AVG Internet Security 2013

Руководство пользователя

Версия документа 2013.01 (30.8.2012)

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

Этот продукт использует RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc., созданный в 1991.
В этом продукте используется код из библиотеки C-SaCzech, (c) Яромир Долечек (Jaromir Dolecek) (dolecek@ics.muni.cz), 1996-2001.
В этом продукте используется библиотека сжатия zlib, © Жан-Луп Гайлли (Jean-loup Gailly) и Марк Адлер (Mark Adler), 1995-2002.
В этом продукте использована библиотека компрессии libbzip2, © Джулиан Севард (Julian R. Seward), 1996-2002.

Содержимое

1. Введение 5

2. Требования для установки AVG 6

2.1 Поддерживаемые операционные системы 6
2.2 Минимальные требования и рекомендуемое оборудование 6

3. Процесс установки AVG 7

3.1 Добро пожаловать! Выбор языка 7
3.2 Добро пожаловать! Лицензионное соглашение 8
3.3 Активация лицензии 9
3.4 Выбор типа установки 10
3.5 Пользовательские параметры 12
3.6 Состояние процесса установки 13
3.7 Установка выполнена успешно 14

4. После установки 15

4.1 Регистрация продукта 15
4.2 Доступ к интерфейсу пользователя 15
4.3 Сканирование всего компьютера 15
4.4 Тестирование Eicar 15
4.5 Конфигурация AVG по умолчанию 16

5. Интерфейс пользователя AVG 17

5.1 Верхняя строка навигации 18
5.2 Информация о состоянии безопасности 23
5.3 Обзор компонентов 24
5.4 Мои приложения 25
5.5 Сканировать / Обновить быстрые ссылки 26
5.6 Значок на панели задач 26
5.7 Гаджет AVG 28
5.8 Советник AVG 29
5.9 AVG Accelerator 30

6. Компоненты AVG 31

6.1 Компьютер 31
6.2 Просмотр веб-узлов 33
6.3 Учетные данные 35
6.4 Сообщения электронной почты 37

6.5 Firewall 39
6.6 PC Analyzer 42

7. Панель безопасности AVG 44

8. AVG Do Not Track 46

8.1 Интерфейс AVG Do Not Track 46
8.2 Информация о следящих процессах 47
8.3 Блокировка следящих процессов 48
8.4 Настройки AVG Do Not Track 49

9. Расширенные настройки AVG 51

9.1 Внешний вид 51
9.2 Звуки 54
9.3 Временно отключить защиту AVG 55
9.4 Защита компьютера 56
9.5 Сканер электронной почты 61
9.6 Защита просмотра веб-узлов 75
9.7 Identity Protection 79
9.8 Сканирования 80
9.9 Расписания 85
9.10 Обновление 95
9.11 Исключения 100
9.12 Хранилище вирусов 101
9.13 Самозащита AVG 102
9.14 Настройки конфиденциальности 102
9.15 Игнорировать состояние ошибки 105
9.16 Советник — известные сети 106

10. Параметры Firewall 108

10.1 Общие сведения 108
10.2 Приложения 110
10.3 Общий доступ к файлам и принтерам 111
10.4 Дополнительные параметры 113
10.5 Определенные сети 114
10.6 Системные службы 115
10.7 Журналы 117

11. Сканирование AVG 119

11.1 Предопределенные сканирования 121

11.2 Сканирование в Проводнике Windows 129
11.3 Сканирование с помощью командной строки 129
11.4 Расписание сканирования 132
11.5 Результаты сканирования 140
11.6 Сведения о результатах сканирования 142

12. Хранилище вирусов 143

13. История 145

13.1 Результаты сканирования 145
13.2 Обнаружение Resident Shield 147
13.3 Обнаружение защиты электронной почты 149
13.4 Полученные данные Online Shield 150
13.5 Журнал событий 152
13.6 Журнал Firewall 153

14. Обновления AVG 155

14.1 Запуск обновления 155
14.2 Ход обновления 155
14.3 Уровни обновлений 156

15. Часто задаваемые вопросы и техническая поддержка 157

1. Введение

В руководстве пользователя содержится вся необходимая документация для **AVG Internet Security 2013**.

AVG Internet Security 2013 обеспечивает многоуровневую защиту в Интернете, поэтому вам не придется беспокоиться о кражах личных данных, вирусах и вредоносных сайтах. В программу также включены такие функции, как технология AVG Protective Cloud Technology и AVG Community Protection Network, благодаря которым мы можем собирать последние данные об угрозах, а затем делиться ими с нашим сообществом, в результате чего вы получаете лучшую защиту. Можно спокойно совершать покупки и банковские операции через Интернет, общаться с друзьями в социальных сетях, просматривать веб-страницы и пользоваться поиском, обладая надежной защитой в реальном времени.

2. Требования для установки AVG

2.1. Поддерживаемые операционные системы

AVG Internet Security 2013 обеспечивает защиту рабочих станций, на которых используются следующие операционные системы.

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

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

***Примечание**. Компонент Identity не поддерживается в 64-разрядной версии Windows XP. В этой операционной системе можно установить AVG Internet Security 2013, но только без компонента IDP.*

2.2. Минимальные требования и рекомендуемое оборудование

Минимальные требования к оборудованию для **AVG Internet Security 2013**.

- Процессор Intel Pentium с тактовой частотой 1,5 ГГц или выше
- 512 МБ (Windows XP) / 1024 МБ (Windows Vista, Windows 7) оперативной памяти
- 1,3 ГБ дискового пространства *(для установки)*

Рекомендуемые требования к оборудованию для **AVG Internet Security 2013**

- Процессор Intel Pentium с тактовой частотой 1,8 ГГц или выше
- 1024 МБ оперативной памяти
- 1,6 ГБ дискового пространства *(для установки)*

3. Процесс установки AVG

Как получить файл установки?

Для установки **AVG Internet Security 2013** на компьютер требуется файл установки последней версии. Для установки актуальной версии **AVG Internet Security 2013** рекомендуется загрузить файл установки с веб-сайта AVG (http://www.avg.com/). В разделе ***Поддержка / Загрузки*** можно ознакомиться с подробным обзором файлов установки для каждой версии AVG.

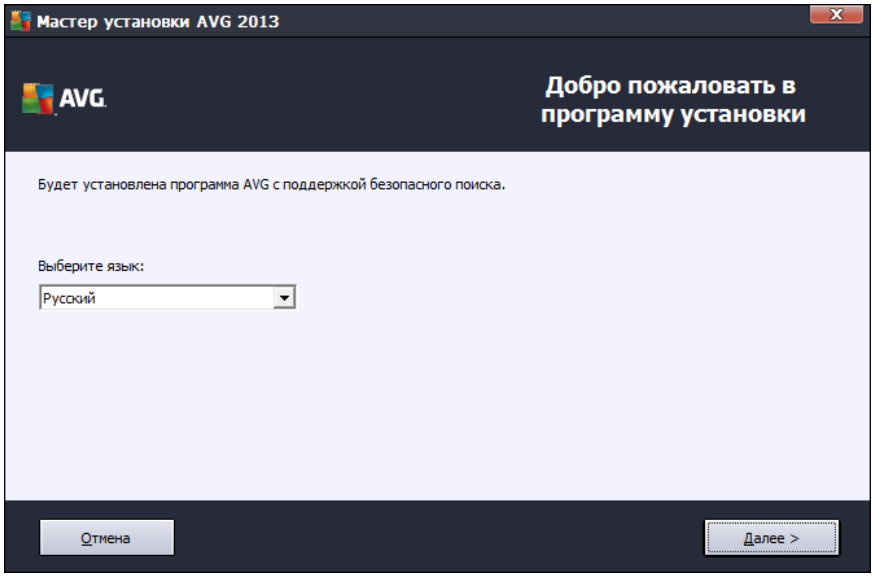
Если вы точно не знаете, какой именно файл необходимо загружать и устанавливать, воспользуйтесь службой ***Выбор продукта*** в нижней части веб-страницы. Получив ответы на три простых вопроса, служба сама подберет необходимые вам файлы. Нажмите кнопку ***Продолжить***, чтобы перейти к полному списку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

Как выглядит процесс установки?

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

3.1. Добро пожаловать! Выбор языка

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

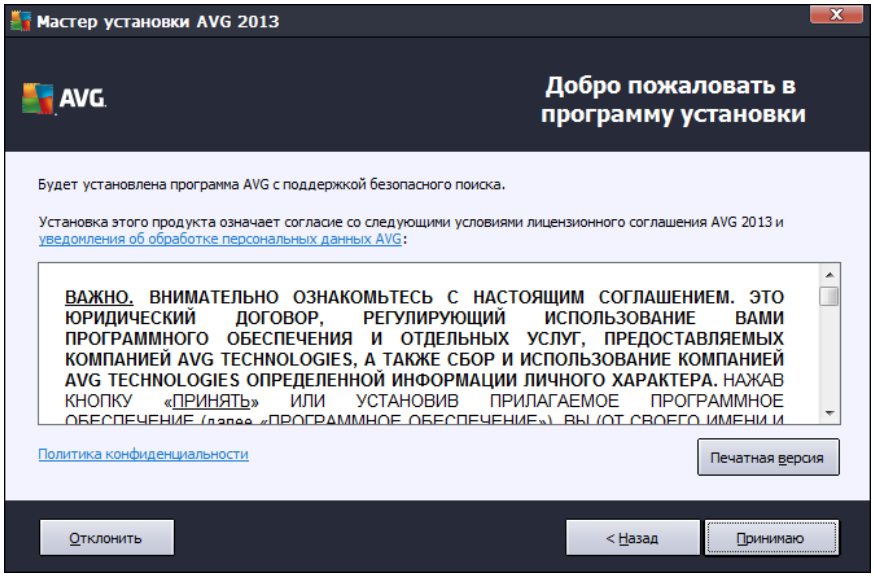


В этом диалоговом окне можно выбрать язык, который будет использоваться в процессе установки. Щелкните поле со списком, чтобы войти в меню выбора языка. Выберите необходимый язык, и процесс установки продолжится на выбранном языке.

Внимание! В данном окне выбирается только язык процесса установки. Приложение AVG Internet Security 2013 будет установлено на выбранном языке, а также на английском, который устанавливается автоматически. В дальнейшем для работы с AVG Internet Security 2013 можно будет установить любые другие языки. Дополнить список языков можно в диалоговом окне установки Пользовательские параметры.

3.2. Добро пожаловать! Лицензионное соглашение

В диалоговом окне ***Добро пожаловать в программу установки AVG*** представлен полный текст лицензионного соглашения AVG.



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

Политика конфиденциальности AVG

Кроме лицензионного соглашения, в окне установки можно подробнее ознакомиться с ***Заявлением компании AVG о защите персональных данных*** и ***Политикой конфиденциальности компании AVG*** *(вся упомянутая информация представлена в виде активных гиперссылок на веб-сайт, где приведен полный текст документов)*. Щелкните ссылку для перехода на веб-сайт компании AVG (http://www.avg.com/), где можно ознакомиться с полным текстом этих документов.

Кнопки управления

Как и в первом диалоговом окне установки, в дальнейшем будет всего две кнопки управления.

- ***Версия для печати*** — нажмите кнопку, чтобы показать в интерфейсе браузера

полную версию лицензионного соглашения AVG, оптимизированную для печати.

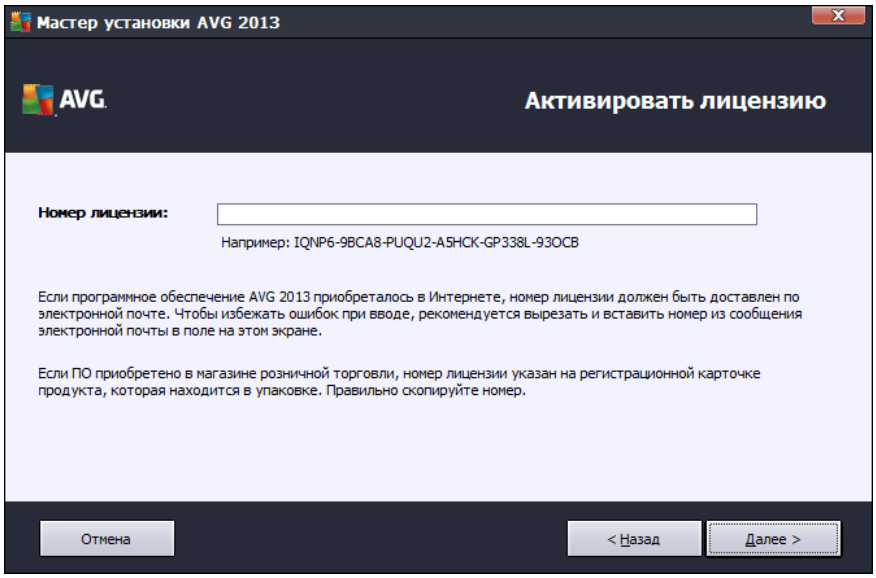
- ***Не принимаю*** — нажмите, чтобы отклонить условия лицензионного соглашения. Процесс установки при этом будет закрыт. **AVG Internet Security 2013** не будет установлена.

- ***Назад*** — нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.

- ***Принимаю*** — нажмите, чтобы подтвердить, что вы прочитали, понимаете и принимаете условия соглашения. Таким образом установка продолжится и вы перейдете к диалоговому окну следующего шага установки.

3.3. Активация лицензии

В диалоговом окне ***Активация лицензии*** предлагается ввести номер лицензии в соответствующее текстовое поле.



Как определить номер лицензии

Номер продажи указан на футляре компакт-диска из коробки **AVG Internet Security 2013** . Номер лицензии будет указан в сообщении электронной почты, которое вы получите после оформления покупки **AVG Internet Security 2013** через Интернет. Необходимо правильно ввести номер. Номер лицензии в цифровом формате (*приведенный в сообщении электронной почты*) рекомендуется вводить с использованием стандартного метода копирования и вставки.

Как пользоваться методом копирования и вставки

Использование метода ***копирования и вставки*** при вводе номера лицензии **AVG Internet Security 2013** гарантирует правильное введение номера. Выполните данные шаги:

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

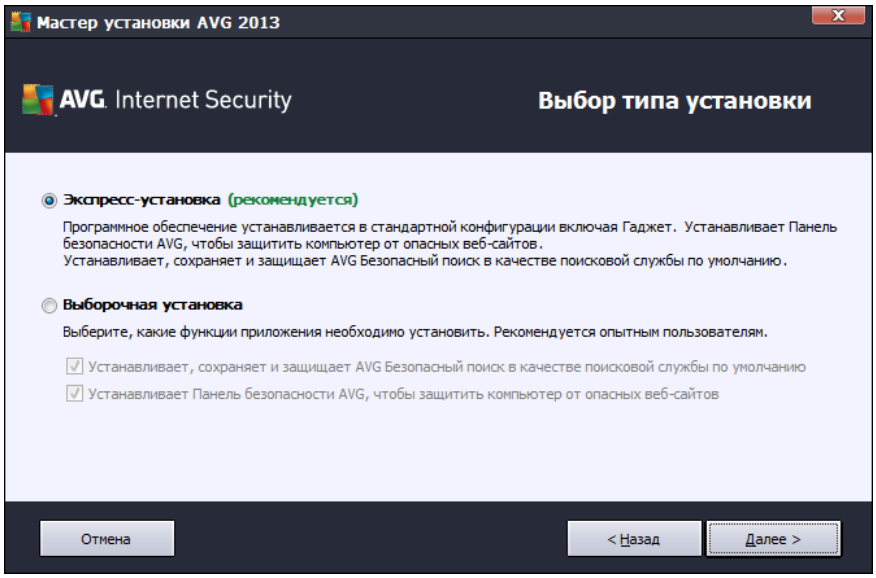
Кнопки управления

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

- ***Отмена*** — нажмите для немедленного выхода из процесса установки; **AVG Internet Security 2013** установка не будет выполнена.
- ***Назад*** — нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.
- ***Далее*** — нажмите для продолжения установки и перехода на один шаг вперед.

3.4. Выбор типа установки

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



Быстрая установка

Для большинства пользователей настоятельно рекомендуется использовать обычный вариант — ***Быстрая установка***. Это полностью автоматический вариант установки **AVG Internet Security 2013** с параметрами производителя по умолчанию, в которую входят Гаджет AVG, Панель безопасности AVG и Безопасный поиск AVG в качестве поисковой службы. Данный вариант установки обеспечивает максимальный уровень защиты наряду с оптимальным уровнем использования ресурсов. Если в дальнейшем потребуется изменить конфигурацию, это всегда можно будет сделать непосредственно в приложении **AVG Internet Security 2013**.

Нажмите кнопку ***Далее***, чтобы перейти к следующему этапу установки.

Выборочная установка

Выборочную установку следует выбирать только опытным пользователям, у которых есть веские основания для установки программы **AVG Internet Security 2013** с настройками, отличными от стандартных (например, при наличии определенных системных требований). В данном разделе можно выбрать компоненты установки *(оба компонента отмечены флажками и будут установлены, если вы не решите иначе)*.

- ***Установить безопасный поиск AVG поисковой службой по умолчанию и препятствовать попыткам ее изменения*** — не снимайте флажок, чтобы использовать безопасный поиск AVG, который совместно с компонентом Link Scanner Surf Shield обеспечивает максимальный уровень безопасности в Интернете.

- ***Установить панель безопасности AVG для защиты от вредоносных веб-сайтов*** — установите этот флажок, чтобы установить Панель безопасности AVG, которая обеспечивает максимальную защиту в Интернете.

При выборе этого параметра в диалоговом окне появляется раздел ***Папка назначения***. Здесь должно быть указано местоположение, куда нужно установить **AVG Internet Security 2013**. По умолчанию установка **AVG Internet Security 2013** выполняется в папку «Program Files», которая расположена на диске C:, как указано в текстовом поле диалогового окна. Чтобы изменить это местоположение, нажмите кнопку ***Обзор***, чтобы отобразить структуру дисков, и выберите соответствующую папку. Чтобы восстановить папку назначения по умолчанию, предустановленную поставщиком программного обеспечения, нажмите кнопку ***По умолчанию*** .

Нажмите кнопку ***Далее***, чтобы перейти к диалоговому окну Пользовательские параметры.

Кнопки управления

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

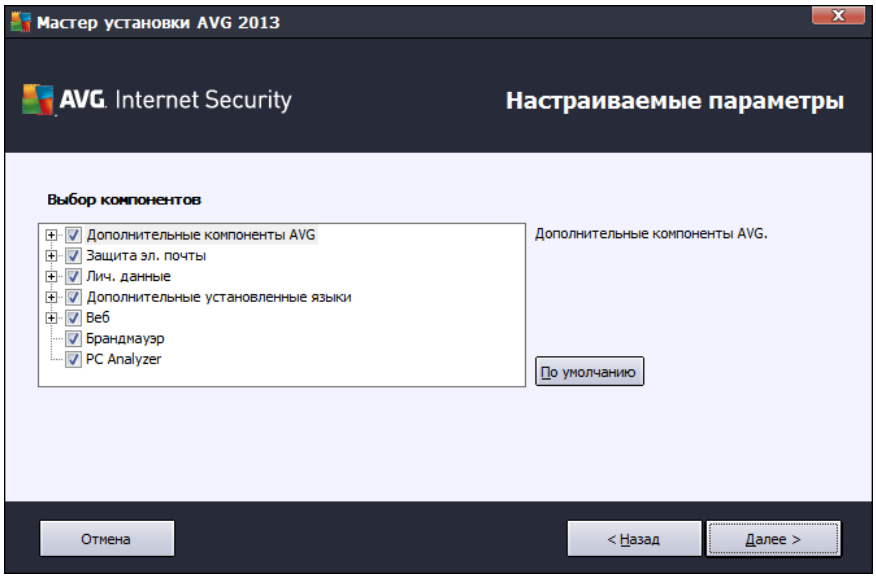
- ***Отмена*** — нажмите для немедленного выхода из процесса установки; **AVG Internet Security 2013** установка не будет выполнена.

- ***Назад*** — нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.

- ***Далее*** — нажмите для продолжения установки и перехода на один шаг вперед.

3.5. Пользовательские параметры

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



В разделе ***Выбор компонентов*** содержится список всех компонентов **AVG Internet Security 2013**, которые можно установить. Если значения параметров по умолчанию не подходят, можно добавить или удалить определенные компоненты.

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

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

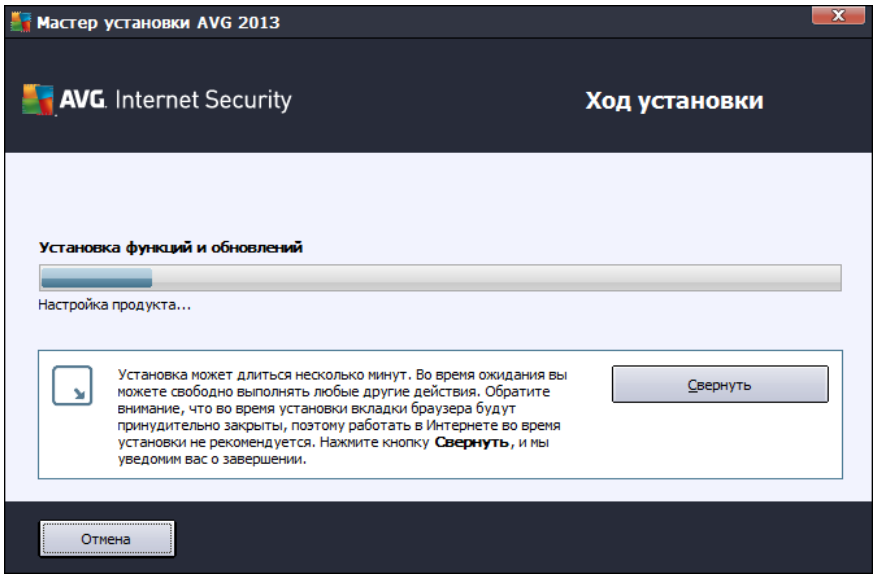
Кнопки управления

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

- ***Отмена*** — нажмите для немедленного выхода из процесса установки; **AVG Internet Security 2013** установка не будет выполнена.
- ***Назад*** — нажмите для возврата на один шаг назад к предыдущему диалоговому окну установки.
- ***Далее*** — нажмите для продолжения установки и перехода на один шаг вперед.

3.6. Состояние процесса установки

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



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

Кнопки управления

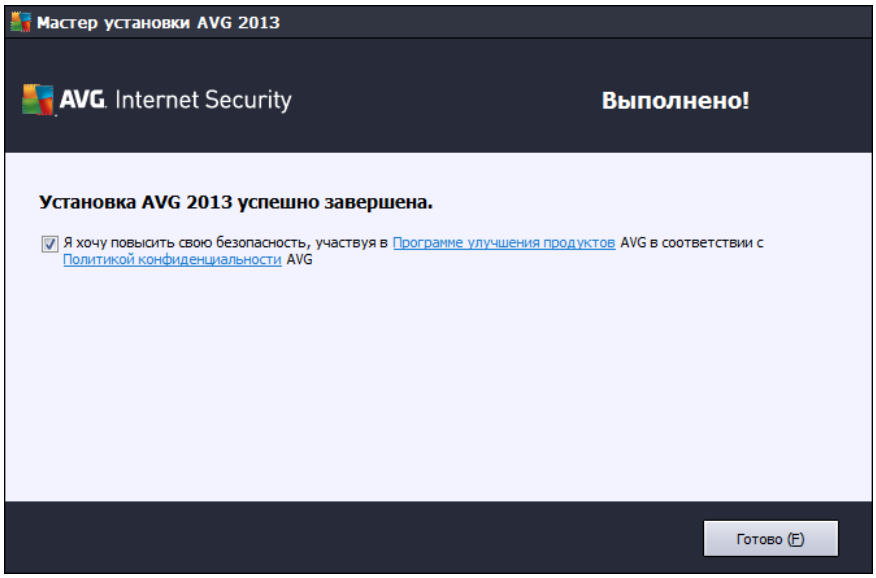
В данном диалоговом окне есть две кнопки управления.

- ***Свернуть*** — установка может занять несколько минут. Нажмите кнопку, чтобы свернуть окно в значок на панели задач. После завершения установки окно появится снова.

- ***Отмена*** — эту кнопку следует использовать, только когда нужно прервать процесс установки. Обратите внимание, что в таком случае программа **AVG Internet Security 2013** установлена не будет.

3.7. Установка выполнена успешно

Диалоговое окно ***Установка выполнена успешно*** отображается для подтверждения того, что программа **AVG Internet Security 2013** полностью установлена и настроена:



Программа улучшения продуктов AVG и политика конфиденциальности компании AVG

Здесь можно дать свое согласие на участие в ***Программе улучшения продуктов AVG*** (*дополнительные сведения см. в разделе Расширенные настройки AVG / Программа улучшения продуктов*), в рамках которой выполняется сбор анонимных сведений об обнаруженных угрозах с целью повышения общего уровня безопасности в Интернете. Сохраняется полная конфиденциальность в соответствии с политикой конфиденциальности AVG. Щелкните ссылку ***Политика конфиденциальности*** для перехода на веб-сайт компании AVG (http://www.avg.com/), где можно детальнее ознакомиться с этой политикой. Если вы принимаете ее, оставьте этот флажок *(по умолчанию он установлен)*.

Перезагрузка компьютера

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

4. После установки

4.1. Регистрация продукта

После завершения установки **AVG Internet Security 2013** выполните регистрацию продукта через Интернет на веб-сайте компании AVG *(http://www.avg.com/)*. После регистрации вы получите полный доступ к учетной записи пользователя AVG, информационному бюллетеню обновлений AVG, а также к другим службам, доступ к которым имеют только зарегистрированные пользователи. Самым простым способом является регистрация непосредственно из интерфейса пользователя **AVG Internet Security 2013**. Откройте в верхней строке навигации пункт Настройки / Зарегистрировать сейчас. Будет выполнено перенаправление на страницу ***Регистрация*** веб-сайта AVG *(http://www.avg.com/)*. Следуйте инструкциям, приведенным на странице.

4.2. Доступ к интерфейсу пользователя

Доступ к главному диалоговому окну AVG можно получить одним из следующих способов:

- дважды щелкните значок AVG на панели задач
- дважды щелкните значок AVG на рабочем столе
- в меню ***Пуск / Все программы / AVG / AVG 2013***

4.3. Сканирование всего компьютера

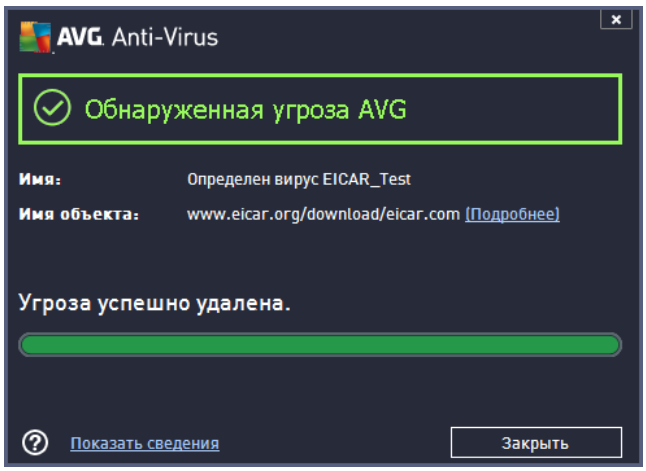
Существует потенциальная опасность того, что до установки **AVG Internet Security 2013** компьютер был заражен вирусом. Поэтому необходимо запустить операцию Сканирование всего компьютера, чтобы убедиться, что компьютер не заражен. Первое сканирование может занять достаточно много времени *(около часа)*, но рекомендуется запустить его, чтобы компьютер не был подвержен угрозам. Инструкции относительно запуска Сканирования всего компьютера см. в главе Сканирование AVG.

4.4. Тестирование Eicar

Чтобы проверить правильность установки **AVG Internet Security 2013**, можно выполнить тест EICAR.

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

Загрузите файл *eicar.com* и сохраните его на локальном диске. Сразу же после подтверждения загрузки тестового файла **AVG Internet Security 2013** отреагирует на него предупреждением. Данное оповещение означает, что программа AVG на компьютере установлена правильно.



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

4.5. Конфигурация AVG по умолчанию

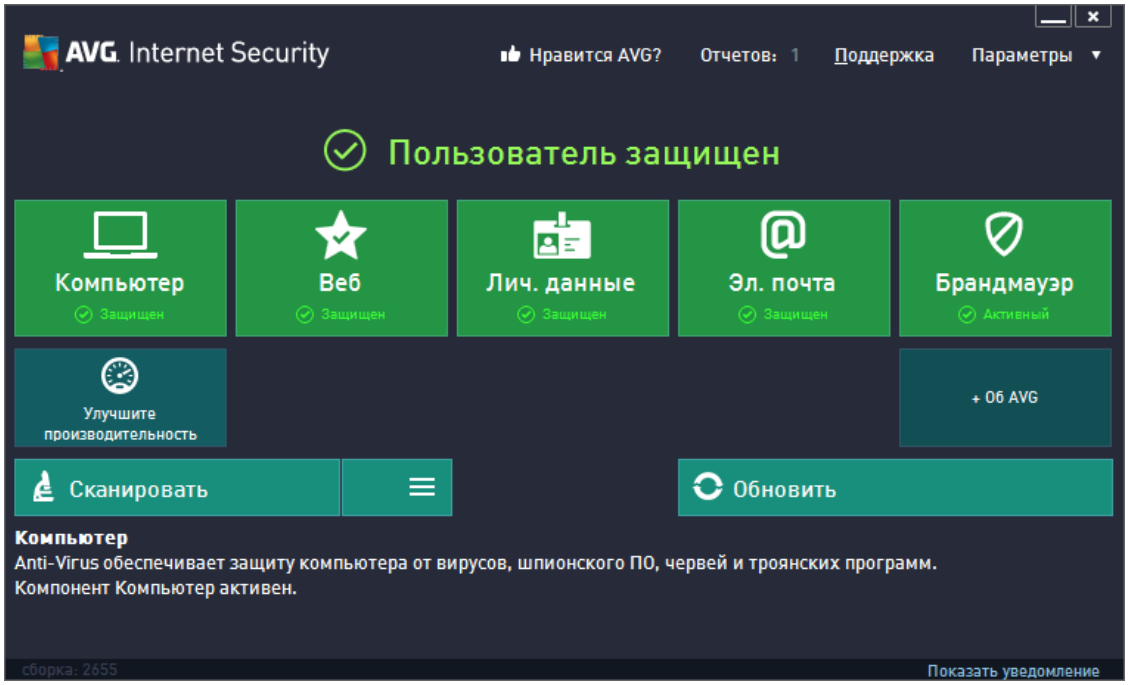
Параметры по умолчанию (*т. е. параметры приложения после установки*) **AVG Internet Security 2013** настроены поставщиком ПО так, чтобы все компоненты и функции обеспечивали оптимальную производительность.

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. Если вам нужно изменить конфигурацию AVG, перейдите в раздел Расширенные настройки AVG. Выберите пункт *Главное меню/Расширенные настройки* и измените конфигурацию AVG в открывшемся диалоговом окне Расширенные настройки AVG.

5. Интерфейс пользователя AVG

AVG Internet Security 2013 открывается в главном окне.



Главное окно состоит из нескольких разделов.

- ***Верхняя строка навигации*** представляет собой четыре активные ссылки в верхней части главного окна *(Нравится AVG, Отчеты, Поддержка, Настройки).* Сведения >>
- ***Информация о состоянии безопасности*** — отображает общие сведения о текущем состоянии **AVG Internet Security 2013**. Сведения >>
- ***Информацию об установленных компонентах*** можно найти на горизонтальной ленте в центральной части главного окна. Компоненты представлены в виде светло-зеленых квадратов со значками соответствующих программ, на которых находится информация об их состоянии. Сведения >>
- ***Значок Мои приложения*** отображается в нижней части центральной ленты главного окна, он содержит информацию о дополнительных приложениях**AVG Internet Security 2013** , которые уже установлены на вашем компьютере или рекомендуются для установки. Сведения >>
- ***Кнопки быстрых ссылок сканирования и обновления*** находятся в нижнем ряду значков главного окна. С помощью этих кнопок можно получить доступ к важнейшим и часто используемым функциям AVG. Сведения >>

Вне главного окна **AVG Internet Security 2013** есть еще два элемента управления, которые могут понадобиться для работы с приложением.

- ***Значок на панели задач*** — находится в нижнем правом углу экрана *(на панели*

задач) и отображает текущее состояние **AVG Internet Security 2013**. Сведения >>

- ***Гаджет AVG*** — расположен на боковой панели Windows (*поддерживается только в Windows Vista/7/8*) и обеспечивает быстрый доступ к функциям сканирования и обновления **AVG Internet Security 2013**. Сведения >>

5.1. Верхняя строка навигации

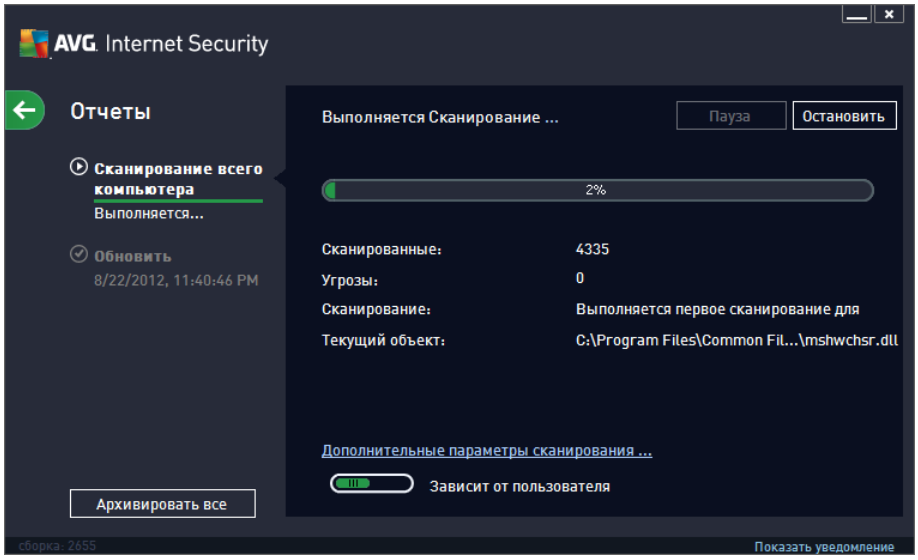
Верхняя строка навигации — это несколько активных ссылок в верхней части главного окна. В строке навигации содержатся следующие кнопки управления.

5.1.1. Мне нравится AVG

Щелкните ссылку, чтобы присоединиться к сообществу AVG в сети Facebook и получать актуальную информацию об AVG, новости, советы и подсказки для максимальной безопасности в Интернете.

5.1.2. Отчеты

Открытие диалогового окна ***Отчеты***, в котором представлен обзор отчетов о всех выполненных ранее операциях сканирования и обновления. Если в данный момент выполняется сканирование или обновление, рядом с надписью ***Отчеты*** в верхней строке навигации главного интерфейса пользователя появится вращающийся кружок. Щелкните этот кружок для открытия диалогового окна выполняемого процесса.



5.1.3. Поддержка

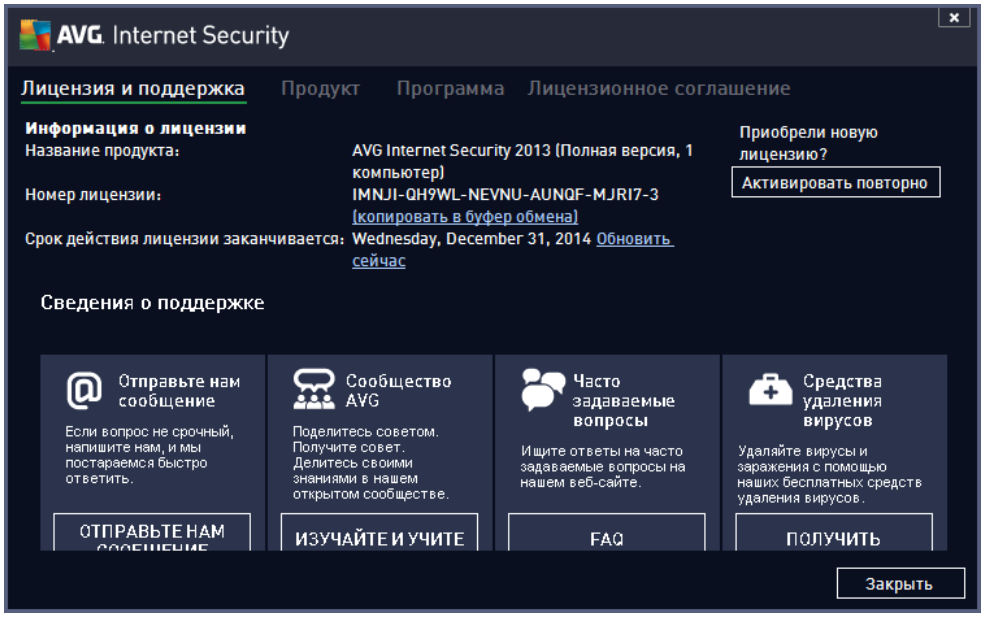
Открывает новое диалоговое окно с четырьмя вкладками, в которых содержится вся необходимая информация о **AVG Internet Security 2013**.

- ***Лицензия и поддержка*** — вкладка содержит сведения о продукте, номере лицензии и сроке ее действия. В нижней части диалогового окна в наглядной форме приведены контактные данные службы поддержки пользователей. На вкладке присутствуют несколько активных ссылок и кнопок.

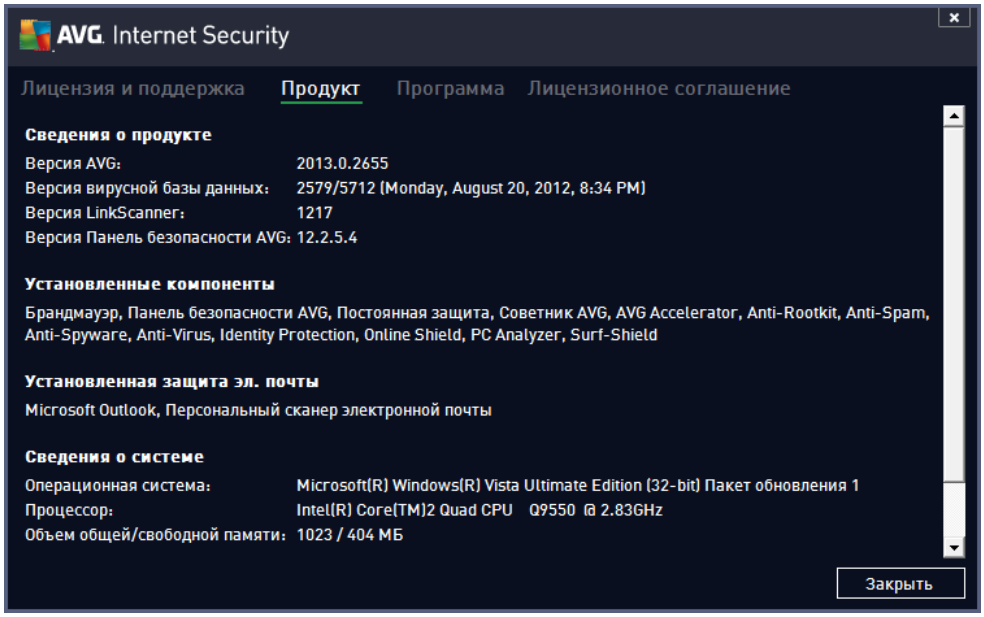
- *Активация (повторная активация)* — щелкните, чтобы открыть новое диалоговое окно ***Активация программного обеспечения AVG***. В соответствующем поле введите номер лицензии, чтобы заменить им номер продажи *(номер, который использовался при установке AVG Internet Security 2013)* или изменить текущий номер лицензии *(например, при обновлении до нового продукта AVG)*.

- *Копировать в буфер обмена* — с помощью этой ссылки можно скопировать номер лицензии и вставить его в нужном месте. Этот способ гарантирует правильность ввода номера лицензии.

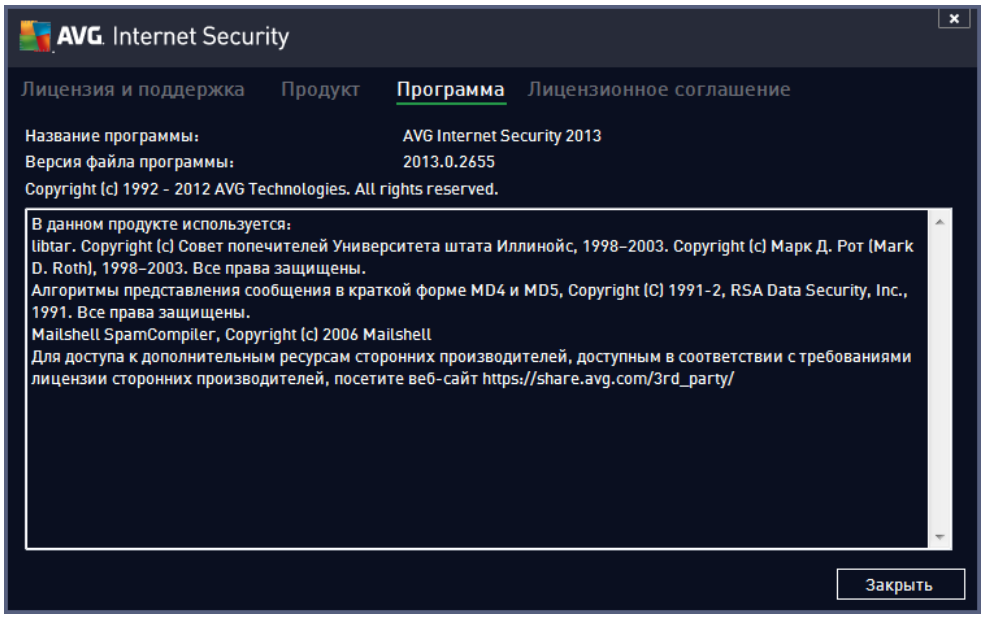
- *Продлить сейчас* — рекомендуется заблаговременно продлевать лицензию **AVG Internet Security 2013**, не позднее чем за месяц до срока ее истечения. Вы будете уведомлены о приближении срока истечения лицензии. Нажав на эту ссылку, вы будете перенаправлены на веб-сайт компании AVG *(http://www.avg.com/)*, на котором можно найти подробную информацию о лицензии, сроке ее действия, а также продлить или обновить вашу лицензию.



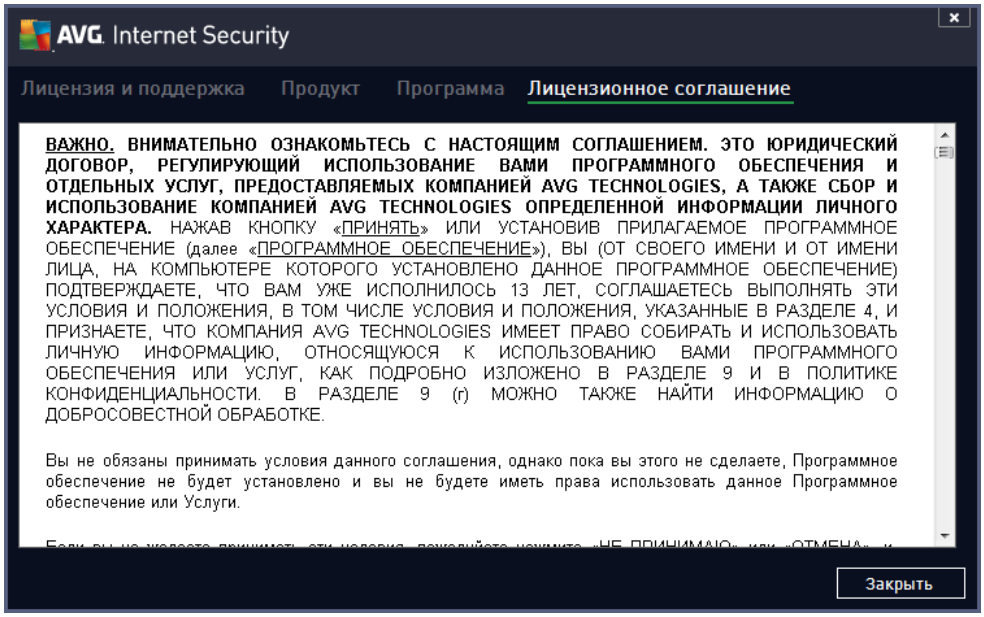
- ***Продукт*** — на данной вкладке содержатся основные **AVG Internet Security 2013** технические данные, в том числе информация о продукте и установленных компонентах, защите электронной почты и сведения о системе.



- ***Программа*** — вкладка содержит информацию о версии программы и программных кодах, использованных в продукте.



- ***Лицензионное соглашение*** — на вкладке можно ознакомиться с полным текстом лицензионного соглашения между пользователем и компанией AVG Technologies.



5.1.4. Настройки

Обслуживание **AVG Internet Security 2013** можно выполнить в меню ***Настройки***. Щелкните стрелку, чтобы открыть раскрывающееся меню.

- ***Сканировать компьютер*** — запускает сканирование всего компьютера.
- ***Сканировать выбранную папку...*** — выполняет переход к интерфейсу сканирования AVG, который позволяет с помощью структуры дерева определить, какие файлы и папки должны быть просканированы.
- ***Сканировать файл...*** — позволяет выполнить проверку отдельного файла по требованию. Выберите этот параметр, чтобы открыть новое окно с деревом структуры диска. Выберите нужный файл и подтвердите запуск сканирования.
- ***Обновить*** — автоматически запускает процесс обновления **AVG Internet Security 2013**.
- ***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, при отсутствии подключения к Интернету (например, если 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.
- ***Хранилище вирусов*** — отображает интерфейс карантина Хранилища вирусов, куда программа AVG отправляет все обнаруженные зараженные файлы, которые по какой-либо причине не удалось вылечить автоматически. В зоне карантина зараженные файлы изолированы и не представляют угрозы для безопасности компьютера, но в то же время они сохраняются для их возможного восстановления в будущем.
- ***История*** — открывает несколько других подменю для особых настроек.

- *Результаты сканирования* — открывает диалоговое окно со сведениями о результатах сканирования.
- *Обнаружение Resident Shield* — открывает диалоговое окно с обзором угроз, обнаруженных компонентом «Постоянная защита».
- *Обнаружение защиты электронной почты* — открывает диалоговое окно с обзором вложений сообщений электронной почты, признанных опасными компонентом «Защита электронной почты».
- *Полученные данные Online Shield* — отображает диалоговое окно с обзором угроз, обнаруженных компонентом Online Shield.
- *Журнал событий* — отображает интерфейс журнала событий, содержащего обзор всех зарегистрированных в нем **AVG Internet Security 2013** действий.
- *Журнал Firewall* — отображает диалоговое окно с описанием всех действий компонента Firewall.

