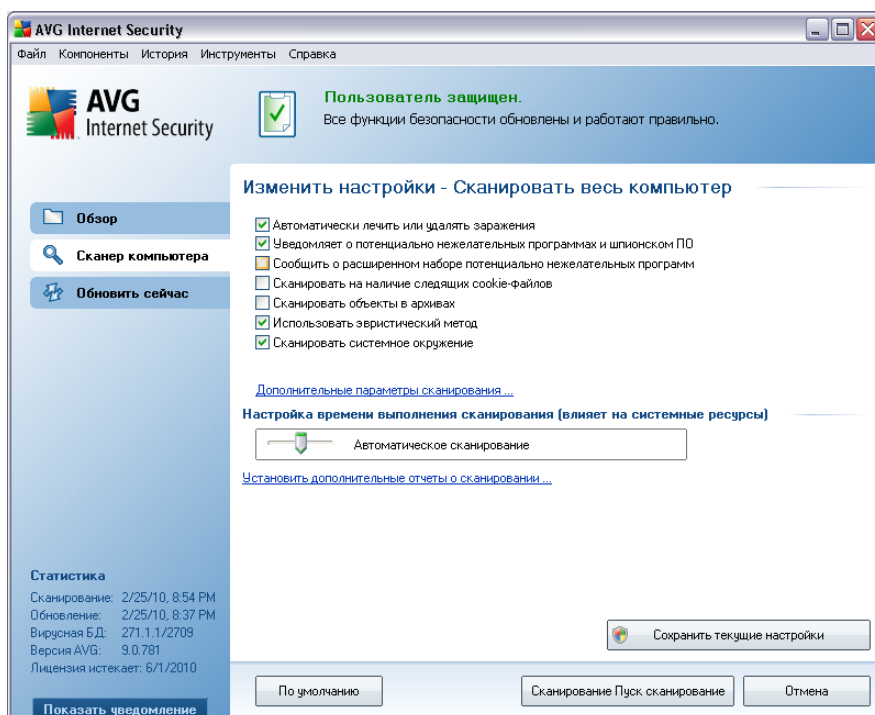


прервать (**Пауза**) или отменить (**Отмена**).

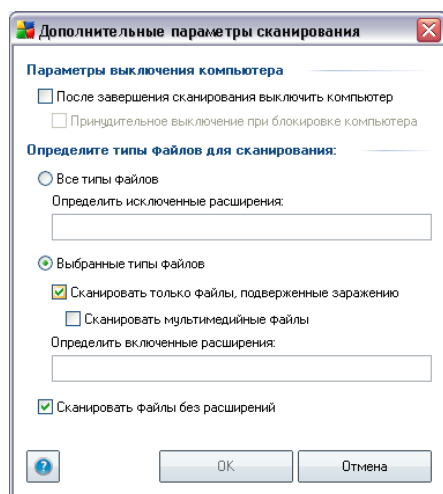


Изменение параметров сканирования

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



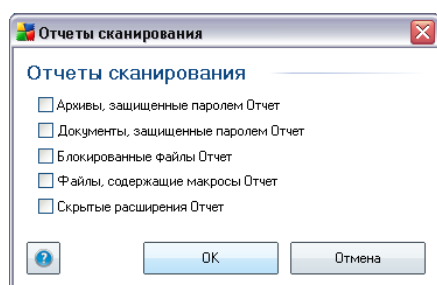
- **Параметры сканирования** — в списке параметров сканирования можно включить или выключить определенные параметры при необходимости. По умолчанию большинство параметров включены и используются автоматически при сканировании.
- **Дополнительные параметры сканирования** — эта ссылка открывает новое диалоговое окно **Дополнительные параметры сканирования**, где можно указывать следующие параметры.



- o **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**).
- o **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 выбрать параметр **Сканировать файлы**

без расширений — этот параметр установлен по умолчанию. Рекомендуется не изменять его до появления веской причины. Файлы без расширения являются подозрительными, поэтому необходимо проводить их сканирование каждый раз.

- **Приоритет процесса сканирования** — для изменения приоритета процесса сканирования используйте ползунок. По умолчанию установлен средний уровень приоритета (*Автоматическое сканирование*), который обеспечивает оптимальную скорость процессора и использование системных 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 главе [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 использовались каждый раз при сканировании всего компьютера.

12.2.2. Сканирование определенных 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



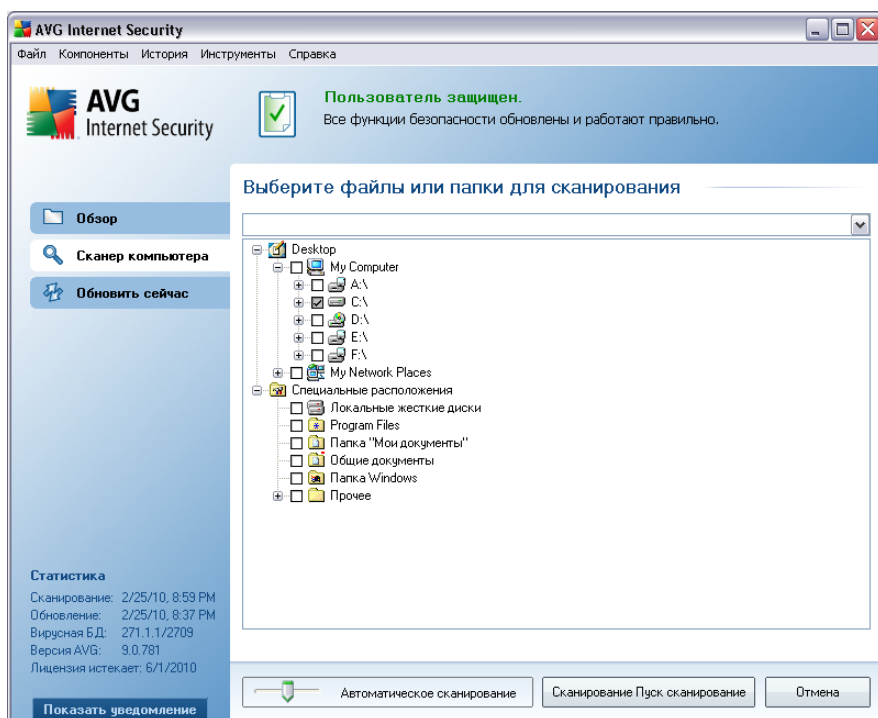
компьютера: найденные вирусы подвергаются лечению или удаляются в [хранилище вирусов](#). Сканирование отдельных файлов и папок можно использовать при создании пользовательских проверок и их расписаний.

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.

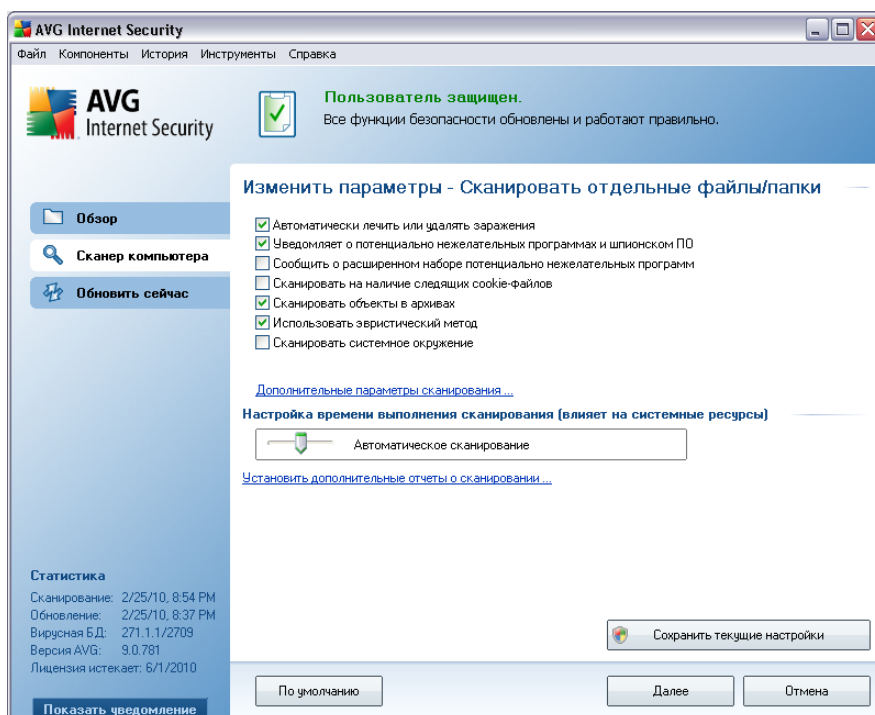
Существует также возможность сканирования определенных папок без сканирования соответствующих подпапок; чтобы выполнить такое сканирование, введите значок минус "-" перед автоматически созданным путем (см. *снимок экрана*). Чтобы исключить всю папку из процесса сканирования, используйте параметр "!".

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

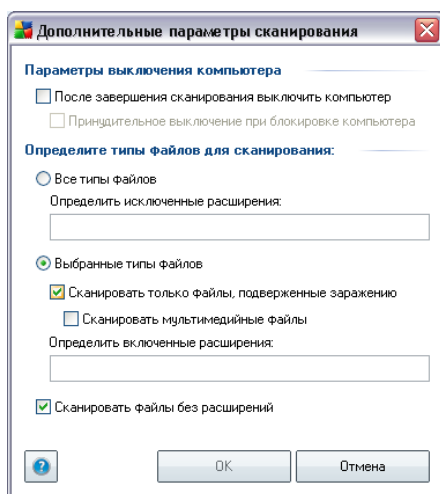


Изменение параметров сканирования

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!**



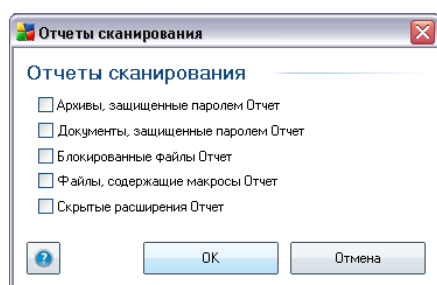
- **Параметры сканирования** — в списке параметров сканирования можно включить или отключить определенные параметры при необходимости (*подробное описание данных параметров см. в разделе [Расширенные настройки AVG/Сканирования/Сканирование отдельных файлов и папок](#)*).
- **Дополнительные параметры сканирования** — эта ссылка открывает новое диалоговое окно "Дополнительные параметры сканирования", где можно указывать следующие параметры.



- o **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**).
- o **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 выбрать параметр **Сканировать файлы**

без расширений — этот параметр установлен по умолчанию. Рекомендуется не изменять его до появления веской причины. Файлы без расширения являются подозрительными, поэтому необходимо проводить их сканирование каждый раз.

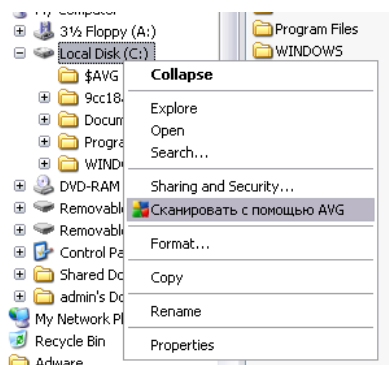
- **Приоритет процесса сканирования** — для изменения приоритета процесса сканирования используйте ползунок. По умолчанию установлен средний уровень приоритета (*Автоматическое сканирование*), который обеспечивает оптимальную скорость процессора и использование системных ресурсов. Также можно запустить 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 главе [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](#)).