- ***Дополнительные параметры...*** — открывает диалоговое окно «Расширенные настройки AVG», которое позволяет изменять параметры программы **AVG Internet Security 2013**. В общем случае рекомендуется сохранить настройки приложения по умолчанию, определенные производителем.
- ***Параметры Firewall...*** — открывает отдельное диалоговое окно, содержащее дополнительные параметры компонента Firewall.
- ***Справка*** — открывает файлы справки AVG.
- ***Поддержка*** — открывает веб-сайт AVG *(http://www.avg.com/)* на странице центра поддержки пользователей.
- ***Пользовательская сеть AVG*** — открывает веб-сайт AVG *(http://www.avg.com/).*
- ***О вирусах и угрозах*** — открывает интерактивную энциклопедию вирусов, в которой можно найти подробные сведения об обнаруженных вирусах.
- ***Активация (повторная активация)*** — открывает диалоговое окно ***Активация AVG***, в котором содержатся данные, указанные вами в процессе установки. В этом диалоговом окне можно ввести номер лицензии, чтобы заменить им номер продажи (*номер, который использовался при установке AVG*) или заменить старый номер лицензии (*например, при обновлении до новой версии продукта AVG*).
- ***Зарегистрировать сейчас*** — выполняет переход на страницу регистрации веб-сайта компании AVG (http://www.avg.com/). Введите данные для регистрации. Бесплатную техническую поддержку могут получать только клиенты, зарегистрировавшие свой продукт AVG. При использовании пробной версии **AVG Internet Security 2013** вместо последних двух элементов будут отображаться пункты ***Купить*** и ***Активировать***, которые позволяют сразу приобрести полную версию программы. Для программы **AVG Internet Security 2013**, при установке которой был указан номер продажи, будут отображаться пункты ***Зарегистрировать*** и ***Активировать***.

- ***Сведения об AVG*** — открывает новое диалоговое окно с четырьмя вкладками, в котором представлены сведения о лицензии, доступной поддержке, информация о продукте и программах, а также полный текст лицензионного соглашения.

5.2. Информация о состоянии безопасности

Раздел ***Информация о состоянии безопасности*** расположен в верхней части главного окна **AVG Internet Security 2013**. Этот раздел позволяет быстро определить текущее состояние безопасности **AVG Internet Security 2013**. Ознакомьтесь со значками, представленными в данном разделе, и их значением.

— зеленый значок означает, что программа ***AVG Internet Security 2013 работает правильно***. Ваш компьютер полностью защищен, установлены все необходимые обновления. Все установленные компоненты работают правильно.

— желтый значок означает, что ***один или несколько компонентов настроены неправильно***. Необходимо проверить их свойства или настройки. Нет серьезных проблем, связанных с работой программы **AVG Internet Security 2013**. Скорее всего, компонент был по какой-либо причине отключен. Компьютер находится под защитой. Однако необходимо уделить внимание настройке компонента. Неправильно настроенный компонент будет отображаться в главном интерфейсе пользователя с оранжевой предупреждающей полоской.

Желтый значок отображается также в том случае, если по какой-либо причине было принято решение игнорировать состояние ошибки компонента. Параметр ***Игнорировать состояние ошибки*** доступен на ветке с аналогичным названием в Дополнительных параметрах. Выбор данного параметра означает, что вам известно о состоянии ошибки компонента **AVG Internet Security 2013**, но вы не хотите получать уведомления об этом. Использование данного параметра может потребоваться в определенной ситуации, при этом настоятельно рекомендуется как можно скорее возвратить параметр ***Игнорировать состояние ошибки*** в исходное состояние.

Также желтый значок будет отображаться, если **AVG Internet Security 2013** требует перезагрузки компьютера (***Требуется перезагрузка***). Обратите внимание на это предупреждение и выполните перезагрузку компьютера.

— оранжевый значок указывает на критическое состояние программы ***AVG Internet Security 2013***. Один или несколько компонентов работают неправильно, программа **AVG Internet Security 2013** не может защитить компьютер. Необходимо немедленно устранить указанные проблемы! Если проблему не удается устранить самостоятельно, обратитесь в службу технической поддержки компании AVG.

В случае если программа AVG Internet Security 2013 не обеспечивает оптимальной производительности, появится дополнительная кнопка «Быстрое исправление» (или «Исправить все», если проблема с несколькими компонентами). Нажмите эту кнопку, чтобы запустить автоматическую проверку и настройку программы. Это наиболее простой способ достичь оптимальной производительности программы AVG Internet Security 2013 и обеспечить максимальный уровень безопасности.

Настоятельно рекомендуется обращать внимание на раздел ***Информация о состоянии безопасности***. В случае возникновения проблемы постарайтесь незамедлительно ее

устранить. В противном случае безопасность компьютера может быть под угрозой.

Примечание. *Узнать о состоянии безопасности AVG Internet Security 2013 можно в любое время с помощью значка на панели задач.*

5.3. Обзор компонентов

Информацию об установленных компонентах можно найти на горизонтальной ленте в центральной части главного окна. Компоненты представлены в виде светло-зеленых кнопок со значками соответствующих компонентов. На каждой кнопке отображается информация о текущем состоянии защиты. Если компонент правильно настроен и выполняет все свои функции, текст отображается зеленым цветом. Если компонент остановлен, его функциональность ограничена, а также если он находится в состоянии ошибки, вы будете уведомлены об этом при помощи предупреждения на оранжевом фоне. ***Настоятельно рекомендуем обращать внимание на параметры компонента!***

Наведите указатель мыши на компонент. Появится краткое описание в нижней части главного окна. Вы увидите общие сведения о функциях данного компонента. Также отображается текущее состояние компонента и указывается, какая из служб компонента настроена неправильно.

Список установленных компонентов

В **AVG Internet Security 2013** раздел ***Обзор компонентов*** содержит сведения о следующих компонентах:

- ***Компьютер*** — этот компонент включает в себя две службы. ***Антивирусная защита*** обнаруживает в вашей системе вирусы, шпионское ПО, червей, «троянских коней», нежелательные выполнимые файлы или библиотеки и защищает от вредоносного рекламного ПО, а компонент ***Anti-Rootkit*** сканирует на наличие руткитов, которые маскируются под приложения, драйвера или библиотеки. Сведения >>
- ***Работа в Интернете*** — обеспечивает защиту от интернет-атак, пока вы работаете или выполняете поиск в Интернете. Сведения >>
- ***Защита учетных данных*** — этот компонент запускает службу ***Identity Shield*** , которая обеспечивает постоянную защиту цифровых данных от новых и еще неизвестных интернет-угроз. Сведения >>
- ***Электронная почта*** — проверяет все входящие сообщения электронной почты на наличие спама, блокирует вирусы, фишинг-атаки и другие угрозы. Сведения >>
- ***Firewall*** — контролирует весь обмен данными на каждом сетевом порте, защищая от вредоносных атак и блокируя любые попытки вторжения. Сведения >>

Доступные действия

- ***Для выделения любого из компонентов*** в обзоре следует навести курсор мыши на значок компонента. При этом в нижней части интерфейса пользователя отобразится

описание основных функций компонента.

- ***Щелчок значка компонента*** открывает интерфейс компонента с информацией о его текущем состоянии и доступе к параметрам и статистическим данным.

5.4. Мои приложения

В разделе ***Мои приложения*** *(ряд зеленых кнопок ниже перечня компонентов)* находится список приложений AVG, которые или уже установлены на компьютере или рекомендуются для установки. Эти кнопки отображаются по желанию пользователя и предоставляют доступ к следующим приложениям.

- ***Mobile protection*** — приложение для защиты сотового телефона от вирусов и вредоносного ПО. Также в нем есть функция определения местонахождения вашего смартфона, если вы его где-нибудь забыли или потеряли.

- ***LiveKive*** предназначен для резервного копирования данных через Интернет на защищенные серверы. LiveKive позволяет автоматически выполнять резервное копирование файлов, фотографий и музыки в общее безопасное пространство. К этим файлам можно затем предоставлять общий доступ для членов семьи или друзей, а также получать доступ с любого устройства, подключенного к Интернету, например iPhone или Android.

- ***Family Safety*** позволяет защитить детей от веб-сайтов, мультимедийных материалов и результатов поиска, которые им не рекомендуется просматривать, а также предоставляет отчеты о деятельности детей в Интернете. AVG Family Safety использует технологию слежения за нажатием клавиш, чтобы контролировать деятельность ребенка в тематических чатах и на сайтах социальных сетей. При обнаружении слов, выражений или языка, использующихся в Интернете для обмана детей, вы будете немедленно уведомлены об этом SMS-сообщением или по электронной почте. Можно назначить необходимый уровень защиты для каждого ребенка, а затем отслеживать их по отдельности с помощью уникальных имен пользователей.

- ***PC Tuneup*** представляет собой расширенное средство для выполнения подробного анализа системы и внесения исправлений для увеличения быстродействия и улучшения общей производительности компьютера.

- ***Приложение MultiMi*** — единый центр доступа к вашим учетным записям в социальных сетях и почтовых службах, который облегчает процесс общения с друзьями и родственниками, просмотр веб-узлов, обмен фотографиями, видео и другими файлами в Интернете. В состав MultiMi входит служба LinkScanner, которая защищает вас от растущего числа интернет-угроз, проверяя безопасность всех ссылок на веб-страницах, которые вы просматриваете.

- ***Панель инструментов AVG*** встраивается непосредственно в ваш веб-браузер и обеспечивает максимальный уровень безопасности в Интернете.

Чтобы получить подробные сведения о том или ином приложении из числа представленных в разделе ***Мои приложения***, нажмите на соответствующую кнопку. Откроется соответствующая веб-страница компании AVG, на которой можно быстро загрузить необходимый компонент.

5.5. Сканировать / Обновить быстрые ссылки

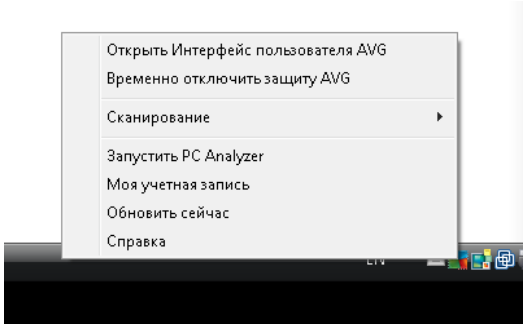
Быстрые ссылки расположены в левой части интерфейса пользователя **AVG Internet Security 2013**. Данные ссылки позволяют получить быстрый доступ к наиболее важным и часто используемым функциям приложения, таким как сканирование и обновление. Быстрые ссылки доступны из всех диалоговых окон интерфейса пользователя.

- ***Сканировать сейчас*** — эта кнопка графически разделена на две части. Щелкните ссылку ***Сканировать сейчас*** для немедленного запуска операции Сканировать весь компьютер. В окне Отчеты, которое откроется автоматически, отобразится ход и результаты сканирования. Кнопка ***Настройки*** открывает диалоговое окно ***Параметры сканирования***, в котором можно управлять запланированными сканированиями и изменять параметры операций Сканировать весь компьютер и Сканирование определенных файлов или папок. *(Для получения подробных сведений см. главу Сканирование AVG)*

- ***Обновить сейчас*** — нажмите кнопку, чтобы немедленно приступить к обновлению программы. За процессом обновления и его результатами можно наблюдать в окне ***Отчеты***. *(Для получения подробных сведений см. главу Обновление AVG)*

5.6. Значок на панели задач

Значок AVG на панели задач *(на панели задач Windows, правая нижняя часть экрана)* — отображает текущее состояние **AVG Internet Security 2013**. Этот значок всегда отображается на панели задач независимо от того, открыт ли интерфейс пользователя **AVG Internet Security 2013.**



Отображение значка AVG на панели задач

- При полноцветном отображении значок на панели задач указывает, что все **AVG Internet Security 2013** компоненты активны и работают правильно. Однако полноцветный значок может также отображаться в случае, если один из компонентов находится в состоянии ошибки, но был выбран параметр Игнорировать состояние компонентов. *(Выбрав параметр «Игнорировать состояние компонентов», пользователь показывает, что ему известно о состоянии ошибки компонента, но по какой-либо причине не требуется изменять данное состояние и нет необходимости получать предупреждения о данной ситуации.)*

- Значок с восклицательным знаком указывает на ошибку в компоненте *(или в*

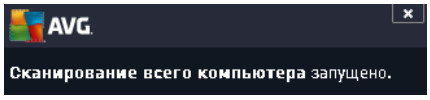
нескольких компонентах). Всегда обращайте внимание на подобные предупреждения и старайтесь должным образом настроить компонент и исправить неполадку. Чтобы изменить настройки данного компонента, дважды щелкните значок на панели задач и откройте интерфейс пользователя приложения. Подробные сведения о том, какой именно компонент находится в состоянии ошибки, см. в разделе Сведения о состоянии безопасности.

- Значок на панели задач может также отображаться в полном цвете с мигающим и крутящимся лучом света. Такое отображение означает, что запустился процесс обновления.

- Полноцветный значок со стрелкой сигнализирует о том, что выполняется **AVG Internet Security 2013** то или иное сканирование.

Информация на значке AVG на панели задач

Значок AVG на панели задач сообщает о всех действиях **AVG Internet Security 2013** и возможных изменениях состояния программы (*например, об автоматическом запуске сканирования или обновления, переключении профиля Firewall, изменениях в состоянии компонентов, ошибках и т. п.*) с помощью всплывающих окон над панелью задач.



Действия, доступные из значка AVG на панели задач

Дважды щелкнув ***значок AVG на панели задач***, можно быстро получить доступ к интерфейсу пользователя **AVG Internet Security 2013**. Если щелкнуть правой кнопкой мыши значок на панели задач, откроется краткое контекстное меню, содержащее следующие пункты:

- ***Открыть интерфейс пользователя AVG*** — открытие интерфейса пользователя **AVG Internet Security 2013**.

- ***Временно отключить защиту AVG*** — данный параметр позволяет полностью выключить защиту, обеспечиваемую **AVG Internet Security 2013**. Используйте этот параметр только в случае крайней необходимости! В большинстве случаев программу **AVG Internet Security 2013** не рекомендуется выключать перед установкой нового ПО или драйверов, даже если программа или мастер установки рекомендует завершить все запущенные программы и приложения, чтобы они не препятствовали процессу установки. Если вам пришлось временно выключить защиту **AVG Internet Security 2013**, включите ее, как только завершите установку. Если вы подключены к Интернету или локальной сети, но антивирусная защита выключена, ваш компьютер может подвергнуться атакам.

- ***Сканирование*** — щелкните, чтобы открыть контекстное меню предварительно настроенных сеансов сканирования (*Сканировать весь компьютер*, *Сканировать отдельные файлы/папки*), и выберите соответствующий вариант. Сканирование будет запущено немедленно.

- ***Запущенные сканирования...*** — данный элемент отображается, только если на компьютере выполняется сканирование. Для запущенного сканирования можно назначить приоритет. Кроме того, его можно приостановить или остановить полностью. Также можно выполнить и другие действия: *«Установить приоритет для всех сканирований», «Приостановить все сканирования»* и *«Остановить все сканирования»*.

- ***Запустить Быстрая настройка*** — щелкните, чтобы запустить компонент Быстрая настройка.

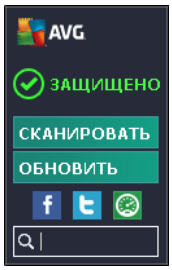
- ***Моя учетная запись*** — открывает домашнюю страницу MyAccount, где можно управлять подписками, приобретать дополнительную защиту, загружать установочные файлы, просматривать ваши предыдущие заказы и счета ,а также изменять персональные данные.

- ***Обновить сейчас*** — немедленный запуск обновления.

- ***Справка*** — открытие файла справки на начальной странице.

5.7. Гаджет AVG

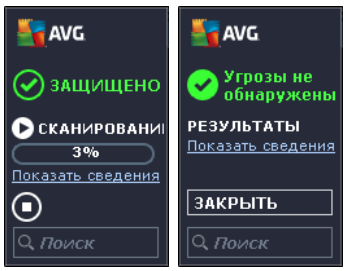
Гаджет AVG отображается на рабочем столе Windows (*на боковой панели Windows*). Это приложение поддерживает только операционные системы Windows Vista и Windows 7/8. ***Гаджет AVG*** позволяет мгновенно получить доступ к самым важным функциям **AVG Internet Security 2013**, например к операциям сканирования и обновления**.**



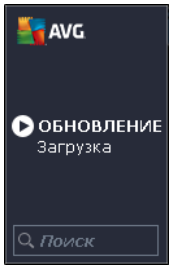
Элементы управления гаджетом AVG

При необходимости с помощью гаджета AVG можно мгновенно запустить сканирование или обновление; он также имеет возможности для быстрого поиска и выхода в основные социальные сети.

- ***Сканировать сейчас***. Щелкните ссылку ***Сканировать сейчас***, чтобы запустить сканирование всего компьютера. Процесс сканирования будет также отображаться в пользовательском интерфейсе гаджета. Краткая статистическая сводка содержит сведения о количестве сканированных объектов, обнаруженных и устраненных угроз. Процесс сканирования можно приостановить или остановить в любой момент. Подробные результаты сканирования можно просмотреть в диалоговом окне Обзор результатов сканирования, которое можно открыть непосредственно из гаджета с помощью параметра ***Показать сведения*** *(соответствующие результаты сканирования отобразятся в разделе Сканирование с помощью гаджета на боковой панели)*.



- ***Обновить сейчас*** — щелкните ссылку ***Обновить сейчас*** **AVG Internet Security 2013**, чтобы запустить процесс обновления непосредственно в гаджете.



- ***Ссылка на Twitter*** — открывает новый интерфейс ***гаджета AVG***, содержащий сводку последних новостей AVG, опубликованных в Twitter. Щелкните ссылку ***Просмотреть все каналы AVG в Twitter*** , чтобы открыть в новом окне браузера страницу Twitter с новостями компании.

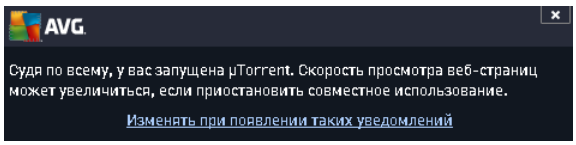
- ***Ссылка на Facebook*** — открывает в веб-браузере страницы ***сообщества AVG*** на веб-сайте Facebook.

- ***Поле поиска*** — отображает результаты поиска по ключевому слову в новом окне браузера по умолчанию.

5.8. Советник AVG

Советник AVG был разработан для поиска неполадок, которые замедляют работу компьютера или являются опасными для него. Он также позволяет найти способы их решения. Если вам кажется, что компьютер внезапно стал работать медленнее *(при навигации в Интернете или использовании обычных приложений)*, установить причину этого и решить проблему бывает нелегко. В таких случаях поможет ***Советник AVG***. Он отобразит уведомление на панели задач о возможной проблеме и предложит способ ее устранения. ***Советник AVG*** контролирует все текущие процессы вашего компьютера и предлагает решение проблем.

Советник AVG отображается в форме всплывающего окна над панелью задач.



В частности, ***Советник AVG*** выполняет следующее.

- ***Проверка состояния любого открытого веб-браузера***. Эти приложения могут использовать чрезмерное количество памяти, особенно когда открыто большое количество вкладок или окон, и потреблять много системных ресурсов — другими словами, замедлять работу компьютера. В таком случае обычно достаточно перезагрузить веб-браузер.

- ***Создание однорангового подключения***. Даже после того как пользователь прекратил использование однорангового подключения, оно может оставаться активным, в определенной степени снижая пропускную способность. В результате работа веб-браузера замедляется.

- ***Неизвестная сеть со знакомым именем***. Обычно это касается лишь пользователей, которые подключаются к разнообразным сетям, используя в основном портативные компьютеры. Если новая неизвестная сеть имеет то же имя, что и уже известная и часто используемая *(например, Home или MyWifi)*, их легко перепутать и случайно подключиться к абсолютно незнакомой и потенциально опасной сети. ***Советник AVG*** помогает это предотвратить, предупреждая о попытке подключения к новой сети с таким же именем. Конечно, если пользователь посчитает ее безопасной, он может занести ее в список известных сетей ***Советника AVG***, после чего уведомление больше не появится.

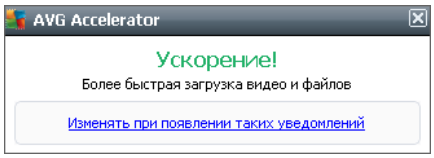
В каждой из этих ситуаций ***Советник AVG*** предупреждает о возможной проблеме и предоставляет название и значок конфликтующего процесса или приложения. Также ***Советник AVG*** предлагает меры, которые следует принять во избежание возможных проблем.

Поддерживаемые веб-браузеры

Данная функция работает в таких браузерах: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.9. AVG Accelerator

Ускоритель AVG обеспечивает более стабильное воспроизведение видеороликов в Интернете, а также ускоряет процессы загрузки. При запуске процесса видеоускорения на панели задач появится всплывающее окно с уведомлением.



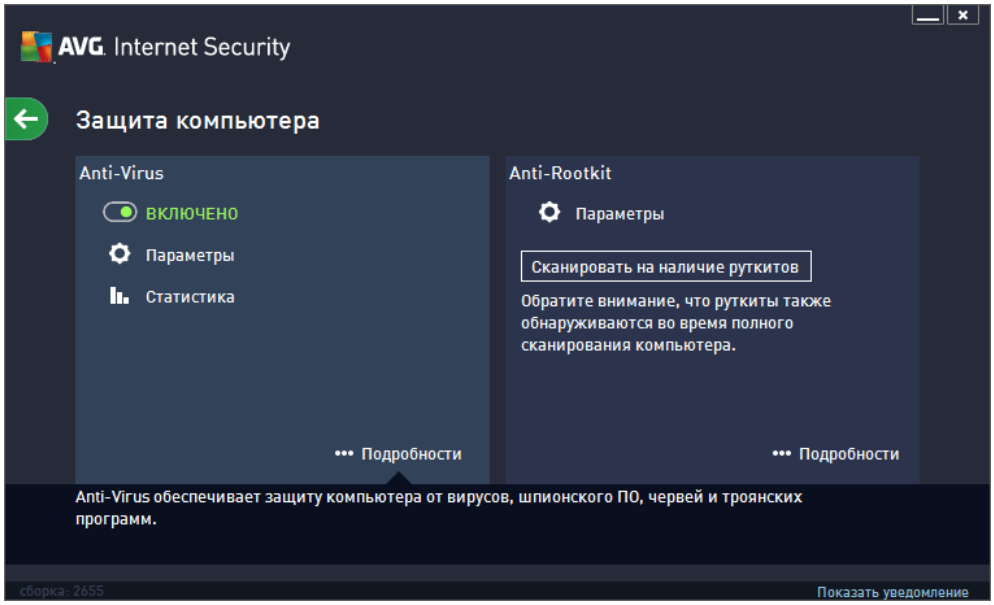
6. Компоненты AVG

6.1. Компьютер

Компонент ***Компьютер*** состоит из двух основных служб: ***Anti-Virus*** и ***Anti-Rootkit***.

- ***Служба Anti-Virus*** представляет собой модуль сканирования, который обеспечивает защиту файлов, системных областей компьютера и съемных носителей *(флэш-дисков и т. п.)* и сканирует на наличие известных вирусов. Каждый обнаруженный вирус блокируется, удаляется или помещается в Хранилище вирусов. Пользователь даже не замечает этого процесса, поскольку эта такая — «постоянная» — защита работает в фоновом режиме. Данный компонент также использует эвристический анализ, при котором файл исследуется на наличие типичных характеристик вирусов. Это означает, что Anti-Virus может обнаружить новый, неизвестный вирус, если он содержит некоторые типичные признаки уже существующих вирусов. **AVG Internet Security 2013** Приложение способно анализировать и обнаруживать исполняемые приложения или библиотеки DLL, использование которых в системе может быть потенциально нежелательным *(различные виды шпионского и рекламного ПО и т. п.).*. Более того, Anti-Virus сканирует системный реестр на наличие подозрительных записей, временных интернет-файлов, следящих файлов cookie и позволяет поступать с потенциально вредоносными элементами так же, как и с другими зараженными объектами.

- ***Компонент Anti-Rootkit*** — это специальное средство, предназначенное для обнаружения и эффективного удаления опасных пакетов руткитов — то есть программ и технологий, позволяющих скрывать вредоносное ПО, присутствующее на компьютере. Руткиты имеют целью полный захват управления системой компьютера без разрешения владельцев систем и законных управляющих. Компонент Anti-Rootkit позволяет обнаруживать руткиты с помощью предварительно настроенного набора правил. Если компонент Anti-Rootkit обнаружил руткит, это еще не значит, что обнаруженный пакет программ заражен. Иногда руткиты используются в качестве драйверов или являются частью безопасных приложений.



Элементы управления диалогового окна

Чтобы перейти из одного раздела диалогового окна в другой, просто щелкните в любом месте панели данной службы. После этого панель станет светло-синего цвета. Данные элементы управления находятся в обеих частях диалогового окна. Их назначение одинаково для обеих служб *(Anti-Virus u Anti-Rootkit)*.

Включен / Отключен — эта кнопка по внешнему виду и принципу действия напоминает светофор. Щелкните мышью, чтобы переключиться из одного положения в другое. Зеленый цвет соответствует положению ***Включен*** — служба Anti-Virus активна и выполняет все функции. Красный цвет соответствует положению ***Отключен*** — компонент деактивирован. Настоятельно рекомендуется не изменять значения по умолчанию для всех параметров безопасности, если у вас нет веских причин для отключения службы. Параметры по умолчанию гарантируют оптимальную производительность приложения и максимальный уровень безопасности. Если вы по какой-либо причине все же захотите отключить службу, сразу же отобразится красный ***предупреждающий*** знак, сигнализирующий об опасности, и сообщение о том, что защита не является полной. ***Не забудьте как можно скорее включить службу снова!***

Параметры — нажмите эту кнопку, чтобы перейти в интерфейс дополнительных параметров. Другими словами, откроется соответствующее диалоговое окно, где вы сможете настроить параметры служб Anti-Virus или Anti-Rootkit. Интерфейс дополнительных параметров позволяет изменить любые параметры служб **AVG Internet Security 2013** , но выполнять подобные действия рекомендуется только опытным пользователям.

Статистические данные — нажмите эту кнопку, чтобы перейти на соответствующую страницу веб-сайта AVG (http://www.avg.com/). На этой странице можно посмотреть подробный статистический обзор всех действий **AVG Internet Security 2013**, выполненных на вашем компьютере за определенный промежуток

времени или за все время.

Сведения — нажмите эту кнопку, и в нижней части диалогового окна появится краткое описание выделенной службы.

— используйте зеленую стрелку в верхней левой части диалогового окна для возврата к главному интерфейсу пользователя с общими сведениями о компонентах.

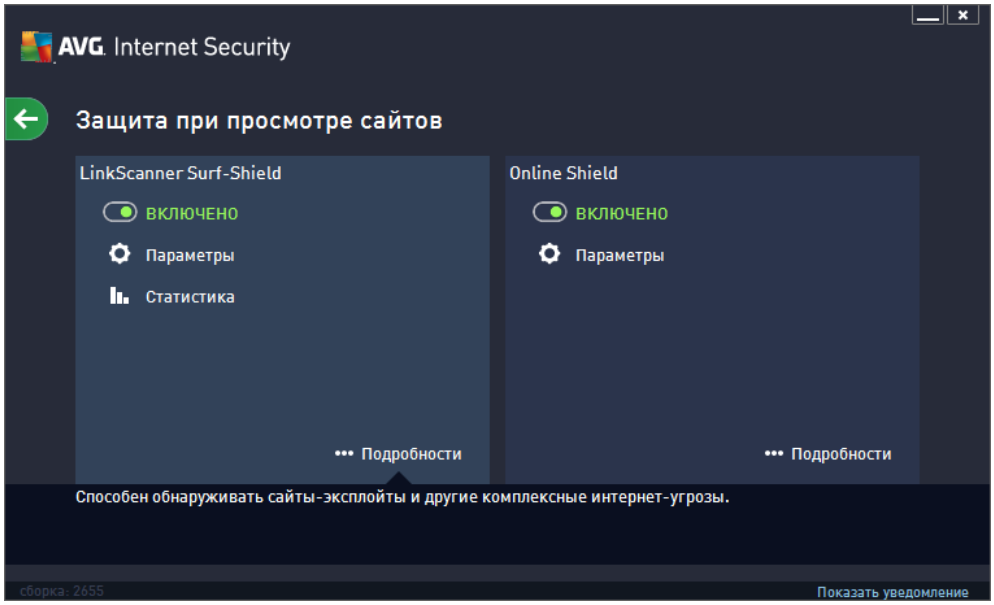
В разделе Anti-Rootkit вы также найдете специальную кнопку ***Сканировать на наличие руткитов***, с помощью которой можно запустить отдельное сканирование на наличие руткитов *(однако нужно помнить, что подобное сканирование выполняется в рамках Сканирования всего компьютера)*.

6.2. Просмотр веб-узлов

Компонент ***Защита при просмотре веб-сайтов*** включает в себя две службы: ***LinkScanner Surf-Shield*** и ***Online Shield***.

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

- ***Online Shield*** — это разновидность постоянной защиты в режиме реального времени, которая сканирует содержимое посещаемых веб-страниц и файлов, которые содержат эти страницы, до того, как они отобразятся в веб-браузере или будут загружены на компьютер. Компонент Online Shield предназначен для обнаружения на открываемой веб-странице небезопасных объектов javascript и предотвращения отображения данной страницы. Кроме того, она способна определить наличие вредоносного ПО на странице и остановить его загрузку, чтобы оно не попало на компьютер. Данное мощное средство защиты предназначено для блокировки загрузки вредоносного содержимого открываемых веб-страниц 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. Важно помнить, что эксплойты могут проникнуть на ваш компьютер, даже если вы просто зашли на зараженный сайт. ***Служба Online Shield не предназначена для использования на серверных платформах.***



Элементы управления диалогового окна

Чтобы перейти из одного раздела диалогового окна в другой, просто щелкните в любом месте панели данной службы. После этого панель станет светло-синего цвета. Данные элементы управления находятся в обеих частях диалогового окна. Их назначение одинаково для обоих компонентов *(Link Scanner Surf-Shield и Online Shield)*.

Включен / Отключен — эта кнопка по внешнему виду и принципу действия напоминает светофор. Щелкните мышью, чтобы переключиться из одного положения в другое. Зеленый цвет соответствует положению ***Включен*** — служба LinkScanner Surf-Shield (или Online Shield) активна и выполняет все функции. Красный цвет соответствует положению ***Отключен*** — компонент деактивирован. Настоятельно рекомендуется не изменять значения по умолчанию для всех параметров безопасности, если у вас нет веских причин для отключения службы. Параметры по умолчанию гарантируют оптимальную производительность приложения и максимальный уровень безопасности. Если вы по какой-либо причине все же захотите отключить службу, сразу же отобразится красный ***предупреждающий*** знак, сигнализирующий об опасности, и сообщение о том, что защита не является полной. ***Не забудьте как можно скорее включить службу снова!***

Параметры — нажмите эту кнопку, чтобы перейти в интерфейс дополнительных параметров. Откроется соответствующее диалоговое окно, где вы сможете настроить параметры LinkScanner Surf-Shield или Online Shield. Интерфейс дополнительных параметров позволяет изменить любые параметры служб **AVG Internet Security 2013**, но выполнять подобные действия рекомендуется только опытным пользователям.

Статистические данные — нажмите эту кнопку, чтобы перейти на соответствующую страницу веб-сайта AVG (http://www.avg.com/). На этой странице можно посмотреть подробный статистический обзор всех действий **AVG Internet Security 2013**, выполненных на вашем компьютере за определенный промежуток времени или за все время.

Сведения — нажмите эту кнопку, и в нижней части диалогового окна появится краткое описание выделенной службы.

— используйте зеленую стрелку в верхней левой части диалогового окна для возврата к главному интерфейсу пользователя с общими сведениями о компонентах.

6.3. Учетные данные

Компонент ***Identity protection*** включает в себя две службы: ***Identity Protection*** и ***Identity Alert***.

- ***Identity Protection*** — это компонент, предназначенный для защиты компьютера от всех видов вредоносного ПО (*шпионского ПО, программ-роботов, программ для кражи личных данных и т. п.*) с помощью технологий определения моделей поведения. Этот компонент также обеспечивает защиту «нулевого дня» от новых вирусов. Главной задачей компонента Identity Protection является предотвращение кражи паролей, сведений о банковских счетах, номеров кредитных карт и другой важной личной информации с помощью вредоносных программ *(или вредоносного ПО)*, нацеленных на ваш ПК. Данный компонент обеспечивает правильную работу всех программ на компьютере или в общей сети. Компонент Identity Protection непрерывно ищет и блокирует подозрительные объекты, защищая таким образом компьютер от всех новых разновидностей вредоносного ПО. Компонент Identity Protection обеспечивает защиту компьютеров в режиме реального времени от новых и даже неизвестных угроз. Он отслеживает все процессы *(включая скрытые) и более 285 моделей поведения с целью выявления возможной опасности для системы.* По этой причине возможно обнаружение угроз, еще не описанных в вирусной базе данных. Когда на компьютер попадает незнакомый код, он немедленно проверяется на предмет вредоносного поведения и отслеживается. Если файл определяется как вредоносный, служба Identity Protection переместит код в Хранилище вирусов и отменит все внесенные им в систему изменения *(вставки кодов, изменения реестра, открытие портов и т. д.)*. Не требуется запускать сканирование для обеспечения защиты. Данная технология является упреждающей, редко нуждается в обновлении и постоянно обеспечивает защиту.

- ***Компонент Identity Alert*** предоставляет доступ к веб-службе, предназначенной для дискретного мониторинга персональной информации через Интернет. К такой информации относятся следующие сведения: номера кредитных карт, адреса электронной почты, номера стационарных и *мобильных телефонов* и т. п. Мониторинг выполняется на регулярной основе посредством проверки этих сведений на предмет несанкционированного использования. При обнаружении службой подозрительных действий вы получите уведомление по электронной почте. Обратите внимание, что так как это веб-служба, функционирующая только в Интернете, для доступа к компоненту Identity Alert потребуется подключение к Интернету.

Элементы управления диалогового окна

Чтобы перейти из одного раздела диалогового окна в другой, просто щелкните в любом месте панели данной службы. После этого панель станет светло-синего цвета. Данные элементы управления находятся в обеих частях диалогового окна. Их назначение одинаково для обоих компонентов *(Identity Protection u Identity Alert)*.

Включен / Отключен — эта кнопка по внешнему виду и принципу действия напоминает светофор. Щелкните мышью, чтобы переключиться из одного положения в другое. Зеленый цвет соответствует положению ***Включен*** — компонент Identity Protection активен и выполняет все функции. Красный цвет соответствует положению ***Отключен*** — компонент деактивирован. Настоятельно рекомендуется не изменять значения по умолчанию для всех параметров безопасности, если у вас нет веских причин для отключения службы. Параметры по умолчанию гарантируют оптимальную производительность приложения и максимальный уровень безопасности. Если вы по какой-либо причине все же захотите отключить службу, сразу же отобразится красный ***предупреждающий*** знак, сигнализирующий об опасности, и сообщение о том, что защита не является полной. ***Не забудьте как можно скорее включить службу снова!***

Параметры — нажмите эту кнопку, чтобы перейти в интерфейс дополнительных параметров. Другими словами, откроется соответствующее диалоговое окно, где вы сможете настроить параметры компонента Identity Protection. Интерфейс дополнительных параметров позволяет изменить любые параметры служб **AVG Internet Security 2013**, но выполнять подобные действия рекомендуется только опытным пользователям.

Сведения — нажмите эту кнопку, и в нижней части диалогового окна появится краткое описание выделенной службы.

— используйте зеленую стрелку в верхней левой части диалогового окна для возврата к главному интерфейсу пользователя с общими сведениями о компонентах.

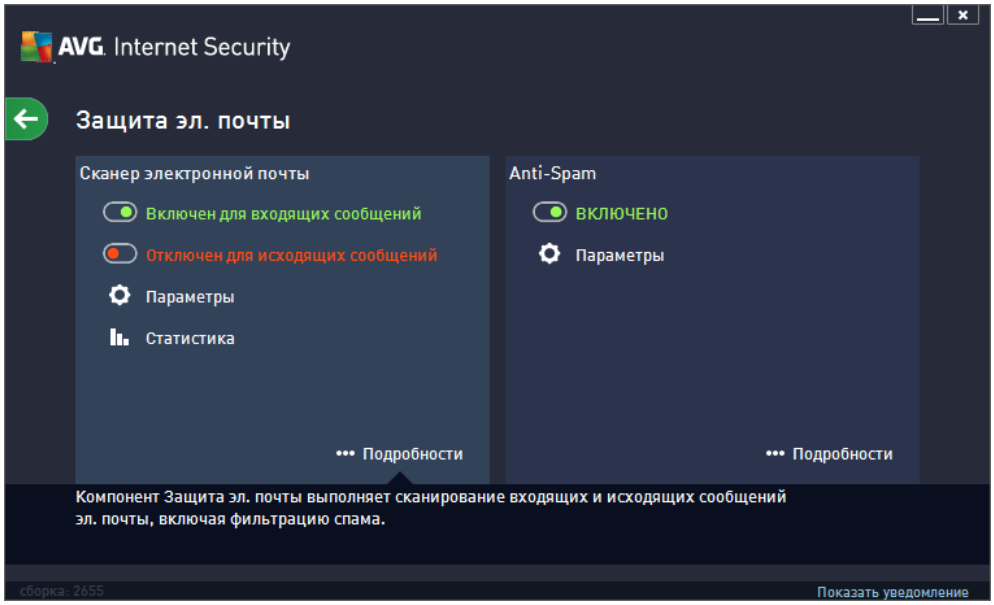
В разделе Identity Alert вы найдете еще одну кнопку — ***Просмотр и настройка учетной записи Identity Alert***. При нажатии этой кнопки откроется веб-страница Identity Alert, где можно выполнить активацию службы.

6.4. Сообщения электронной почты

Компонент ***Защита эл. почты*** включает в себя две защитные службы: ***сканер электронной почты*** и ***Anti-Spam***.

- ***Сканер электронной почты***. Электронная почта — один из основных источников вирусов и троянских программ. Фишинг и спам делают электронную почту еще более опасным источником угроз. Как правило, вредоносные сообщения электронной почты получают владельцы бесплатных учетных записей электронной почты *(так как в них редко используются технологии защиты от спама)*. Несмотря на это, домашние пользователи полностью полагаются на такую электронную почту. При этом домашние пользователи, посещающие неизвестные веб-сайты и заполняющие интерактивные формы личными сведениями *(например, своими адресами электронной почты)*, особенно подвержены атакам по электронной почте. Компании обычно используют корпоративные учетные записи и применяют фильтры нежелательных сообщений электронной почты. Компонент «Защита эл. почты» предназначен для сканирования всех входящих и исходящих сообщений электронной почты; при обнаружении вируса в сообщении электронной почты он сразу же перемещается в Хранилище вирусов. Данный компонент также может фильтровать определенные типы вложений электронной почты и добавлять текст сертификации в безопасные сообщения. ***Компонент «Сканер электронной почты» не предназначен для использования на серверных платформах.***

- ***Компонент Anti-Spam*** проверяет всю входящую электронную почту и помечает нежелательные сообщения как спам *(спамом называют нежелательную почту, в большинстве случаев рекламного характера, массово рассылаемую большому числу адресатов одновременно, которая заполняет почтовые ящики получателей. Спам не является законной коммерческой рассылкой, на которую пользователи давали свое согласие.)*. Компонент Anti-Spam может изменять тему сообщения электронной почты *(помеченного как спам)*, добавляя специальную текстовую строку. Таким образом можно легко фильтровать сообщения электронной почты в почтовом клиенте. Компонент Anti-Spam использует несколько способов анализа для обработки каждого сообщения электронной почты, обеспечивая максимальную защиту от спама. Компонент Anti-Spam использует регулярно обновляемую базу данных для определения спама. Также можно использовать RBL-серверы *(общие базы данных адресов электронной почты «известных распространителей спама»)* и добавить вручную адреса электронной почты в Белый список *(никогда не помечать как спам)* и Черный список *(всегда помечать как спам)*.



Элементы управления диалогового окна

Чтобы перейти из одного раздела диалогового окна в другой, просто щелкните в любом месте панели данной службы. После этого панель станет светло-синего цвета. Данные элементы управления находятся в обеих частях диалогового окна. Их назначение одинаково для обеих служб *(Сканера электронной почты и Anti-Spam)*.

Включен / Отключен — эта кнопка по внешнему виду и принципу действия напоминает светофор. Щелкните мышью, чтобы переключиться из одного положения в другое. Зеленый цвет соответствует положению ***Включен*** — защитная служба активна и выполняет все функции. Красный цвет соответствует положению ***Отключен*** — компонент деактивирован. Настоятельно рекомендуется не изменять значения по умолчанию для всех параметров безопасности, если у вас нет веских причин для отключения службы. Параметры по умолчанию гарантируют оптимальную производительность приложения и максимальный уровень безопасности. Если вы по какой-либо причине все же захотите отключить службу, сразу же отобразится красный ***предупреждающий*** знак, сигнализирующий об опасности, и сообщение о том, что защита не является полной. ***Не забудьте как можно скорее включить службу снова!***

В разделе «Сканер электронной почты» имеется две кнопки, напоминающие светофор. С их помощью можно указать, будет ли сканер электронной почты проверять входящую, исходящую почту или и ту, и другую. По умолчанию включено сканирование только входящих сообщений, так как риск заражения исходящей почты невелик.

Параметры — нажмите эту кнопку, чтобы перейти в интерфейс дополнительных параметров. Другими словами, откроется соответствующее диалоговое окно, где вы сможете настроить параметры Сканера электронной почты или Anti-Spam. Интерфейс дополнительных параметров позволяет изменить любые параметры служб **AVG Internet Security 2013** , но выполнять подобные действия рекомендуется только опытным пользователям.

Статистические данные — нажмите эту кнопку, чтобы перейти на соответствующую страницу веб-сайта AVG (http://www.avg.com/). На этой странице можно посмотреть подробный статистический обзор всех действий **AVG Internet Security 2013**, выполненных на вашем компьютере за определенный промежуток времени или за все время.

Сведения — нажмите эту кнопку, и в нижней части диалогового окна появится краткое описание выделенной службы.

— используйте зеленую стрелку в верхней левой части диалогового окна для возврата к главному интерфейсу пользователя с общими сведениями о компонентах.

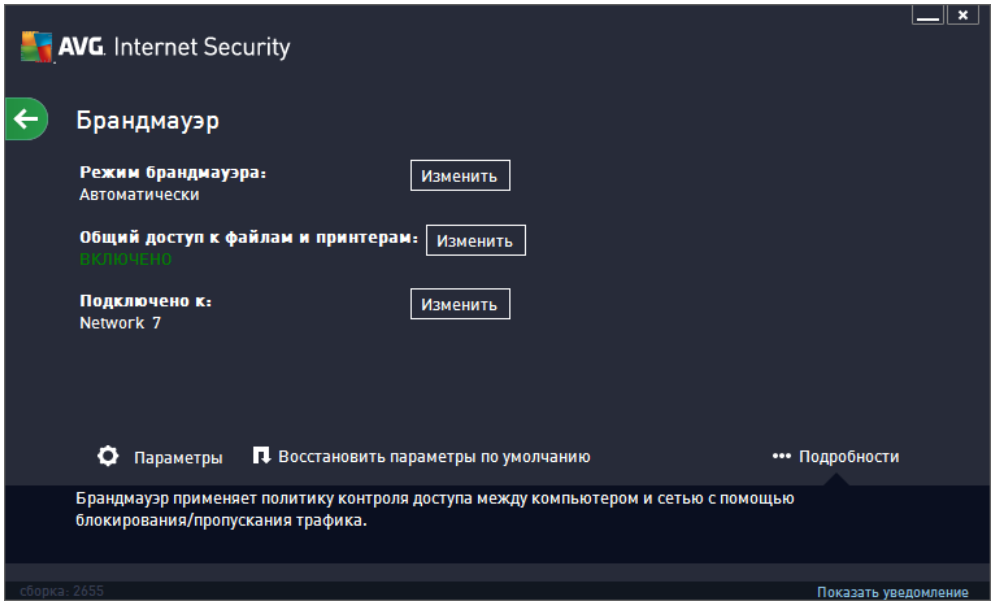
6.5. Firewall

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 блокировано. При обнаружении попыток взлома Firewall «блокирует» данную попытку и не позволяет взломщику получить доступ к компьютеру. Firewall настроен для разрешения или блокировки внешнего или 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 блокирована. 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 отдельных компьютеров от атак, исходящих от внутренних пользователей других компьютеров в сети.

В программе **AVG Internet Security 2013** ***Firewall*** контролирует весь трафик на каждом сетевом порте компьютера. На основе установленных правил 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 Firewall)*, Firewall отображает запрос на разрешение или блокировку попытки обмена данными.

AVG Firewall не предназначен для защиты серверных платформ.

Рекомендации. *В общем случае не рекомендуется использовать на одном компьютере более одного брандмауэра. 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.*



Доступные режимы Firewall

С помощью Firewall можно установить специальные правила безопасности, основанные на том, является ли компьютер частью домена, автономным компьютером или ноутбуком. Для каждого варианта требуется определенный уровень защиты, который обеспечивается в соответствующих режимах. Другими словами, режим Firewall — это особая его конфигурация. Можно использовать несколько предопределенных конфигураций.

- ***Автоматически*** — в этом режиме Firewall применяет параметры автоматически ко всему сетевому трафику. Вам не будет предложено никаких действий. Firewall разрешит подключение со стороны всех известных приложений. Одновременно будет создано правило, разрешающее данному приложение подключаться в будущем. Для прочих приложений Firewall определит, блокировать или разрешать подключение, в соответствии с поведением данных приложений. В этом случае, однако, правило не будет создано, и приложение будет проходить проверку при каждой попытке подключения. Автоматический режим ведет себя достаточно ненавязчиво и рекомендуется для большинства пользователей.

- ***Интерактивный*** — этот режим подходит, если на компьютере нужно полностью контролировать входящий и исходящий сетевой трафик. Firewall будет отслеживать трафик и информировать вас о каждой попытке подключения или передачи данных. При необходимости вы сможете разрешить или заблокировать это действие. Рекомендуется только для опытных пользователей.

- ***Заблокировать доступ в Интернет*** — полная блокировка подключения к Интернету. Нельзя войти в Интернет, доступ к компьютеру извне невозможен. Рекомендуется только в особых случаях и на короткое время.

- ***Отключить Firewall*** — это действие разрешит компьютеру обмен данными по сети. Следовательно, компьютер станет уязвим для атак злоумышленников. Всегда используйте этот параметр с осторожностью.

Обратите внимание, что в Firewall также есть особый автоматический режим. Этот режим активируется автоматически при отключении компонентов Компьютер или Identity protection, вследствие чего компьютер становится боле уязвимым. В таких случаях Firewall будет разрешать подключение со стороны только известных и абсолютно безопасных приложений. Для всех остальных приложений вам будет предложено действие. Эта мера призвана компенсировать отключенные компоненты защиты и тем самым обеспечить безопасность компьютера.

Элементы управления диалогового окна

В данном диалоговом окне даны общие сведения о состоянии компонента Firewall.

- ***Режим Firewall*** — информация об установленном в данное время режиме компонента Firewall. С помощью кнопки ***Изменить***, которая находится рядом с предоставленной информацией, можно войти в интерфейс Параметры Firewall и сменить текущий режим на другой *(описание и советы относительно использования профилей Firewall см. в предыдущем пункте)*.

- ***Общий доступ к файлам и принтерам*** — информирует о возможности доступа к файлам и принтерам *(в обоих направлениях)* в данное время. Предоставить общий доступ к файлам и принтерам означает открыть доступ ко всем файлам и папкам, которые в Windows помечены как «Общие», общие разделы диска, принтеры, сканеры и прочие подобные устройства. Желательно предоставлять общий доступ к таким элементам только в безопасных сетях *(например, домашних сетях, сетях предприятий и учебных заведений)*. Однако если вы подключаетесь к общедоступной сети *(например, к сети Wi-Fi в аэропорту или интернет-кафе)*, предоставлять общий доступ не следует.

- ***Название подключения*** — отображает название сети, к которой вы в данное время подключены. В Windows XP название сети соответствует наименованию, выбранному вами при первом подключении к данной сети. Для Windows Vista и более поздних версий название сети автоматически назначается центром управления сетями и общим доступом.

В диалоговом окне содержатся такие элементы управления.

Изменить — с помощью этой кнопки можно изменить значение того или иного параметра. Подробнее о том, как следует выполнять изменение, читайте в описании соответствующих параметров выше.

Параметры — нажмите на эту кнопку, чтобы перейти в интерфейс Параметры Firewall, где можно изменить конфигурацию Firewall. Любые изменения параметров должны выполнять только опытные пользователи.

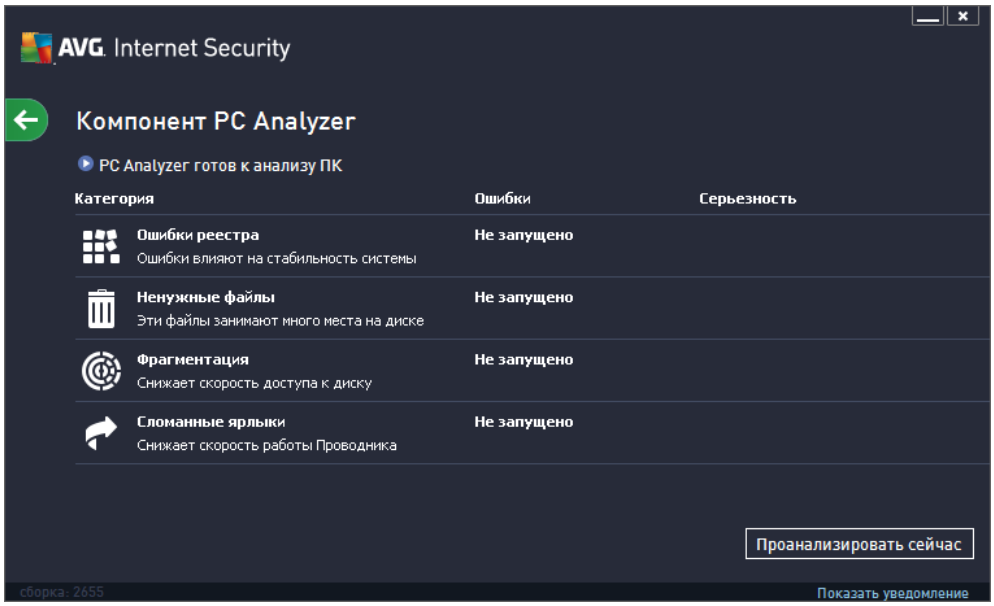
Восстановить значения по умолчанию — нажмите данную кнопку, чтобы сбросить текущую конфигурацию Firewall и восстановить конфигурацию по умолчанию на основе автоматического обнаружения.

Сведения — нажмите эту кнопку, и в нижней части диалогового окна появится краткое описание выделенной службы.

— используйте зеленую стрелку в верхней левой части диалогового окна для возврата к главному интерфейсу пользователя с общими сведениями о компонентах.

6.6. PC Analyzer

Компонент ***PC Analyzer*** предназначен для сканирования компьютера на наличие системных проблем и предоставления пользователю сведений о возможных причинах снижения общей производительности компьютера:



В интерфейсе пользователя компонента отображается таблица, разделенная на четыре строки, относящиеся к соответствующим категориям. ошибки реестра, ненужные файлы, фрагментация и неработающие ярлыки.

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

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

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

Кнопки управления

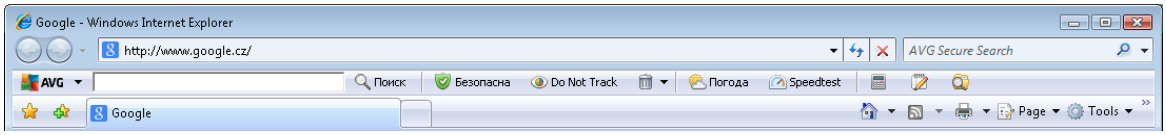
- ***Проанализировать сейчас*** (*отображается до запуска анализа*) — нажмите данную кнопку, чтобы немедленно запустить анализ компьютера.

- ***Исправить*** (*отображается по завершении анализа*) — нажмите данную кнопку, чтобы перейти на страницу веб-сайта компании AVG (http://www.avg.com/), на которой подробно представлены последние сведения о компоненте ***PC Analyzer***.

- ***Отмена*** — нажмите данную кнопку, чтобы остановить выполнение анализа или вернуться к главному диалоговому окну AVG по умолчанию (*Обзор компонентов*) по завершении анализа.

7. Панель безопасности AVG

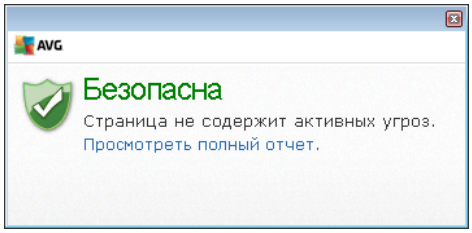
Панель безопасности AVG — это инструмент, активно взаимодействующий с компонентом LinkScanner Surf-Shield и обеспечивающий максимальную защиту во время работы в Интернете. В программе **AVG Internet Security 2013** установка ***Панели безопасности AVG*** является дополнительным параметром. В процессе установки предлагается принять решение о необходимости установки данного компонента. ***Панель безопасности AVG*** встраивается непосредственно в Интернет-браузер. В настоящее время поддерживаются такие Интернет-браузеры: Internet Explorer (*6.0 и более поздних версий*) и/или Mozilla Firefox (*3.0 и более поздних версий*). Другие браузеры не поддерживаются. *При использовании другого интернет-браузера, например Avant, могут возникать неожиданные ошибки.*



Панель безопасности AVG включает в себя следующие элементы.

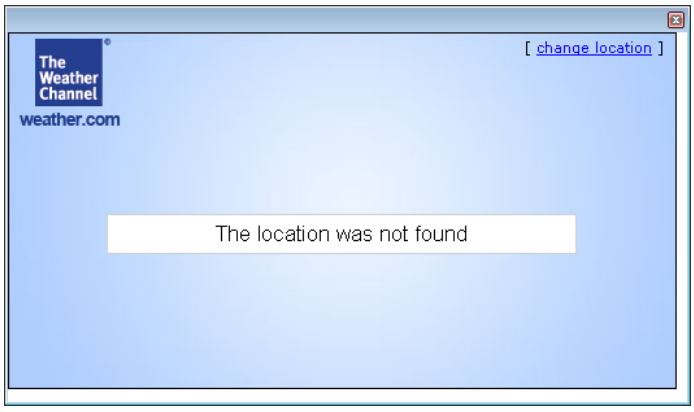
- ***Логотип AVG*** с раскрывающимся меню.
  - ***Использовать безопасный поиск AVG***. Позволяет выполнять поиск непосредственно в ***Панели безопасности AVG*** с помощью поисковой системы ***Безопасный поиск AVG***.
  - ***Текущий уровень угрозы*** — открытие веб-страницы лаборатории вирусов с графическим отображением текущего уровня угроз в Интернете.
  - ***AVG Threat Labs*** — предоставляет доступ к специальному веб-сайту ***Лаборатории угроз AVG*** *(по адресу http://www.avgthreatlabs.com)*, который содержит информацию о безопасности различных веб-сайтов и текущем уровне угроз в Интернете.
  - ***Справка по панели инструментов*** — открывает интерактивную справку, охватывающую все функции ***панели безопасности AVG***.
  - ***Отправить отзыв о продукте*** — открывает веб-страницы с формой, заполнив которую, можно поделиться мнением по поводу использования ***Панели безопасности AVG***.
  - ***Удалить Панель безопасности AVG*** — открывает веб-страницу с детальным описанием процесса деактивации ***Панели безопасности AVG*** для каждого из поддерживаемых веб-браузеров.
  - ***О программе...*** — открывает новое окно с информацией о текущей версии установленной ***Панели безопасности AVG***.
- ***Поле поиска*** — позволяет выполнять поиск в Интернете с помощью ***Панели безопасности AVG*** и быть абсолютно уверенным в максимальной безопасности его результатов. Введите слово или фразу в поле поиска и нажмите кнопку ***Поиск*** *(или клавишу Enter)*.
- ***Безопасность сайта*** — эта кнопка открывает новое диалоговое окно с информацией

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



- ***Удалить*** — кнопка с изображением корзины открывает меню, где можно выбрать элементы для удаления: сведения о просмотре веб-страниц, загрузках, онлайновых формах или весь архив поиска.

- ***Погода*** — нажатие этой кнопки открывает новое диалоговое окно с информацией о текущей погоде в вашем регионе и прогнозом на ближайшие два дня. Эта информация обновляется регулярно каждые 3—6 часов. В данном диалоговом окне можно вручную изменить регион и выбрать отображение температуры по Цельсию или по Фаренгейту.



- ***Facebook***. Эта кнопка позволяют подключиться к социальной сети Facebook непосредственно из ***Панели безопасности AVG***.

- ***Проверка скорости*** — эта кнопка открывает онлайн-приложение, с помощью которого можно определить качество вашего подключения к Интернету *(тест ping)* и скорость загрузки и отправки.

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

8. AVG Do Not Track

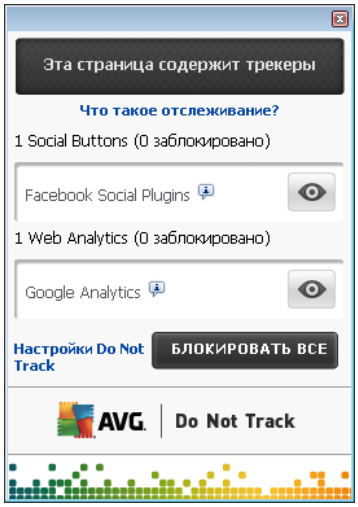
AVG Do Not Track помогает распознавать веб-сайты, которые собирают сведения о ваших действиях в Интернете. С помощью значка в браузере можно узнать, какие веб-сайты и рекламодатели пытаются собирать сведения о ваших действиях и соответственно, разрешить или запретить подобные действия.

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

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

8.1. Интерфейс AVG Do Not Track

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



Все доступные службы сбора данных перечислены в обзоре ***Трекеры на этой странице***.

AVG Do Not Track поддерживает три метода сбора данных.

- ***Веб-аналитика*** *(разрешен по умолчанию):* службы, используемые для улучшения производительности и удобства работы соответствующего веб-сайта. К этой категории относятся такие службы, как Google Analytics, Omniture и Yahoo Analytics. Мы не рекомендуем блокировать службы веб-аналитики, так как это может привести к неправильной работе веб-сайта.

- ***Кнопки социальных сетей*** *(разрешен по умолчанию):* элементы, разработанные для улучшенной работы в социальных сетях. Кнопки социальных сетей служат для выхода в социальные сети с сайта, на котором вы находитесь. Они позволяют собирать сведения о ваших действиях, если вы в сети. Примеры кнопок социальных сетей: социальные плагины Facebook, кнопки Twitter, Google +1.

- ***Рекламные сети*** *(некоторые из них по умолчанию заблокированы):* службы, которые прямо или косвенно собирают или сообщают данные о ваших действиях в сети и размещают персонализированную рекламную информацию (в отличие от тематического размещения рекламы). Это определяется политиками конфиденциальности конкретных рекламных сетей, с которыми можно ознакомиться на их сайтах. Некоторые рекламные сети по умолчанию заблокированы.

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

В диалоговом окне также есть две гиперссылки:

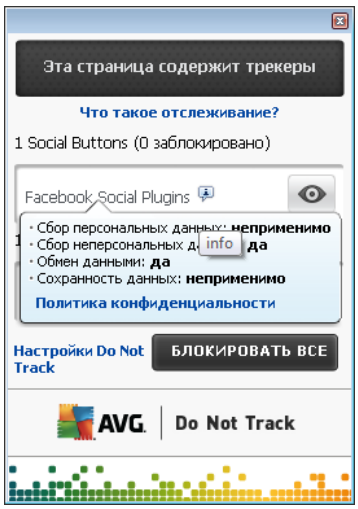
- ***Что такое отслеживание?*** — нажмите на ссылку в верхней части диалогового окна, чтобы перейти на веб-страницу, где детально описаны принципы отслеживания и его конкретные типы.

- ***Настройки*** — нажмите ссылку в нижней части диалогового окна, чтобы перейти на веб-страницу, где можно выбрать конкретную конфигурацию параметров ***AVG Do Not Track*** *(подробную информацию можно найти в разделе Настройки AVG Do Not Track)*

8.2. Информация о следящих процессах

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

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

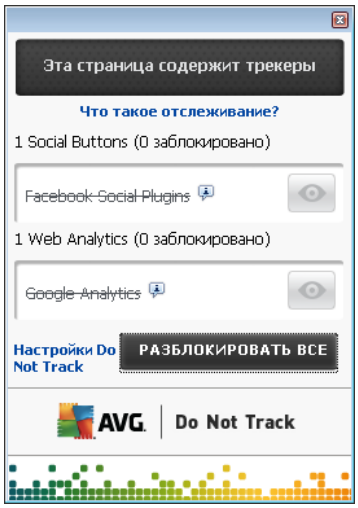


8.3. Блокировка следящих процессов

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

- ***Заблокировать все*** — нажмите эту кнопку, расположенную в нижней области диалогового окна: любые попытки сбора данных будут блокироваться. *(Однако, следует помнить, что это действие может вызвать сбой в работе соответствующей страницы, если служба запущена.)*

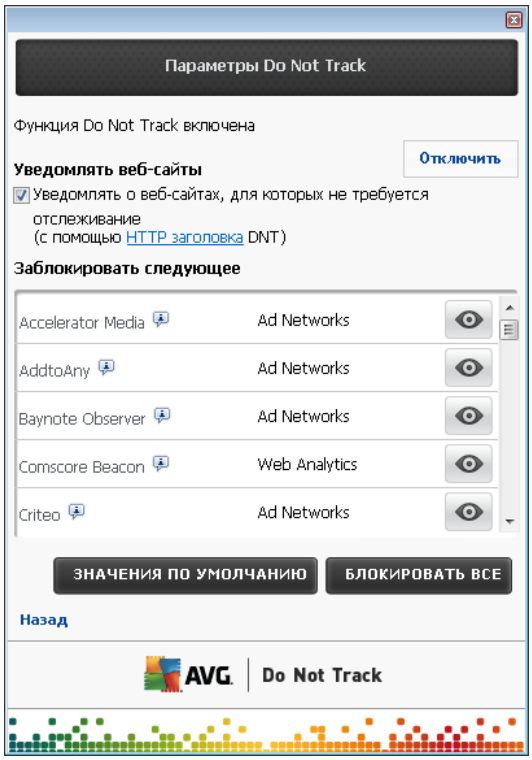
- — если блокировать все обнаруженные службы не требуется, можно для каждой службы указать, следует ли ее разрешить или заблокировать. Можно разрешить функционирование некоторых обнаруженных систем *(например, средств веб-аналитики):* эти системы используют собранные данные для оптимизации своих веб-сайтов, совершенствуя тем самым интернет-среду для всех пользователей. В то же время можно заблокировать попытки сбора данных со стороны процессов, которые относятся к рекламным сетям. Просто щелкните значок рядом с соответствующим процессом, чтобы заблокировать сбор данных *(имя процесса отобразится перечеркнутым)* или снова разрешить их сбор.



8.4. Настройки AVG Do Not Track

Непосредственно в диалоговом окне ***AVG Do Not Track*** есть только один параметр конфигурации: в нижней области находится флажок ***Предупреждать меня при обнаружении активных трекеров.*** . По умолчанию этот параметр выключен. Установите флажок, чтобы подтвердить, что необходимо отображать уведомление каждый раз при посещении веб-страницы, содержащей новый процесс отслеживания, который еще не блокировался. Если флажок установлен, в случае обнаружения функцией ***AVG Do Not Track*** новой системы отслеживания на веб-странице, посещаемой в данный момент, на экране отобразится диалоговое окно уведомления. Если флажок не установлен, вы сможете узнать о недавно обнаруженной службе только с помощью значка ***AVG Do Not Track*** *(размещенного в командной строке браузера)*, который изменит цвет с зеленого на желтый.

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



Уведомлять

- ***Положение уведомления*** *(по умолчанию в правой верхней области).* Откройте раскрывающееся меню, чтобы указать, в каком положении нужно отображать на мониторе диалоговое окно ***AVG Do Not Track***.

- ***Отображать уведомление*** *(по умолчанию — 10).* В этом поле нужно выбрать период *(в секундах)* отображения на экране уведомления ***AVG Do Not Track***. Можно указать от 0 до 60 секунд *(если указать 0, то уведомление на экране не отобразится)*.

- ***Предупреждать меня при обнаружении активных трекеров*** *(по умолчанию выключено).* Установите флажок, чтобы подтвердить, что необходимо отображать уведомление при каждом посещении веб-страницы, содержащей новую службу сбора данных, которая еще не блокировалась. Если флажок установлен, в случае обнаружения функцией ***AVG Do Not Track*** новой системы отслеживания на веб-странице, посещаемой в данный момент, на экране отобразится диалоговое окно уведомления. Если флажок не установлен, вы сможете узнать о недавно обнаруженной службе только с помощью значка ***AVG Do Not Track*** *(размещенного в командной строке браузера)*, который изменит цвет с зеленого на желтый.

- ***Уведомлять веб-сайты, что отслеживание нежелательно*** *(по умолчанию включено).* Не выключайте этот параметр, чтобы подтвердить, что функция ***AVG Do Not Track*** должна информировать провайдера обнаруженной службы сбора данных о том, что отслеживание нежелательно.

Заблокировать следующее

В данном разделе есть окно со списком известных служб, занимающихся сбором данных, которые относятся к категории рекламных сетей. По умолчанию ***AVG Do Not Track*** автоматически блокирует некоторые рекламные сети, а решение о том, нужно ли блокировать остальные, принимаете вы сами. Для этого просто нажмите кнопку ***Заблокировать все*** под списком.

Кнопки управления

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

- ***Заблокировать все*** — блокирует все службы, перечисленные в указанном выше поле, которые классифицируются как рекламные сети;

- ***Разрешить все*** — отменяет блокировку всех заблокированных ранее служб, перечисленных в указанном выше поле, которые классифицируются как рекламные сети;

- ***По умолчанию*** — сброс всех пользовательских настроек и возврат к параметрам по умолчанию;

- ***Сохранить*** — нажмите, чтобы применить и сохранить все указанные настройки;

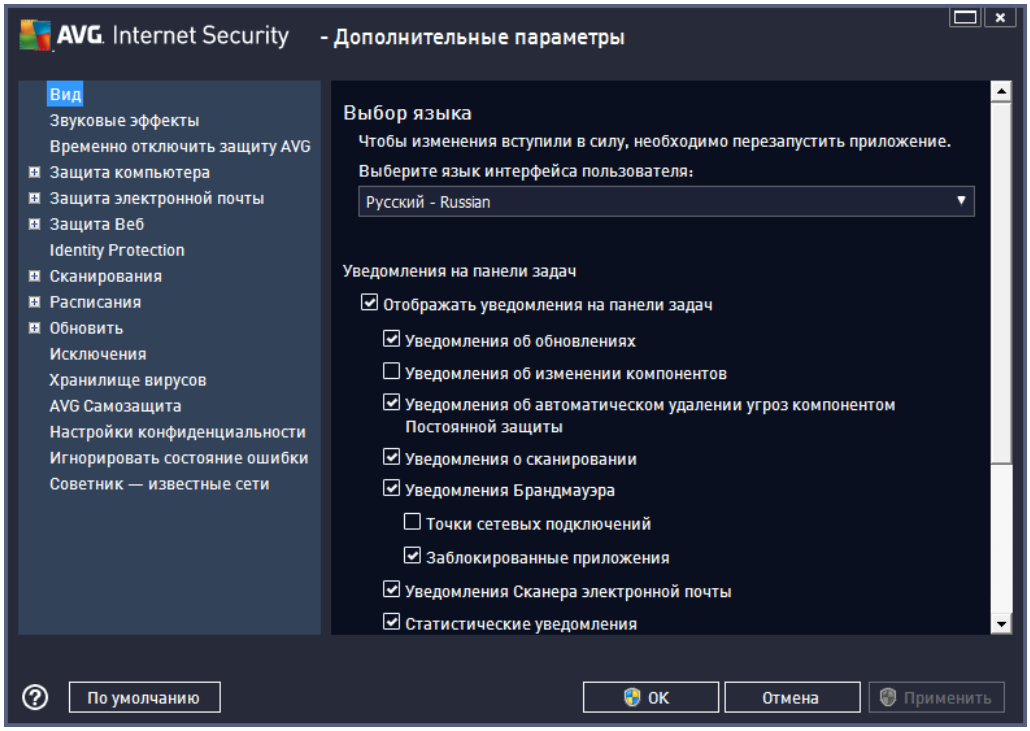
- ***Отмена*** — отмена всех ранее указанных настроек.

9. Расширенные настройки AVG

Параметры дополнительной настройки **AVG Internet Security 2013** 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 его часть*), чтобы открыть диалоговое окно редактирования в правой части окна.

9.1. Внешний вид

Параметр ***Вид***, первый элемент дерева навигации, относится к общим параметрам интерфейса пользователя **AVG Internet Security 2013** и нескольким начальным параметрам поведения приложения.



Выбор языка

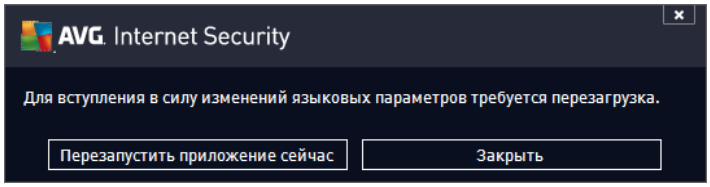
В раскрывающемся меню раздела ***Выбор языка*** можно выбрать необходимый язык. После этого интерфейс пользователя **AVG Internet Security 2013** будет отображаться на выбранном языке. В раскрывающемся меню предлагаются только те языки, которые были выбраны в процессе установки, а также английский (*он устанавливается автоматически, по умолчанию*). Чтобы завершить процесс изменения языка **AVG Internet Security 2013**, необходимо перезапустить приложение. Выполните данные шаги:

- В раскрывающемся меню выберите язык установки.
- Подтвердите свой выбор, нажав кнопку ***Применить*** *(в правом нижнем углу диалогового окна).*

- Для подтверждения нажмите кнопку ***ОК***

- Откроется новое диалоговое окно, информирующее о том, что для изменения языка приложения требуется перезагрузка. **AVG Internet Security 2013**

- Нажмите кнопку ***Перезапустить приложение сейчас***, чтобы подтвердить перезапуск программы, и подождите несколько секунд для вступления в силу изменений языковых параметров.



Уведомления на панели задач

В данном разделе можно отключить отображение на панели задач уведомлений о состоянии приложения **AVG Internet Security 2013**. По умолчанию отображение системных уведомлений включено. Настоятельно рекомендуется не изменять данный параметр. Системные уведомления сигнализируют о таких событиях, как запуск процесса обновления, сканирования или изменение состояния компонента **AVG Internet Security 2013**. Необходимо обращать внимание на эти уведомления.

Однако, если по какой-либо причине необходимо отключить данные уведомления или настроить отображение только определенных уведомлений *(связанных с определенным компонентом AVG Internet Security 2013)*, то это можно сделать, установив или сняв флажки соответствующих параметров.

- ***Отображать уведомления на панели задач*** *(по умолчанию включено)* — по умолчанию отображаются все уведомления. Снимите флажок с данного параметра, чтобы отключить отображение всех системных уведомлений. Если данный параметр включен, можно настроить отображение отдельных уведомлений.

    - ***Отображать уведомления об обновлении*** *(по умолчанию включено)* — позволяет определить, должна ли отображаться информация о запуске процесса обновления **AVG Internet Security 2013**, его состоянии и завершении.

    - ***Отображать уведомления об изменении состояния компонентов*** *(по умолчанию выключено)* — позволяет определить, должна ли отображаться информация об активности или бездействии компонента или о его потенциальных проблемах. Этот параметр, уведомляющий пользователя о состоянии ошибки компонента, является эквивалентом значка на панели задач, который информирует о проблеме, связанной с определенным компонентом **AVG Internet Security 2013**.

    - ***Отображать уведомления компонента «Постоянная защита» на панели задач (выполняется автоматически)*** *(по умолчанию включено)* — определяет, должна ли отображаться информация о процессах сохранения, копирования и открытия файлов (*такая конфигурация доступна только в том случае, функция автоматического лечения компонента «Постоянная*

защита» включена).

- ***Отображать уведомления о сканировании*** на панели задач *(по умолчанию включено)* — определяет, должны ли отображаться сведения об автоматическом запуске запланированного сканирования, его состоянии и результатах.

- ***Отображать уведомления Firewall на панели задач*** *(по умолчанию включено)* — позволяет определить, должна ли отображаться информация о состоянии и процессах брандмауэра (предупреждения об активации и деактивации компонента, возможной блокировке трафика и т. п.). Данный элемент также содержит два дополнительных параметра выбора *(подробные описания для каждого из них смотрите в разделе Firewall данного документа)*.

  - ***Отображать уведомления об изменении профиля*** *(по умолчанию включено)* — уведомляет об автоматическом изменении профилей компонента Firewall.

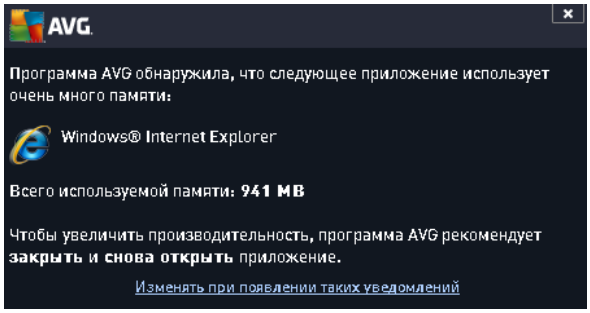
  - ***Отображать уведомления о новых созданных правилах приложений*** *(по умолчанию выключено)* — уведомляет об автоматическом создании компонентом Firewall правил для новых приложений из списка безопасных.

- ***Отображать уведомления компонента Сканер электронной почты на панели задач*** *(по умолчанию включено)* — позволяет определить, должна ли отображаться информация о результатах сканирования всех входящих и исходящих сообщений электронной почты.

- ***Отображать статистические уведомления*** *(по умолчанию включено)* — не снимайте этот флажок, чтобы на панели задач отображались уведомления о регулярных статистических обзорах.

- ***Отображать уведомления AVG Accelerator в области уведомлений*** *(по умолчанию включено)* — позволяет определить, должна ли отображаться информация о действиях ***ускорителя AVG***. ***AVG Accelerator*** обеспечивает более стабильное воспроизведение видеороликов в Интернете, а также ускоряет процессы загрузки.

- ***Отображать уведомления Советника AVG*** *(по умолчанию включено)* — позволяет определить, будет ли отображаться информация о действиях Советника AVG в виде всплывающих окон на панели задач.

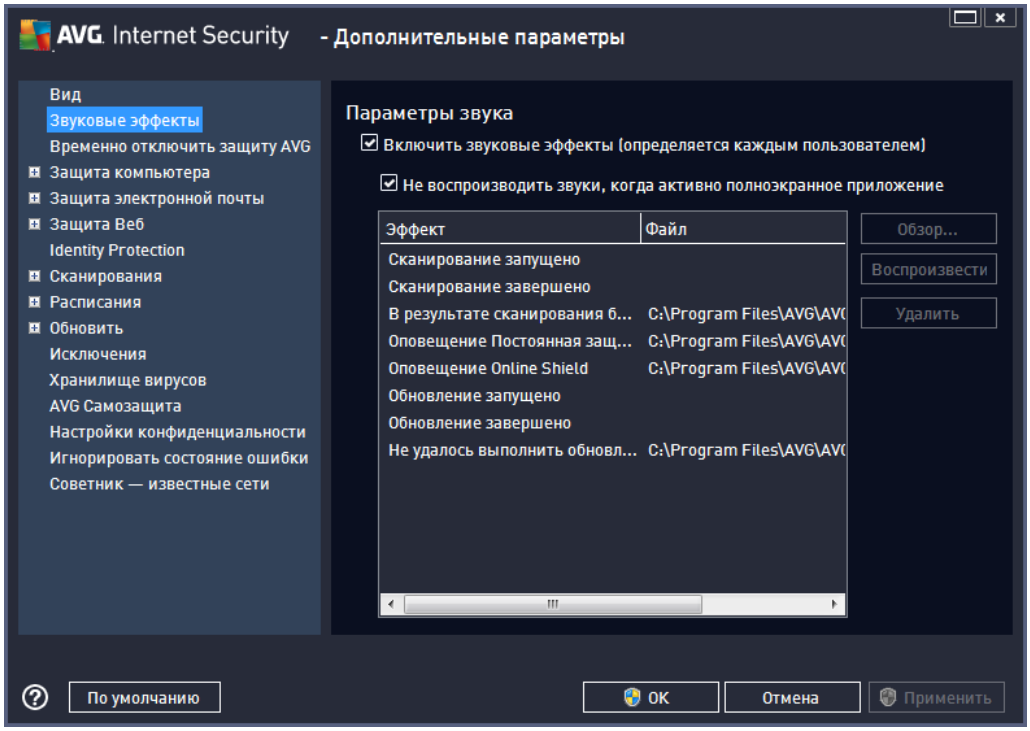


Режим «Во время игры»

Эта функция системы AVG предназначена для полноэкранных приложений, в случае если 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*** (*значение по умолчанию*).

9.2. Звуки

В диалоговом окне ***Звуки*** можно выбрать звуковое уведомление для определенных действий программы **AVG Internet Security 2013**.



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

Кнопки управления

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

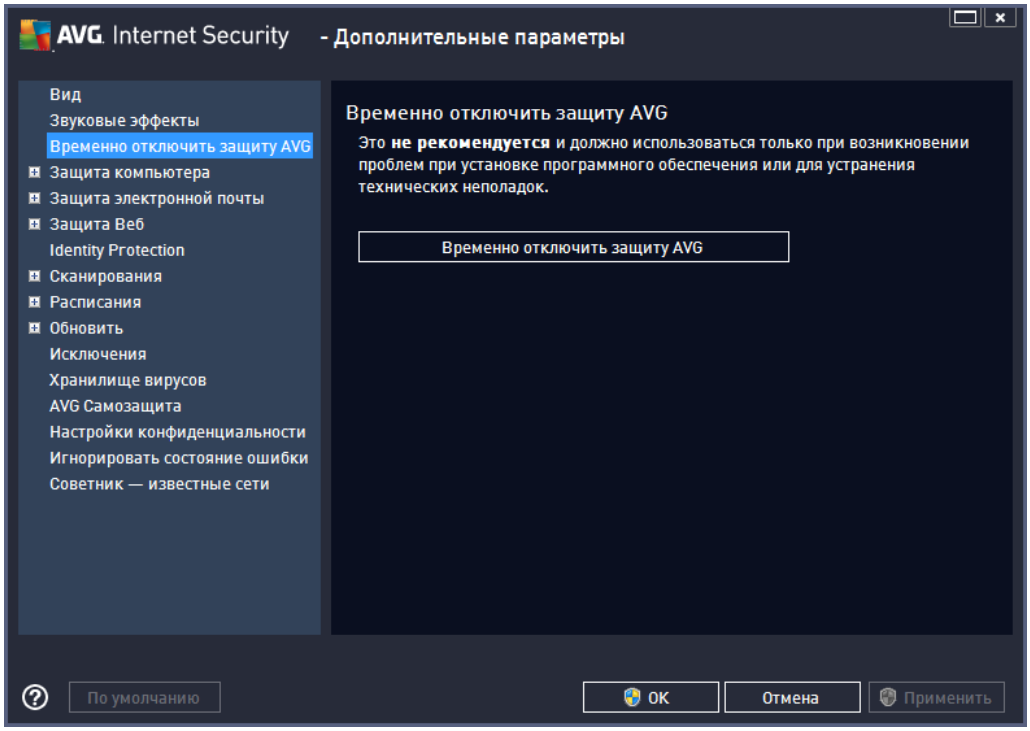
списке и нажмите кнопку ***Воспроизвести***.

- ***Удалить*** — чтобы удалить звук, назначенный для определенного события, нажмите кнопку ***Удалить***.

9.3. Временно отключить защиту AVG

В диалоговом окне ***Временно отключить защиту AVG*** можно полностью выключить защиту, обеспечиваемую программой **AVG Internet Security 2013**.

Используйте этот параметр только в случае крайней необходимости!

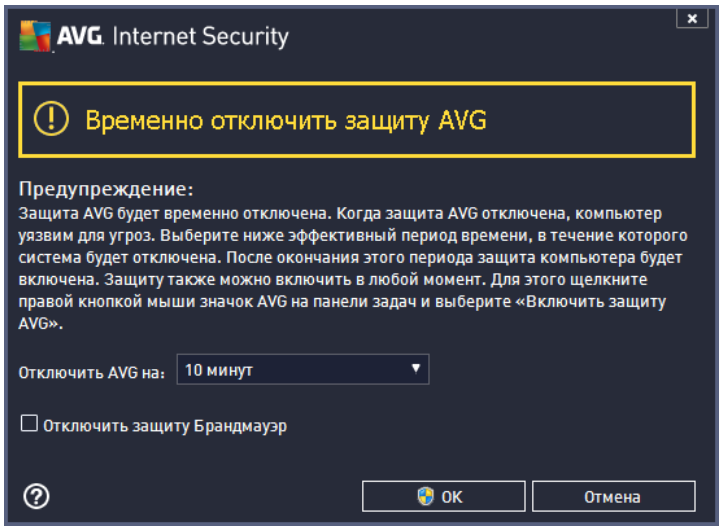


В большинстве случаев программу **AVG Internet Security 2013** ***не рекомендуется*** отключать перед установкой нового ПО или драйверов, даже если программа или мастер установки рекомендует завершить все запущенные программы и приложения, чтобы они не препятствовали процессу установки. Если во время установки возникли проблемы, попробуйте сначала отключить постоянную защиту (*Включить Resident Shield*). Если вам пришлось временно отключить защиту **AVG Internet Security 2013**, включите ее, как только завершите установку. Если вы подключены к Интернету или локальной сети, но антивирусное программное обеспечение отключено, ваш компьютер может подвергнуться атакам.

Отключение защиты AVG

Установите флажок ***Временно отключить защиту AVG*** и подтвердите свой выбор нажатием кнопки ***Применить***. В только что открытом окне ***Временно отключить защиту AVG*** укажите, на какой период времени вы собираетесь отключить **AVG Internet Security 2013**

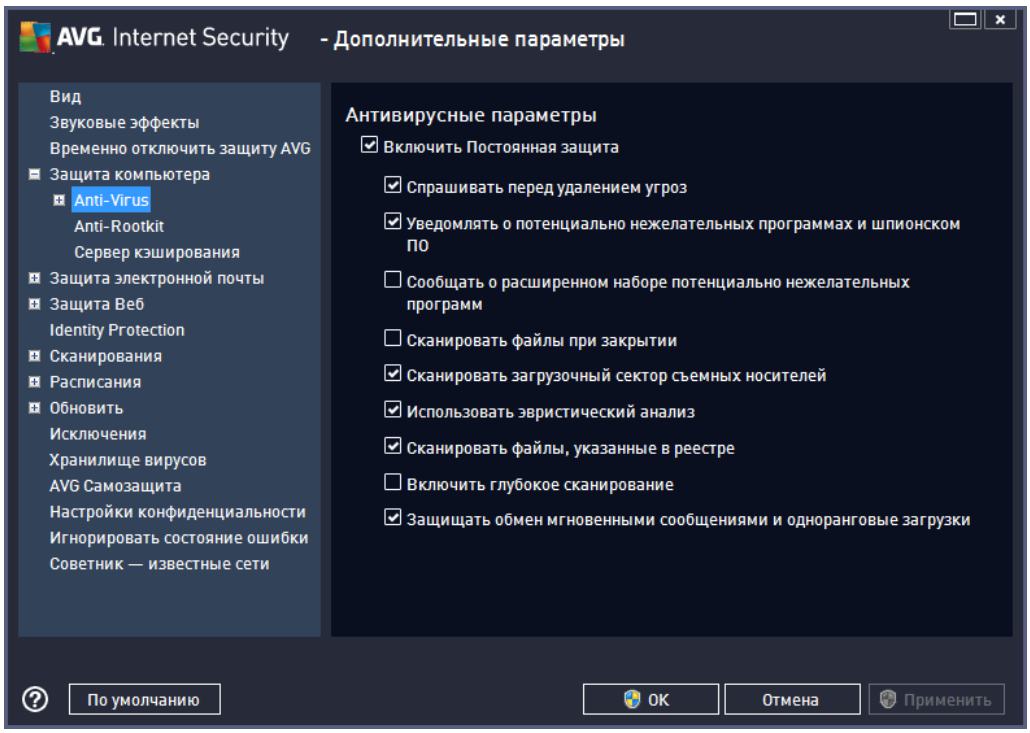
. По умолчанию защита будет отключена в течение 10 минут, чего должно хватить для выполнения наиболее распространенных задач, например установки нового ПО. Можно установить большее время, однако такой вариант рекомендуется лишь в исключительных случаях. По истечению этого времени все отключенные компоненты будут автоматически включены снова. Можно отключать защиту AVG максимум до следующей перезагрузки. Отдельная возможность для отключения компонента ***Firewall*** присутствует в диалоговом окне ***Временно отключить защиту AVG***. Для этого выберите пункт ***Отключить защиту Firewall***.



9.4. Защита компьютера

9.4.1. Anti-Virus

Компонент ***Anti-Virus*** совместно с функцией ***Постоянная защита*** в целом обеспечивает непрерывную защиту компьютера от всех известных разновидностей шпионского и прочего вредоносного ПО *(включая так называемое «спящее» или неактивное вредоносное ПО, т. е. вредоносное ПО, которое загружено, но еще не активировано)*.



В диалоговом окне ***Параметры постоянной защиты*** можно включить или отключить постоянную защиту, установив или сняв флажок параметра ***Включить постоянную защиту*** (*по умолчанию он установлен*). Кроме того, можно активировать следующие отдельные функции постоянной защиты.

- ***Спрашивать перед удалением угроз*** (*по умолчанию включено*) — установите этот флажок, чтобы запретить компоненту «Постоянная защита» автоматически выполнять какие-либо действия. Вместо этого будет отображаться диалоговое окно с описанием обнаруженной угрозы, позволяя пользователю выбрать действие самому. Если не установить флажок, **AVG Internet Security 2013** лечение зараженного объекта выполняется автоматически, а если это невозможно — он переносится в Хранилище вирусов.

- ***Сканировать на наличие следящих файлов cookie*** (*не выбрано по умолчанию*) — этот параметр определяет обнаружение cookie-файлов при сканировании. (*Файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок в Интернете.*)

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** (*по умолчанию включено*) — установите этот флажок, чтобы активировать сканирование 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. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** (*не выбрано по умолчанию*) — установите этот флажок для обнаружения

расширенного набора шпионских программ: это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, дополнительно повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать файлы при закрытии*** (*по умолчанию выключено*) — сканирование программой AVG активных объектов (например, приложений, документов и др.) при открытии, а также при закрытии. Эта функция помогает вам защитить компьютер от некоторых разновидностей самых опасных вирусов.

- ***Сканировать загрузочный сектор съемных носителей*** (*по умолчанию включено*)

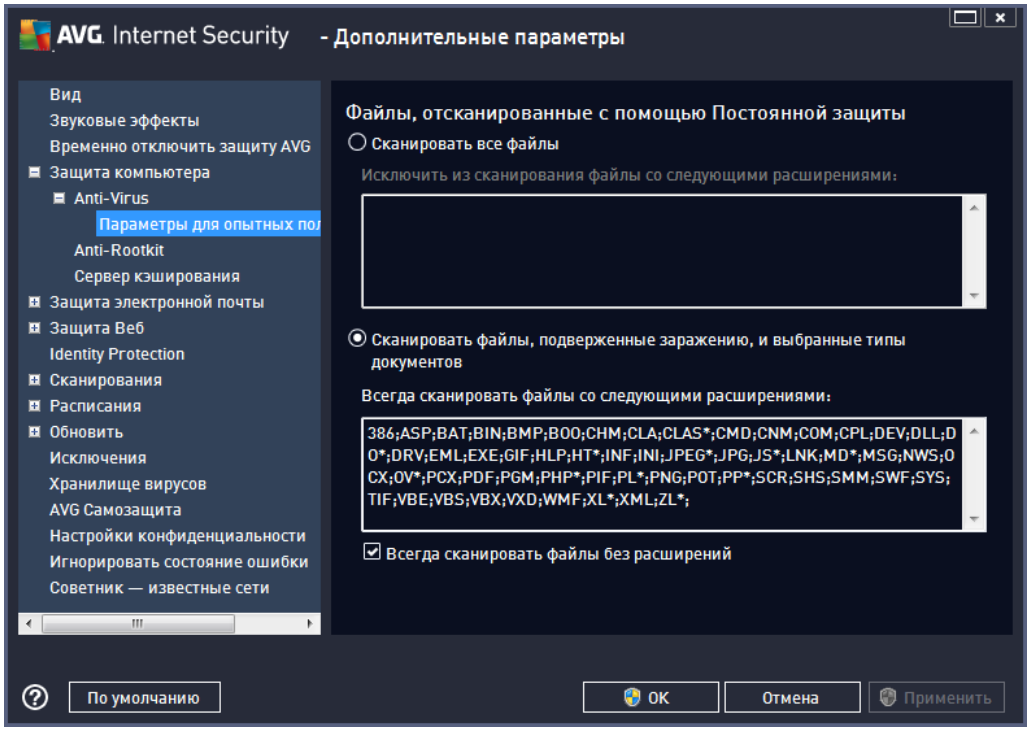
- ***Использовать эвристику*** (*по умолчанию включено*) — для обнаружения будет использован эвристический анализ (*динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде*).

- ***Сканировать файлы, указанные в реестре*** (*выбрано по умолчанию*) — этот параметр определяет, будет ли программа AVG выполнять сканирование всех исполняемых файлов, добавляемых в реестр запуска, во избежание выполнения известных заражений при следующем запуске компьютера.

- ***Включить глубокое сканирование*** (*по умолчанию выключено*) — в определенных случаях (*при крайней необходимости*) установите этот флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые будут углубленно сканировать систему на наличие потенциальных угроз. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

- ***Защищать обмен мгновенными сообщениями и одноранговые загрузки*** (*по умолчанию включено*) — выберите данный параметр, если требуется проверить безопасность обмена мгновенными сообщениями (*например, с помощью AIM, Yahoo!, ICQ, Skype, MSN Messenger и др.*) и данные, загруженные через одноранговые сети *(сети, которые позволяют обмениваться данными напрямую, без помощи сервера. Подобные сети потенциально опасны и, как правило, используются для передачи музыкальных файлов)*.

В диалоговом окне ***Файлы, сканируемые с помощью компонента «Постоянная защита»*** , можно указать файлы, которые необходимо сканировать (*по определенным расширениям*).

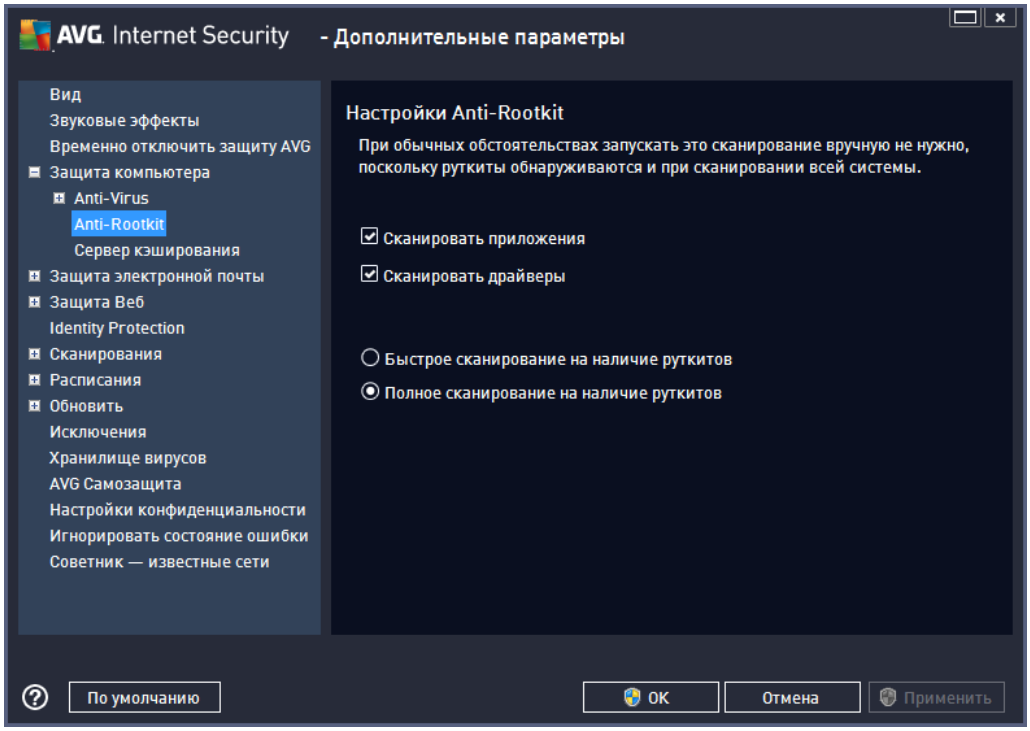


Установите соответствующий флажок для выбора режима сканирования: ***Сканировать все файлы*** или ***Сканировать файлы, подверженные заражению, и документы выбранных типов***. Чтобы ускорить сканирование и в то же время обеспечить максимальную безопасность, рекомендуется сохранить настройки по умолчанию. В этом случае будут сканироваться только зараженные файлы. В соответствующих разделах диалогового окна вы также найдете редактируемый список расширений, в котором перечислены типы файлов, которые будут сканироваться.