12.3. Сканирование в Проводнике Windows

Кроме predetermined сканирований всего компьютера или выбранных областей, программа **AVG 9 Anti-Virus + Firewall** 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

12.4. Сканирование с помощью командной строки

В **AVG 9 Anti-Virus + Firewall** 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 запятыми, 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.

12.4.1. Параметры сканирования с помощью командной строки

Посмотрите список всех параметров для сканирования 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

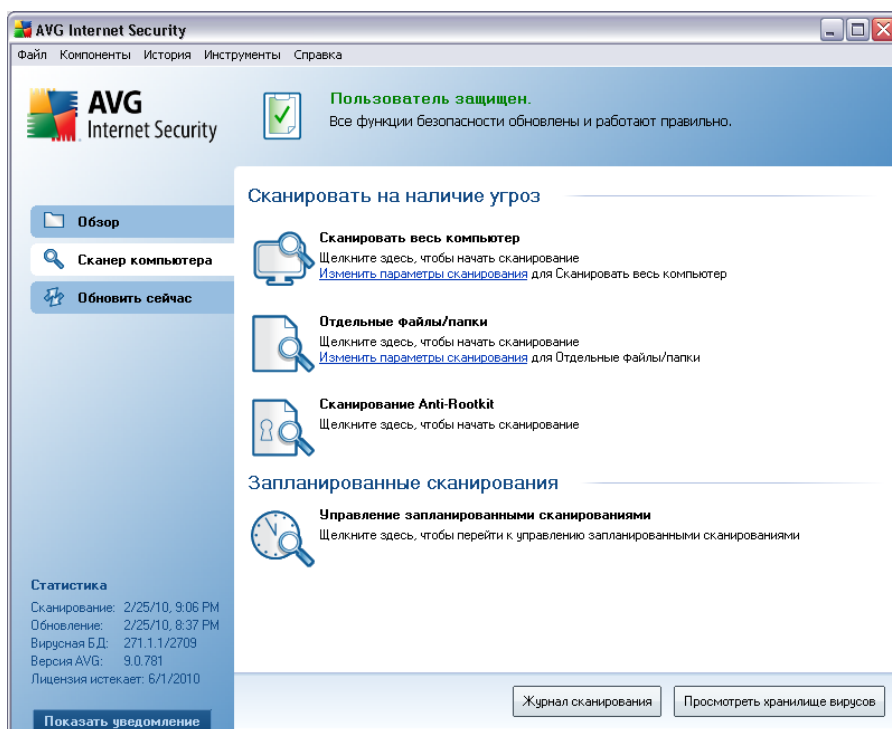
- **/PUP** Сообщать о "[потенциально нежелательных программах](#)"
- **/REG** Сканировать реестр
- **/COO** Сканировать файлы cookie
- **/?** Показать справку по этой теме
- **/HELP** Показать справку по этой теме
- **/PRIORITY** Установить приоритет сканирования /Низкий, Автоматически, Высокий/ (см. [Дополнительные параметры/Сканирование](#))
- **/SHUTDOWN** Выключить компьютер по завершении сканирования
- **/FORCESHUTDOWN** Принудительное выключение компьютера по завершении сканирования
- **/ADS** Сканировать альтернативные потоки данных (только NTFS)

12.5. Расписание сканирования

С помощью **AVG 9 Anti-Virus + Firewall** 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 инфекций, и не придется волноваться о том, нужно ли и когда запускать сканирование.

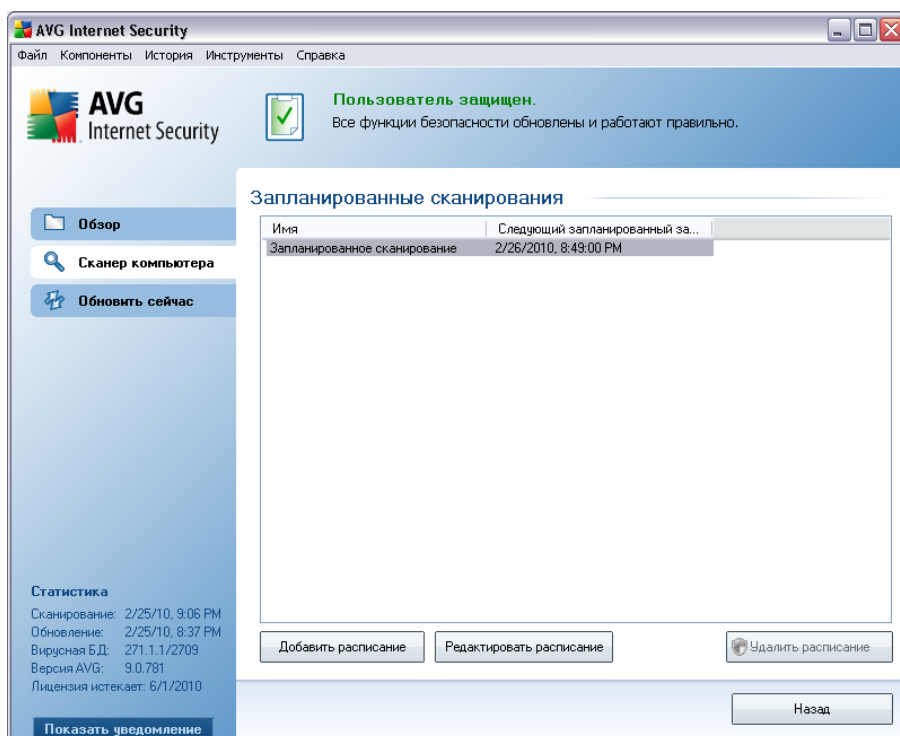
Сканирование всего компьютера необходимо запускать как минимум раз в неделю. Все же, если это возможно, рекомендуется запускать сканирование всего компьютера ежедневно — как настроено в конфигурации расписания сканирования по умолчанию. Если компьютер всегда включен, можно назначить сканирование на нерабочее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