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

9.4.2. Anti-Rootkit

Диалоговое окно ***Параметры Anti-Rootkit*** позволяет изменять конфигурацию служб ***Anti-Rootkit*** и определенные настройки сканирования на наличие руткитов. Сканирование на наличие руткитов — это выбранный по умолчанию процесс, запускающийся вместе с функцией Сканировать весь компьютер.

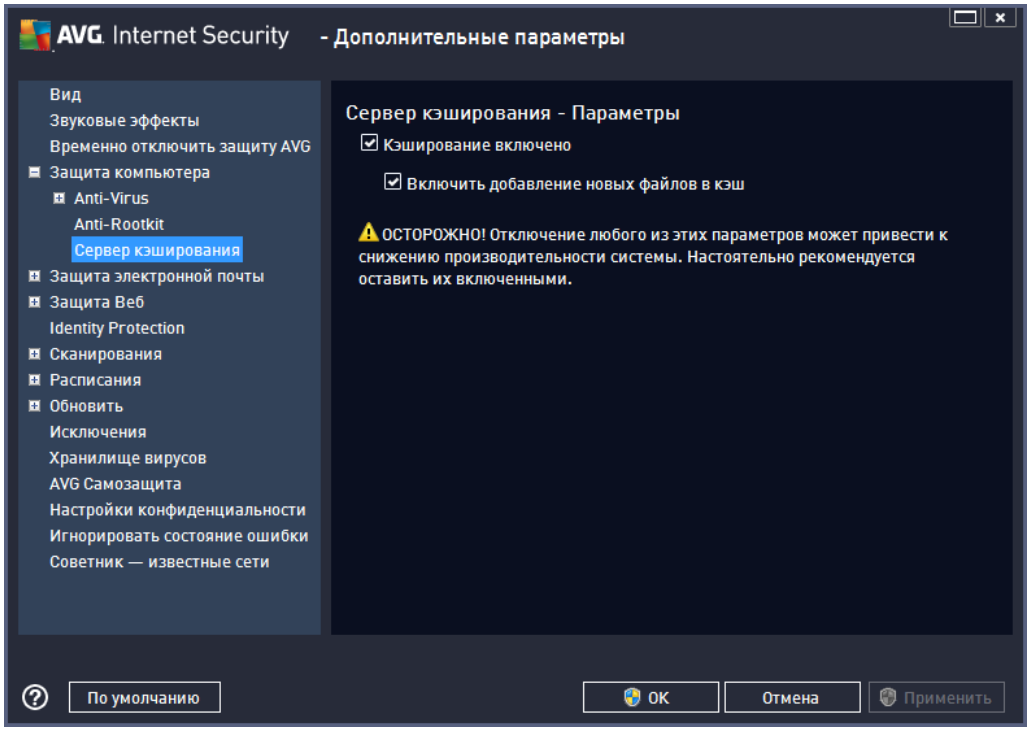


Функции ***Сканирование приложений*** и ***Сканирование драйверов*** позволяют четко определить, что должно быть включено в сканирование на наличие руткитов. Данные настройки предназначены для опытных пользователей. Рекомендуется, чтобы все параметры были включены. Также можно выбрать следующие режимы сканирования на наличие руткитов.

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

9.4.3. Сервер кэширования

Диалоговое окно ***Параметры сервера кэширования*** относится к процессу сервера кэширования, позволяющему ускорить любые операции сканирования **AVG Internet Security 2013**.



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

Диалоговое окно ***Параметры сервера кэширования*** содержит следующие параметры конфигурации.

- ***Кэширование включено*** (*по умолчанию флажок установлен*). Снимите данный флажок, чтобы выключить ***сервер кэширования*** и очистить кэш-память. Примите к сведению, что сканирование может замедлять работу системы и влиять на общую производительность компьютера, так как каждый используемый файл будет проверяться на предмет вирусов и шпионского ПО.

- ***Включить добавление новых файлов в кэш*** (*по умолчанию флажок установлен*). Снимите данный флажок, чтобы остановить добавление новых файлов в кэш-память. Все добавленные в кэш-память файлы будут храниться и использоваться, пока не будет выключено кэширование или не будет обновлена вирусная база.

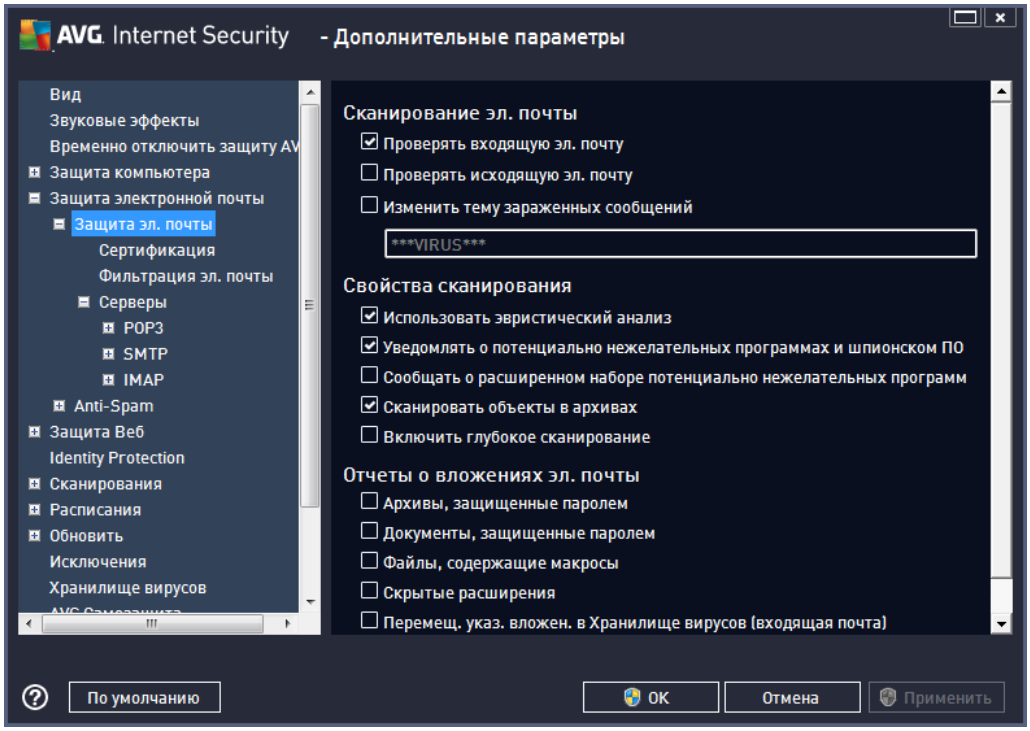
Если нет веских оснований для отключения сервера кэширования, настоятельно рекомендуется не изменять настройки по умолчанию и оставить оба параметра включенными. В противном случае отключение этих параметров может привести к значительному снижению скорости и производительности системы.

9.5. Сканер электронной почты

В этом разделе можно выполнить тонкую настройку компонентов Сканер электронной почты и Anti-Spam.

9.5.1. Сканер электронной почты

Диалоговое окно ***Сканер электронной почты*** состоит из трех разделов.



Сканирование эл. почты

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

- ***Проверять входящую эл. почту*** (*выбрано по умолчанию*) — включение/выключение функции сканирования всех сообщений электронной почты, доставляемых в почтовый клиент.
- ***Проверять исходящую эл. почту*** (*выбрано по умолчанию*) — включение/выключение функции сканирования всех сообщений электронной почты, отправляемых из учетной записи пользователя.
- ***Изменить тему зараженных сообщений*** (*не выбрано по умолчанию*) — для получения предупреждения при определении сканированного сообщения электронной почты как зараженного установите данный флажок и введите необходимый текст в соответствующем поле. В дальнейшем он будет добавляться в поле «Тема» каждого зараженного сообщения электронной почты, что упростит процесс идентификации и фильтрации. По умолчанию установлено значение ***VIRUS***; рекомендуется его сохранить.

Свойства сканирования

В данном разделе можно указать способ сканирования сообщений электронной почты.

- ***Использовать эвристический анализ*** (*по умолчанию включено*) — установите этот флажок, чтобы использовать эвристический метод обнаружения при сканировании сообщений электронной почты. Включение данного параметра позволяет выполнить фильтрацию вложений сообщений электронной почты не только по их расширению, но и с учетом фактического содержимого вложений. Параметры фильтрации можно указать в диалоговом окне Фильтрация эл. почты.

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** (*по умолчанию включено*) — установите этот флажок, чтобы активировать сканирование 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. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** (*не выбрано по умолчанию*) — установите этот флажок для обнаружения расширенного набора шпионских программ: это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него, возможно, будут блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать объекты в архивах*** (*выбрано по умолчанию*) — установите данный флажок, чтобы выполнять сканирование архивов, вложенных в сообщения электронной почты.

- ***Включить глубокое сканирование*** (*не выбрано по умолчанию*) — в определенных случаях (*например, при подозрении, что компьютер заражен вирусом или подвергается атакам злоумышленников*) нужно установить этот флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически никогда не подвергаются заражению. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

Отчеты о вложениях электронной почты

В этом разделе можно настроить функцию предоставления дополнительных отчетов о потенциально опасных или подозрительных файлах. Обратите внимание, что диалоговое окно с предупреждением отображено не будет. Только текст сертификации будет добавлен в конце сообщения электронной почты, а все подобные отчеты будут перечислены в списке диалогового окна Обнаружение сканера электронной почты.

- ***Уведомлять об архивах, защищенных паролем*** — сканирование на наличие вирусов в архивах (*ZIP, RAR и т. п.*), защищенных паролем, невозможно. Установите флажок, чтобы в отчетах они были отмечены как потенциально опасные.

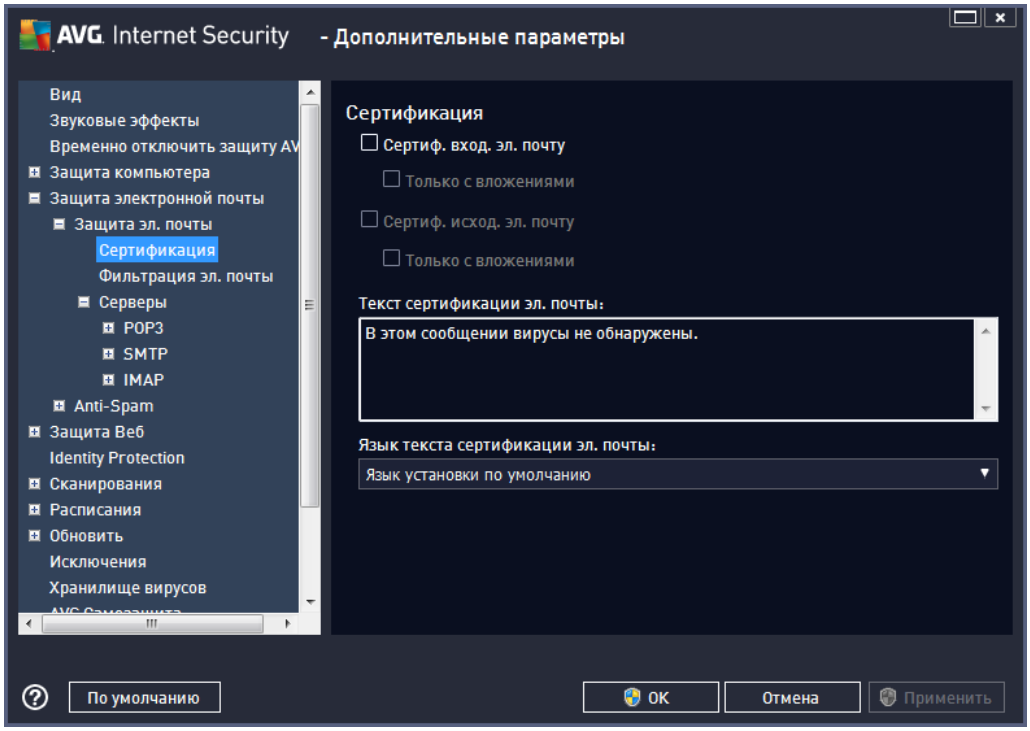
- ***Уведомлять о документах, защищенных паролем*** — проверка на наличие вирусов в документах, защищенных паролем, невозможна. Установите флажок, чтобы в отчетах они были отмечены как потенциально опасные.

- ***Уведомлять 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.

- ***Уведомлять о скрытых расширениях*** — при использовании скрытых расширений подозрительный выполнимый файл something.txt.exe может отображаться как безопасный обычный текстовый файл something.txt. Установите флажок, чтобы в отчетах данные файлы были отмечены как потенциально опасные.

- ***Перемещ. указ. вложен. в Хранилище вирусов*** — необходимо указать, следует ли уведомлять пользователя по электронной почте о защищенных паролями архивах, защищенных паролями документах, файлах, содержащих макросы и/или файлах со скрытыми расширениями, обнаруженных во вложениях сообщений электронной почты. Если подобное сообщение будет обнаружено при сканировании, необходимо определить, следует ли перемещать зараженные объекты в Хранилище вирусов.

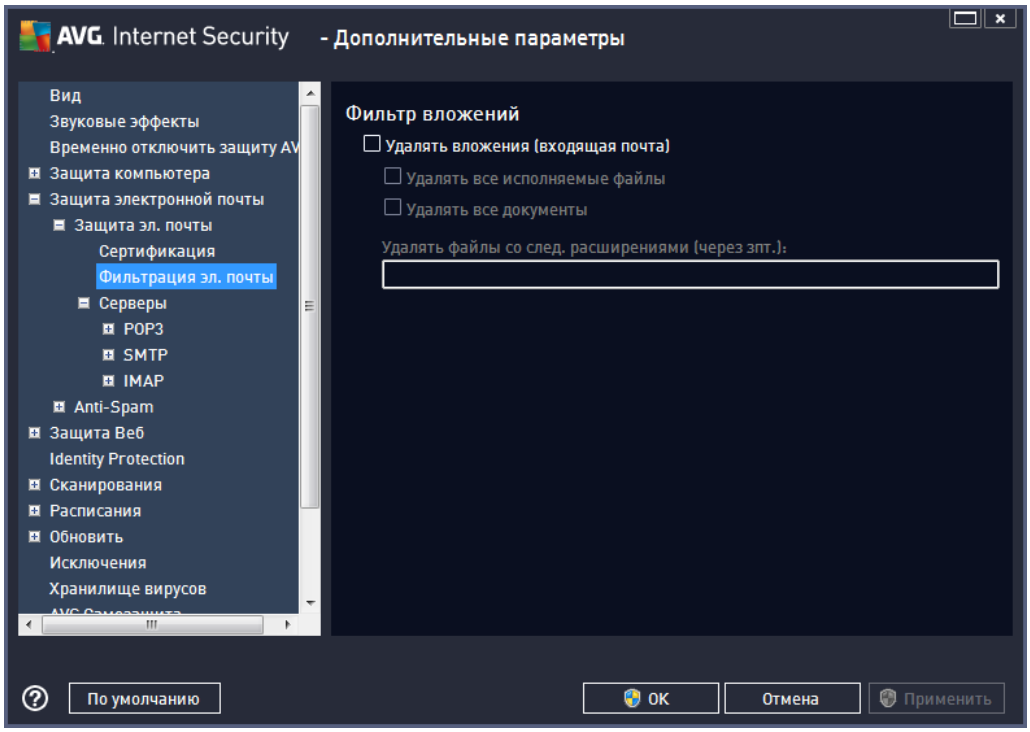
В диалоговом окне ***Сертификация*** можно назначить сертификацию входящей почты (***Сертиф. вход. эл. почту***) и/или исходящей почты (***Сертиф. исход. эл. почту***), установив соответствующие флажки. Для каждого из этих действий можно также выбрать параметр ***Только с вложениями***, при котором сертификация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



По умолчанию текст сертификации содержит основную информацию: *В данном сообщении вирусов не обнаружено.* Однако при необходимости эту информацию можно расширить или изменить. Введите необходимый текст сертификации в поле ***Текст сертификации эл.***

почты. В разделе ***Язык текста сертификации электронной почты*** можно также указать язык, на котором будет отображаться автоматически созданная часть этого текста (*В данном сообщении вирусов не обнаружено*).

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



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

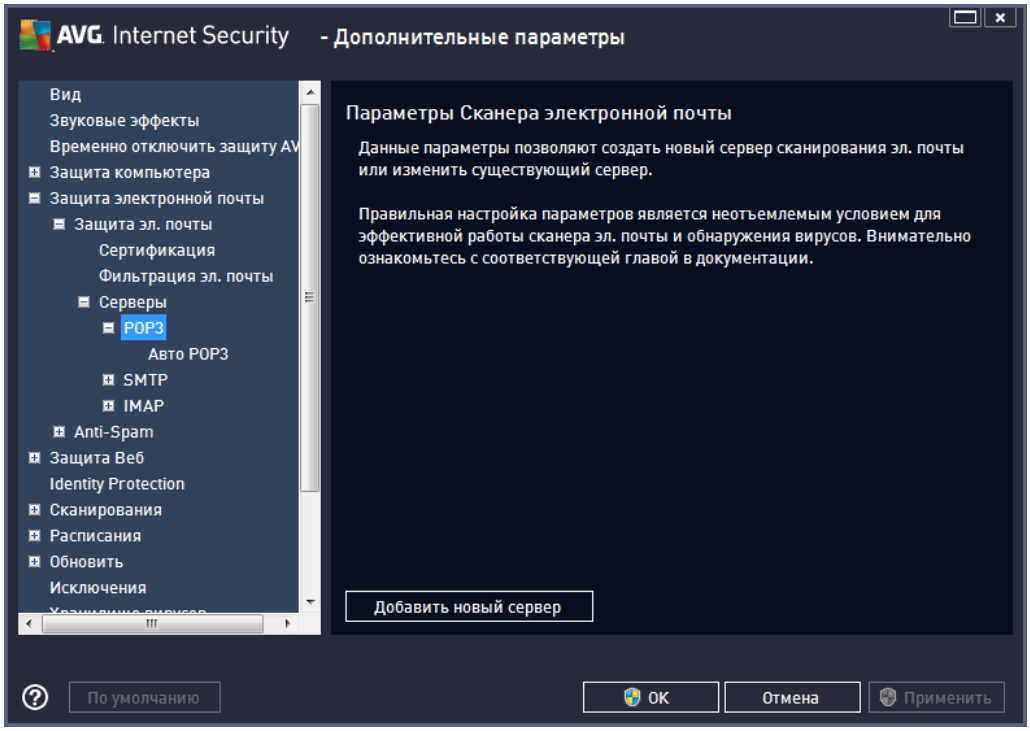
- ***Удалять все исполняемые файлы*** — все файлы *.exe будут удалены.
- ***Удалять все документы*** — все файлы *.doc, *.docx, *.xls, *.xlsx будут удалены.
- ***Удалять файлы со след. расширениями (через зпт.)*** — все файлы с указанными расширениями будут удалены.

В разделе ***Серверы*** можно изменить настройки для серверов Сканер электронной почты.

- Сервер POP3
- Сервер SMTP

- Сервер IMAP

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



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

- ***Имя сервера POP3*** — в данном поле можно указать имя добавленного сервера (*чтобы добавить сервер POP3, щелкните правой кнопкой мыши элемент POP3 в меню навигации слева*). Если вы используете автоматически созданные серверы «AutoPOP3», это поле будет неактивным.

- ***Тип входа*** — метод определения почтового сервера, используемого для входящей почты.

  - ***Автоматически*** — автоматическое выполнение входа в соответствии с параметрами клиента электронной почты.

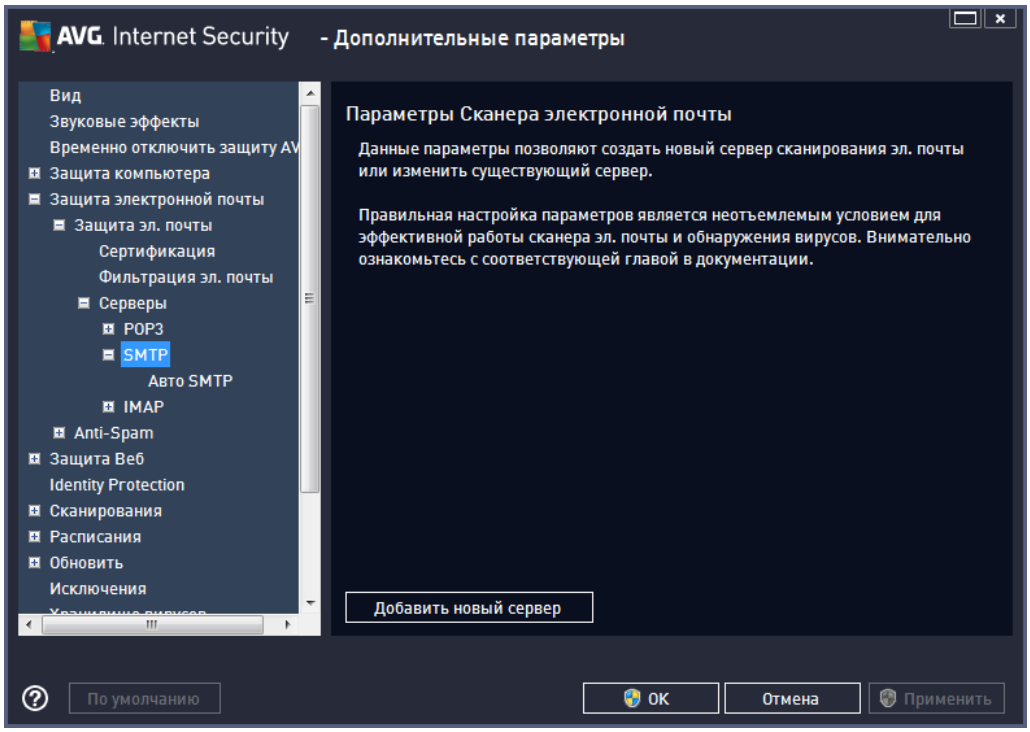
  - ***Фиксированный хост-узел*** — в этом случае программа постоянно использует указанный сервер. Укажите адрес или имя используемого почтового сервера. Имя пользователя не изменяется. В качестве имени можно использовать имя домена (*например, pop.acme.com*) или IP-адрес (*например, 123.45.67.89*). Если почтовый сервер использует нестандартный порт, данный порт можно указать после имени сервера, используя двоеточие в качестве разделителя (*например, pop.acme.com:8200*). Стандартным портом соединения POP3 является порт 110.

- ***Дополнительные параметры*** — определение более подробных параметров.

    - ***Локальный порт*** — определяет порт, используемый почтовым приложением для соединения. Далее в почтовом приложении необходимо указать данный порт в качестве порта соединения POP3.

    - ***Подключение*** — в раскрывающемся меню можно определить необходимый тип подключения (*обычное/SSL/SSL по умолчанию*). При выборе соединения SSL данные отправляются в зашифрованном виде и вероятность их отслеживания или просмотра третьей стороной отсутствует. Данная функция также доступна, только если она поддерживается почтовым сервером назначения.

- ***Активация сервера POP3 клиента электронной почты*** — установите или снимите флажок напротив этого элемента, чтобы активировать или деактивировать указанный сервер POP3.



В данном диалоговом окне (*открытом через* ***Серверы/SMTP***) можно настроить новый сервер Сканер электронной почты, используя протокол SMTP для исходящей почты.

- ***Имя сервера SMTP*** — в этом поле можно указать имя добавленного сервера (*чтобы добавить сервер SMTP, щелкните правой кнопкой мыши элемент SMTP в меню навигации слева*). Если вы используете автоматически созданные серверы «AutoSMTP», данное поле будет неактивным.

- ***Тип входа*** — метод определения почтового сервера, используемого для исходящей почты.

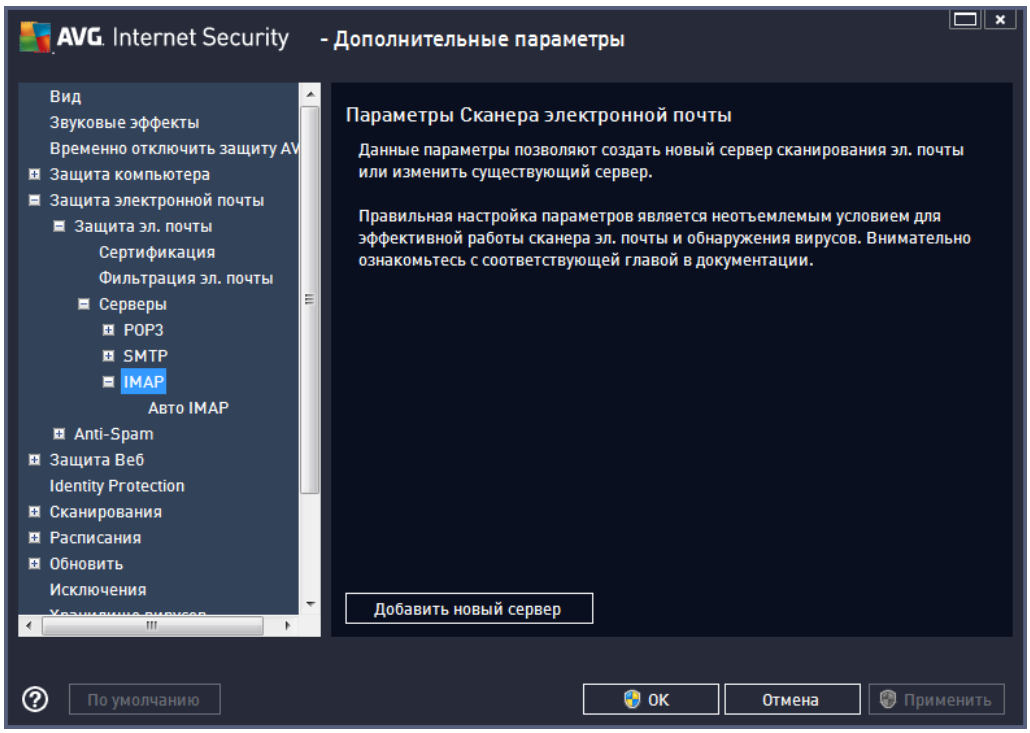
    - ***Автоматически*** — автоматическое выполнение входа в соответствии с

параметрами клиента электронной почты.

- ***Фиксированный хост-узел*** — в этом случае программа постоянно использует указанный сервер. Укажите адрес или имя используемого почтового сервера. В качестве имени можно указать имя домена (*например, smtp.acme.com*) или IP-адрес (*например, 123.45.67.89*). Если почтовый сервер использует нестандартный порт, данный порт можно указать после имени сервера, используя двоеточие в качестве разделителя (*например, smtp.acme.com:8200*). Номер стандартного порта соединения SMTP — 25.

- ***Дополнительные параметры*** — определение более подробных параметров.
  - ***Локальный порт*** — определяет порт, используемый почтовым приложением для соединения. Далее в почтовом клиенте необходимо указать данный порт в качестве порта соединения SMTP.
  - ***Подключение*** — раскрывающееся меню, в котором можно указать необходимый тип подключения (*обычное/SSL/SSL по умолчанию*). При выборе соединения SSL данные отправляются в зашифрованном виде и вероятность их отслеживания или просмотра третьей стороной отсутствует. Данная функция доступна, только если она поддерживается конечным почтовым сервером.

- ***Активация сервера SMTP клиента электронной почты*** — установите или снимите этот флажок, чтобы активировать или деактивировать указанный выше сервер SMTP.



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

- ***Имя сервера IMAP*** — в данном поле можно указать имя добавленного сервера (*чтобы добавить сервер IMAP, щелкните правой кнопкой мыши элемент IMAP в меню навигации слева*). При использовании созданных автоматически серверов «AutoIMAP» данное поле будет неактивным.

- ***Тип входа*** — метод определения почтового сервера, используемого для исходящей почты.

    - ***Автоматически*** — автоматическое выполнение входа в соответствии с параметрами клиента электронной почты.

    - ***Фиксированный хост-узел*** — в этом случае программа постоянно использует указанный сервер. Укажите адрес или имя используемого почтового сервера. В качестве имени можно указать имя домена (*например, smtp.acme.com*) или IP-адрес (*например, 123.45.67.89*). Если почтовый сервер использует нестандартный порт, данный порт можно указать после имени сервера, используя двоеточие в качестве разделителя (*например, imap.acme.com:8200*). Стандартным портом соединения IMAP является порт 143.

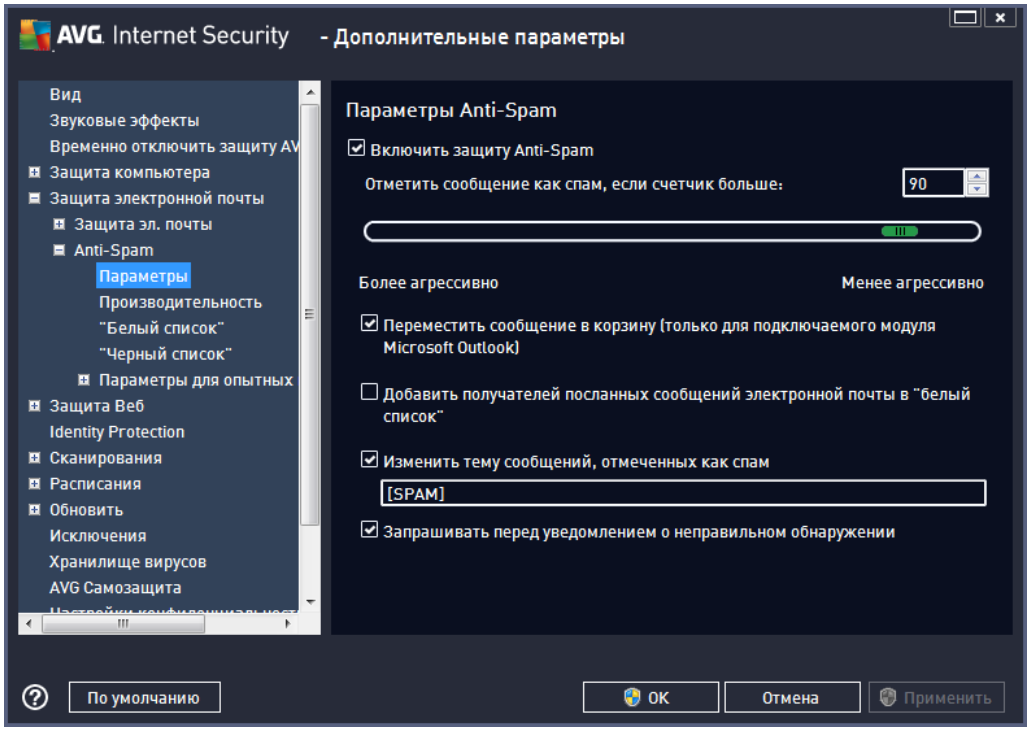
- ***Дополнительные параметры*** — определение более подробных параметров.

    - ***Локальный порт*** — определяет порт, используемый почтовым приложением для соединения. Далее в почтовом клиенте необходимо указать данный порт в качестве порта соединения IMAP.

    - ***Подключение*** — раскрывающееся меню, в котором можно указать необходимый тип подключения (*обычное/SSL/SSL по умолчанию*). При выборе соединения SSL данные отправляются в зашифрованном виде и вероятность их отслеживания или просмотра третьей стороной отсутствует. Данная функция доступна, только если она поддерживается конечным почтовым сервером.

- ***Активация сервера IMAP клиента электронной почты*** — установите или снимите этот флажок, чтобы активировать или деактивировать вышеуказанный сервер SMTP.

9.5.2. Anti-Spam



В диалоговом окне ***Параметры Anti-Spam*** можно установить или снять флажок ***Включить защиту Anti-Spam***, чтобы разрешить или запретить сканирование сообщений электронной почты на наличие спама. По умолчанию данный параметр включен, и в общем случае рекомендуется не снимать данный флажок без крайней необходимости.

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

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

- ***Значения в диапазоне 80—90*** — будет производиться фильтрация сообщений электронной почты, которые, возможно, являются спамом. Некоторые сообщения, которые не являются спамом, могут быть ошибочно помечены как спам.
- ***Значения в диапазоне 60—79*** — значения в данном диапазоне обеспечивают довольно высокий уровень защиты. Будет производиться фильтрация сообщений электронной почты, которые, скорее всего, являются спамом. Сообщения, которые не являются спамом, могут быть определены как спам.
- ***Значения в диапазоне 50—59*** — значения в данном диапазоне обеспечивают очень высокую степень защиты. Сообщения, которые не являются спамом, могут быть определены как настоящий спам. Обычно не рекомендуется использовать пороговые

значения из данного диапазона.

В диалоговом окне ***Параметры Anti-Spam*** можно определить действия в отношении сообщений электронной почты, которые были определены как спам.

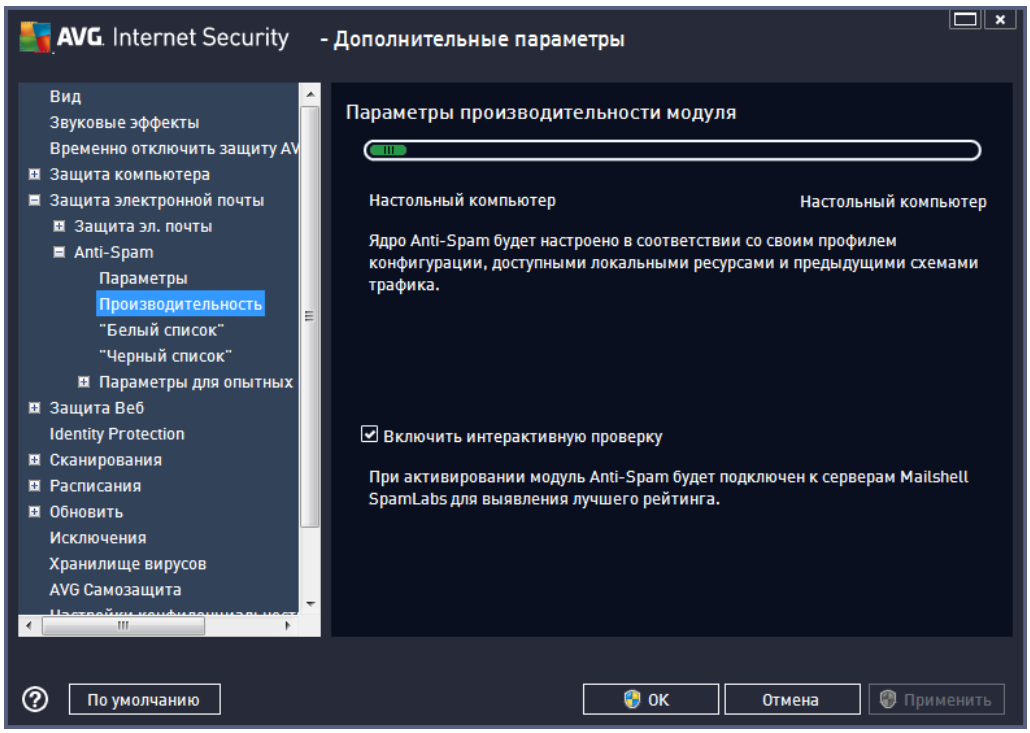
- ***Переместить сообщение в корзину*** *(только для подключаемого модуля Microsoft Outlook)* — установите этот флажок, чтобы каждое сообщение электронной почты, определенное как спам, автоматически перемещалось в папку нежелательной почты клиента электронной почты MS Outlook. На данный момент функция не поддерживается другими почтовыми клиентами.

- ***Добавить получателей посланных сообщений электронной почты в белый список*** — установите этот флажок, чтобы подтвердить, что всем получателям отправленных сообщений электронной почты можно доверять, а все сообщения электронной почты, приходящие с их учетных записей электронной почты, должны быть доставлены.

- ***Изменить тему сообщений, отмеченных как СПАМ*** — установите этот флажок, если необходимо отмечать все сообщения, определенные как спам, специальным словом или символом в поле темы сообщения. Необходимый текст можно ввести в текстовое поле, которое станет активным.

- ***Запрашивать перед уведомлением о неправильном обнаружении*** — установив данный флажок в процессе установки, вы соглашаетесь участвовать в проекте Параметры конфиденциальности. В этом случае вы будете отправлять отчеты об обнаруженных угрозах в компанию AVG. Отчет формируется автоматически. Однако в случае установки данного флажка перед отправкой отчетов об обнаруженном спаме в компанию AVG вы будете получать запрос, позволяющий подтвердить, что сообщение, о котором вы сообщаете, действительно является спамом.

Диалоговое окно ***Параметры производительности модуля*** (*доступное при выборе элемента* ***Производительность*** *на панели навигации слева*) позволяет настроить параметры производительности компонента ***Anti-Spam***.



Переместите ползунок влево или вправо, чтобы изменить уровень производительности при сканировании в диапазоне от ***Малое потребление ресурсов*** до ***Высокое потребление ресурсов***.

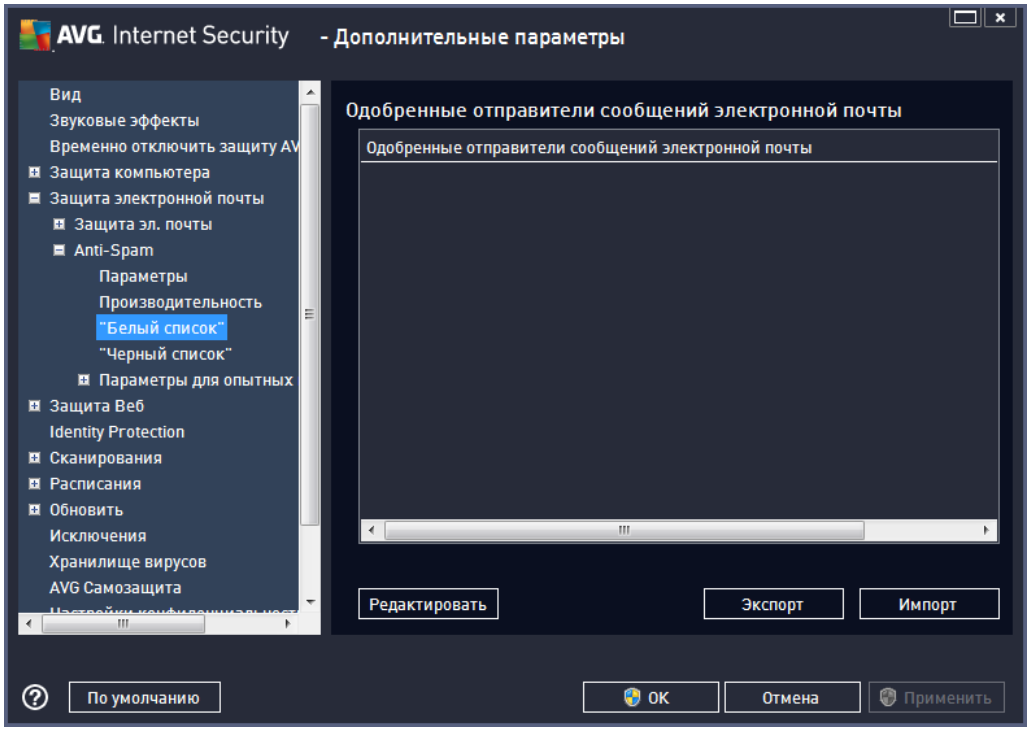
- ***Малое потребление ресурсов*** — при сканировании на предмет спама правила использоваться не будут. Для определения будут использоваться только данные обучения. Данный режим рекомендуется использовать только на компьютерах с действительно низкой конфигурацией.

- ***Высокое потребление ресурсов*** — при работе в данном режиме программа будет использовать большой объем памяти компьютера В процессе сканирования на наличие спама будут использованы такие функции: правила и кэширование базы данных спама, базовые и дополнительные правила, IP-адреса и базы данных спамеров.

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

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

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



В интерфейсе редактирования можно указать список отправителей, которые, как вы считаете, никогда не отправляют нежелательных сообщений (спам). Можно также указать список полных имен доменов (например, *avg.com*), которые, как вы уверены, не генерируют нежелательных сообщений электронной почты. Если у вас уже есть такой список отправителей и/или вы приготовили имена доменов, можно либо непосредственно ввести каждый адрес электронной почты, либо импортировать весь список адресов сразу.

Кнопки управления

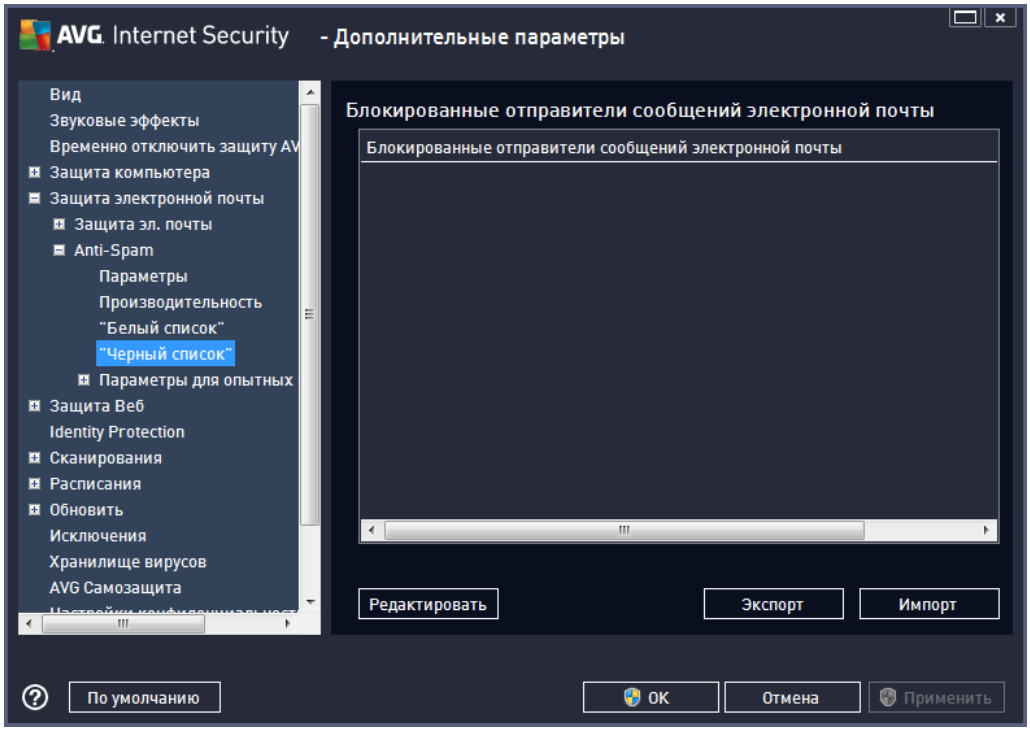
Доступны следующие кнопки управления.

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

- ***Экспорт*** — если по какой-либо причине необходимо экспортировать записи, это можно сделать, нажав данную кнопку. Все записи будут сохранены в формате обычного текста.

- ***Импорт*** — заранее подготовленный текстовый файл с адресами электронной почты или именами доменов можно импортировать, нажав эту кнопку. В каждой строке файла должен содержаться только один элемент (*адрес, имя домена*).

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



В интерфейсе редактирования можно указать список отправителей, рассылающих нежелательные сообщения (*спам)*. Также можно составить список полных имен доменов (*например, spammingcompany.com*), рассылающих нежелательные сообщения. Все сообщения электронной почты с указанных адресов/доменов будут расцениваться как спам. Если у вас уже есть такой список отправителей и/или вы приготовили имена доменов, можно либо непосредственно ввести каждый адрес электронной почты, либо импортировать весь список адресов сразу.

Кнопки управления

Доступны следующие кнопки управления.

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

- ***Экспорт*** — если по какой-либо причине необходимо экспортировать записи, это можно сделать, нажав данную кнопку. Все записи будут сохранены в формате обычного текста.

- ***Импорт*** — заранее подготовленный текстовый файл с адресами электронной почты или именами доменов можно импортировать, нажав эту кнопку.

Ветвь «Параметры для опытных пользователей» содержит расширенные параметры функции Anti-Spam. Данные параметры предназначены только для опытных пользователей, в основном для администраторов сети, которым

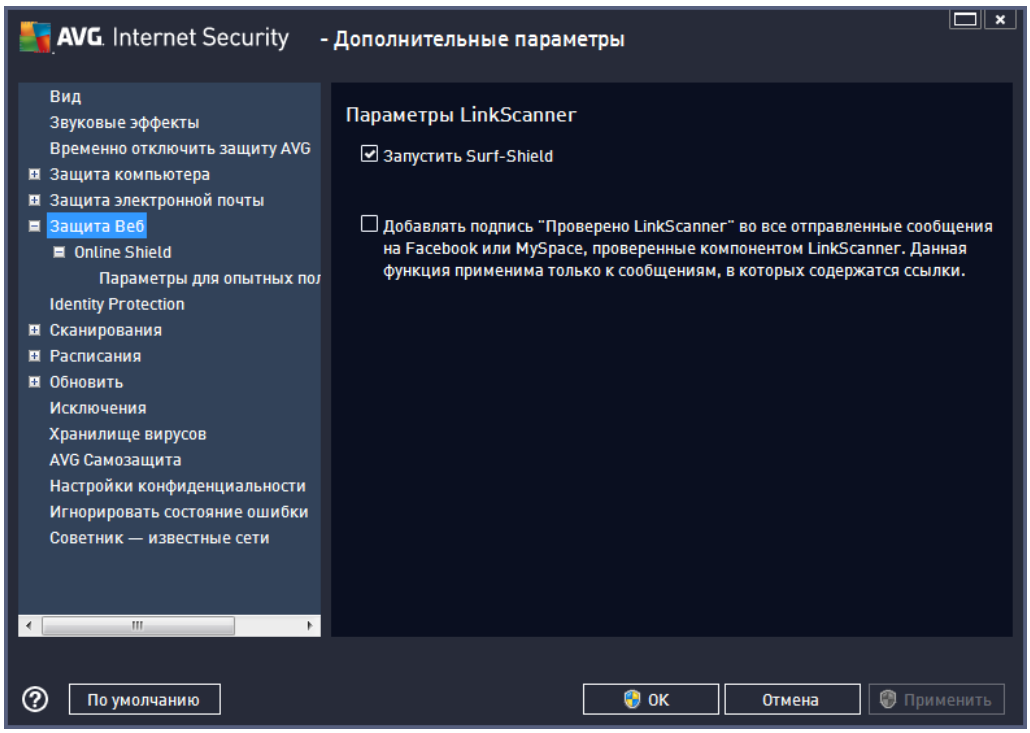
требуется произвести подробные настройки защиты от спама для обеспечения оптимального уровня защиты почтовых серверов. По этой причине дополнительная справочная информация по отдельным диалоговым окнам отсутствует, однако непосредственно в интерфейсе пользователя имеется краткое описание каждого параметра. Не рекомендуется изменять какие-либо параметры до предварительного ознакомления со всеми дополнительными параметрами компонента Spamcatcher (MailShell Inc.). Любые неправильные корректировки могут привести к снижению производительности или неправильной работе компонента.

Чтобы изменить дополнительные параметры компонента Anti-Spam, следуйте инструкциям, приведенным непосредственно в интерфейсе пользователя. Как правило, каждая конкретная функция имеет отдельное диалоговое окно настройки. Ее описание также находится в диалоговом окне. Можно изменить следующие параметры.

- ***Фильтрация*** — список языков, список стран, одобренные IP-адреса, блокируемые IP-адреса, блокируемые страны, блокируемые кодировки, ложные отправители.
- ***RBL*** — серверы RBL, множественные совпадения, порог, время ожидания, максимальное количество IP-адресов.
- ***Интернет-соединение*** — время ожидания, прокси-сервер, проверка подлинности прокси-сервера.

9.6. Защита просмотра веб-узлов

В диалоговом окне ***Параметры LinkScanner*** можно настроить следующие параметры.

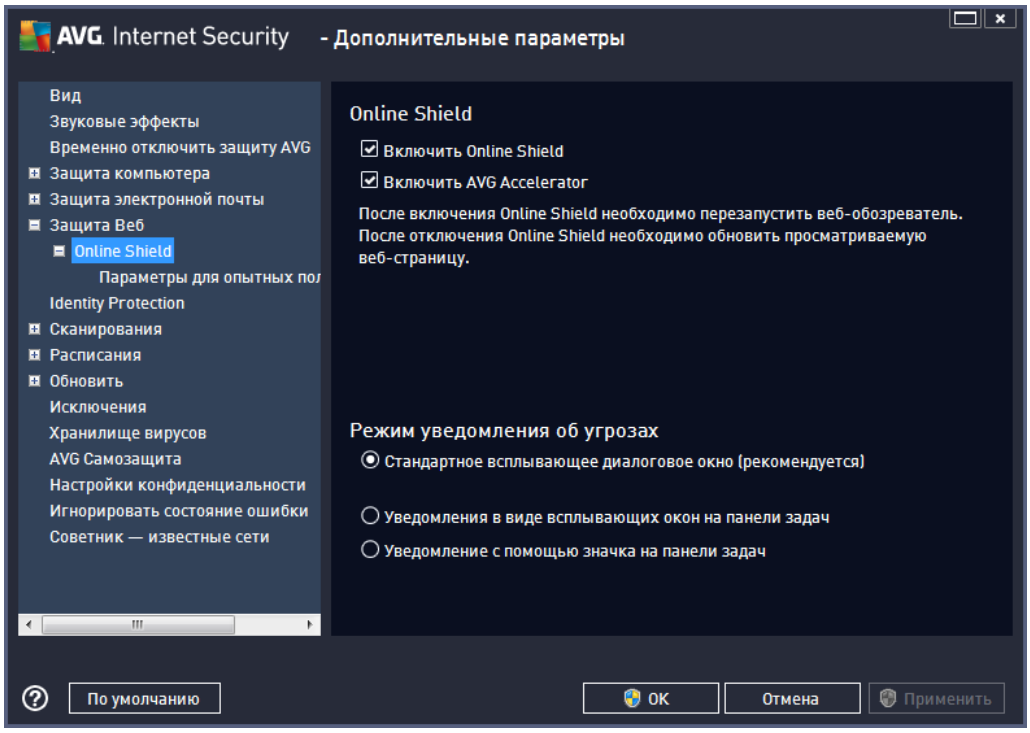


- ***Включить Surf-Shield*** — (*по умолчанию включено*) — активная защита (*в реальном*

времени) при посещении сайтов с эксплойтами. Известные вредоносные сайты и их зараженное эксплойтами содержимое блокируется при доступе к ним через веб-браузер (*или любое другое приложение, использующее HTTP*).

- ***Добавить «Проверено LinkScanner»...*** — (*не выбрано по умолчанию*) — установите этот параметр, чтобы все сообщения из социальных сетей Facebook и MySpace, в которых имеются активные гиперссылки, содержали текст сертификации LinkScanner.

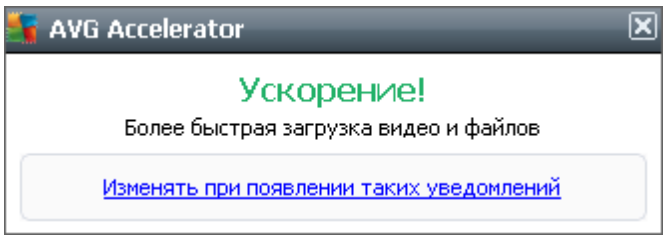
9.6.1. Online Shield



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

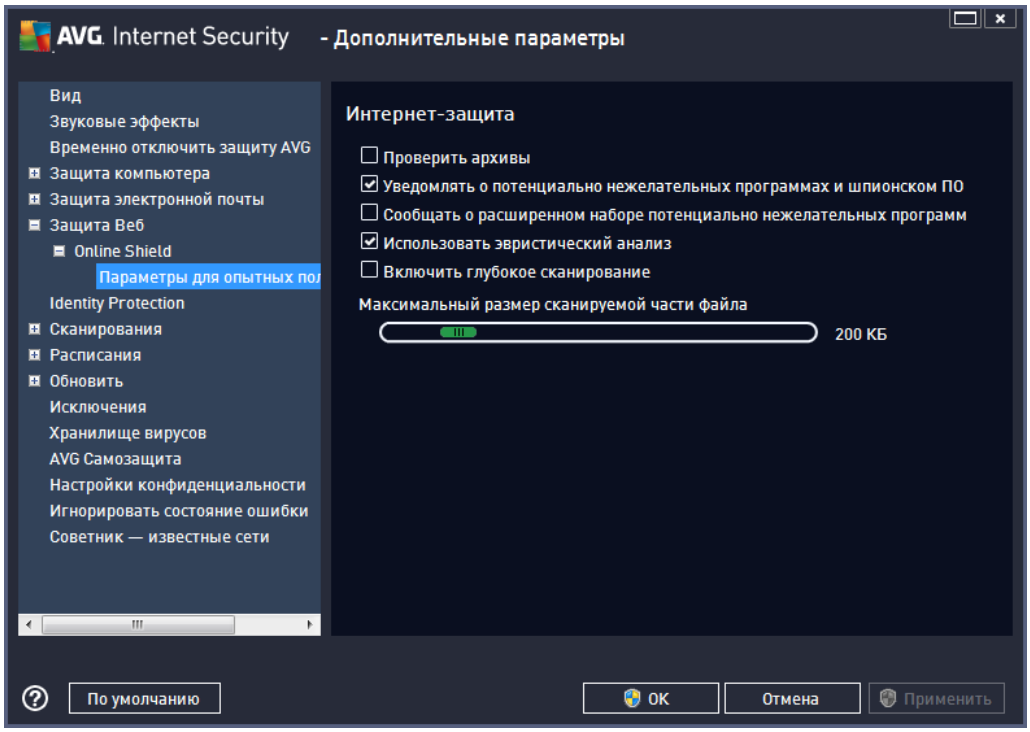
- ***Включить Online Shield*** *(по умолчанию включено)* — включение или выключение службы ***Online Shield***. Для доступа к другим дополнительным параметрам компонента ***Online Shield*** перейдите к следующему диалоговому окну Интернет-защита.

- ***Включить AVG Accelerator*** *(по умолчанию включено)* — включение или выключение службы AVG Accelerator. AVG Accelerator обеспечивает более стабильное воспроизведение видеороликов в Интернете, а также ускоряет процессы загрузки. При запуске процесса видеоускорения на панели задач появится всплывающее окно с уведомлением:



Режим уведомления об угрозах

В нижней части диалогового окна выберите способ информирования о возможных угрозах: с помощью обычных всплывающих окон, шаровидных уведомлений на панели задач или с помощью значка на панели задач.



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

- ***Включить интернет-защиту*** — этот параметр подтверждает, что компонент ***Online Shield*** должен выполнять сканирование содержимого интернет-страницы. Этот параметр (*выбран по умолчанию*) также позволяет включать/отключать следующие элементы.
    - ***Проверить архивы*** (*по умолчанию выключено*) — сканирование содержимого архивов, которые могут содержаться на отображаемых интернет-страницах.

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** (*по умолчанию включено*) — установите флажок для активации модуля Anti-Spyware и сканирования на наличие шпионского ПО и вирусов. Шпионские программы относят к категории сомнительного вредоносного ПО: несмотря на то что они, как правило, представляют угрозу безопасности, некоторые из этих программ могут устанавливаться намеренно. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** (*по умолчанию выключено*) — установите данный флажок для обнаружения расширенного пакета шпионского ПО. Программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него, возможно, будут блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Использовать эвристический анализ*** (*по умолчанию выключено*) — сканирование содержимого отображаемой страницы с использованием метода эвристического анализа (*динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде*).

- ***Включить глубокое сканирование*** (*по умолчанию выключено*) — в определенных случаях (*например, при подозрении, что компьютер заражен*) можно установить данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

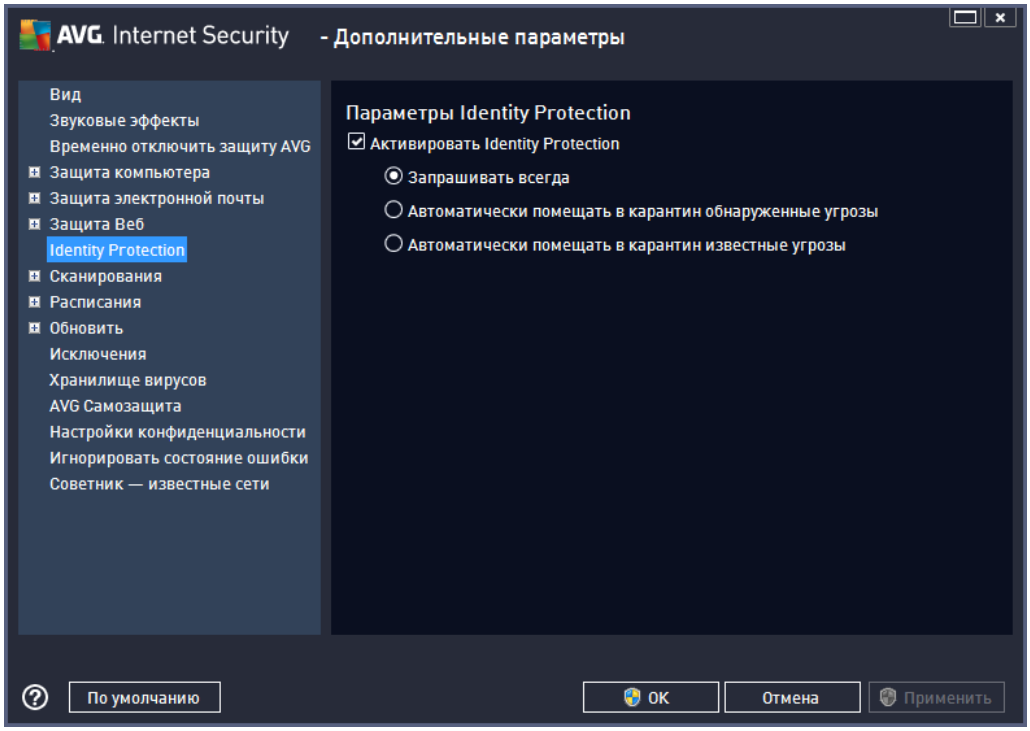
- ***Максимальный размер файла для сканирования*** — если на отображенной странице имеются файлы, можно выполнить сканирование их содержимого даже до момента их загрузки на компьютер. Однако сканирование больших файлов занимает определенное количество времени и может значительно замедлить загрузку страницы. Используйте полосу прокрутки для определения максимального размера файла, сканирование которого все же необходимо выполнить с помощью компонента ***Online Shield***. Даже если загруженный файл больше указанного размера и, следовательно, Online Shield не будет сканировать его, ваша защита не пострадает. Если файл содержит угрозу, компонент ***Постоянная защита*** сразу же обнаружит ее.

- ***Исключить хост/IP-адрес/домен*** — можно ввести в текстовое поле точное имя сервера (*хост, IP-адрес, IP-адрес с маской, URL*) или домен, который не должен сканироваться компонентом ***Online Shield***. Поэтому следует исключить только те хосты, которые точно не содержат вредоносного веб-содержимого.

9.7. Identity Protection

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

В окне ***Параметры Identity Protection*** можно включить или отключить основные функции компонента Identity Protection.



Активировать Identity Protection (*выбрано по умолчанию*) — снимите этот флажок, чтобы отключить компонент Identity Protection.

Настоятельно рекомендуется не делать это без необходимости.

Если компонент Identity Protection активирован, можно определить его действия при обнаружении угрозы.

- ***Запрашивать всегда*** (*выбрано по умолчанию*) — при обнаружении угрозы отобразится запрос на перемещение опасного объекта в карантин, чтобы избежать случайного удаления запускаемых приложений.

- ***Автоматически помещать в карантин обнаруженные угрозы*** — установите флажок, чтобы все обнаруженные угрозы сразу же помещались в безопасное место — Хранилище вирусов. В случае сохранения параметров по умолчанию при обнаружении угрозы отобразится запрос на перемещение опасного объекта в карантин, чтобы избежать случайного удаления запускаемых приложений.

- ***Автоматически помещать в карантин известные угрозы*** — установите этот флажок, чтобы все приложения, определенные как потенциально вредоносное ПО, автоматически перемещались в Хранилище вирусов.

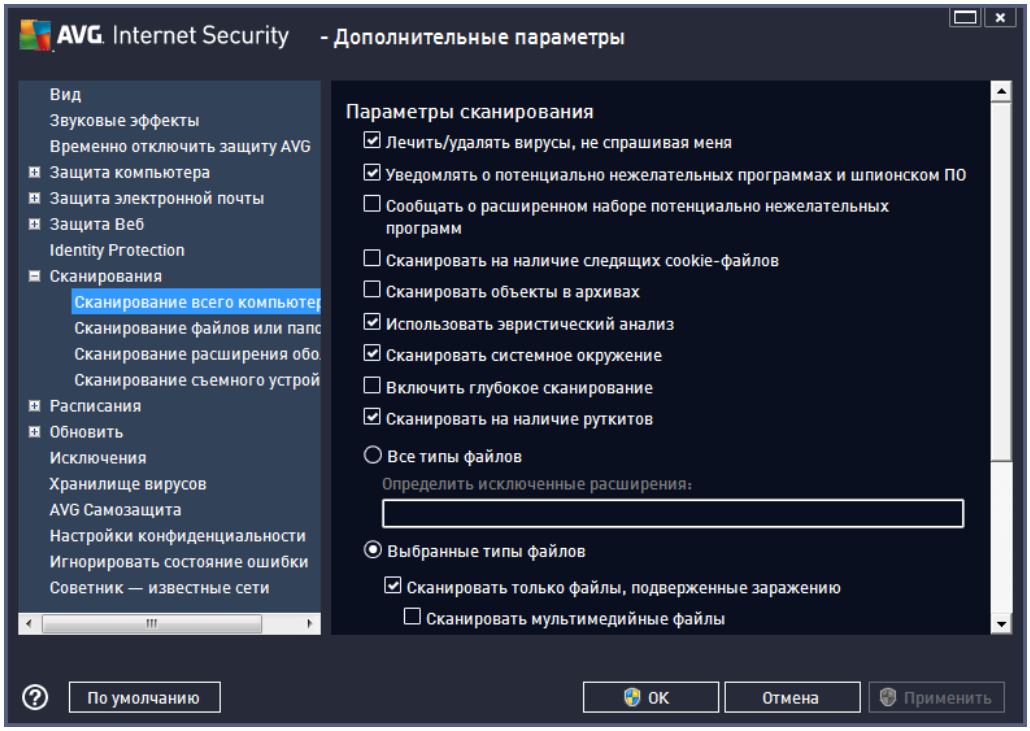
9.8. Сканирования

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

- ***Сканировать весь компьютер*** — стандартное предварительно настроенное сканирование всего компьютера.
- ***Сканирование расширения оболочки*** **—** особое сканирование выбранного объекта непосредственно в среде проводника Windows.
- ***Сканирование определенных файлов или папок*** — стандартное предварительно настроенное сканирование выбранных областей компьютера.
- ***Сканирование съемного устройства*** — специальное сканирование съемных устройств, подключенных к компьютеру.

9.8.1. Сканировать весь компьютер

Параметр ***Сканировать весь компьютер*** позволяет редактировать параметры одного из сканирований, предварительно определенных производителем — Сканировать весь компьютер .



Параметры сканирования

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

- ***Автоматически лечить или удалять зараженные вирусами объекты*** (*выбрано по умолчанию*) — обнаруженный при сканировании вирус будет удален автоматически, если лечение возможно. Если не удалось автоматически вылечить зараженный файл, зараженный объект будет перемещен в Хранилище вирусов.

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** (*по умолчанию включено*) — установите этот флажок, чтобы активировать сканирование 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. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** (*по умолчанию выключено*) — установите этот флажок для обнаружения расширенного набора шпионских программ: это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него, возможно, будут блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать на наличие следящих cookie-файлов*** (*по умолчанию выключено*) — этот параметр предусматривает обнаружение файлов cookie; (*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*** (*по умолчанию не включено*) — этот параметр позволяет при сканировании проверять все файлы, хранящиеся в архивах, например ZIP, RAR и т. п.

- ***Использовать эвристический анализ*** (*по умолчанию включено*) — эвристический анализ (*динамичная эмуляция команд сканированных объектов в среде виртуального компьютера*) является одним из способов, используемых для обнаружения вирусов при сканировании.

- ***Сканировать системное окружение*** (*по умолчанию включено*) — при сканировании также будут проверены системные области компьютера.

- ***Включить глубокое сканирование*** (*по умолчанию выключено*) — в определенных случаях (*например, при подозрении, что компьютер заражен*) можно установить этот флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

- ***Сканировать на наличие руткитов*** (*по умолчанию включено*) — компонент Anti-Rootkit сканирует компьютер на возможное наличие пакетов руткитов (программ и технологий, стремящихся скрыть вредоносную активность на компьютере). Если

руткит обнаружен, это еще не значит, что компьютер заражен. В некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за руткиты.

Вы должны также определить объекты сканирования

- ***Все типы файлов*** с возможностью определения исключений для сканирования посредством создания 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 в принципе могут быть заражены (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы имеют довольно большой размер и вероятность их заражения вирусом мала*). С помощью расширений можно указать типы файлов, которые необходимо сканировать всегда.

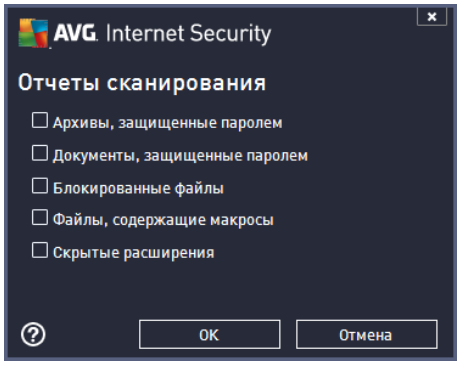
- Дополнительно можно установить флажок ***Сканировать файлы без расширений*** (он установлен по умолчанию). Рекомендуется не снимать его без веских причин. Файлы без расширений являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

Настройка времени выполнения сканирования

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

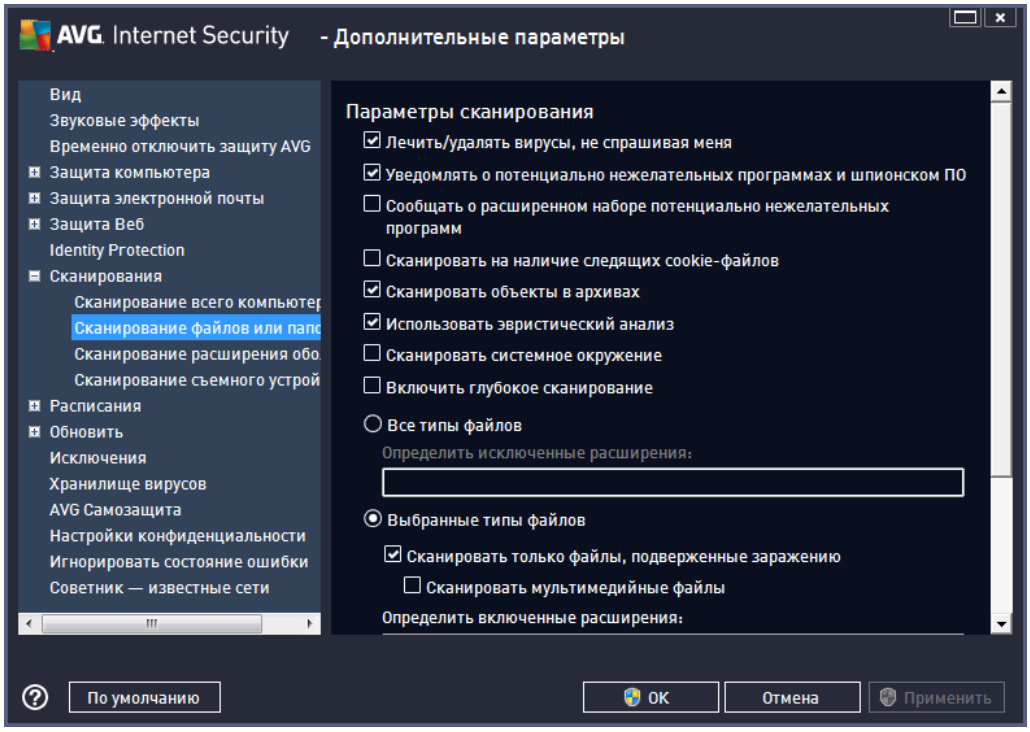
Установить дополнительные отчеты о сканировании ...

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



9.8.2. Сканирование файлов или папок

Интерфейс редактирования ***Сканировать отдельные файлы/папки*** выглядит идентично диалоговому окну редактирования Сканировать весь компьютер. Все параметры конфигурации также не отличаются; однако параметры по умолчанию являются более строгими при сканировании всего компьютера:



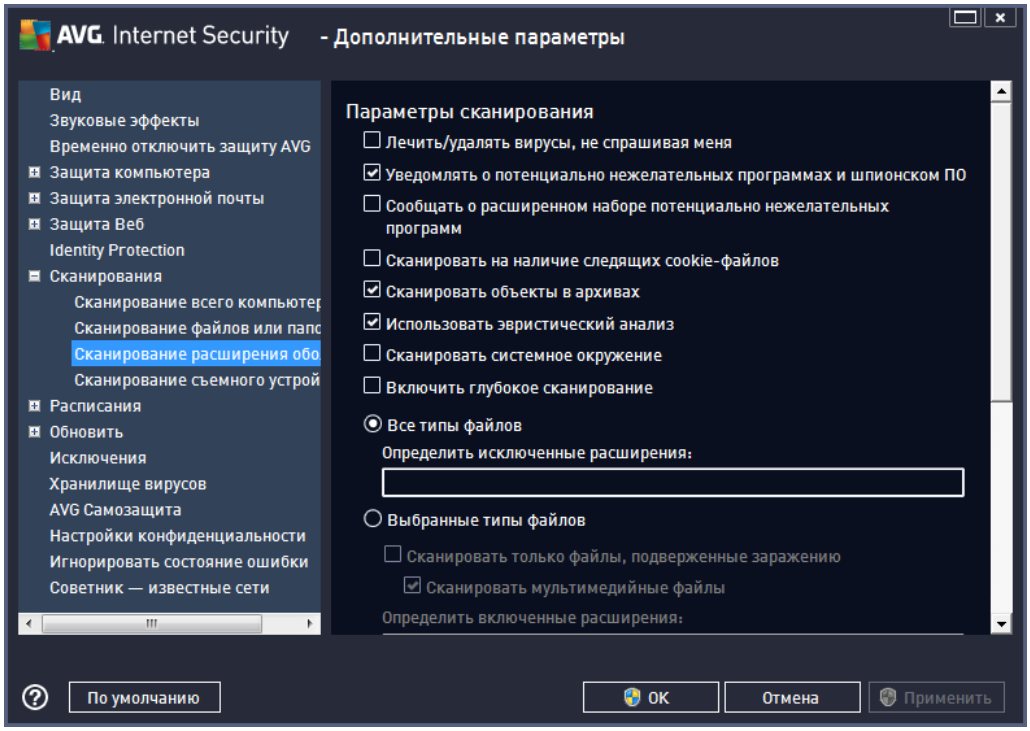
Все параметры, настроенные в данном диалоговом окне, применяются только к областям, выбранным для сканирования определенных файлов или папок!

Примечание. *Описание конкретных параметров приведено в главе Расширенные настройки AVG / Сканирования / Сканировать весь компьютер.*

9.8.3. Сканирование расширения оболочки

Как и предыдущий элемент Сканировать весь компьютер, элемент ***Сканирование расширения оболочки***, содержит несколько предварительно установленных поставщиком ПО параметров для настройки сканирования. Данные параметры предназначены для настройки сканирования определенных объектов, запускаемых непосредственно из проводника Windows

(*расширение оболочки*), см. главу Сканирование в проводнике Windows.



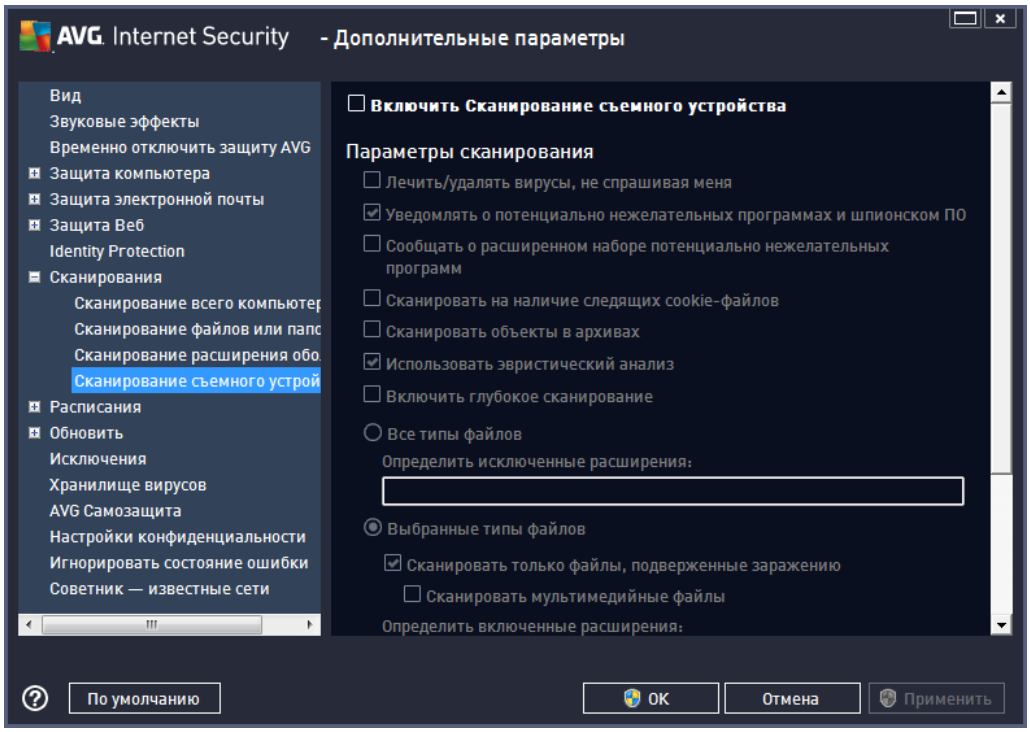
Перечень параметров тот же, что и для варианта Сканирование всего компьютера. Однако параметры по умолчанию отличаются (*например, при сканировании всего компьютера по умолчанию не выполняется проверка архивов, однако выполняется сканирование системной среды, а при сканировании расширения оболочки — наоборот*).

Примечание. *Описание конкретных параметров приведено в главе Расширенные настройки AVG / Сканирования / Сканировать весь компьютер.*

В отличие от окна Сканировать весь компьютер, диалоговое окно ***Сканирование расширения оболочки*** содержит раздел ***Другие параметры интерфейса пользователя AVG***, в котором можно указать, будет ли отображаться процесс выполнения сканирования и результаты сканирования в интерфейсе пользователя AVG. Также можно указать, чтобы результаты сканирования отображались только в случае обнаружения заражения при сканировании.

9.8.4. Сканирование съемного устройства

Интерфейс редактирования операции ***Сканирование съемного устройства*** выглядит аналогично диалоговому окну редактирования операции Сканировать весь компьютер.



Диалоговое окно ***Сканирование съемного устройства*** открывается автоматически после подключения съемного устройства к компьютеру. По умолчанию данное 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 конкретных параметров приведено в главе Расширенные настройки AVG / Сканирования / Сканировать весь компьютер.*

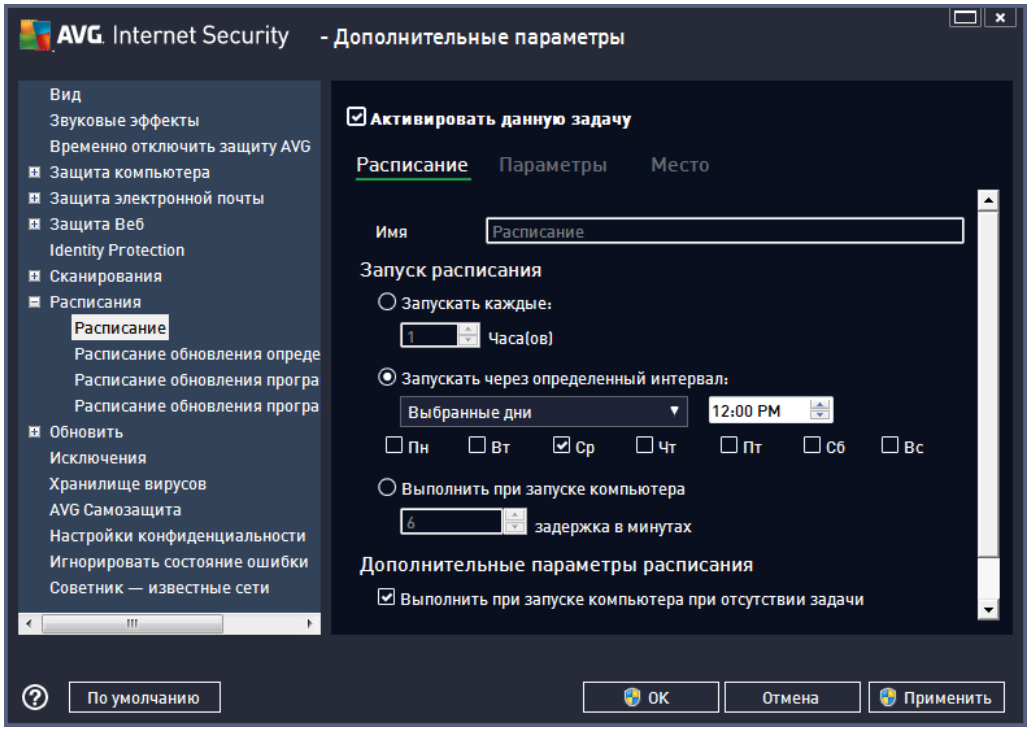
9.9. Расписания

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

- Запланированное сканирование
- Расписание обновления определений
- Расписание обновления программы
- Расписание обновления Anti-Spam

9.9.1. Запланированное сканирование

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



Далее в текстовом поле ***Имя*** (*неактивном для всех расписаний по умолчанию*) указывается имя, назначенное данному расписанию поставщиком программы. Для новых расписаний (*чтобы добавить новое расписание, щелкните правой кнопкой мыши элемент* ***Запланированное сканирование*** *в левом дереве навигации*) можно указать собственное имя. При этом текстовое поле будет доступно для редактирования. Старайтесь использовать краткие, содержательные и понятные названия сканирований, чтобы в дальнейшем их было легче отличить от остальных.

Например, *не следует присваивать такие имена, как «Новое сканирование» или «Мое сканирование», т. к. данные имена не имеют отношения к сканируемым объектам. И наоборот, название «Сканирование системных областей» является хорошим содержательным названием. Хотя не обязательно указывать в названии сканирования, является ли оно сканированием всего компьютера или лишь выбранных файлов или папок, созданные сканирования будут определяться как разновидности [сканирования выбранных файлов и папок](#).*

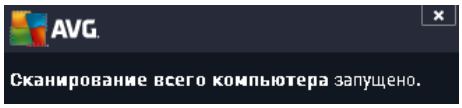
В данном диалоговом окне можно определить следующие параметры сканирования.

Выполняемое расписание

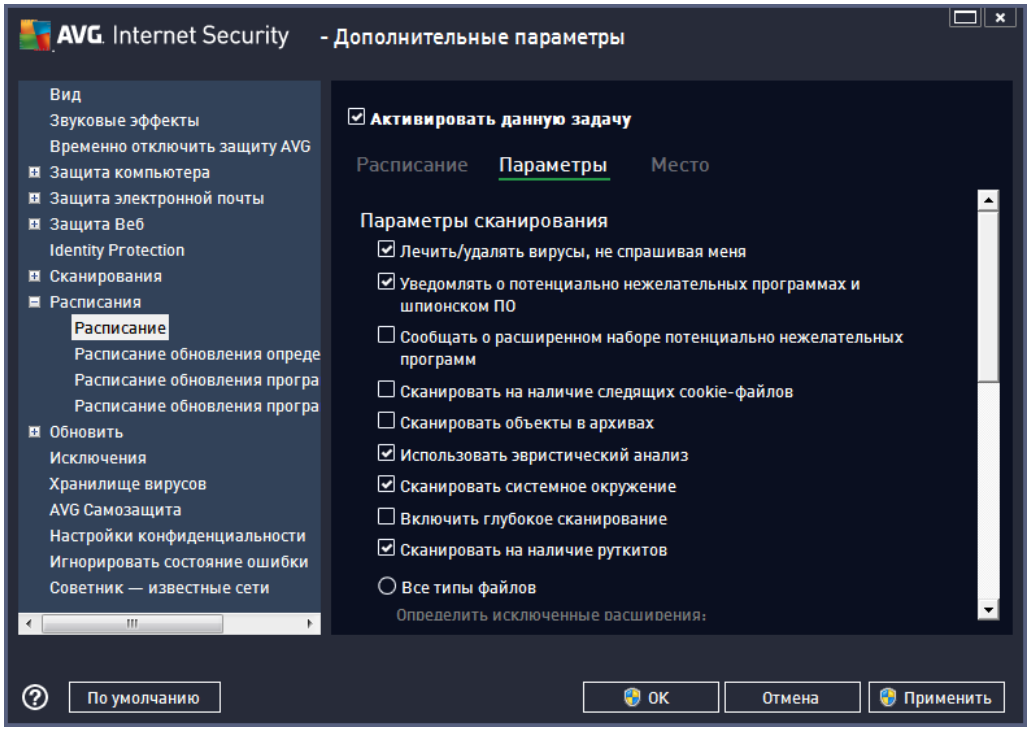
Здесь можно указать временные интервалы запуска нового запланированного сканирования. Запуск процесса сканирования можно назначить через определенные промежутки времени (***Запускать каждые ...***), указав точные дату и время запуска сканирования (***Запускать в определенное время ...***), или определить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

Дополнительные параметры расписания

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



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



На вкладке ***Параметры*** приведен список параметров сканирования, которые при необходимости можно включить или отключить. По умолчанию большинство параметров включены и используются при сканировании. ***Если нет веских оснований для изменения***

данных параметров, рекомендуется не изменять стандартную конфигурацию.

- ***Автоматически лечить или удалять зараженные вирусами объекты*** *(выбрано по умолчанию):* обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если не удалось автоматически вылечить зараженный файл, зараженный объект будет перемещен в Хранилище вирусов.

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** *(выбрано по умолчанию)* — установите этот флажок, чтобы сканировать на наличие как шпионского ПО, так 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. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** (*не выбрано по умолчанию*): установите этот флажок для обнаружения расширенного пакета шпионского ПО — это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него, возможно, будут блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать на наличие следящих файлов cookie*** (*по умолчанию выключено*) — этот параметр позволяет в процессе сканирования обнаруживать файлы cookie *(файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок в Интернете)*.

- ***Сканировать объекты в архивах*** *(не выбрано по умолчанию)* — при выборе данного параметра сканирование затронет все файлы, даже внутри архивов, например ZIP, RAR и т. п.

- ***Использовать эвристический анализ*** (*выбрано по умолчанию*) — эвристический анализ (*динамичная эмуляция команд сканированных объектов в виртуальной компьютерной среде*) является одним из способов, используемых для выявления вирусов при сканировании.

- ***Сканировать системное окружение*** (*выбрано по умолчанию*) — в результате сканирования также будут проверены участки системы компьютера.

- ***Включить глубокое сканирование*** (*не выбрано по умолчанию)* — в определенных случаях (*например, при подозрении на заражение компьютера*) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

- ***Сканировать на наличие руткитов*** *(выбрано по умолчанию) — компонент* Anti-Rootkit сканирует компьютер на возможное наличие пакетов программ rootkit (программы и технологии, позволяющие скрыть вредоносную активность на компьютере). Если руткит обнаружен, это еще не значит, что компьютер заражен. В

некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за руткиты.

Вы должны также определить объекты сканирования

- ***Все типы файлов*** с возможностью определения исключений для сканирования посредством создания 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 в принципе могут быть заражены (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы имеют довольно большой размер и вероятность их заражения вирусом мала*). С помощью расширений можно указать типы файлов, которые необходимо сканировать всегда.

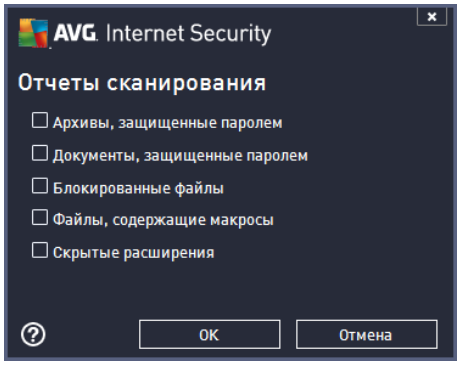
- Дополнительно можно установить флажок ***Сканировать файлы без расширений*** (он установлен по умолчанию). Рекомендуется не снимать его без веских причин. Файлы без расширений являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

Настройка времени выполнения сканирования

В дальнейшем в данном разделе можно указать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Если необходимо, чтобы процесс сканирования выполнялся быстрее, это займет меньше времени, но во время этого процесса будет значительно увеличено потребление системных ресурсов, что снизит производительность других процессов, выполняемых на компьютере (*этот параметр можно включить, если компьютер включен и не используется*). И наоборот, можно снизить потребление системных ресурсов, увеличив продолжительность сканирования.

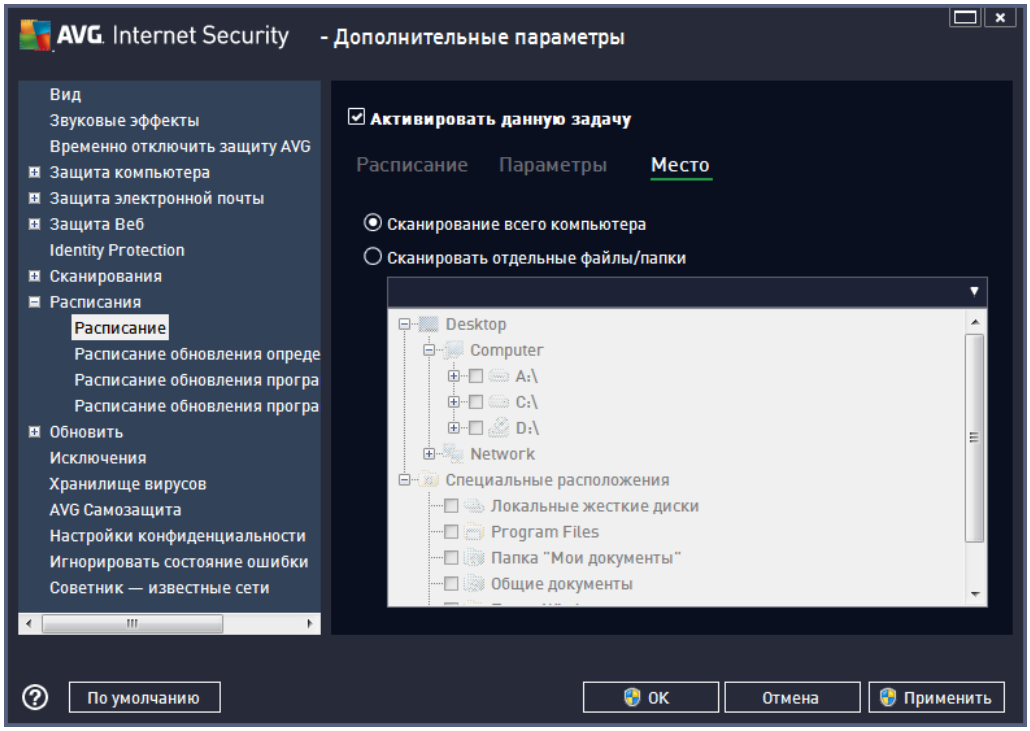
Установить дополнительные отчеты о сканировании

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



Параметры выключения компьютера

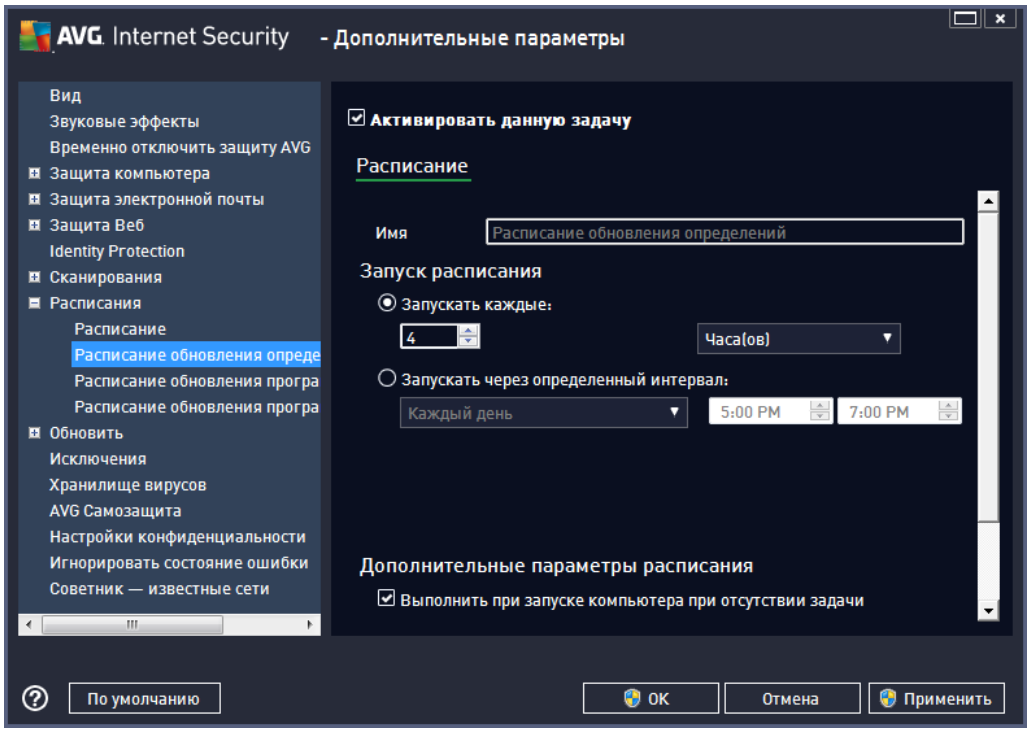
В разделе ***Параметры выключения компьютера*** можно определить, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (***После завершения сканирования выключить компьютер***) становится доступен новый параметр, позволяющий выключать 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.

9.9.2. Расписание обновления определений

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



В этом диалоговом окне можно более полно настроить параметры для расписания обновлений определений вирусов. В текстовом поле ***Имя*** (*неактивном для всех расписаний по умолчанию*) отображается имя, назначенное данному расписанию поставщиком программы.

Выполняемое расписание

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

Дополнительные параметры расписания

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

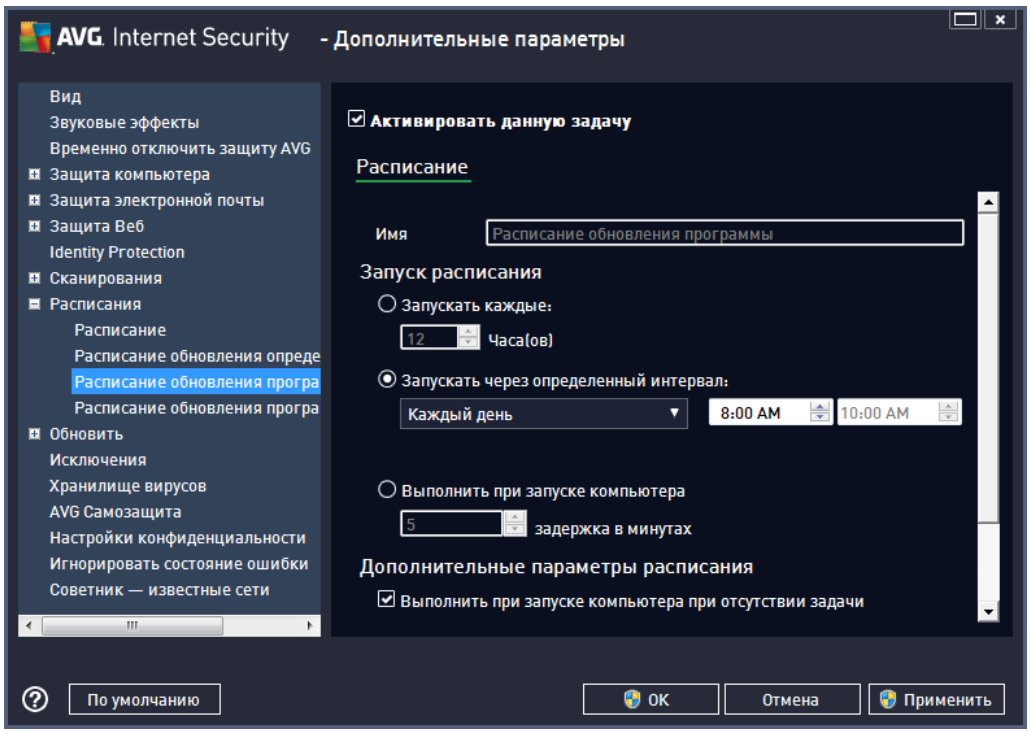
Другие параметры обновления

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

Интернету, чтобы в случае разрыва соединения с Интернетом и сбоя процесса обновления данная операция была выполнена сразу после восстановления подключения к сети. После запуска в назначенное время запланированного обновления отображается всплывающее окно с уведомлением о данном событии над значком AVG на панели задач (*если параметры по умолчанию диалогового окна Дополнительные параметры/Вид не были изменены)*.

9.9.3. Расписание обновления программы

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



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

Выполняемое расписание

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

Дополнительные параметры расписания

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

режиме или выключен.