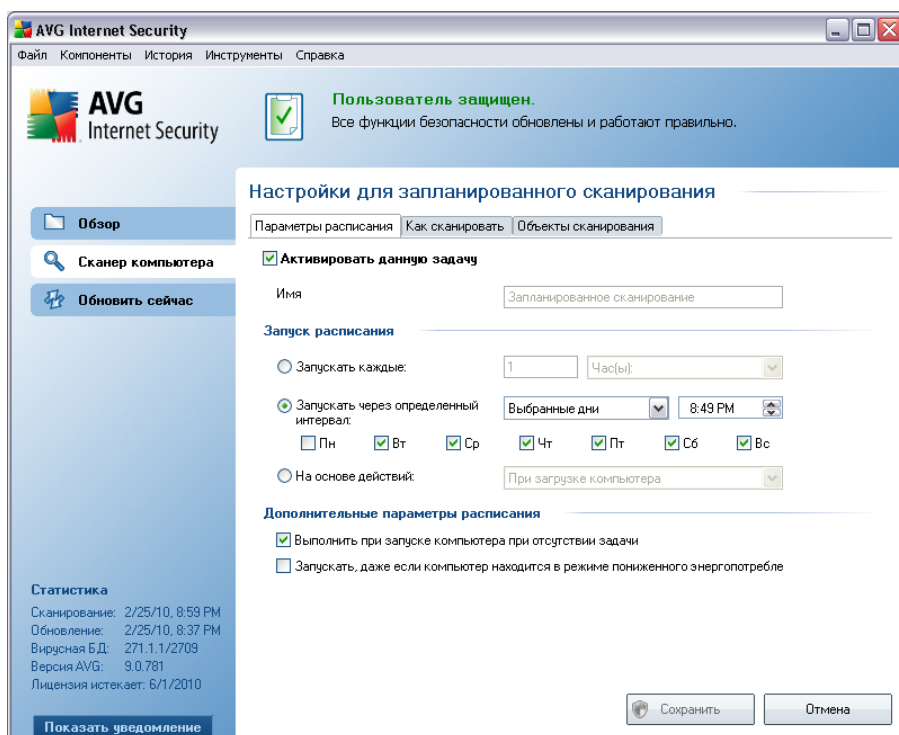
- **Добавить расписание сканирования** — открытие диалогового окна **Параметры запланированного сканирования**, вкладки **Параметры расписания**. В данном диалоговом окне можно указать параметры новой созданной проверки.
- **Редактировать расписание сканирования** — используется, только если текущая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

12.5.1. 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 содержит три вкладки. **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 **Название**. 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.

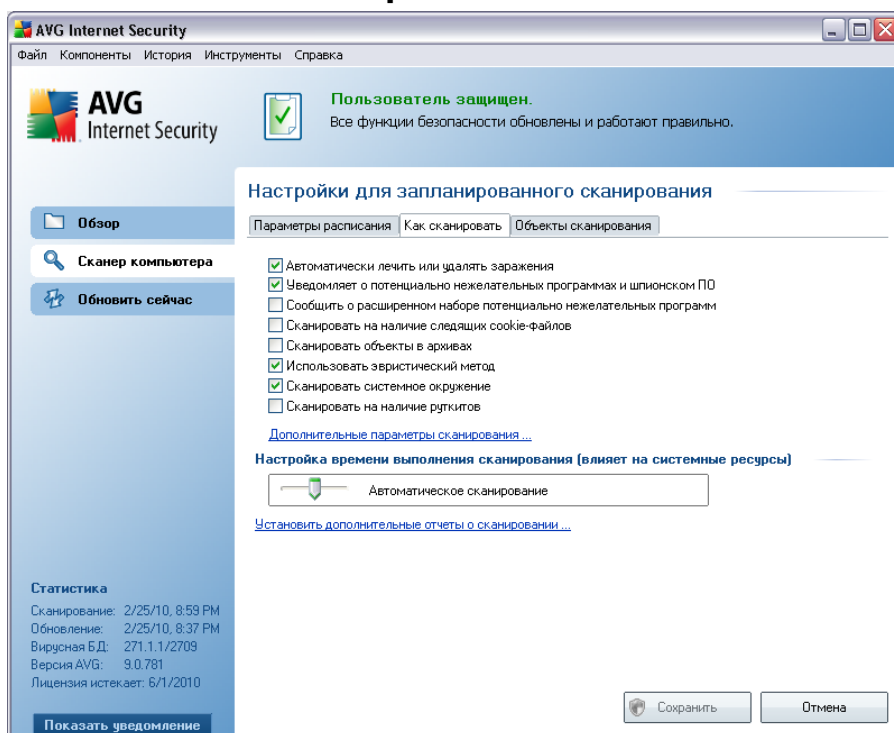
Кнопки управления параметрами диалогового окна запланированного сканирования

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](#).

12.5.2. Способы сканирования



На вкладке **Способ сканирования** можно найти 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.