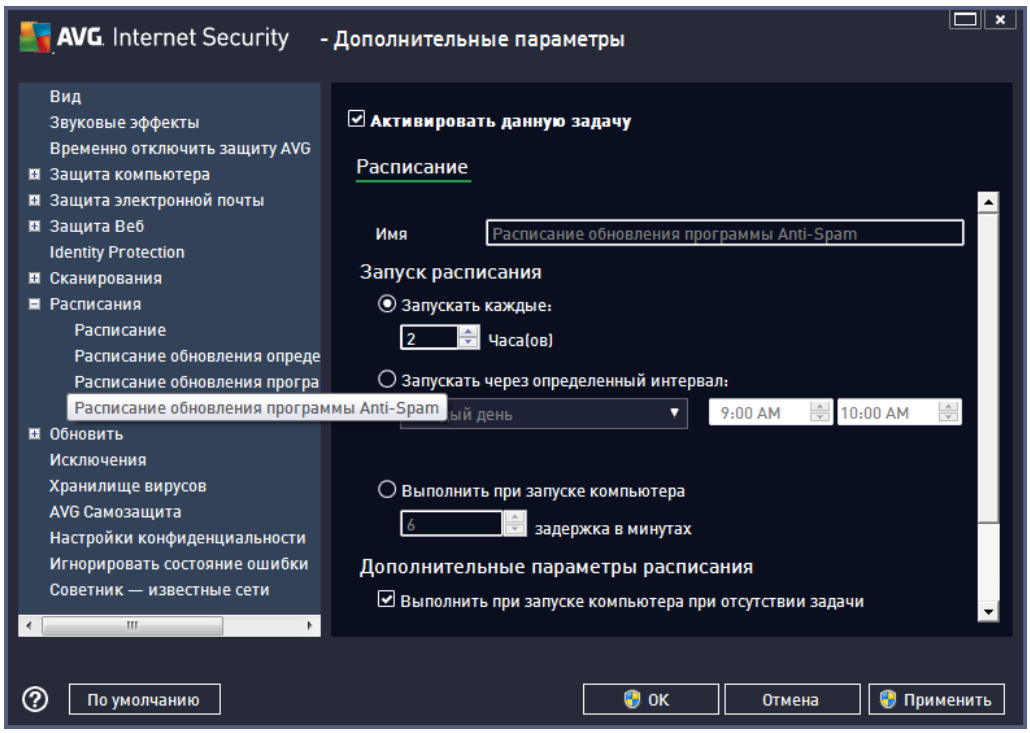
Другие параметры обновления

Установите флажок ***Возобновлять обновление при восстановлении подключения к Интернету***, чтобы в случае разрыва соединения с Интернетом и сбоя процесса обновления эта операция была выполнена сразу после восстановления подключения к Интернету. После запуска в назначенное время запланированного обновления появится всплывающее окно с уведомлением о данном событии над значком AVG в панели задач (*при условии, что параметры по умолчанию диалогового окна Дополнительные параметры / Вид не были изменены*).

Примечание. *Если запланированное обновление программы и сканирование придутся на одно и то же время, сканирование будет прервано, так как процесс обновления имеет более высокий приоритет.*

9.9.4. Расписание обновления компонента Anti-Spam

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



В этом диалоговом окне можно более полно настроить параметры для расписания обновлений. В текстовом поле ***Имя*** (*неактивном для всех расписаний по умолчанию*) указывается имя, назначенное данному расписанию поставщиком программы.

Выполняемое расписание

Укажите временные интервалы для запуска нового запланированного обновления компонента Anti-Spam. Временные интервалы также могут быть определены с помощью повторного запуска обновления компонента Anti-Spam через определенный промежуток времени (***Запускать через каждые ...***), указания точной даты и времени (***Запускать в определенное время ...***), а также определения события, с которыми должен быть связан запуск обновления (***Действие связано с включением компьютера***).

Дополнительные параметры расписания

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

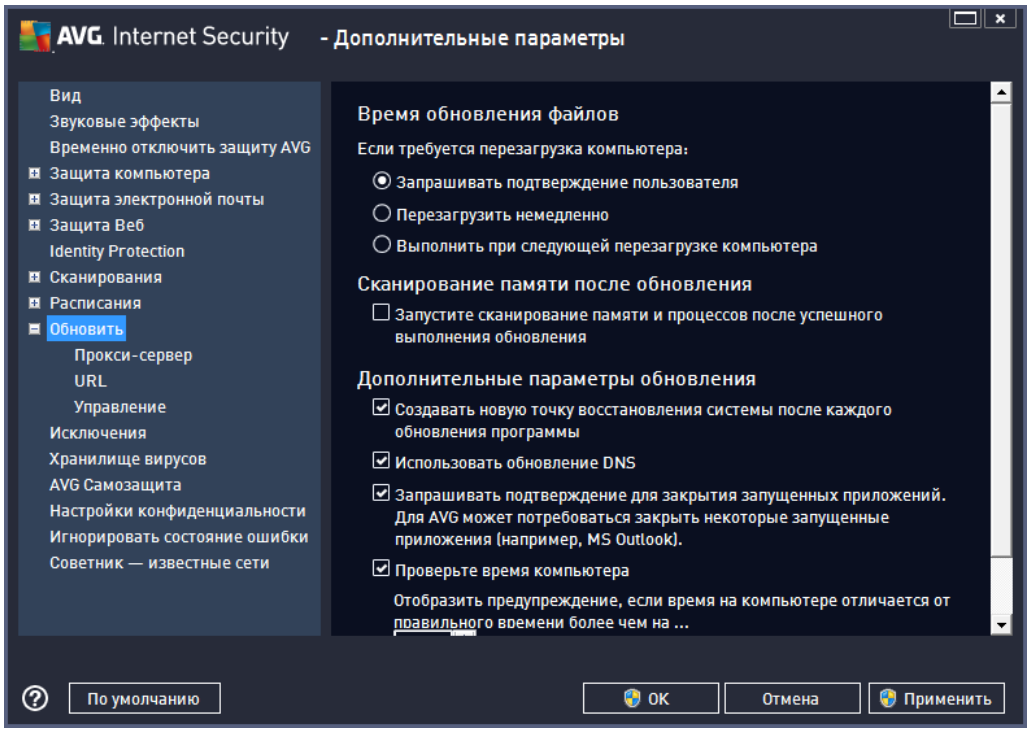
Другие параметры обновления

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

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

9.10. Обновление

Элемент навигации ***Обновление*** открывает новое диалоговое окно, в котором можно указать общие параметры обновления продукта AVG.



Время обновления файлов

В данном разделе можно выбрать одно из трех действий, которые будут использоваться, если в процессе обновления потребуется перезагрузка ПК. Завершение обновления можно запланировать при следующей перезагрузке ПК, а можно выполнить перезагрузку сразу же.

- ***Запрашивать подтверждение пользователя*** *(по умолчанию)* — отобразится запрос на подтверждение перезагрузки ПК, необходимой для завершения процесса обновления
- ***Перезагрузить немедленно*** — перезагрузка будет выполнена автоматически сразу после завершения процесса обновления. Запрос на подтверждение отображаться не будет.
- ***Выполнить при следующей перезагрузке компьютера*** — завершение процесса обновления будет отложено до следующей перезагрузки. Помните, что данный параметр рекомендуется выбирать, только если перезагрузка компьютера происходит регулярно, как минимум раз в день!

Сканирование памяти после обновления

Установите этот флажок, если требуется запускать сканирование памяти после каждого успешно завершенного обновления. В последнем загруженном обновлении могут быть новые определения вирусов, которые сразу должны быть применены при сканировании.

Дополнительные параметры обновления

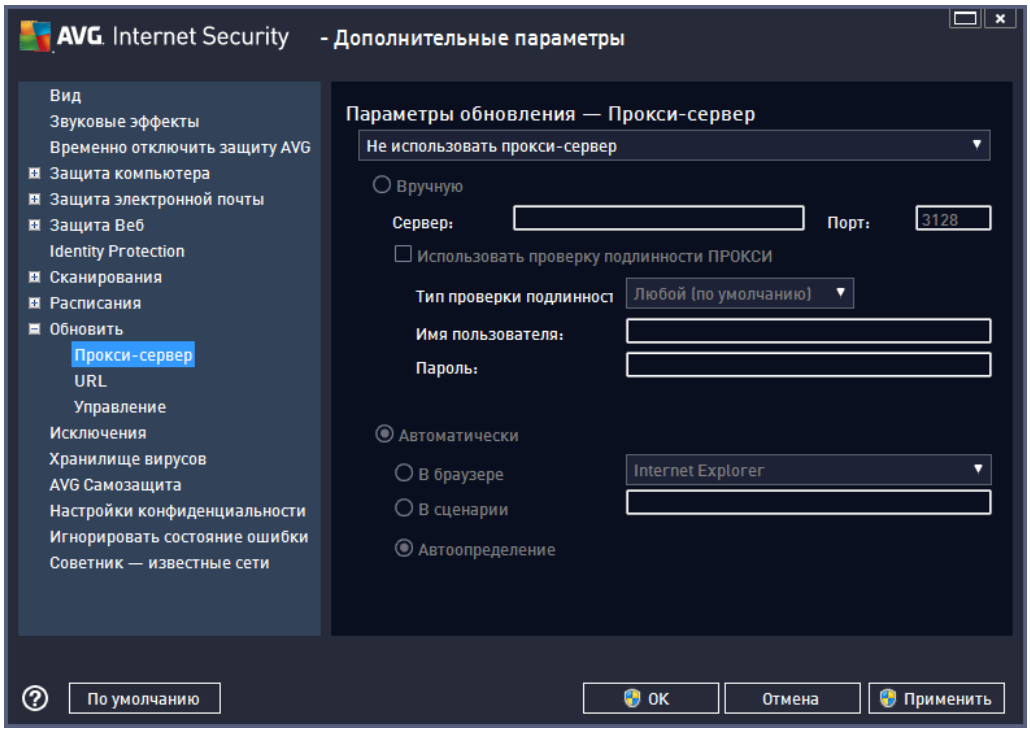
- ***Создавать новую точку восстановления системы после каждого обновления программы*** — перед каждым запуском обновления программы AVG будет создаваться точка восстановления системы. Если не удастся выполнить обновление или произойдет сбой в работе ОС, всегда можно будет восстановить начальную конфигурацию ОС с этой точки. Данный параметр доступен в меню Пуск / Все программы / Стандартные / Служебные / Восстановление системы. Однако любые изменения следует вносить только опытным пользователям. Не снимайте этот флажок, если данный параметр будет использоваться.

- ***Использовать обновление DNS*** (*включено по умолчанию*) — если этот флажок установлен, после запуска обновления программа **AVG Internet Security 2013** запросит на DNS-сервере сведения о последней версии вирусной базы данных и программы. После этого будут загружены и установлены только самые маленькие обязательные файлы обновления. Таким образом, удастся уменьшить количество загружаемых данных и выполнить процесс быстрее.

- ***Запрашивать подтверждение на закрытие запущенных приложений*** (*выбрано по умолчанию*) — этот параметр гарантирует, 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 уведомлений в случаях, когда время компьютера отличается от правильного на указанное количество часов.

9.10.1. 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.

- ***Не использовать прокси-сервер*** — этот параметр установлен по умолчанию.
- ***Использовать прокси-сервер***
- ***Попытаться использовать прокси-сервер, при неудаче подключиться напрямую***

Если вы решили использовать 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)

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

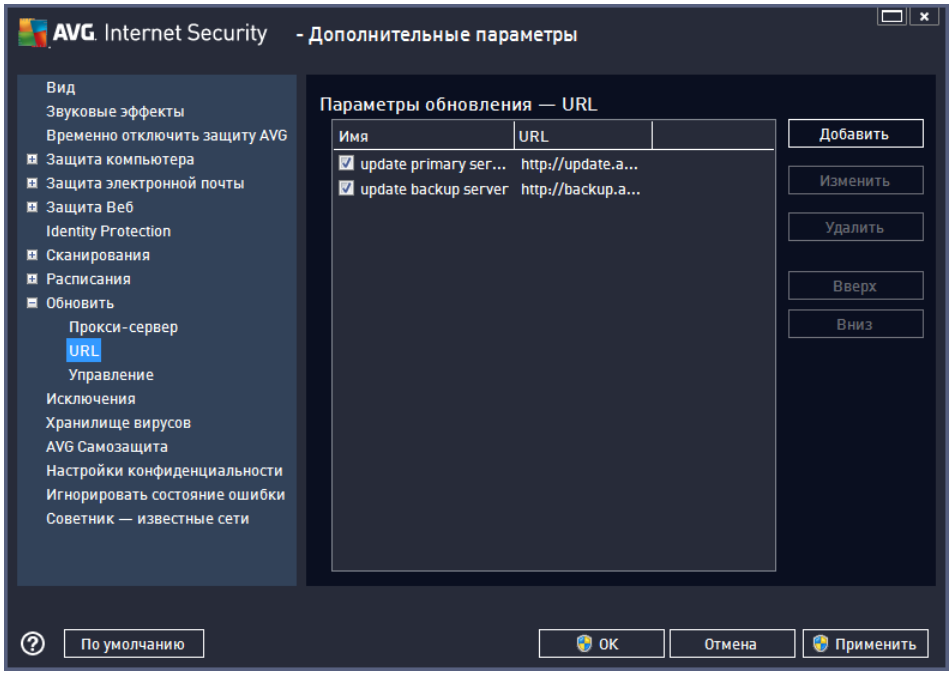
Автоматическая настройка

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

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

9.10.2. URL-адрес

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



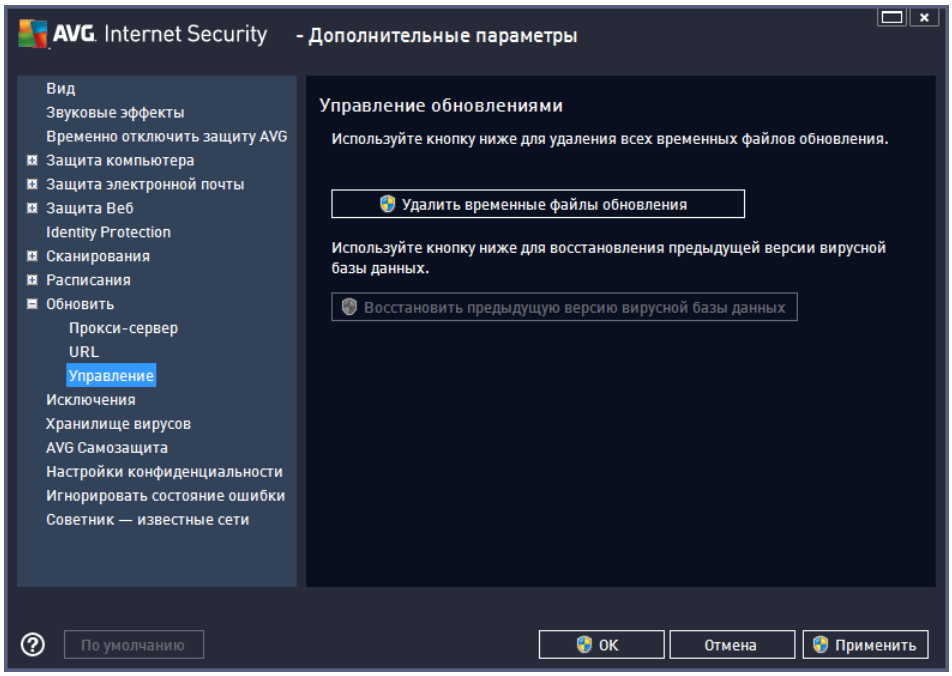
Кнопки управления

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

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

9.10.3. Управление

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

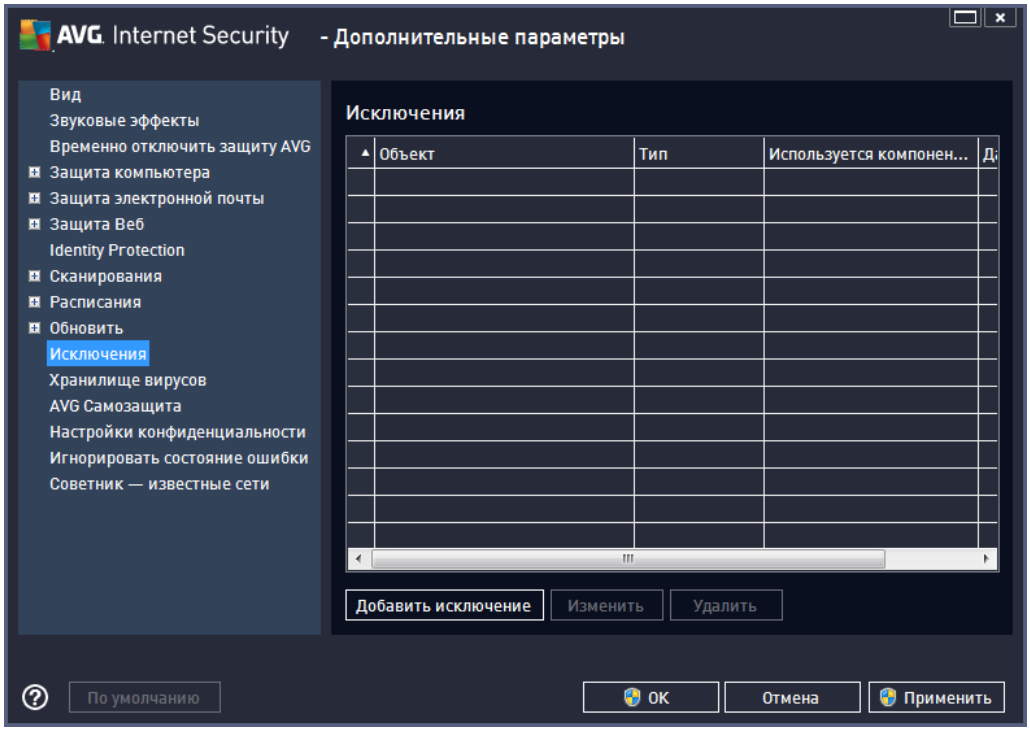


- ***Удалить временные файлы обновления*** — нажмите эту кнопку, чтобы удалить все резервные файлы обновлений с жесткого диска (*по умолчанию эти файлы сохраняются в течение 30 дней*)
- ***Восстановить предыдущую версию вирусной базы данных*** — нажмите эту кнопку, чтобы удалить последнюю версию вирусной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

9.11. Исключения

В диалоговом окне ***Исключения*** можно определить исключения, т. е. объекты, которые **AVG Internet Security 2013** будет игнорировать. Как правило, назначить исключение требуется, если AVG постоянно определяет программу или файл как угрозу или блокирует какой-либо безопасный сайт как опасный. Добавьте такой файл или сайт в список исключений, и AVG больше не будет сообщать о нем и блокировать его.

Вы должны быть абсолютно уверены в том, что данный файл, программа или веб-сайт действительно безопасны.



В таблице, приведенной в диалоговом окне, вы увидите список исключений, если они были назначены. Рядом с каждым пунктом находится флажок. Если флажок установлен, то элемент исключен; в противном случае исключение определено, но не используется. Щелкните заголовок столбца для сортировки элементов по другому критерию.

Кнопки управления

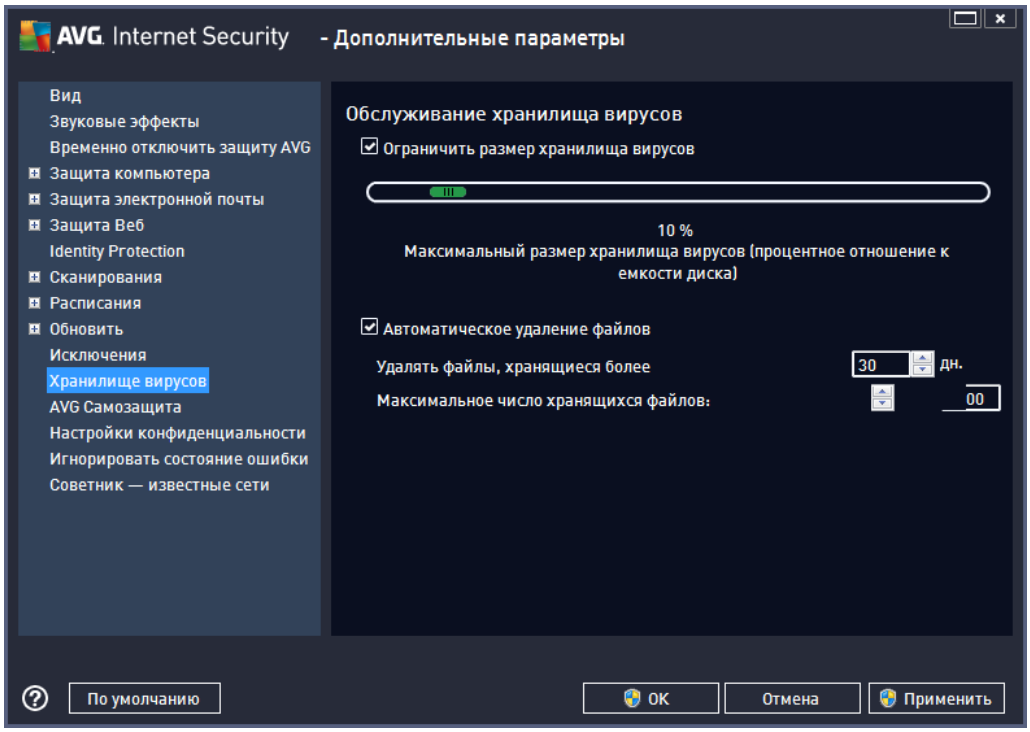
- ***Добавить исключение*** — щелкните эту кнопку, чтобы открыть новое диалоговое окно, где можно указать объекты, которые не будут сканироваться AVG. Прежде всего вам будет предложено определить тип объекта (файл, папка или URL-адрес). После этого потребуется открыть нужную директорию, чтобы указать путь к данному объекту, или ввести URL-адрес. Наконец, вам будет предложено выбрать функции AVG, которые будут игнорировать указанный объект *(постоянная защита, защита учетных данных, сканирование, Anti-Rootkit)*.

- ***Редактировать*** — эта кнопка активна только в случае, если исключения уже определены и перечислены в таблице. В таком случае можно ее использовать для

открытия диалогового окна для данного исключения, а затем настроить его параметры.

- ***Удалить*** — эта кнопка отменяет определенное ранее исключение. Можно удалять исключения по одному или выделить группу исключений из списка и удалить их одновременно. После удаления исключения соответствующие файлы, папки и URL-адреса будут снова проверяться AVG. Обратите внимание, что файлы и папки не удаляются; будет удалено только исключение!

9.12. Хранилище вирусов

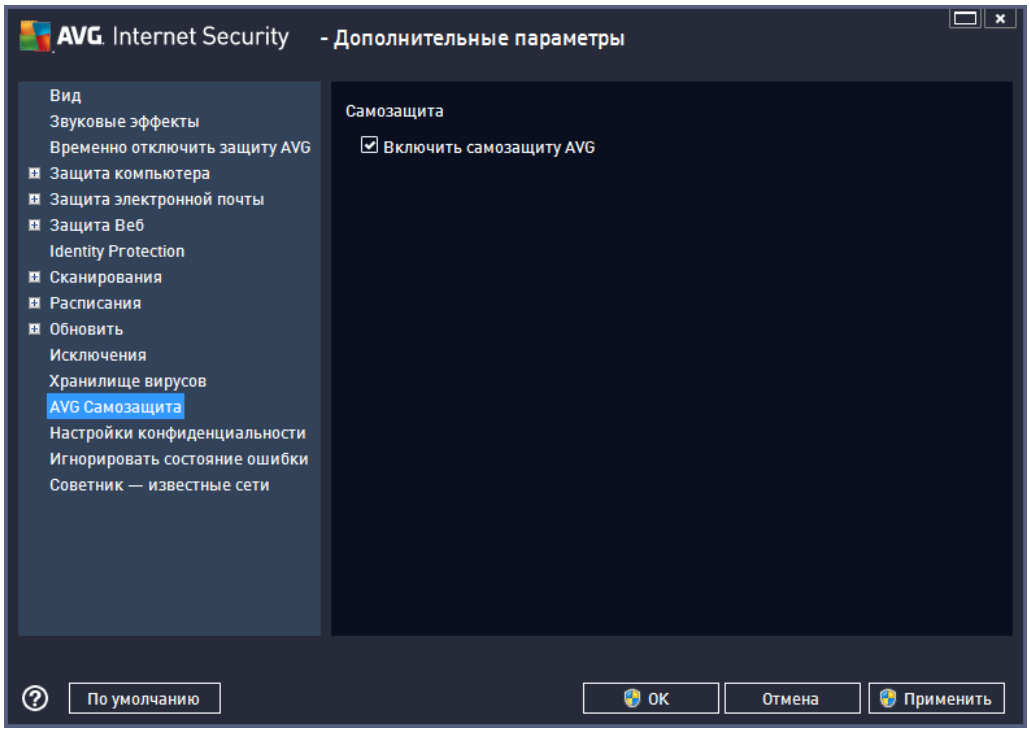


Диалоговое окно ***Обслуживание хранилища вирусов*** позволяет определить несколько параметров администрирования объектов, находящихся в хранилище вирусов:

- ***Предельный размер хранилища вирусов***. Установите максимальный размер хранилища вирусов с помощью ползунка. Размер хранилища указывается пропорционально размеру локального диска.

- ***Автоматическое удаление файлов*** — в данном разделе можно указать максимальное время хранения объектов в хранилище вирусов (***Удалять файлы, хранящиеся более ... дней***), а также максимальное количество файлов, хранящихся в хранилище вирусов (***Максимальное число хранящихся файлов***).

9.13. Самозащита AVG

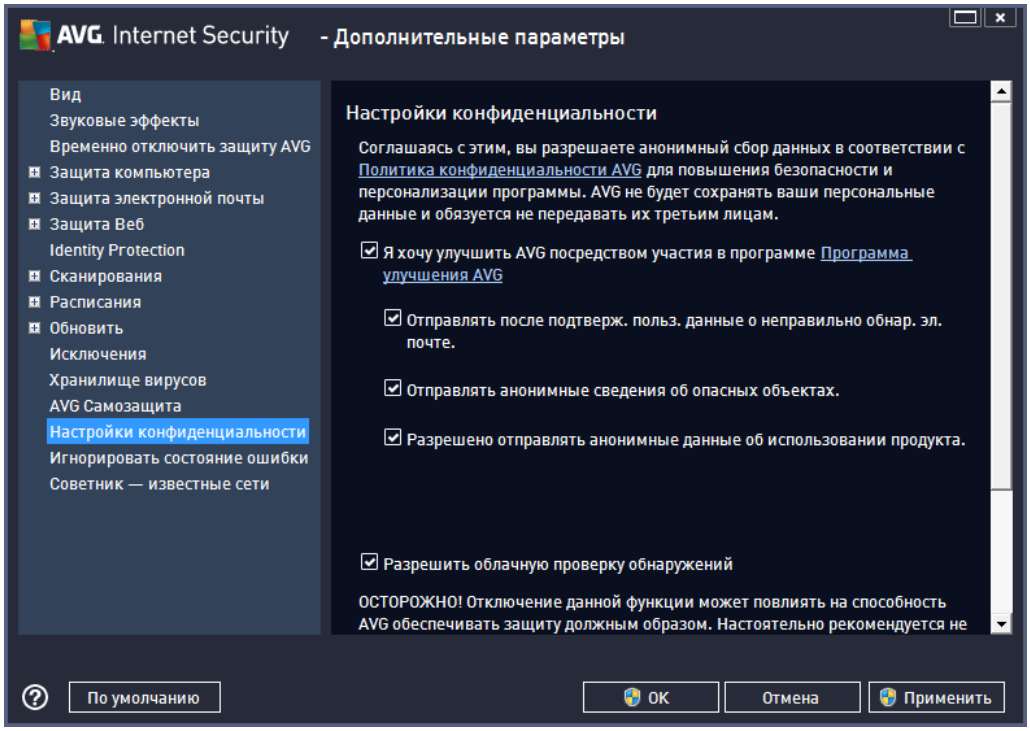


Компонент ***Самозащита AVG*** обеспечивает программе **AVG Internet Security 2013** защиту собственных процессов, файлов, ключей реестра от изменения или деактивации. Необходимость такого вида защиты объясняется тем, что некоторые особо сложные виды угроз пытаются отключить антивирусную защиту, чтобы затем беспрепятственно причинять вред компьютеру.

Не рекомендуется отключать эти параметры!

9.14. Настройки конфиденциальности

В диалоговом окне ***Настройки конфиденциальности*** вы можете принять участие в программе улучшения продуктов AVG и помочь нам повысить общий уровень безопасности в Интернете. Ваши отчеты помогут нам собирать актуальные сведения о последних угрозах от пользователей по всему миру и улучшить защиту. Отправка отчетов происходит автоматически и не доставляет неудобств. Личные данные не включаются в отчеты. Передача отчетов об обнаруженных угрозах является необязательным параметром, однако мы настоятельно рекомендуем оставить его включенным. Это поможет нам улучшать вашу защиту, а также защиту других пользователей AVG.



В этом диалоговом окне доступны приведенные ниже настройки параметров.

- ***Я хочу помочь компании AVG улучшить свои продукты и принимаю участие в программе улучшения продуктов AVG*** *(выбрано по умолчанию)* — если вы хотите помочь усовершенствовать продукты **AVG Internet Security 2013**, не изменяйте этот параметр. В этом случае в компанию AVG будут отправляться отчеты обо всех обнаруженных угрозах, что позволит нам собирать актуальные сведения о вредоносном ПО от пользователей по всему миру и улучшить общую защиту всех пользователей в Интернете. Отправка отчетов происходит автоматически и не доставляет неудобств. Персональные данные в отчеты не включаются.

    - ***Разрешить отправлять данные о неправильно определенной электронной почте после подтверждения пользователя*** *(выбрано по умолчанию)* — отправка сведений о сообщениях электронной почты, которые были по ошибке определены как спам, и о нежелательных сообщениях, которые не удалось обнаружить компоненту Anti-Spam. При отправке таких сведений отображается запрос на подтверждение.

    - ***Разрешить отправлять анонимные данные об обнаруженных или подозрительных угрозах*** *(выбрано по умолчанию)* — отправлять сведения обо всех подозрительных или опасных кодах, а также обнаруженных на компьютере моделях поведения *(это может быть вирус, шпионское ПО или вредоносная веб-страница, на которую вы собираетесь перейти)* .

    - ***Разрешить отправлять анонимные данные об использовании продукта*** *(выбрано по умолчанию)* — отправка основных статистических данных об использовании приложения: количество обнаруженных угроз, запущенные сканирования, успешные или неуспешные обновления и т. п.

- ***Разрешить проверку обнаружений в облаке*** *(выбрано по умолчанию)* — проверка обнаруженных угроз на предмет ложных срабатываний.

Наиболее распространенные угрозы

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

- ***Вирус*** — это вредоносный код, способный к самостоятельному копированию и распространению, который трудно заметить, пока он не повредит систему. Некоторые вирусы представляют собой серьезную угрозу, удаляя или намеренно изменяя файлы, в то время как другие вирусы могут оказаться вполне безобидными, например они могут просто воспроизводить отрывок какой-то мелодии. Тем не менее все вирусы являются опасными из-за способности к саморазмножению, и даже самый простой вирус может очень быстро занять всю память компьютера и привести к сбою системы.

- ***Червь*** — подкатегория вирусов, для которых, в отличие от обычных вирусов, не требуется объект-носитель; он самостоятельно распространяется на другие компьютеры, обычно по электронной почте, и приводит к перегрузке почтовых серверов и сетей.

- ***Шпионское ПО*** — обычно относится к категории вредоносных (*вредоносное ПО = любое вредоносное программное обеспечение, включая вирусы*) исполняемых программ. Обычно это «троянские кони», нацеленные на кражу личной информации, паролей, номеров кредитных карт либо на проникновения в компьютер, чтобы дать злоумышленнику возможность управлять им удаленно. Разумеется, все это происходит без ведома или согласия владельца компьютера.

- ***Потенциально нежелательные программы*** — разновидность шпионского ПО, которая не обязательно представляет опасность для компьютера. В качестве конкретного примера PUP можно привести рекламное ПО. Это специальное программное обеспечение, предназначенное для распространения рекламы, как правило, посредством отображения всплывающих окон, что вызывает раздражение, но не представляет опасности.

- ***Кроме того, следящие файлы cookie*** могут также рассматриваться как разновидность шпионского ПО, так как эти небольшие файлы, хранящиеся в веб-браузере и автоматически отправляющиеся к «родительскому» веб-сайту при повторном его посещении, могут содержать сведения о просмотренных страницах в Интернете и другую аналогичную информацию.

- ***Эксплойт*** — этот вредоносный код пользуется недостатками или уязвимыми местами операционной системы, интернет-браузера и других важных программ.

- ***Фишинг*** — способ получения важных личных данных, при котором мошенники представляются сотрудниками надежных и хорошо известных организаций. Обычно потенциальным жертвам отправляются сообщения электронной почты с запросом, например на обновление сведений о банковском счете. В этих сообщениях пользователям предлагается перейти по ссылке, которая ведет на поддельный веб-сайт банка.

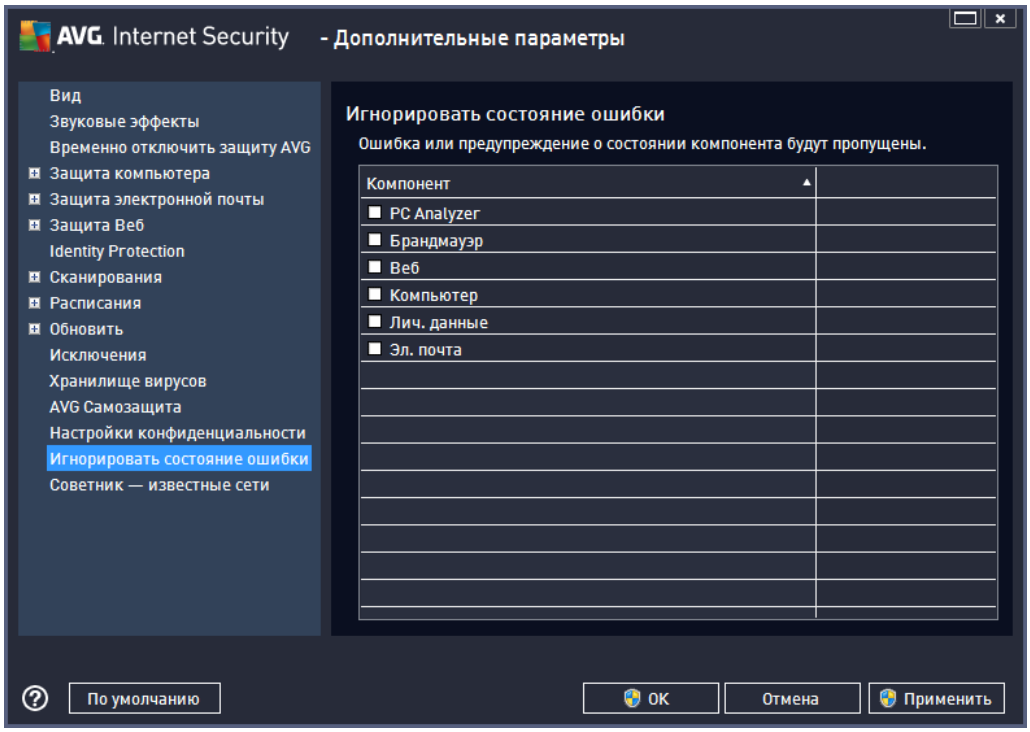
- ***Ложное сообщение*** — данная угроза представляет собой нежелательное сообщение электронной почты, содержащее опасные, подозрительные или просто бесполезные сведения. Многие из вышеперечисленных угроз распространяются посредством ложных сообщений электронной почты.

- ***Вредоносные веб-сайты*** — сайты, которые преднамеренно устанавливают вредоносное ПО на вашем компьютере, а также взломанные сайты, которые являются законными и распространяют вирусы в результате взлома.

Для защиты от всех перечисленных угроз AVG Internet Security 2013 предлагает ряд специальных компонентов. Краткое описание см. в разделе Обзор компонентов данного документа.

9.15. Игнорировать состояние ошибки

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



По умолчанию в этом списке не выбрано никаких компонентов. Это означает, что если компонент переходит в состояние ошибки, сразу же появится уведомление с помощью следующих сигналов.

- Значок на панели задач — во время безупречной работы всех компонентов AVG значок отображается четырьмя цветами; при появлении ошибок на значке появляется желтый восклицательный знак.

- Текстовое описание существующей проблемы в разделе Сведения о состоянии безопасности на главном окне AVG.

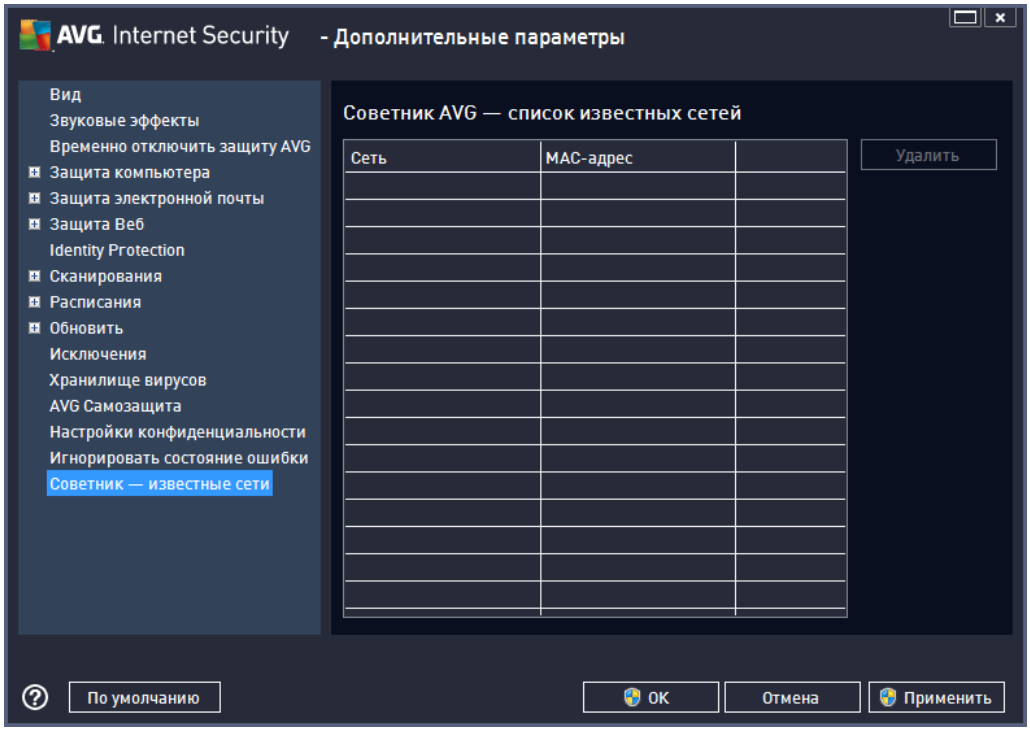
Бывают ситуации, когда по той или иной причине требуется временно отключить компонент. ***Это не рекомендуется делать, следует всегда оставлять включенными все компоненты и сохранять параметры по умолчанию***, однако такое возможно. В этом случае значок на панели задач автоматически оповестит о состоянии ошибки компонента. Тем не менее, в данной ситуации настоящей ошибки не возникает, так как пользователь преднамеренно ее вызвал и был предварительно предупрежден о возможном риске. В то же время, если значок отобразился серым цветом, он не может оповещать о дальнейших возможных ошибках.

В такой ситуации в диалоговом окне ***Игнорировать состояние ошибки*** можно выбрать компоненты, которые могут находиться в состоянии ошибки (*или быть отключены*), и о которых не требуется получать информацию. Для подтверждения нажмите кнопку ***OK***.

9.16. Советник — известные сети

Советник AVG выполняет функцию отслеживания сетей, с которыми работает пользователь. Если обнаруживается новая сеть *(с уже используемым сетевым именем, в связи с чем может возникнуть путаница)*, появляется уведомление с рекомендацией проверить ее безопасность. Если вы уверены в безопасности данной сети, ее также можно занести в этот список *(посредством ссылки в уведомлении Советника AVG, которое появляется в области уведомлений каждый раз, когда обнаружена неизвестная сеть. Для получения подробных сведений см. главу Советник AVG)*. Советник AVG запомнит уникальные характеристики сети *(в частности, MAC-адрес)* и не будет больше отображать уведомления. Каждая сеть, к которой вы подключаетесь, будет автоматически считаться известной и добавляться в список. С помощью кнопки ***Удалить*** можно исключить любые записи. Соответствующая сеть снова будет считаться неизвестной и потенциально опасной.

В данном диалоговом окне можно выбрать сети, которые будут считаться известными.



Примечание. *Функция известных сетей в Советнике AVG не поддерживается в 64-разрядных версиях Windows XP.*

10. Параметры Firewall

Конфигурация компонента Firewall открывается в новом окне, где с помощью нескольких диалоговых окон можно настроить дополнительные параметры для компонента. В новом окне открывается конфигурация компонента Firewall, где на нескольких вкладках можно изменить его дополнительные параметры. Конфигурация отображается либо в базовом режиме, либо в режиме для опытных пользователей. При первом открытии окна конфигурации отображается базовая версия, в которой можно изменить следующие параметры.

- Общие сведения
- Приложения
- Общий доступ к файлам и принтерам

В нижней части окна находится кнопка ***Режим «Для опытных пользователей»***. Нажмите эту кнопку, чтобы получить доступ к дополнительным параметрам, позволяющим более точно настроить конфигурацию компонента Firewall.

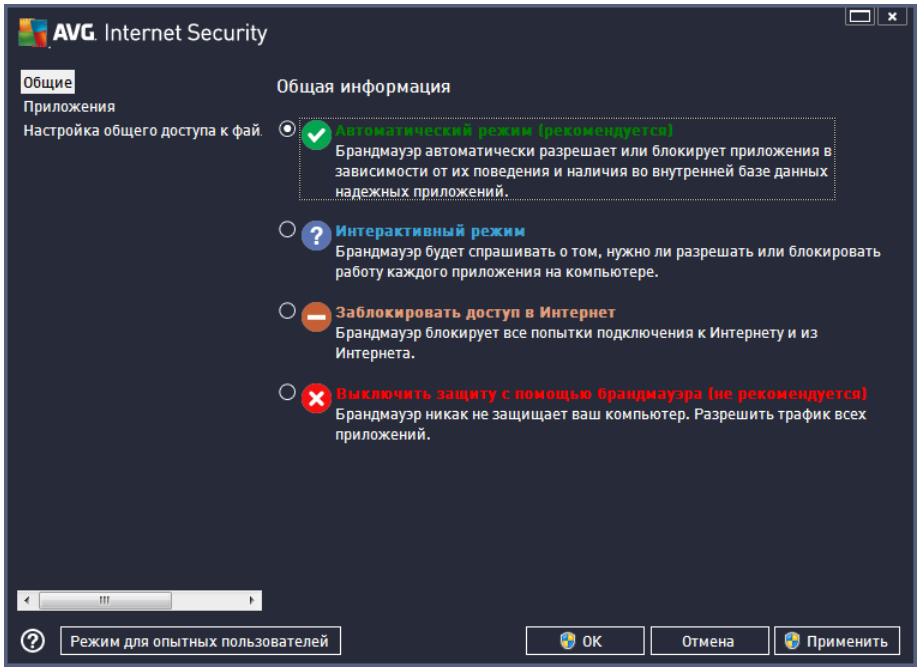
- Дополнительные параметры
- Определенные сети
- Системные службы
- Журналы

Однако все компоненты AVG Internet Security 2013 настроены поставщиком ПО для обеспечения оптимальной производительности. Не изменяйте настройки по умолчанию без необходимости. Все изменения настроек должны выполняться только опытными пользователями!

10.1. Общие сведения

В диалоговом окне ***Общие сведения*** предоставляются краткие сведения о режимах компонента Firewall. Текущий режим Firewall можно изменить, просто выбрав в меню другой режим.

Однако все компоненты AVG Internet Security 2013 настроены поставщиком ПО для обеспечения оптимальной производительности. Не изменяйте настройки по умолчанию без необходимости. Все изменения настроек должны выполняться только опытными пользователями!



С помощью Firewall можно установить специальные правила безопасности, основанные на том, является ли компьютер частью домена, автономным компьютером или ноутбуком. Для каждого варианта требуется определенный уровень защиты, который обеспечивается в соответствующих режимах. Другими словами, режим Firewall — это особая его конфигурация. Можно использовать несколько предопределенных конфигураций.

- ***Автоматически*** — в этом режиме Firewall применяет параметры автоматически ко всему сетевому трафику. Вам не будет предложено никаких действий. Firewall разрешит подключение со стороны всех известных приложений. Одновременно будет создано правило, разрешающее данному приложение подключаться в будущем. Для прочих приложений Firewall определит, блокировать или разрешать подключение, в соответствии с поведением данных приложений. В этом случае, однако, правило не будет создано, и приложение будет проходить проверку при каждой попытке подключения. ***Автоматический режим ведет себя достаточно ненавязчиво и рекомендуется для большинства пользователей.***

- ***Интерактивный*** — этот режим подходит, если на компьютере нужно полностью контролировать входящий и исходящий сетевой трафик. Firewall будет отслеживать трафик и информировать вас о каждой попытке подключения или передачи данных. При необходимости вы сможете разрешить или заблокировать это действие. Рекомендуется только для опытных пользователей.

- ***Заблокировать доступ в Интернет*** — полная блокировка подключения к Интернету. Нельзя войти в Интернет, доступ к компьютеру извне невозможен. Рекомендуется только в особых случаях и на короткое время.

- ***Отключить Firewall*** — это действие разрешит компьютеру обмен данными по сети. Следовательно, компьютер станет уязвим для атак злоумышленников. Всегда используйте этот параметр с осторожностью.

Обратите внимание, что в Firewall также есть особый автоматический режим. Этот режим

активируется автоматически при отключении компонентов Компьютер или Identity protection, вследствие чего компьютер становится боле уязвимым. В таких случаях Firewall будет разрешать подключение со стороны только известных и абсолютно безопасных приложений. Для всех остальных приложений вам будет предложено действие. Эта мера призвана компенсировать отключенные компоненты защиты и тем самым обеспечить безопасность компьютера.

10.2. Приложения

Диалоговое окно ***Приложение*** содержит список всех приложений, которые пытались установить подключение по сети, а также значки назначенных действий.

Приложения, указанные в ***Списке приложений***, были обнаружены на компьютере (*и им были назначены соответствующие действия*). Можно назначать следующие действия:

- — разрешить обмен данными для всех сетей;
- — блокировать подключение
- — отображать диалоговое окно запроса (*при каждой попытке приложения установить подключение по сети необходимо будет подтвердить разрешение или блокировку подключения*);
- — определены дополнительные параметры.