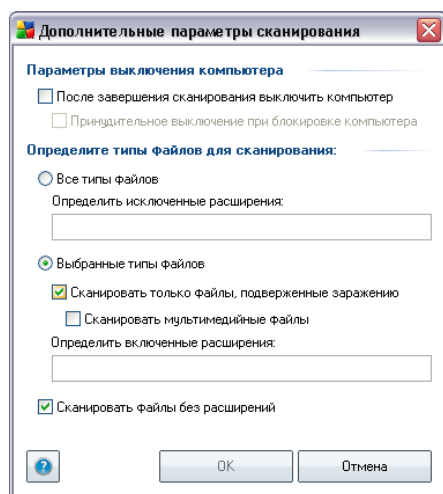
- **Автоматически лечить или удалять заражения** — (включено по умолчанию): обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если зараженный файл невозможно вылечить автоматически или данный параметр отключен, отобразится уведомление об обнаружении вируса с выбором действия по отношению к зараженному объекту. Рекомендуется переместить зараженный файл в [хранилище вирусов](#).
- **Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО** (флажок установлен 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.** Если предыдущий параметр активирован, можно также выбрать данный параметр для определения расширенного набора [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 cookie-файлов** — (включено по умолчанию): благодаря данному параметру компонента [Anti-Spyware](#) программа сканирует систему на наличие файлов cookie (*HTTP cookie-файлы используются для аутентификации, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержанием корзин для покупок через Интернет*);
- **Сканировать объекты в архивах** (включен 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** (включен 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** — (включен по умолчанию): при сканировании также будут проверены системные области компьютера.

Затем, чтобы изменить параметры сканирования, выполните следующие действия.

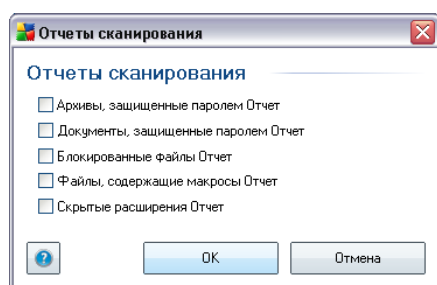
- **Дополнительные параметры сканирования** — эта ссылка открывает новое диалоговое окно **Дополнительные параметры сканирования**, где можно указывать следующие параметры.



- o **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**).
- o **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 выбрать параметр **Сканировать файлы**

без расширений — этот параметр установлен по умолчанию. Рекомендуется не изменять его до появления веской причины. Файлы без расширения являются подозрительными, поэтому необходимо проводить их сканирование каждый раз.

- **Приоритет процесса сканирования** — для изменения приоритета процесса сканирования используйте ползунок. По умолчанию установлен средний уровень приоритета (*Автоматическое сканирование*), который обеспечивает оптимальную скорость процессора и использование системных 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.

верхней части диалогового окна, а в выпадающем 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.

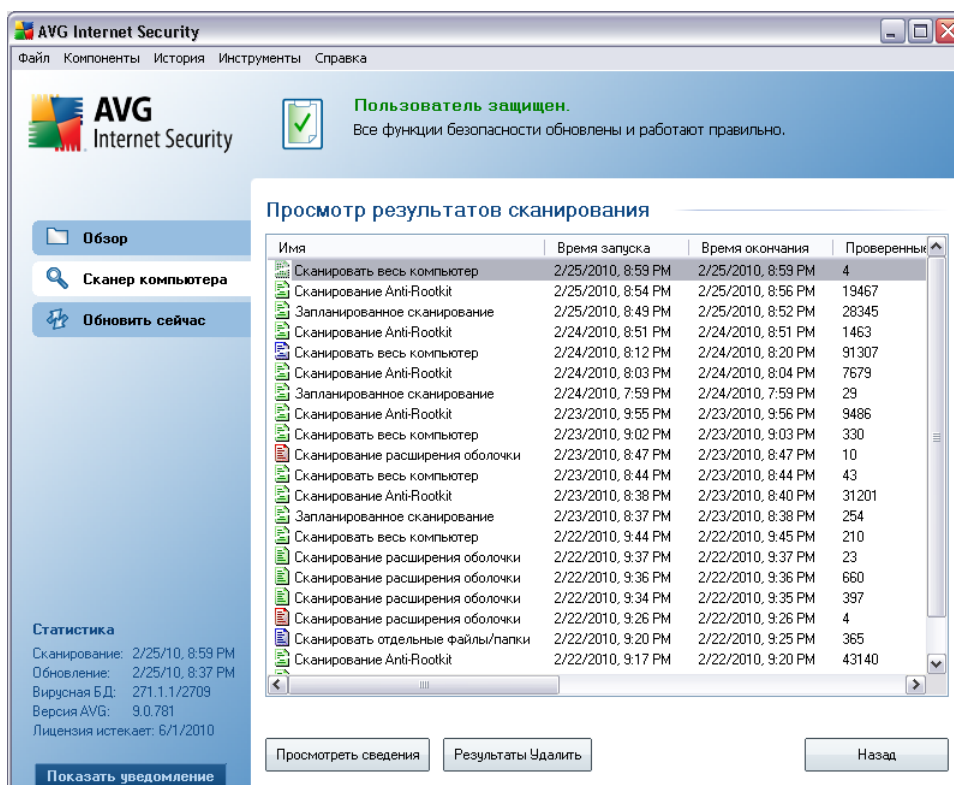
- **Локальные жесткие диски.** Все жесткие диски компьютера.
- **Программные файлы.** Папка C:\Program Files\.
- **Мои документы.** Папка C:\Documents and Settings\Пользователь\Мои документы\.
- **Общие документы.** Папка C:\Documents and Settings\All Users\Документы\.
- **Папка Windows** — C:\Windows\
- **Прочее**
 - **Системный диск.** Жесткий диск, на котором установлена операционная система (обычно диск C:).
 - **Системная папка.** Папка Windows/System32.
 - **Папка временных файлов.** Папка Documents and Settings/Пользователь/Local Settings/Temp.
 - **Временные файлы Интернета.** Папка Documents and Settings/Пользователь/Local Settings/Temporary Internet Files.

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](#).