Обратите внимание, что можно обнаружить только установленные приложения. 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 сохранить 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 с приоритетом относительно правил других приложений. ***Другие правила приложений*** (*внизу списка*) используются в последнюю очередь, если не назначено особых правил приложений, например для неизвестного или неопределенного приложения. Выберите действие, которое будет выполняться при попытке подключения по сети: «Блокировать» *(обмен данными будет заблокирован)*, «Разрешить» *(будет разрешен обмен данными в любых сетях)*, «Спрашивать» *(вам будет предложено самостоятельно решить, блокировать или разрешить приложение)*. ***Параметры данных элементов отличаются от параметров обычных приложений и предназначены только для опытных пользователей. Настоятельно рекомендуется не изменять параметры.***

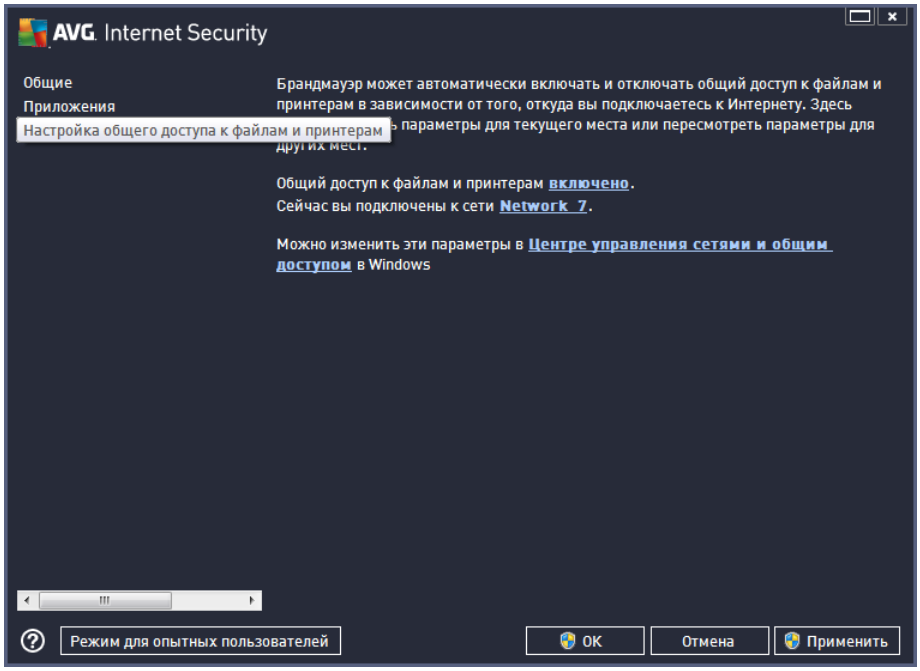
Кнопки управления

Данный список можно редактировать с помощью следующих кнопок управления.

- ***Добавить*** — открытие пустого диалогового окна, в котором можно определить правила для нового приложения.
- ***Редактировать*** — открытие того же диалогового окна с данными для редактирования существующего набора правил для приложения.
- ***Удалить*** — удаление выбранного приложения из списка.

10.3. Общий доступ к файлам и принтерам

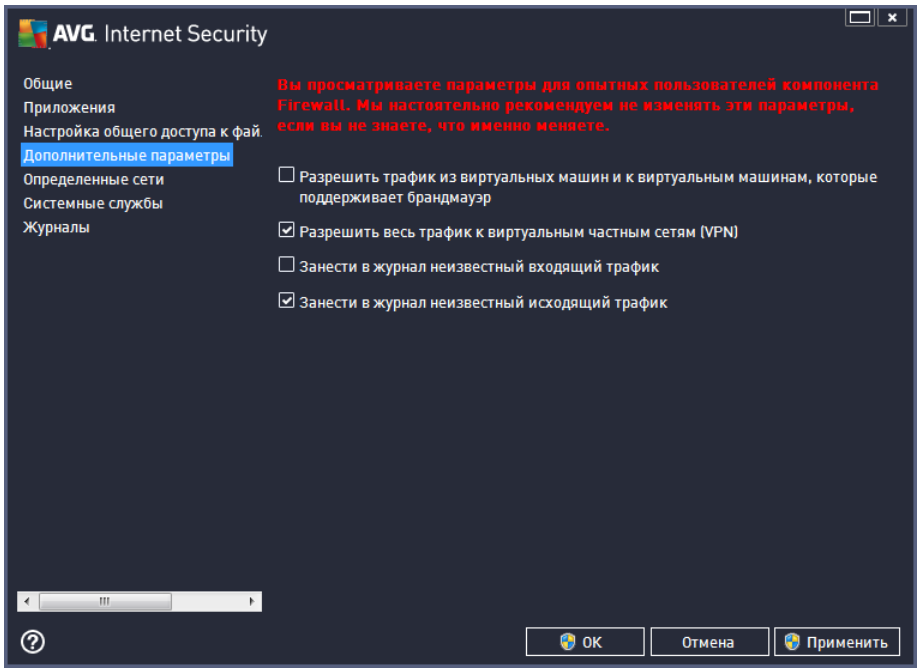
Предоставить общий доступ к файлам и принтерам означает открыть доступ ко всем файлам и папкам, которые в Windows помечены как «Общие», общие разделы диска, принтеры, сканеры и прочие подобные устройства. Желательно предоставлять общий доступ к таким элементам только в безопасных сетях *(например, домашних сетях, сетях предприятий и учебных заведений)*. Однако если вы подключаетесь к общедоступной сети *(например, к сети Wi-Fi в аэропорту или интернет-кафе)*, предоставлять общий доступ не следует. С помощью AVG Firewall можно с легкостью заблокировать или разрешить обмен данными, а также сохранять данные параметры безопасности для уже известных сетей.



В диалоговом окне ***Общий доступ к файлам и принтерам*** можно изменить параметры общего доступа для данных объектов и подключенных в данное время сетей. В Windows XP название сети соответствует наименованию, выбранному вами при первом подключении к данной сети. Для Windows Vista и более поздних версий название сети автоматически назначается центром управления сетями и общим доступом.

10.4. Дополнительные параметры

Любое изменение настроек в диалоговом окне «Дополнительные параметры» должно выполняться ТОЛЬКО ОПЫТНЫМИ ПОЛЬЗОВАТЕЛЯМИ!



В диалоговом окне ***Дополнительные параметры*** можно выбрать следующие параметры компонента Firewall.

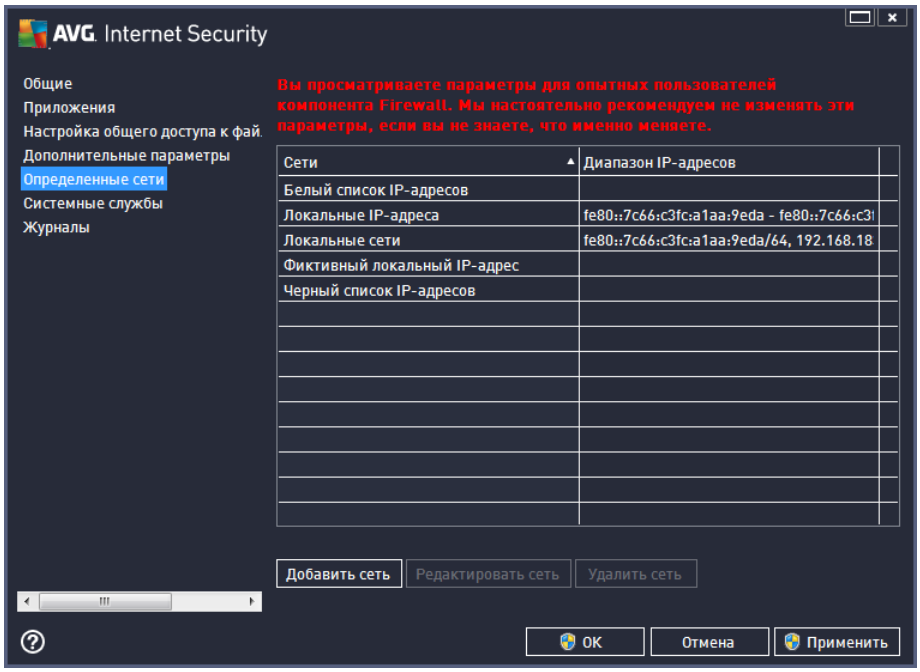
- ***Разрешить входящий и исходящий трафик для виртуальных машин, поддерживаемых брандмауэром*** — поддержка сетевых соединений для виртуальных машин, например VMWare.

- ***Разрешить трафик в частных виртуальных сетях*** — поддержка подключения к виртуальным частным сетям (VPN) *(используемых для подключения к удаленным компьютерам)*.

- ***Вести журнал неизвестного входящего и исходящего трафика*** — все попытки *входящих и исходящих подключений* со стороны неизвестных приложений будут зарегистрированы в Журнале Firewall.

10.5. Определенные сети

Любое изменение настроек в диалоговом окне «Определенные сети» должно выполняться ТОЛЬКО ОПЫТНЫМИ ПОЛЬЗОВАТЕЛЯМИ!

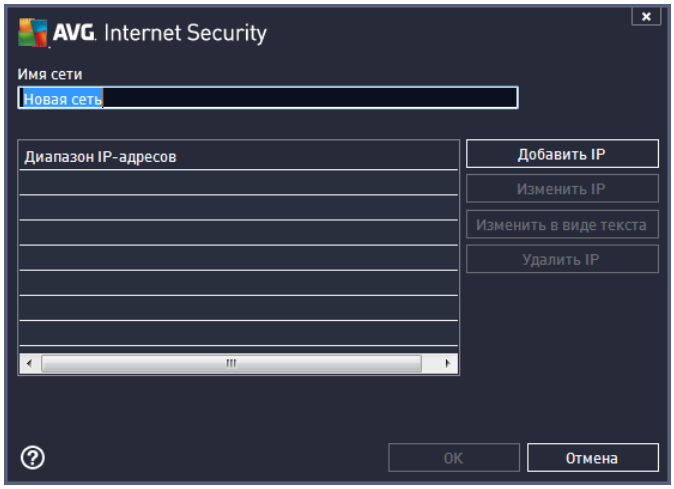


Диалоговое окно ***Определенные сети*** содержит список всех сетей, к которым подключен компьютер. В данном списке отображается следующая информация по каждой обнаруженной сети.

- ***Сети*** — список имен всех сетей, к которым подключен компьютер.
- ***Диапазон IP-адресов*** — каждая сеть будет обнаружена автоматически и указана в виде диапазонов IP-адресов.

Кнопки управления

- ***Добавить сеть*** — открывает новое диалоговое окно, в котором можно изменить параметры недавно определенных сетей, например, чтобы ввести ***Имя сети*** и указать ***диапазон IP-адресов***.

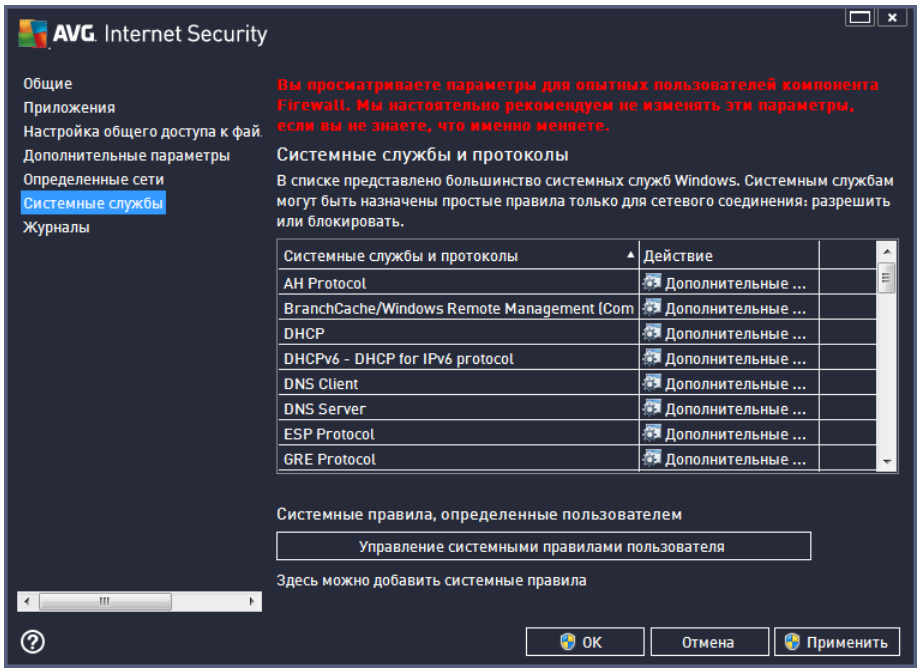


- ***Редактировать сеть*** — открывает диалоговое окно ***Свойства сети*** (*см. выше*), в котором можно редактировать параметры уже определенной сети (*данное диалоговое окно идентично диалоговому окну добавления новых сетей, см. описание в предыдущем абзаце*).

- ***Удалить сеть*** — удаляет ссылки на выбранную сеть из списка сетей.

10.6. Системные службы

Редактирование параметров в диалоговом окне «Системные службы и протоколы» должно выполняться ТОЛЬКО ОПЫТНЫМИ ПОЛЬЗОВАТЕЛЯМИ.



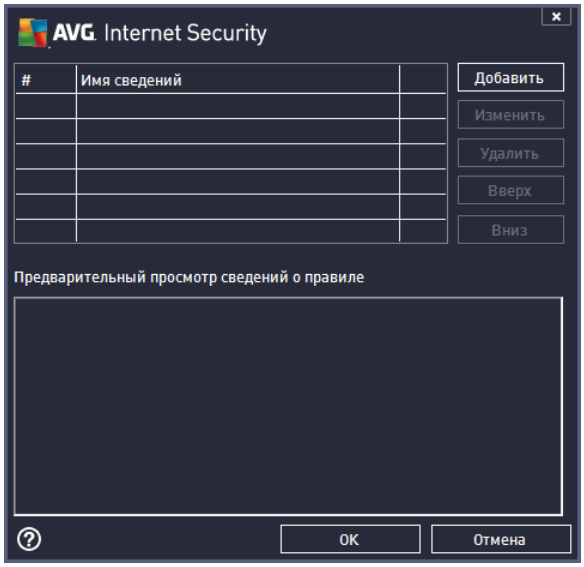
В диалоговом окне ***Системные службы и протоколы*** перечислены стандартные системные службы Windows и протоколы, необходимые для передачи данных по сети. Таблица содержит следующие столбцы.

- ***Системные службы 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
  - Блокировать подключение

Для редактирования параметров элементов в списке (*включая назначенные действия*) щелкните правой кнопкой мыши элемент и выберите ***Редактировать***. ***Изменение системного правила должно выполняться только опытным пользователем; настоятельно рекомендуется оставить системное правило без изменений.***

Определяемые пользователем системные правила

Чтобы открыть новое диалоговое окно для определения правила системной службы (*см. рисунок ниже*), нажмите кнопку ***Управление системными правилами пользователя***. То же диалоговое окно открывается при изменении параметров остальных компонентов из числа системных служб и протоколов. В верхней части данного диалогового окна представлен обзор всех сведений изменяемого в настоящее время системного правила, в нижней части представлены выбранные сведения. С помощью кнопок можно редактировать, добавлять или удалять параметры правил.



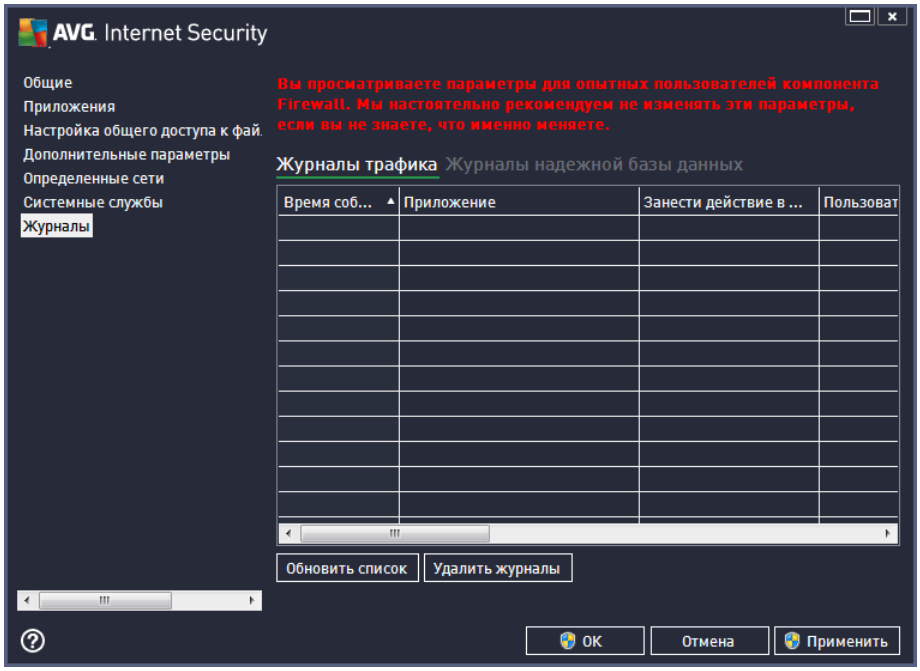
Не забывайте, что детальная настройка правил предполагает определенный уровень компетентности и предназначена в первую очередь для сетевых администраторов, которым необходим полный контроль над конфигурацией компонента Firewall. Если вам неизвестны типы протоколов обмена данными, номера сетевых портов, определения IP-адресов и т. д., не изменяйте эти параметры! Если требуется изменить конфигурацию, ознакомьтесь с файлами справки соответствующих диалоговых окон.

10.7. Журналы

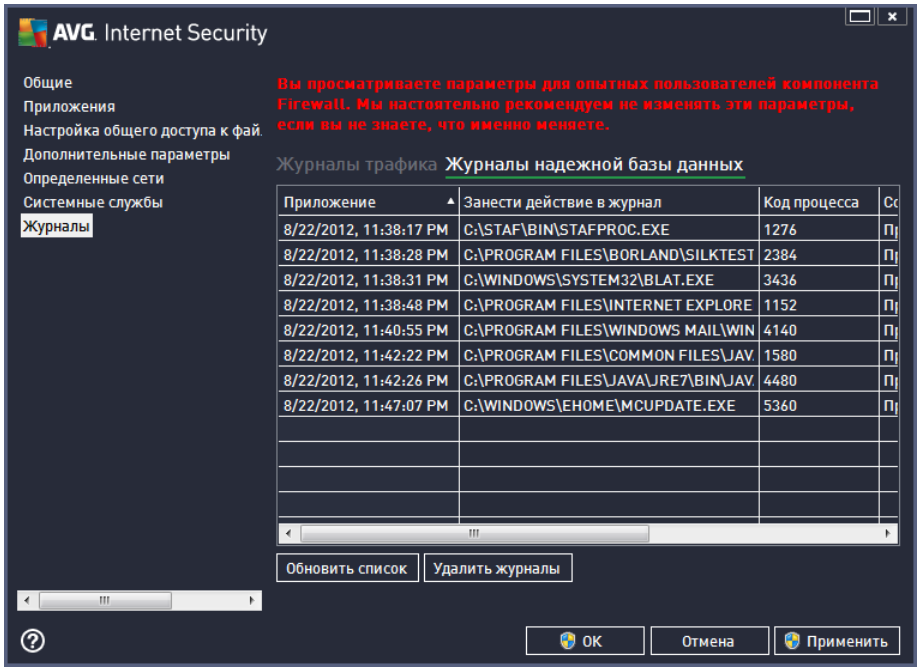
Любое изменение настроек в диалоговом окне «Журналы» должно выполняться ТОЛЬКО ОПЫТНЫМИ ПОЛЬЗОВАТЕЛЯМИ!

В диалоговом окне ***Журналы*** можно просмотреть список всех занесенных в журнал действий и событий компонента Firewall, а также подробное описание соответствующих параметров.

- ***Журналы трафика*** — на этой вкладке содержатся сведения о действиях всех приложений, которые выполняли попытки подключиться к сети. Каждая запись содержит данные о времени события, названии приложения, соответствующем действии в журнале, идентификаторе, направлении подключения, типе протокола, номерах удаленных и локальных портов, а также сведения о локальных и удаленных IP-адресах.



- ***Журналы надежной базы данных***: *надежная база данных* — это внутренняя база данных AVG, содержащая сведения о сертифицированных и надежных приложениях, которым всегда разрешен доступ в Интернет. Если новое приложение первый раз пытается подключиться к сети (*т. е. для него еще не создано правило брандмауэра*), необходимо выбрать — 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 данные об этом приложении, отобразится запрос в отдельном окне, в котором необходимо определить, разрешить ли доступ в сеть для данного приложения.



Кнопки управления

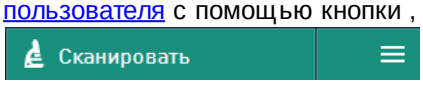
- ***Обновить список*** — все записанные в журнале параметры можно упорядочить по выбранному атрибуту: хронологически (*по дате*) или в алфавитном порядке (*другие столбцы*) — просто щелкните заголовок соответствующего столбца. Используйте кнопку ***Обновить список***, чтобы обновить отображаемую информацию.

- ***Удалить журналы*** — нажмите, чтобы удалить все записи в таблице.

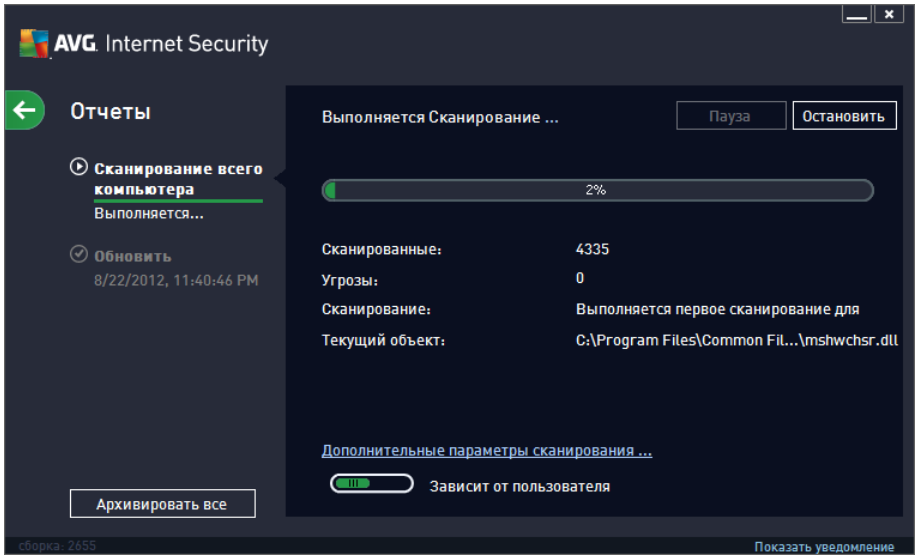
11. Сканирование AVG

По умолчанию **AVG Internet Security 2013** не запускает операции сканирования, так как после начального сканирования *(которое вам будет предложено выполнить)* вы будете полностью защищены благодаря компонентам **AVG Internet Security 2013**, которые всегда на страже и не позволяют вредоносным кодам проникать в систему. Однако при необходимости можно запланировать сканирование, которое будет выполняться через определенные промежутки времени или запустить сканирование вручную.

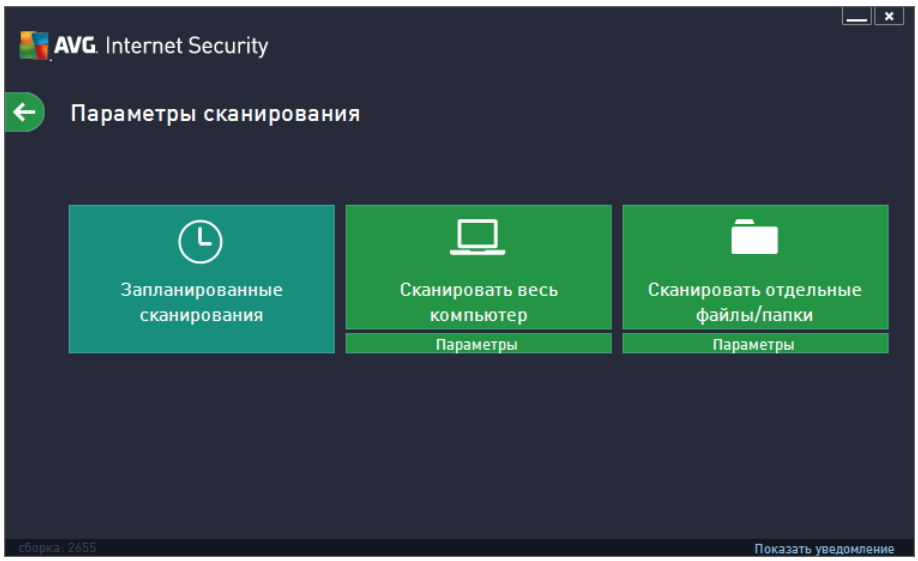
Получить доступ к интерфейсу сканирования AVG можно из основного интерфейса пользователя с помощью кнопки , графически разделенной на две части:



- ***Сканировать сейчас*** — нажмите эту кнопку, чтобы сразу запустить Сканировать весь компьютер и наблюдать за ходом сканирования и его результатами в автоматически открывшемся окне Отчеты.



- ***Настройки*** — воспользуйтесь этой кнопкой *(в виде трех горизонтальных линий на зеленом поле)*, чтобы открыть диалоговое окно ***Параметры сканирования***, в котором можно управлять запланированными сканированиями и изменять параметры для операций Сканировать весь компьютер и Сканирование определенных файлов или папок.



Диалоговое окно ***Параметры сканирования*** разделено на три основных группы параметров.

- ***Управление запланированными сканированиями*** — в этой группе отображаются общие сведения обо всех запланированных сканированиях. Если вы еще не запланировали сканирования, в таблице будет отображаться только сканирование, предопределенное поставщиком программного обеспечения. Данное сканирование по умолчанию отключено. Чтобы включить его, щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт *Активировать задание*. После активации запланированного сканирования можно изменить его параметры с помощью кнопки *Редактировать расписание*. С помощью кнопки *Добавить расписание* также можно создать свое расписание сканирований.

- ***Сканирование всего компьютера / Параметры*** — эта кнопка разделена на две части. Выберите вариант *Сканировать весь компьютер*, чтобы немедленно выполнить полное сканирование компьютера *(подробную информацию об этом виде сканирования см. в соответствующей главе под названием Предварительно настроенное сканирование / Сканирование всего компьютера)*. Нажав на кнопку *Параметры*, вы перейдете в диалоговое окно настройки параметров сканирования всего компьютера.

- ***Сканировать отдельные файлы/папки / Параметры*** — эта кнопка также разделена на две части. Нажмите кнопку *Сканировать отдельные файлы/папки*, чтобы немедленно запустить сканирование выбранных вами областей компьютера *(подробнее о сканировании отдельных файлов и папок см. в соответствующей главе под названием Предварительно настроенные сканирования / Сканировать отдельные файлы/папки)*. Нажав на кнопку *Параметры*, вы перейдете в диалоговое окно настройки параметров сканирования определенных файлов и папок.

11.1. Предопределенные сканирования

Одна из главных функций **AVG Internet Security 2013** — сканирование по требованию. Проверки по требованию предназначены для сканирования различных частей компьютера при подозрении на заражение вирусом. Рекомендуется проводить такие проверки регулярно, даже если, по вашему мнению, вирусы на компьютере отсутствуют.

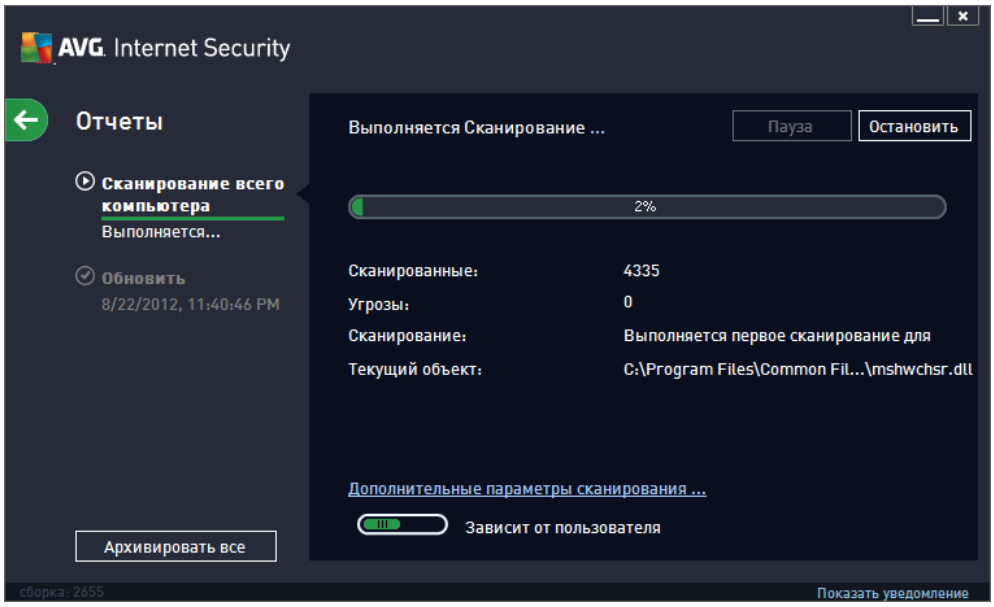
В системе **AVG Internet Security 2013** доступны следующие типы сканирования, предопределенные поставщиком программного обеспечения.

11.1.1. 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 компьютере как минимум один раз в неделю.

Запуск сканирования

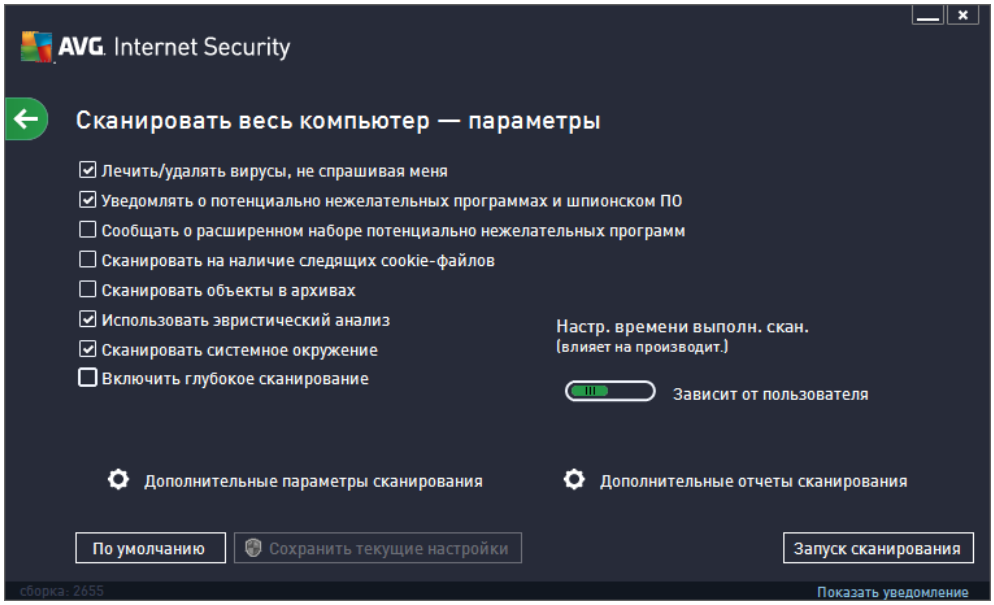
Операцию ***Сканировать весь компьютер*** можно запустить непосредственно из основного интерфейса пользователя, нажав кнопку ***Сканировать сейчас***. Этот тип сканирования не требует какой-либо дополнительной настройки, оно будет запущено сразу. В диалоговом окне ***Выполняется сканирование всего компьютера*** (*см. снимок экрана*) можно увидеть ход сканирования и его результаты. При необходимости сканирование можно приостановить (***Пауза***) или отменить (***Отмена***).



Изменение параметров сканирования

Параметры операции ***Сканировать весь компьютер*** можно изменить, открыв диалоговое окно «Параметры» под кнопкой ***Сканировать весь компьютер*** *(данное диалоговое окно*

откроется, если нажать ссылку «Параметры» в разделе Параметры сканирования для варианта «Сканировать весь компьютер»). ***Рекомендуется сохранять установленные по умолчанию настройки, если у вас нет достаточных оснований для их изменения!***



В списке параметров сканирования можно включить или выключить определенные параметры при необходимости:

- ***Лечить/удалять вирусы, не спрашивая меня*** *(выбрано по умолчанию)* — обнаруженный при сканировании вирус будет удален автоматически, если лечение возможно. Если не удалось автоматически вылечить зараженный файл, зараженный объект будет перемещен в Хранилище вирусов.

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** *(по умолчанию включено)* — установите данный флажок, чтобы активировать сканирование 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. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** *(не выбрано по умолчанию)* — установите этот флажок для обнаружения расширенного набора шпионских программ: это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него, возможно, будут блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать на наличие следящих файлов cookie*** *(не выбрано по умолчанию)* — данный параметр позволяет обнаруживать файлы cookie *(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).

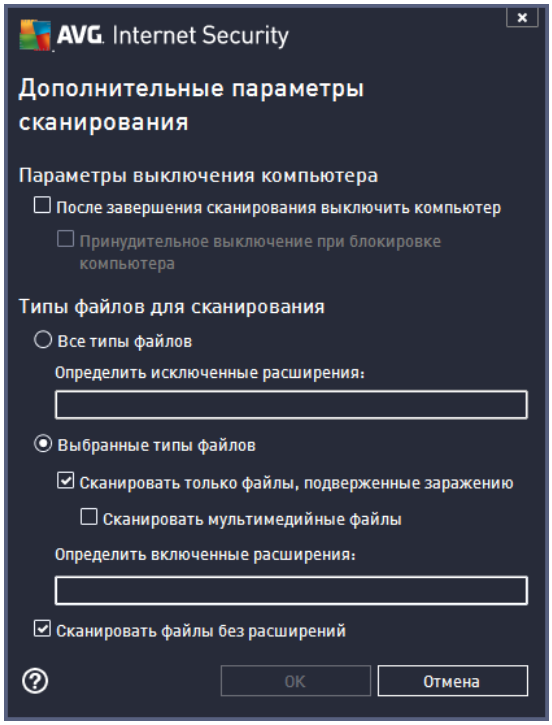
- ***Сканировать объекты в архивах*** *(по умолчанию не включено)* — данный параметр позволяет при сканировании проверять все файлы, хранящиеся в архивах, например ZIP, RAR и т. п.

- ***Использовать эвристический анализ*** *(выбрано по умолчанию)*: эвристический анализ *(динамическая эмуляция инструкций сканированных объектов в среде виртуального компьютера)* — это один из методов обнаружения вирусов при сканировании.

- ***Сканировать системное окружение*** *(по умолчанию включено)* — при сканировании также будут проверены системные области компьютера.

- ***Включить глубокое сканирование*** *(не выбрано по умолчанию)* — в определенных случаях *(например, при подозрении, что компьютер заражен)* можно установить этот флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

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



  - ***Параметры выключения компьютера*** — определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (***После завершения сканирования выключить компьютер***) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (

Принудительное выключение при блокировке компьютера).

- ***Определение типов файлов для сканирования*** — следует также указать типы файлов для сканирования.

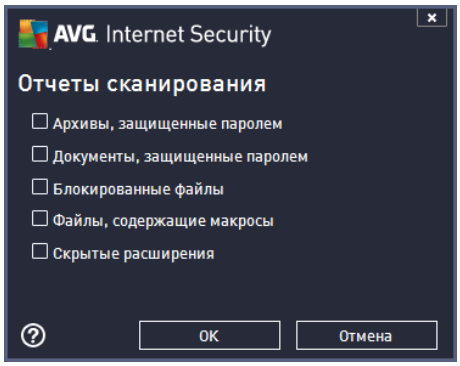
  - ***Все типы файлов*** — с возможностью определения исключений из сканирования путем создания списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет;

  - ***Выбранные типы файлов*** — можно указать сканирование только тех файлов, которые в принципе могут быть заражены (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы имеют довольно большой размер и вероятность их заражения вирусом мала*). С помощью расширений можно указать типы файлов, которые необходимо сканировать всегда.

  - Дополнительно можно выбрать параметр ***Сканировать файлы без расширений*** (по умолчанию включено). Не рекомендуется изменять его без веских причин. Файлы без расширений являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

- ***Настройка времени выполнения сканирования*** — для изменения приоритета процесса сканирования используйте ползунок. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).

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



Предупреждение. *Перечисленные параметры сканирования действительны также для вновь создаваемого сканирования, как описано в разделе Сканирование AVG / Планирование сканирования / Способы сканирования. Если потребуется изменить конфигурацию по умолчанию параметра* ***Сканирование всего компьютера****, можно затем сохранить новые параметры в качестве конфигурации по умолчанию, чтобы они использовалась каждый раз*

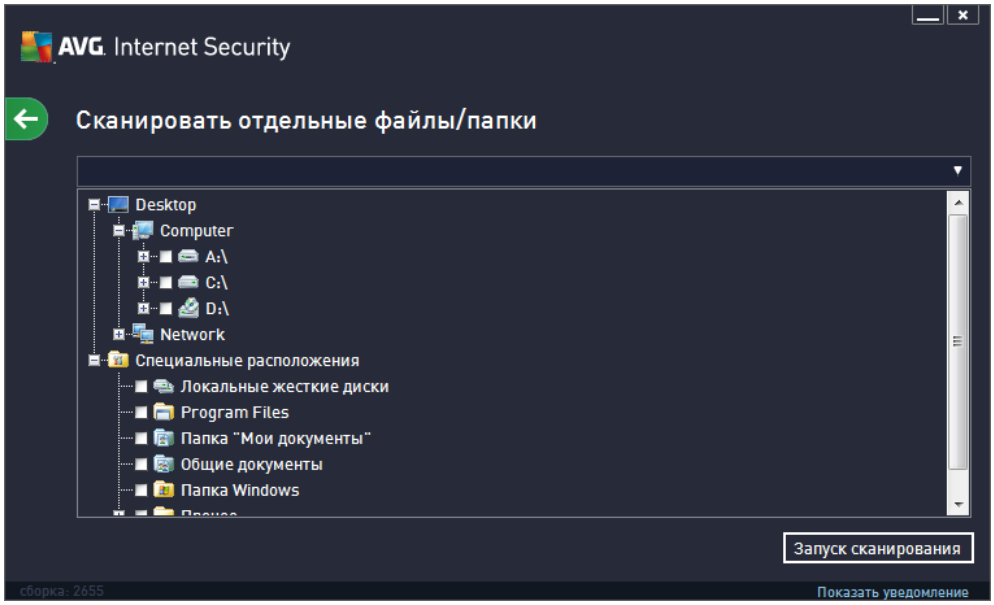
для сканирования всего компьютера.

11.1.2. Сканировать отдельные файлы/папки

Сканировать отдельные файлы/папки — при данном типе сканирования проверяются только области компьютера, выбранные для сканирования (*выбранные папки, жесткие диски, гибкие диски, компакт-диски и т. п.*). Ход сканирования в случае обнаружения вирусов и их дальнейшего лечения не отличается от обычного при сканировании всего компьютера: обнаруженные вирусы проходят процедуру лечения или помещаются в Хранилище вирусов. Сканирование отдельных файлов и папок можно использовать при создании пользовательских проверок и их расписаний.

Запуск сканирования

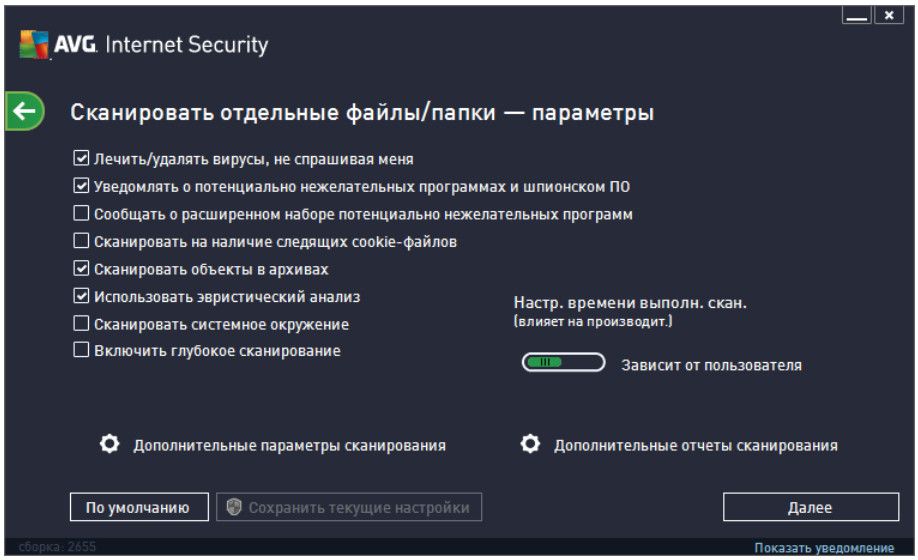
Сканирование определенных файлов или папок можно запустить непосредственно в диалоговом окне Параметры сканирования, нажав кнопку **Сканировать отдельные файлы/папки**. Откроется новое диалоговое окно ***Выбор отдельных файлов или папок для сканирования***. В древовидной структуре компьютера выберите папки, которые вы хотите просканировать. Путь к каждой выбранной папке будет создан автоматически и отобразится в текстовом поле в верхней части данного диалогового окна. Можно также выполнить сканирование 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 ***Запуск сканирования***; данный процесс сканирования практически не отличается от процесса Сканировать весь компьютер.



Изменение параметров сканирования

Можно изменить параметры ***Сканировать отдельные файлы/папки*** в диалоговом окне ***Сканировать отдельные файлы/папки — Параметры*** *(в данное диалоговое окно можно перейти по ссылке «Сканировать отдельные файлы/папки» в диалоговом окне Параметры*

сканирования). ***Рекомендуется сохранять установленные по умолчанию настройки, если у вас нет достаточных оснований для их изменения!***



В списке параметров сканирования можно при необходимости включить или выключить следующие определенные параметры.

- ***Автоматически лечить или удалять зараженные вирусами объекты*** *(выбрано по умолчанию)* — обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если не удалось автоматически вылечить зараженный файл, зараженный объект будет перемещен в Хранилище вирусов.

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** *(выбрано по умолчанию)* — установите этот этот флажок, чтобы сканировать на наличие как шпионского ПО, так 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. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** *(не выбрано по умолчанию)*: установите этот флажок для обнаружения расширенного пакета шпионского ПО — это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него, возможно, будут блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать на наличие следящих файлов cookie*** *(умолчанию выключено)* — этот параметр позволяет обнаруживать файлы cookie *(файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок в Интернете)*.

- ***Сканировать объекты в архивах*** *(выбрано по умолчанию)* — при выборе этого

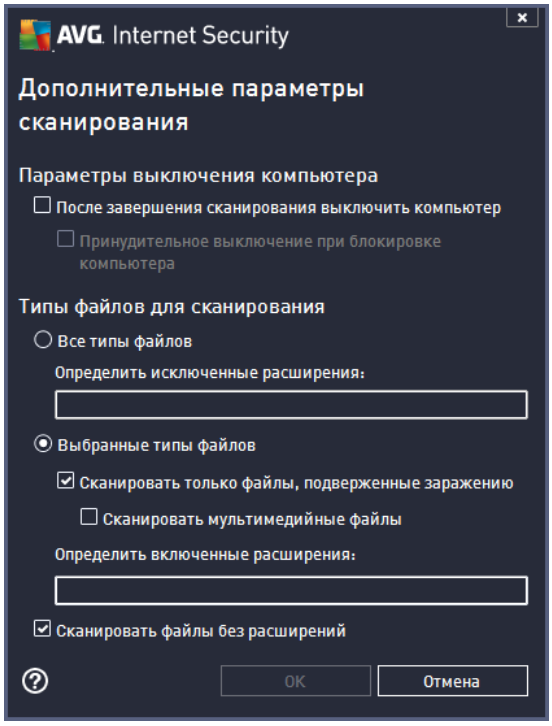
параметра сканирование затронет все файлы внутри архивов, например ZIP, RAR и т. п.

- ***Использовать эвристический анализ*** *(выбрано по умолчанию)*: эвристический анализ *(динамическая эмуляция инструкций сканированных объектов в среде виртуального компьютера)* — это один из методов, используемых для обнаружения вирусов при сканировании.

- ***Сканировать системное окружение*** *(не выбрано по умолчанию)* — в результате сканирования также будут проверены участки системы компьютера.

- ***Включить глубокое сканирование*** *(не выбрано по умолчанию)* — в определенных случаях (*например, при подозрении заражения компьютера*) нужно установить этот флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

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



  - ***Параметры выключения компьютера*** — определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (***После завершения сканирования выключить компьютер***) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (***Принудительное выключение при блокировке компьютера***).

- ***Определение типов файлов для сканирования*** — следует также указать типы файлов для сканирования.

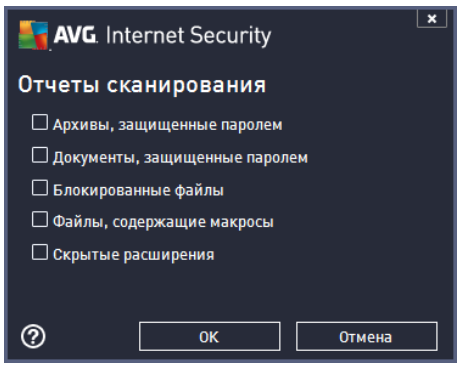
  - ***Все типы файлов*** с возможностью определения исключений из сканирования путем создания списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет.

  - ***Выбранные типы файлов*** — можно указать сканирование только тех файлов, которые в принципе могут быть заражены (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы имеют довольно большой размер и вероятность их заражения вирусом мала*). С помощью расширений можно указать типы файлов, которые необходимо сканировать всегда.

  - Дополнительно можно выбрать параметр ***Сканировать файлы без расширений*** (по умолчанию включено). Не рекомендуется изменять его без веских причин. Файлы без расширений являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

- ***Настройка времени выполнения сканирования*** — для изменения приоритета процесса сканирования используйте ползунок. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).

- ***Установить дополнительные отчеты о сканировании*** — при нажатии этой ссылки открывается диалоговое окно ***Отчеты о сканировании***, в котором можно выбрать типы объектов, сведения о которых должны отображаться в отчете.