12.6. 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](#)

12.7. Результаты сканирования Сведения

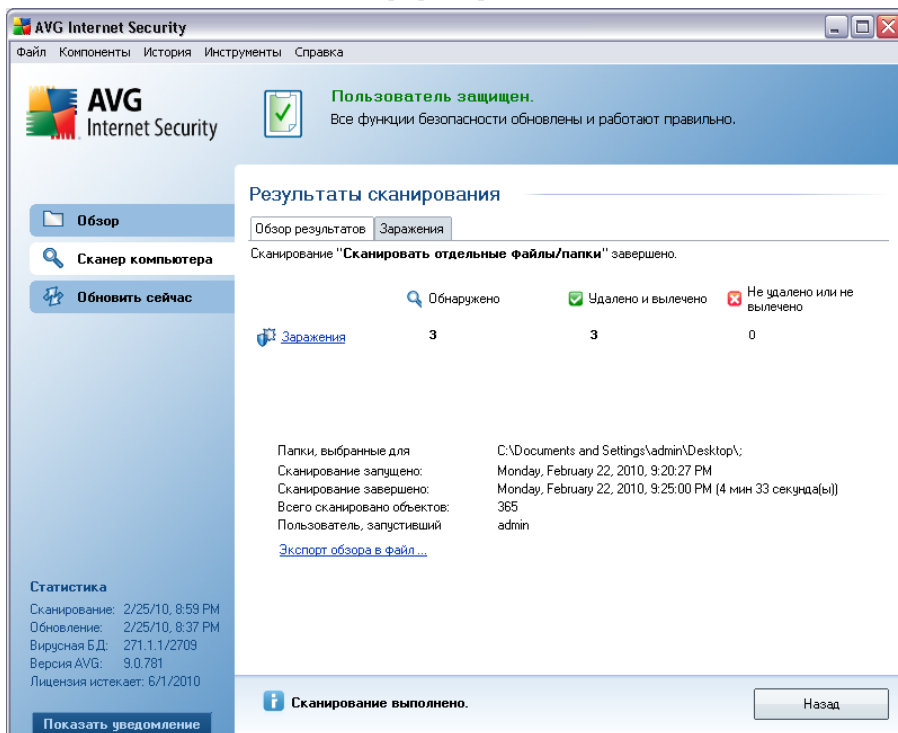
Если в диалоговом окне [Обзор результатов сканирования](#) выбрано определенное сканирование, можно нажать кнопку **Просмотреть сведения** для перехода к диалоговому окну **Результаты сканирования**. В данном окне приведены подробные сведения о процессе и результате выбранного сканирования.

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.
- **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).

12.7.1. Вкладка "Обзор результатов"



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

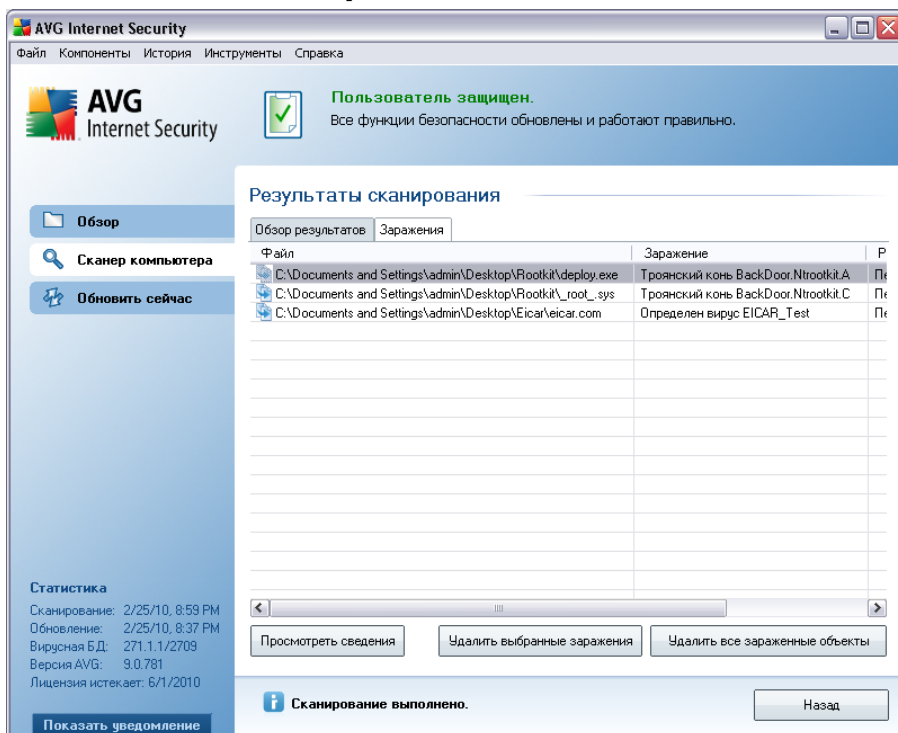
- обнаруженные [вирусы/шпионское ПО](#)
- Удаленные [заражения/шпионское ПО](#).
- количество [вирусов/объектов шпионского ПО](#), которые не могут быть удалены или вылечены

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 **Закреть результаты** выполняет переход обратно к диалоговому окну [Обзор результатов сканирования](#).

12.7.2. 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

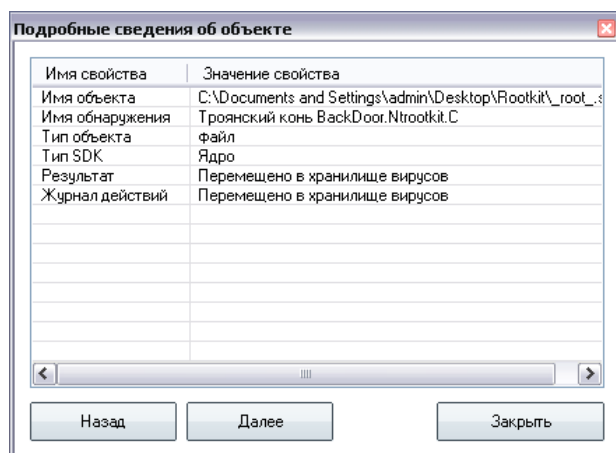
параметрах сканирования_отключен параметр автоматического лечения).

- o **Вылечен.** Зараженный объект вылечен автоматически, его начальное местоположение сохранено.
- o **Перемещен в хранилище вирусов** — зараженный объект помещен на карантин в [хранилище вирусов](#).
- o **Удален.** Зараженный объект удален.
- o **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).
- o **Заблокированный файл — не проверен** — объект заблокирован, поэтому AVG не может выполнить его сканирование.
- o **Потенциально опасный объект** — объект является потенциально опасным, но не заражен (например, содержит макросы); данная информация имеет лишь предупредительный характер.
- o **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 с указанным именем **Подробная информация о результатах сканирования:**



В данном диалоговом окне приведена информация о местоположении обнаруженного зараженного объекта (**Имя свойства**). С помощью кнопок **Предыдущий/Следующий** можно просматривать сведения об определенных обнаруженных объектах. Чтобы закрыть диалоговое окно, нажмите кнопку **Заккрыть**.

- **Удалить выбранные зараженные объекты** — 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** — закрытие окна просмотра сведений и возврат к окну [Просмотр результатов сканирования](#).

12.7.3. 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.

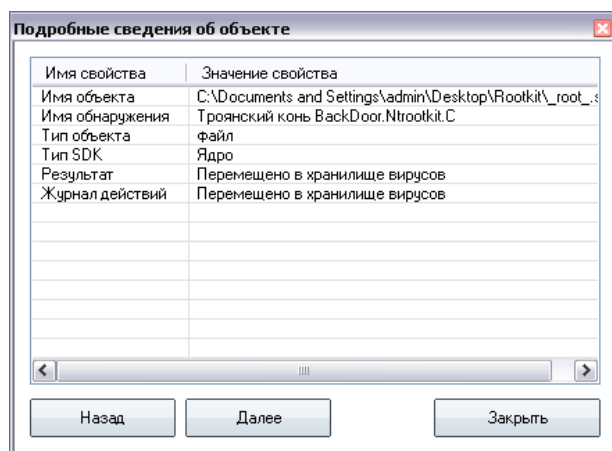
- **Файл**. Полный путь к исходному местоположению зараженного объекта.
- **Зараженный объект**. Имя обнаруженного [шпионского ПО](#) (подробные сведения об определенных вирусах см. в интерактивной [энциклопедии вирусов](#)).

- **Результат** — определяет текущее состояние объекта, обнаруженного при сканировании.
 - **Заражен** — зараженный объект обнаружен, его начальное местоположение сохранено (например, если в особых настройках сканирования [отключен параметр автоматического лечения](#))
 - **Вылечен**. Зараженный объект вылечен автоматически, его начальное местоположение сохранено.
 - **Перемещен в хранилище вирусов**. Зараженный объект помещен на карантин в [хранилище вирусов](#).
 - **Удален**. Зараженный объект удален.
 - **Добавлен в список исключений PUP** — обнаруженный объект получил статус исключения и добавлен в список исключений PUP (настроенный в диалоговом окне дополнительных параметров Исключения PUP).
 - **Заблокированный файл — не проверен** — объект заблокирован, поэтому AVG не может выполнить его сканирование.
 - **Потенциально опасный объект** — объект является потенциально опасным, но не заражен (например, содержит макросы); данная информация имеет лишь предупредительный характер.
 - **Для завершения процесса требуется перезагрузка** — невозможно удалить зараженный объект; необходимо перезагрузить компьютер, чтобы полностью удалить объект.

Кнопки управления

В данном диалоговом окне доступны три кнопки управления.

- **Просмотреть сведения** — в результате нажатия данной кнопки открывается новое диалоговое окно с указанным именем **Подробная информация о результатах сканирования**:

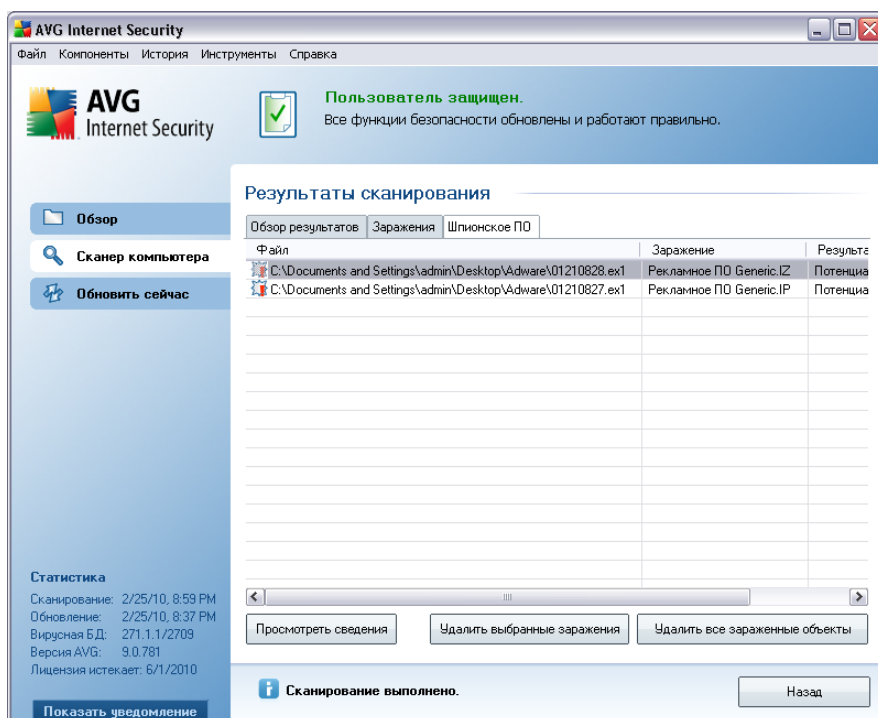


В данном диалоговом окне приведена информация о местоположении обнаруженного зараженного объекта (**Имя свойства**). С помощью кнопок **Предыдущий/Следующий** можно просматривать сведения об определенных обнаруженных объектах. Чтобы закрыть диалоговое окно, нажмите кнопку **Заккрыть**.

- **Удалить выбранные зараженные объекты** — 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** — закрытие окна просмотра сведений и возврат к окну [Просмотр результатов сканирования](#).

12.7.4. 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.

12.7.5. Вкладка "Средства rootkit"

На вкладке **Rootkits** отображаются сведения о средствах rootkit, обнаруженных во время сканирования, если было запущено **сканирование Anti-Rootkit** или в окне [Сканирование всего компьютера](#) вручную был добавлен параметр сканирования Anti-Rootkit (по умолчанию этот параметр отключен).

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 скрывание запущенных процессов от следящих программ, а файлов и системных данных — от операционных систем.

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

12.7.6. 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).

12.8. 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 предлагает обзор сведений о зараженных объектах, помещенных в карантин.

- **Серьезность** — 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** — данная кнопка позволяет переместить обнаруженный зараженный объект из **хранилища вирусов** в выбранную папку. При этом обнаруженные и подозрительные объекты сохраняются под своими исходными именами. Если исходное имя неизвестно, будет использоваться стандартное имя.
- **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).

13. Обновления AVG

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

Во время [установки AVG](#) необходимо было указать частоту обновления продуктов AVG. Доступные варианты: **Каждые 4 часа** или **Каждый день** (см. диалоговое окно [Планирование регулярных сканирований и обновлений](#)). 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 9 Anti-Virus + Firewall** будет находиться в обновленном состоянии в течение всего дня.

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

13.2. 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 чего запланированное обновление будет периодически выполняться в соответствии с установленными параметрами. При появлении новых файлов обновлений в указанном местоположении они будут загружены напрямую из Интернета или из

сетевого каталога. Если обновления недоступны, ничего не будет происходить.

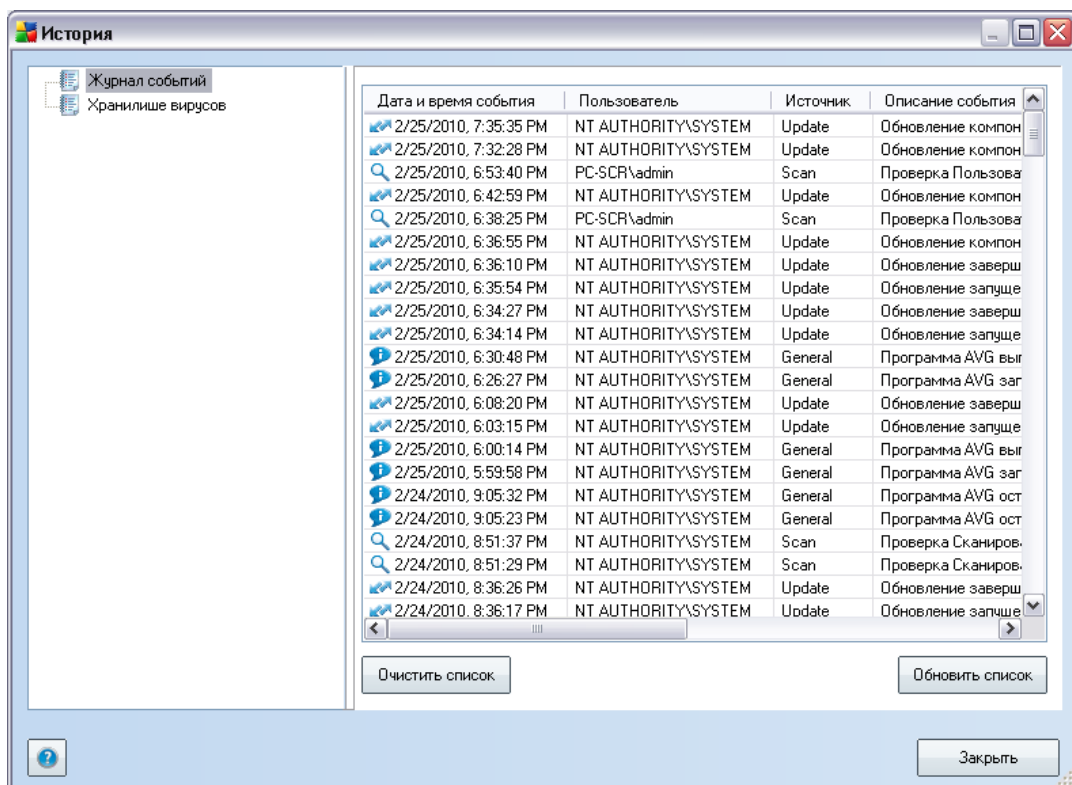
13.3. Процесс обновления

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.

14. Журнал событий



Диалоговое окно **История событий** доступно в [системном меню](#) при выборе элементов **История/Журнал истории событий**. В этом окне можно посмотреть перечень важных событий, произошедших во время работы **AVG 9 Anti-Virus + Firewall**. В журнале **История событий** 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

Кнопки управления



- **Очистить список** — удаляет все записи из списка событий
- **Обновить список** — обновляет все записи в списке событий



15. 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**.