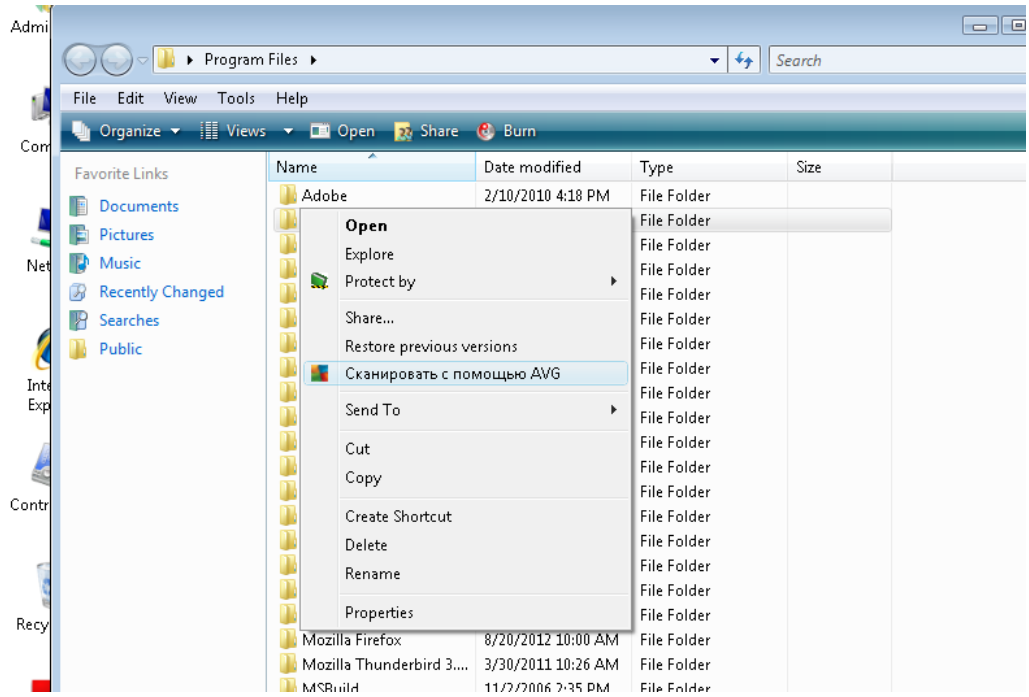


Предупреждение. *Перечисленные параметры сканирования действительны также для вновь создаваемого сканирования, как описано в разделе Сканирование AVG / Планирование сканирования / Способы сканирования. Если потребуется изменить конфигурацию по умолчанию параметра* ***Сканировать отдельные файлы/папки****, можно сохранить новые параметры как конфигурацию по умолчанию, чтобы она использовалась каждый раз при сканировании отдельных файлов или папок. Кроме того, созданная конфигурация может затем использоваться в качестве шаблона для новых запланированных сканирований (все*

пользовательские сканирования основаны на текущей конфигурации сканирования выбранных файлов и папок).

11.2. Сканирование в Проводнике Windows

Кроме предопределенных сканирований всего компьютера или выбранных областей, программа **AVG Internet Security 2013** также имеет функцию быстрого сканирования выбранного объекта непосредственно в Проводнике Windows. Если необходимо открыть неизвестный файл, содержимое которого не вызывает доверия, можно проверить такой файл по запросу. Выполните следующие действия.



- В проводнике Windows выделите файл *(или папку)*, который необходимо проверить
- Откройте контекстное меню, щелкнув объект правой кнопкой мыши
- Выберите элемент меню ***Сканировать с помощью AVG***, чтобы начать сканирование файла с помощью **AVG Internet Security 2013**

11.3. Сканирование с помощью командной строки

В **AVG Internet Security 2013** 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 следует набирать в одну строку и отделять пробелом и косой чертой,
- если для какого-либо параметра необходимо указать определенное значение (например, параметр ***/scan***, которому необходимы сведения о том, какие области на компьютере необходимо сканировать, а также прямой путь к выбранному разделу), значения отделяются точкой с запятой, например ***avgscanx /scan=C:\;D:***

Параметры сканирования

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

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

Сканирование из командной строки запущено с помощью графического интерфейса

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

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

11.3.1. Параметры сканирования с помощью командной строки

Ниже приведен список всех параметров для сканирования командной строки.

- /SCAN Сканировать отдельные файлы/папки /SCAN=путь;путь *(например, /SCAN=C:\;D:\)*
- /COMP Сканировать весь компьютер
- /HEUR Использовать эвристический анализ

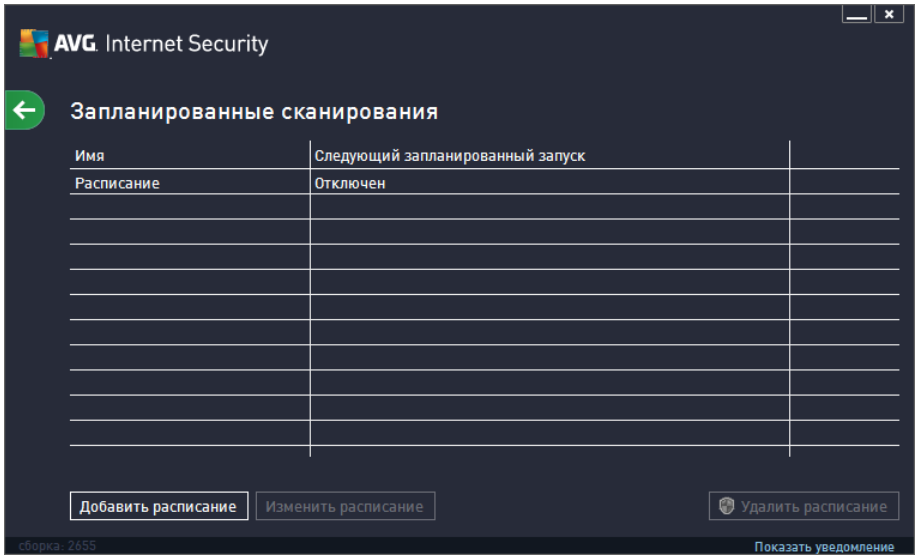
- /EXCLUDE Исключить путь или файлы из сканирования
- /@ Командный файл /имя файла/
- /EXT Сканировать эти расширения /например, EXT=EXE,DLL/
- /NOEXT Не сканировать эти расширения /например, NOEXT=JPG/
- /ARC Сканировать архивы
- /CLEAN Автоматическая очистка
- /TRASH Переместить зараженные файлы в Хранилище вирусов
- /QT Быстрая проверка
- /LOG Создать файл результата сканирования
- /MACROW Сообщать о макросах
- /PWDW Сообщать о файлах, защищенных паролем
- /ARCBOMBSW Сообщать об «архивных бомбах» *(многократно сжатых архивах)*
- /IGNLOCKED Пропускать заблокированные файлы
- /REPORT Отчет в файл /имя файла/
- /REPAPPEND Добавить в файл отчета
- /REPOK Сообщать о незараженных файлах
- /NOBREAK Запретить остановку по нажатию CTRL-BREAK
- /BOOT Включить проверку сектора MBR/загрузочного сектора
- /PROC Сканировать активные процессы
- /PUP Сообщать о потенциально нежелательных программах
- /PUPEXT Уведомлять о расширенном наборе потенциально нежелательных программ
- /REG Сканировать реестр
- /COO Сканировать файлы cookie
- /? Показать справку по этой теме
- /HELP Показать справку по этой теме
- /PRIORITY Установить приоритет сканирования /Низкий, Автоматически, Высокий/ *(см. Дополнительные параметры/Сканирование)*

- /SHUTDOWN После завершения сканирования выключить компьютер
- /FORCESHUTDOWN Принудительное выключение компьютера по завершении сканирования
- /ADS Сканировать альтернативные потоки данных *(только NTFS)*
- /HIDDEN Сообщать о файлах со скрытым расширением
- /INFECTABLEONLY Сканировать только файлы с подверженными заражению расширениями
- /THOROUGHSCAN Включить глубокое сканирование
- /CLOUDCHECK Проверять на наличие ложных срабатываний
- /ARCBOMBSW Сообщать о повторно сжатых архивных файлах

11.4. Расписание сканирования

С помощью **AVG Internet Security 2013** можно запустить сканирование по требованию *(например, если вы подозреваете, что компьютер заражен)* или запланированное сканирование. Настоятельно рекомендуется выполнять сканирование по расписанию. Таким образом вы устраните всякую возможность заражения компьютера и вам не придется беспокоиться о том, нужно ли выполнить сканирование и когда это нужно делать. Операцию Сканировать весь компьютер 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 будет выполняться сразу же при включении компьютера, если сканирование в заданное время было пропущено.

Расписание сканирования можно создать и изменить в диалоговом окне ***Запланированные сканирования***, если нажать кнопку ***Управление запланированными сканированиями*** в окне Параметры сканирования. В новом окне ***Запланированные сканирования*** вы увидите полный обзор всех недавних запланированных сканирований.

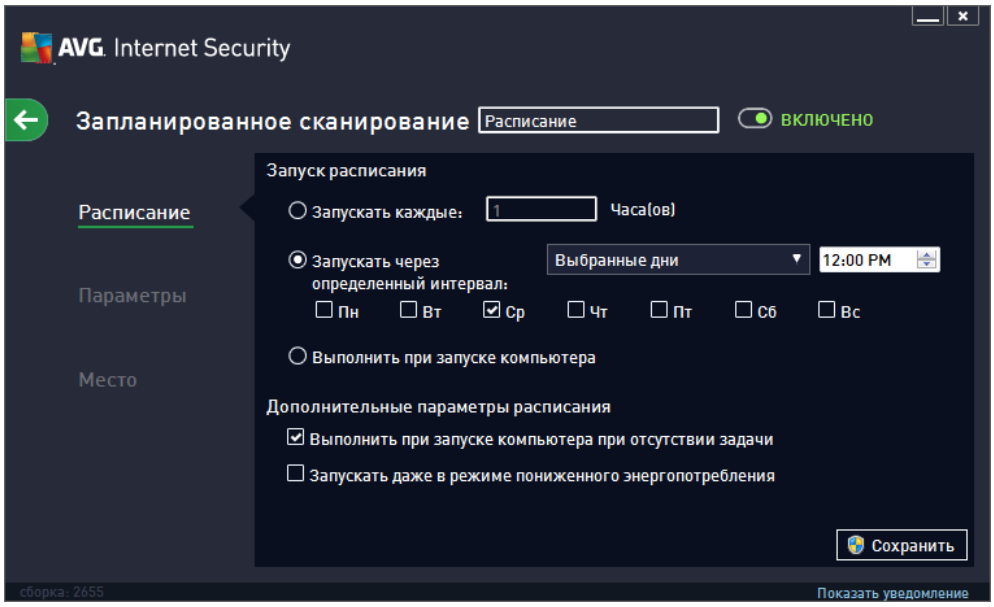


Если вы еще не запланировали сканирования, в таблице будет отображаться только сканирование, предопределенное поставщиком программного обеспечения. Данное сканирование по умолчанию отключено. Чтобы включить его, щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт ***Активировать задание***. После активации запланированного сканирования можно изменить его параметры с помощью кнопки ***Редактировать расписание***. С помощью кнопки ***Добавить расписание*** также можно создать свое расписание сканирований. С помощью следующих трех вкладок можно изменить параметры запланированного сканирования (*или создать новое расписание*).

- Расписание
- Параметры
- Объекты сканирования

На каждой вкладке с помощью переключателя-«светофора» можно легко отключить на время запланированную проверку и при необходимости запустить ее снова.

11.4.1. Расписание



В верхней части вкладки ***Расписание*** в текстовом поле можно указать название расписания сканирования, для которого выполняется настройка. Старайтесь использовать краткие, содержательные и понятные названия сканирований, чтобы в дальнейшем их было легче отличить от остальных. Например, не следует присваивать такие имена, как «Новое сканирование» или «Мое сканирование», т. к. данные имена не имеют отношения к сканируемым объектам. И наоборот, название «Сканирование системных областей» является хорошим содержательным названием.

В данном диалоговом окне можно определить следующие параметры сканирования.

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

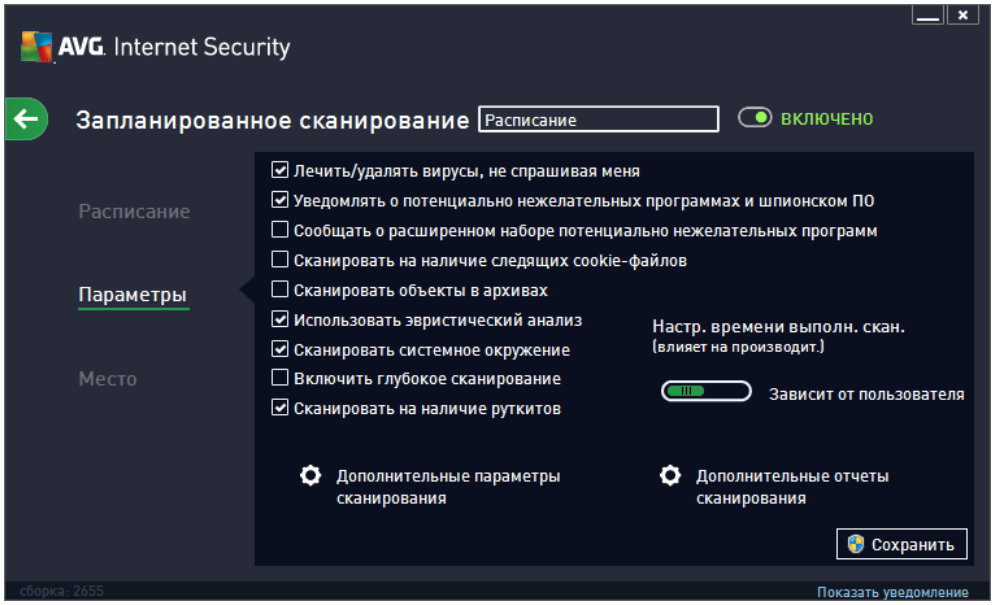
- ***Дополнительные параметры расписания*** — данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск сканирования, если компьютер находится в ждущем режиме или полностью выключен. После запуска обновления в указанное время появится всплывающее окно с уведомлением о данном событии над значком AVG на панели задач. Затем появится новый значок AVG на панели задач (цветной мигающий значок), сообщающий о том, что запланированное сканирование запущено. Щелкните правой кнопкой мыши значок запущенного сканирования AVG, чтобы открыть контекстное меню, с помощью которого можно приостановить, завершить, а также изменить приоритет запущенного сканирования.

Элементы управления диалогового окна

- ***Сохранить*** — сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, и возврат в окно общих сведений о запланированных сканированиях. Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.

- — используйте зеленую стрелку в верхней левой части диалогового окна для возврата к общим сведениям о запланированных сканированиях.

11.4.2. Параметры



В верхней части вкладки ***Параметры*** в текстовом поле можно указать название расписания сканирования, для которого выполняется настройка. Старайтесь использовать краткие, содержательные и понятные названия сканирований, чтобы в дальнейшем их было легче отличить от остальных. Например, не следует присваивать такие имена, как «Новое сканирование» или «Мое сканирование», т. к. данные имена не имеют отношения к сканируемым объектам. И наоборот, название «Сканирование системных областей» является хорошим содержательным названием.

На вкладке ***Параметры*** приведен список параметров сканирования, которые при необходимости можно включить или отключить. ***Если нет веских оснований для изменения данных параметров, рекомендуется не изменять стандартную конфигурацию***.

- ***Автоматически лечить или удалять зараженные вирусами объекты*** *(выбрано по умолчанию):* обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если не удалось автоматически вылечить зараженный файл, зараженный объект будет перемещен в Хранилище вирусов.

- ***Уведомлять о потенциально нежелательных программах и шпионском ПО*** *(выбрано по умолчанию)* — установите этот флажок, чтобы сканировать на наличие как

шпионского ПО, так 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. Рекомендуем включить эту функцию, поскольку она позволяет значительно улучшить безопасность компьютера.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** (*не выбрано по умолчанию*): установите этот флажок для обнаружения расширенного пакета шпионского ПО — это программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Этот параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него, возможно, будут блокироваться некоторые безопасные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать на наличие следящих файлов cookie*** (*по умолчанию выключено*) — этот параметр позволяет в процессе сканирования обнаруживать файлы cookie *(файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок в Интернете)*.

- ***Сканировать объекты в архивах*** *(не выбрано по умолчанию)* — при выборе данного параметра сканирование затронет все файлы, даже внутри архивов, например ZIP, RAR и т. п.

- ***Использовать эвристический анализ*** (*выбрано по умолчанию*) — эвристический анализ (*динамичная эмуляция команд сканированных объектов в виртуальной компьютерной среде*) является одним из способов, используемых для выявления вирусов при сканировании.

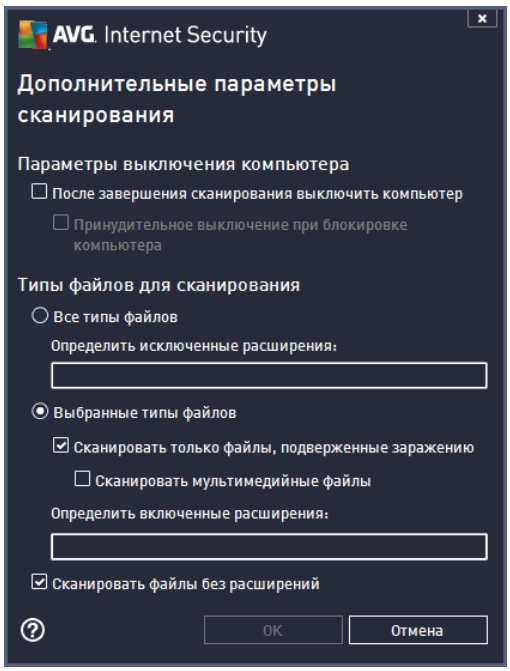
- ***Сканировать системное окружение*** (*выбрано по умолчанию*) — в результате сканирования также будут проверены участки системы компьютера.

- ***Включить глубокое сканирование*** (*не выбрано по умолчанию)* — в определенных случаях (*например, при подозрении на заражение компьютера*) установите данный флажок, чтобы активировать самые тщательные алгоритмы сканирования, которые для полной уверенности в безопасности будут сканировать даже те области компьютера, которые практически не подвержены риску заражения. Обратите внимание, что для выполнения такого сканирования потребуется много времени.

- ***Сканировать на наличие руткитов*** *(выбрано по умолчанию) — компонент* Anti-Rootkit сканирует компьютер на возможное наличие пакетов программ rootkit (программы и технологии, позволяющие скрыть вредоносную активность на компьютере). Если руткит обнаружен, это еще не значит, что компьютер заражен. В некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за руткиты.

Дополнительные настройки сканирования

Эта ссылка открывает новое диалоговое окно ***Дополнительные настройки сканирования***, где можно указать следующие параметры.



- ***Параметры выключения компьютера*** — определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (*После завершения сканирования выключить компьютер*) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (*Принудительное выключение при блокировке компьютера*).

- ***Определение типов файлов для сканирования*** — следует также указать типы файлов для сканирования.

    - ***Все типы файлов*** — с возможностью определения исключений из сканирования путем создания списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет;

    - ***Выбранные типы файлов*** — можно указать сканирование только тех файлов, которые в принципе могут быть заражены *(файлы, не подверженные заражению, не будут сканироваться, например простые текстовые или другие неисполняемые файлы)*, включая мультимедийные файлы *(видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы имеют довольно большой размер и вероятность их заражения вирусом крайне мала)*. С помощью расширений можно указать типы файлов, которые необходимо сканировать всегда.

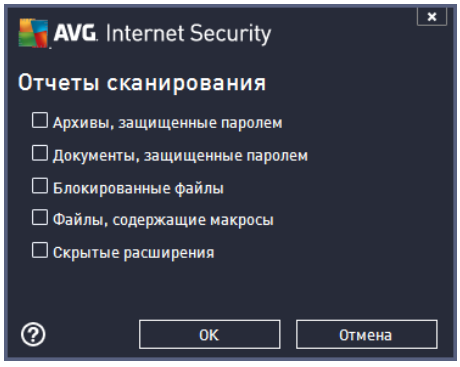
    - Дополнительно можно установить флажок ***Сканировать файлы без расширений*** (он установлен по умолчанию). Рекомендуется не снимать его без веских причин. Файлы без расширений являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

Настройка времени выполнения сканирования

В дальнейшем в данном разделе можно указать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлен *пользовательский уровень* автоматического использования ресурсов. Если необходимо, чтобы процесс сканирования выполнялся быстрее, это займет меньше времени, но во время этого процесса будет значительно увеличено потребление системных ресурсов, что снизит производительность других процессов, выполняемых на компьютере (*этот параметр можно включить, если компьютер включен и не используется*). И наоборот, можно снизить потребление системных ресурсов, увеличив продолжительность сканирования.

Установить дополнительные отчеты о сканировании

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

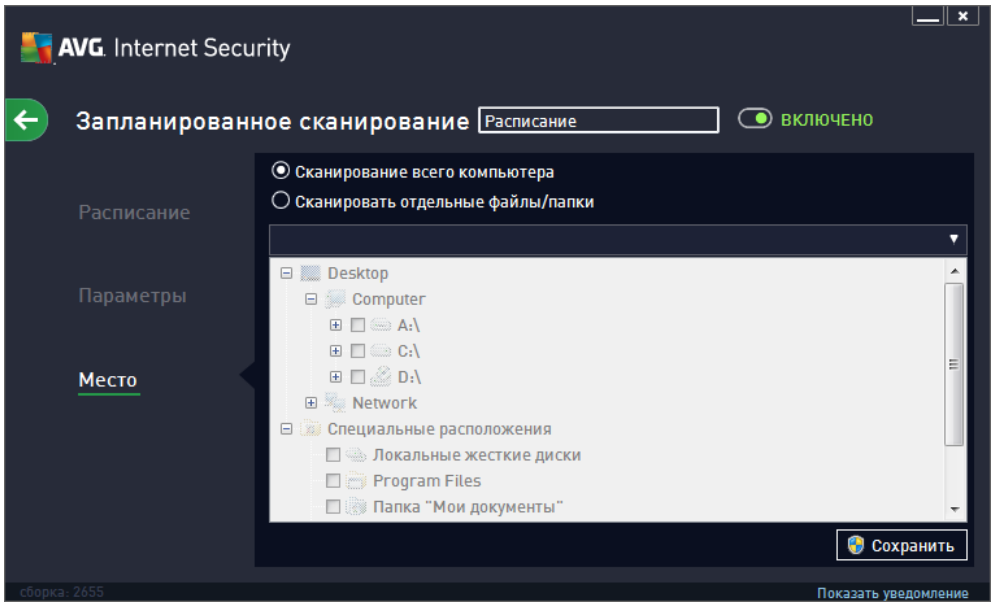


Элементы управления диалогового окна

- ***Сохранить*** — сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, и возврат в окно общих сведений о запланированных сканированиях. Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.

- — используйте зеленую стрелку в верхней левой части диалогового окна для возврата к общим сведениям о запланированных сканированиях.

11.4.3. Объекты сканирования



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

В структуре дерева также отображается ветвь ***Специальные расположения***. Если установить соответствующий флажок, ниже появится список объектов для дальнейшего сканирования.

- ***Локальные жесткие диски*** — все жесткие диски компьютера.
- ***Program Files***
  - C:\Program Files\
  - *в 64-разрядной версии* C:\Program Files (x86)
- ***Папка Мои документы***
  - *для Win XP:* C:\Documents and Settings\Default User\My Documents\
  - *для Windows Vista/7*: C:\Users\user\Documents\
- ***Общие документы***
  - *для Win XP*: C:\Documents and Settings\All Users\Documents\

- *для Windows Vista/7*: C:\Users\Public\Documents\

- ***Папка Windows*** — C:\Windows\

- ***Прочее***

  - *Системный диск* — жесткий диск, на котором установлена операционная система (обычно диск C:).

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

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

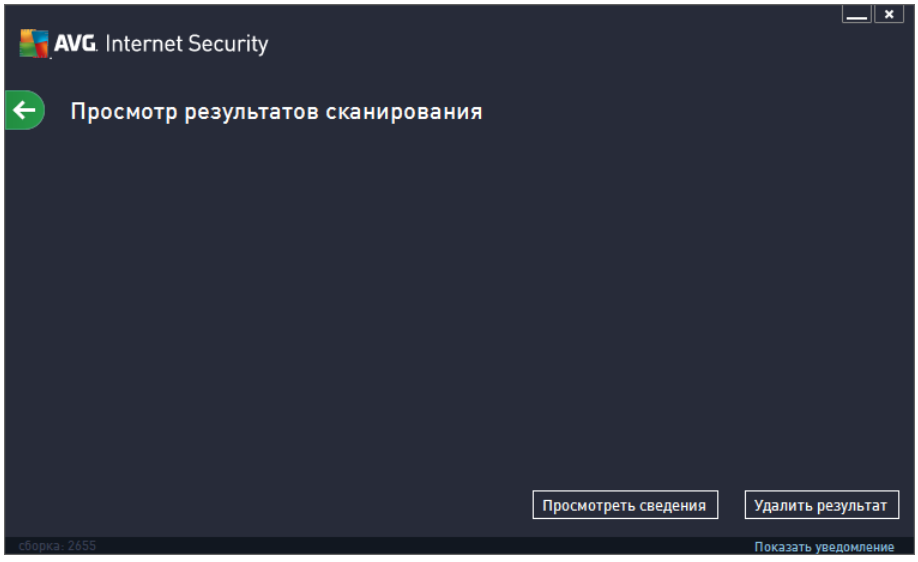
  - *Временные файлы Интернета* — C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); или C:\Users\user\AppData\Local\Temp\Microsoft\Windows\Временные файлы Интернета (*Windows Vista/7*)

Элементы управления диалогового окна

- ***Сохранить*** — сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, и возврат в окно общих сведений о запланированных сканированиях. Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.

- — используйте зеленую стрелку в верхней левой части диалогового окна для возврата к общим сведениям о запланированных сканированиях.

11.5. Результаты сканирования



В диалоговом окне ***Обзор результатов сканирования*** перечислены результаты всех завершенных на данное время сканирований. В таблице отображается следующая информация по каждому результату сканирования.

- ***Значок*** — в первом столбце отображается значок состояния сканирования:
  - Вирусы не обнаружены, сканирование завершено
  - Вирусы не обнаружены, сканирование было прервано до завершения
  - Вирусы обнаружены и не устранены, сканирование завершено
  - Вирусы обнаружены и не устранены, сканирование было прервано до завершения
  - Вирусы обнаружены и устранены или удалены, сканирование завершено
  - Вирусы обнаружены и устранены или удалены, сканирование было прервано до завершения
- ***Имя*** — название соответствующего сканирования. Это либо один из двух вариантов предопределенного сканирования, либо созданное вами запланированное сканирование.
- ***Время запуска*** — точная дата и время запуска процесса сканирования.
- ***Время завершения*** — точная дата и время, когда процесс сканирования был завершен, приостановлен пользователем или иным образом прерван.
- ***Проверенные объекты*** — общее количество просканированных объектов.
- ***Заражения*** — количество удаленных угроз из общего числа обнаруженных.
- ***Высокая / Средняя / Низкая*** — в этих трех последовательных столбцах показано число угроз каждой из трех степеней опасности.
- ***Руткиты*** — общее число руткитов, обнаруженных во время сканирования.

Элементы управления диалогового окна

Просмотреть сведения — нажмите эту кнопку, чтобы получить подробную информацию о выбранном сканировании *(выделенном в таблице выше)*.

Удалить результаты — удаление результатов выбранного сканирования из таблицы.

— используйте зеленую стрелку в верхней левой части диалогового окна для возврата к главному интерфейсу пользователя с общими сведениями о компонентах.

11.6. Сведения о результатах сканирования

Чтобы получить подробные данные о результатах выбранного сканирования, нажмите кнопку ***Просмотреть сведения*** в диалоговом окне Обзор результатов сканирования. В этом же окне отобразится детальная информация о результатах данного сканирования. Информация представлена на трех вкладках.

- ***Сводка*** — на этой вкладке представлена основная информация о сканировании: было ли оно успешно завершено, были ли обнаружены угрозы и какие действия предприняты.

- ***Сведения*** — на этой вкладке отображается полная информация о сканировании, в том числе подробности по каждой обнаруженной угрозе. С помощью функции «Экспортировать в файл» можно сохранить полученные данные в формате CSV.

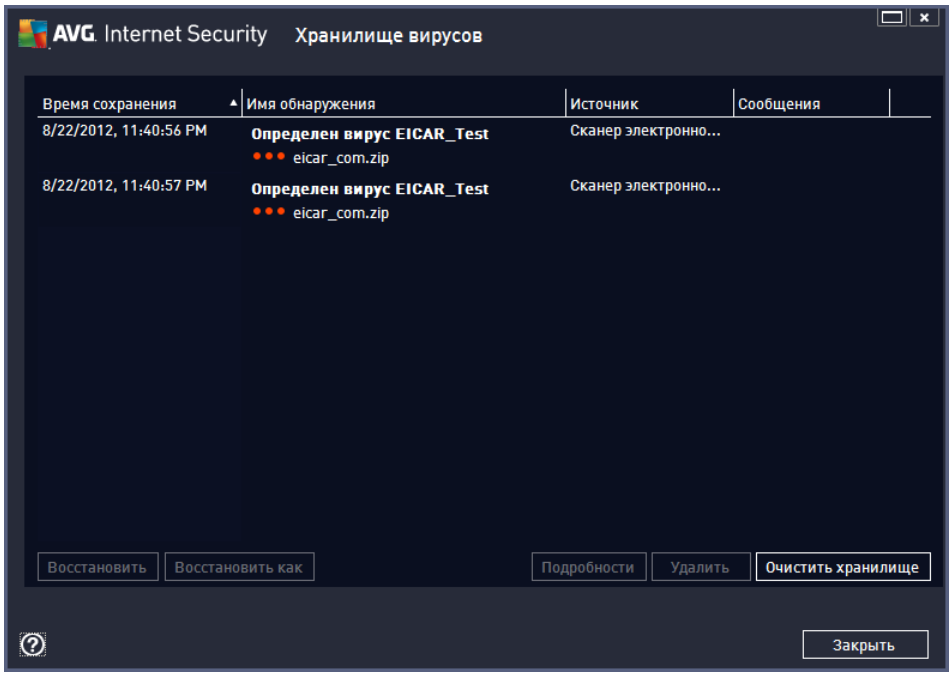
- ***Обнаруженные объекты*** — эта вкладка отображается, если в ходе сканирования были обнаружены угрозы. Здесь вы найдете подробные сведения об угрозах:

  Низкая степень опасности: информация или предупреждения, а не реальная угроза. Как правило, документы с макросами, документы или архивы, защищенные паролем, заблокированные файлы и т. п.

  Средняя степень опасности: как правило, *потенциально нежелательные программы (например, рекламное ПО)* или следящие файлы cookie

  Высокая степень опасности: серьезные угрозы, такие как вирусы, «троянские кони», эксплойты и т. п. Также объекты, обнаруженные с помощью эвристического метода, т. е. угрозы, еще не описанные в вирусной базе данных.

12. 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.

В интерфейсе ***Хранилища вирусов***, которое открывается в отдельном окне, представлены общие сведения о зараженных объектах, помещенных в карантин.

- ***Степень опасности*** — если у вас установлен компонент Identity в составе **AVG Internet Security 2013**, в данном разделе отображается степень опасности того или иного обнаруженного объекта по четырехбалльной шкале: самым безопасным объектам соответствуют *три зеленых точки*, а наиболее опасным — *три красных точки*; а также тип угрозы (*эти данные показывают уровень заражения, так как все перечисленные объекты или действительно заражены, или подвержены заражению*).
- ***Имя вируса*** — наименование угрозы по данным энциклопедии вирусов
- ***Путь к файлу*** — полный путь к исходному местоположению зараженного объекта.
- ***Дата хранения*** — дата и время обнаружения подозрительного файла и его перемещения в Хранилище вирусов

Кнопки управления

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

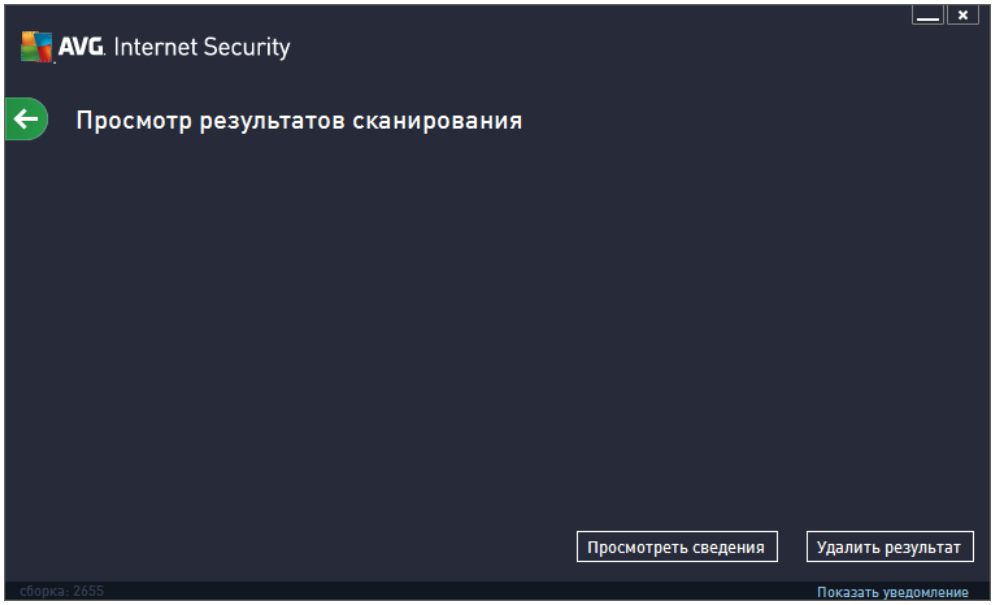
- ***Восстановить*** — перемещение зараженного файла в исходное местоположение на диске.
- ***Восстановить как*** — перемещение зараженного файла в выбранную папку
- ***Сведения*** — чтобы получить подробную информацию об угрозе, помещенной в ***Хранилище вирусов***, выделите нужный объект в списке и нажмите кнопку ***Сведения***. Откроется диалоговое окно с описанием обнаруженной угрозы.
- ***Удалить*** — полное удаление зараженного файла из ***Хранилища вирусов***.
- ***Очистить Хранилище*** — полное 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. История

В ***Истории*** содержится информация обо всех произошедших событиях *(например, обновлениях, сканированиях, обнаруженных угрозах и т. д.),* а также отчеты о них. В этот раздел можно перейти из главного интерфейса пользователя, открыв в меню пункт ***Настройки / История***. Кроме того, история событий имеет следующие разделы.

- Результаты сканирования
- Обнаружение Resident Shield
- Обнаружение защиты электронной почты
- Полученные данные Online Shield
- Журнал событий
- Журнал Firewall

13.1. Результаты сканирования



В диалоговое окно ***Обзор результатов сканирования*** можно перейти в меню ***Настройки / История / Результаты сканирования*** в верхней строке навигации на главном окне **AVG Internet Security 2013**. 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
- ***Высокая / Средняя*** / ***Низкая*** — в этих столбцах показано количество удаленных и общее число обнаруженных угроз в соответствии с уровнем их опасности.
- ***Сводка*** — данные о процессе и результатах сканирования *(обычно при завершении или прерывании операции).*
- ***Rootkit*** — количество обнаруженных руткитов

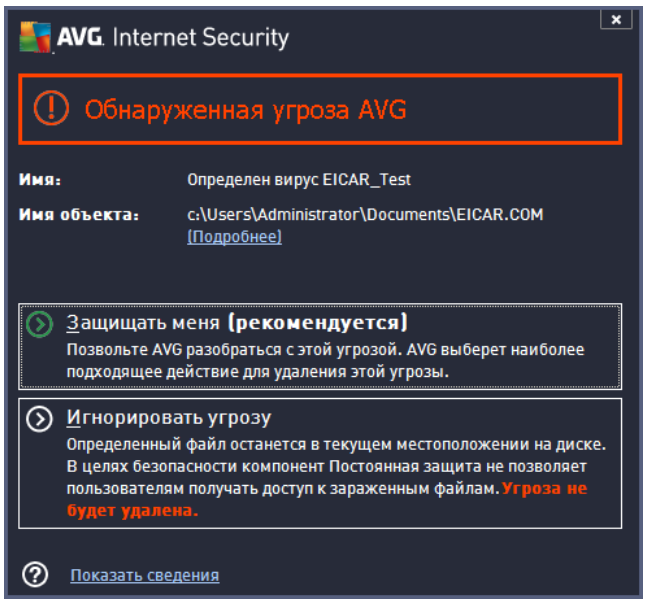
Кнопки управления

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.
- — возврат к стандартному главному окну AVG *(обзор компонентов)* с помощью стрелки в левом верхнем углу диалогового окна.

13.2. Обнаружение Resident Shield

Компонент ***Постоянная защита*** является частью компонента ***Компьютер*** и предназначен для сканирования файлов при операциях копирования, открытия или сохранения. При обнаружении вируса или угрозы сразу же появляется предупреждение в следующем диалоговом окне:

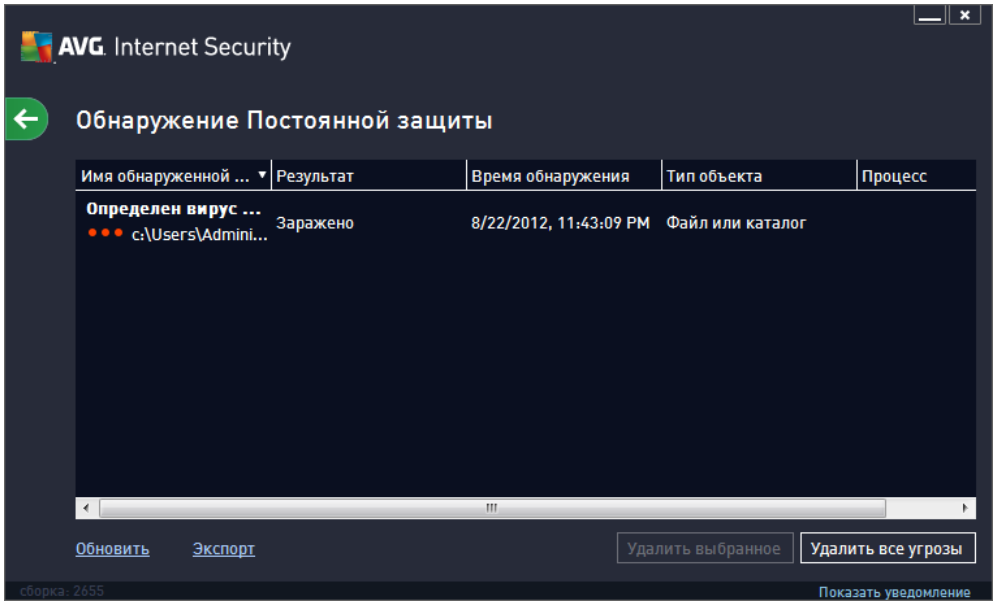


В данном диалоговом окне предупреждения отображаются сведения об обнаруженных зараженных объектах (*Имя*) и краткие характеристики данной угрозы (*Описание*). Щелкнув ссылку Показать сведения, вы перейдете на страницу энциклопедии вирусов, где можно найти информацию обо всех известных угрозах. В данном диалоговом окне вам будут показаны доступные действия для той или иной угрозы. Один из вариантов будет помечен как рекомендуемый. ***Защищать сейчас (рекомендуется). По возможности всегда используйте этот вариант.***

Примечание. *Размер обнаруженного объекта может превышать объем свободного места в Хранилище вирусов. В этом случае при попытке переместить зараженный объект в Хранилище вирусов отобразится всплывающее предупреждение о проблеме. Однако объем Хранилища вирусов можно изменить. Он определяется в процентном соотношении с фактическим объемом жесткого диска. Чтобы увеличить объем Хранилища вирусов, откройте диалоговое окно Хранилище вирусов в меню Расширенные настройки AVG с помощью параметра «Ограничить размер Хранилища вирусов».*

В нижней части окна вы найдете ссылку ***Показать сведения***. Щелкните ее. Откроется новое окно с подробной информацией о процессах, которые выполнялись в момент обнаружения угрозы и идентификаторах этих процессов.

Перечень объектов, обнаруженных компонентом «Постоянная защита», находится в диалоговом окне ***Обнаружение Resident Shield***. Чтобы открыть его, найдите пункт ***Настройки / История / Обнаружение Resident Shield*** в верхней строке навигации главного окна **AVG Internet Security 2013. В этом окне представлен обзор объектов, обнаруженных компонентом «Постоянная защита» и определенных как опасные, которые были вылечены или помещены в** Хранилище вирусов.



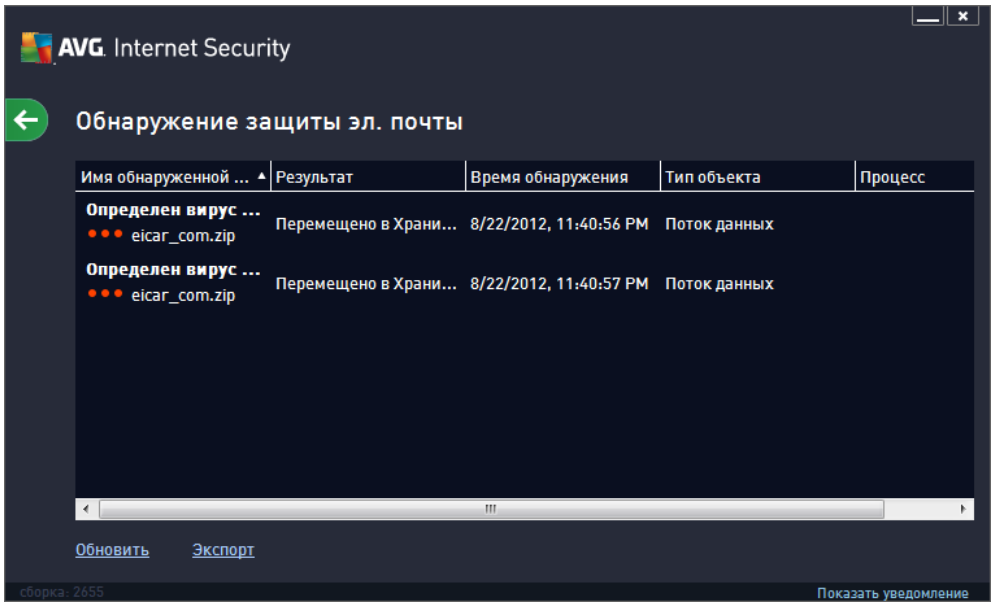
По каждому обнаруженному объекту предоставляется следующая информация.

- ***Название объекта*** — описание (*возможно даже имя*) обнаруженного объекта и его расположение
- ***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.

Кнопки управления

- ***Обновить*** — обновление списка объектов, обнаруженных с помощью ***Online Shield***
- ***Экспорт*** — передать весь список обнаруженных объектов в файл.
- ***Удалить выбранное*** — вы можете выделить несколько записей в списке, а затем с помощью этой кнопки удалить их.
- ***Удалить все угрозы*** — стирание всех записей в диалоговом окне.
- — возврат к стандартному главному окну AVG *(обзор компонентов)* с помощью стрелки в левом верхнем углу диалогового окна.

13.3. Обнаружение защиты электронной почты



Диалоговое окно ***Обнаружение сканера электронной почты*** можно открыть, найдя в меню соответствующий пункт: ***Настройки / История / Обнаружение сканера электронной почты*** в верхней строке навигации на главном окне **AVG Internet Security 2013** . В данном окне находится список объектов, обнаруженных компонентом Защита эл. почты. По каждому обнаруженному объекту предоставляется следующая информация.

- ***Заражение*** — описание (возможно, даже имя) обнаруженного объекта.
- ***Объект*** — местоположение объекта.
- ***Результат*** — действие, выполненное в отношении обнаруженного объекта.
- ***Время обнаружения*** — дата и время обнаружения подозрительного объекта.
- ***Тип объекта*** — тип обнаруженного объекта.

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

Кнопки управления

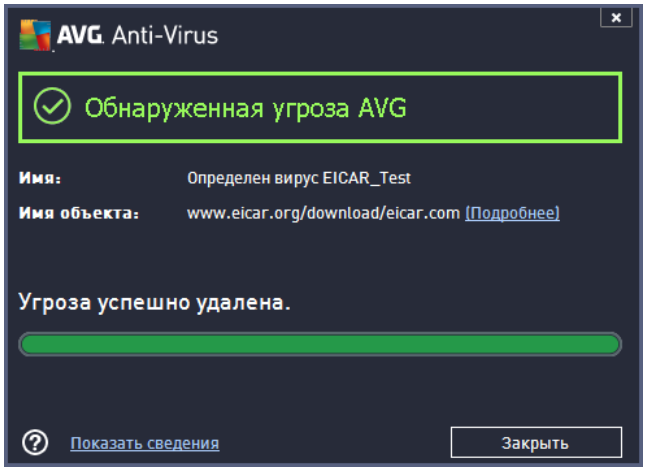
В интерфейсе компонента ***Сканер электронной почты*** имеются следующие кнопки управления.

- ***Обновить список*** — обновление списка обнаруженных угроз.
- — возврат к стандартному главному окну AVG *(обзор компонентов)* с помощью

стрелки в левом верхнем углу диалогового окна.

13.4. Полученные данные Online Shield

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

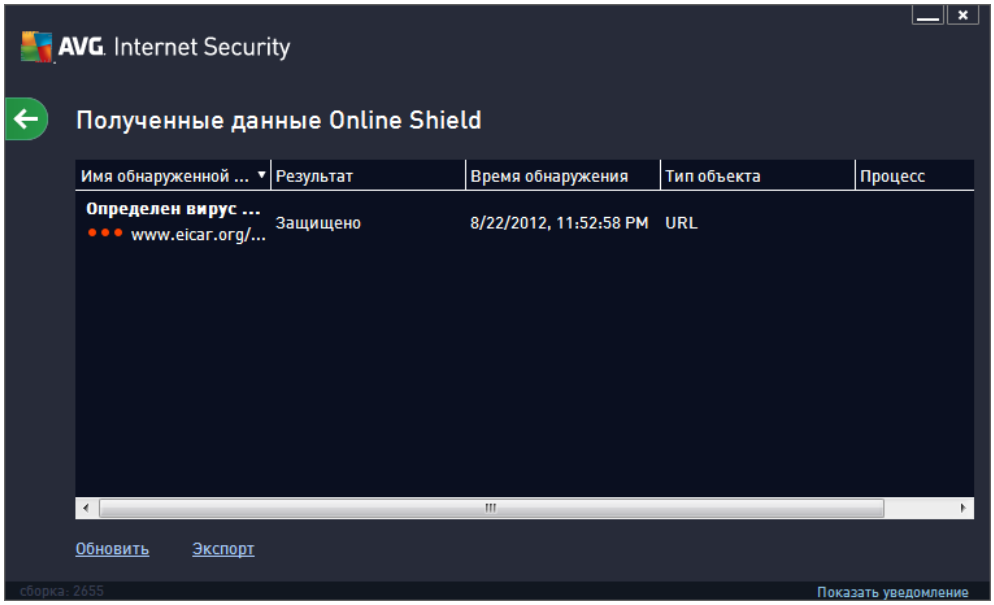


В данном диалоговом окне предупреждения отображаются сведения об обнаруженных зараженных объектах (*Имя*) и краткие характеристики данной угрозы (*Описание*). Щелкнув ссылку Показать сведения, вы перейдете на страницу энциклопедии вирусов, где можно найти информацию обо всех известных угрозах. В диалоговом окне содержатся следующие элементы управления:

- ***Показать сведения*** — щелкните эту ссылку, чтобы открыть новое всплывающее окно, в котором содержатся сведения о процессе, запущенном в момент обнаружения заражения, и идентификации процесса.

- ***Закрыть*** — нажмите эту кнопку, чтобы закрыть окно с предупреждением.

Подозрительная страница не будет открыта, а данные об обнаруженной угрозе будут занесены в список ***Полученные данные Online Shield***. Обзор обнаруженных угроз можно просмотреть, открыв пункт меню ***Настройки / История / Полученные данные Online Shield*** в верхней строке навигации главного окна **AVG Internet Security 2013**.



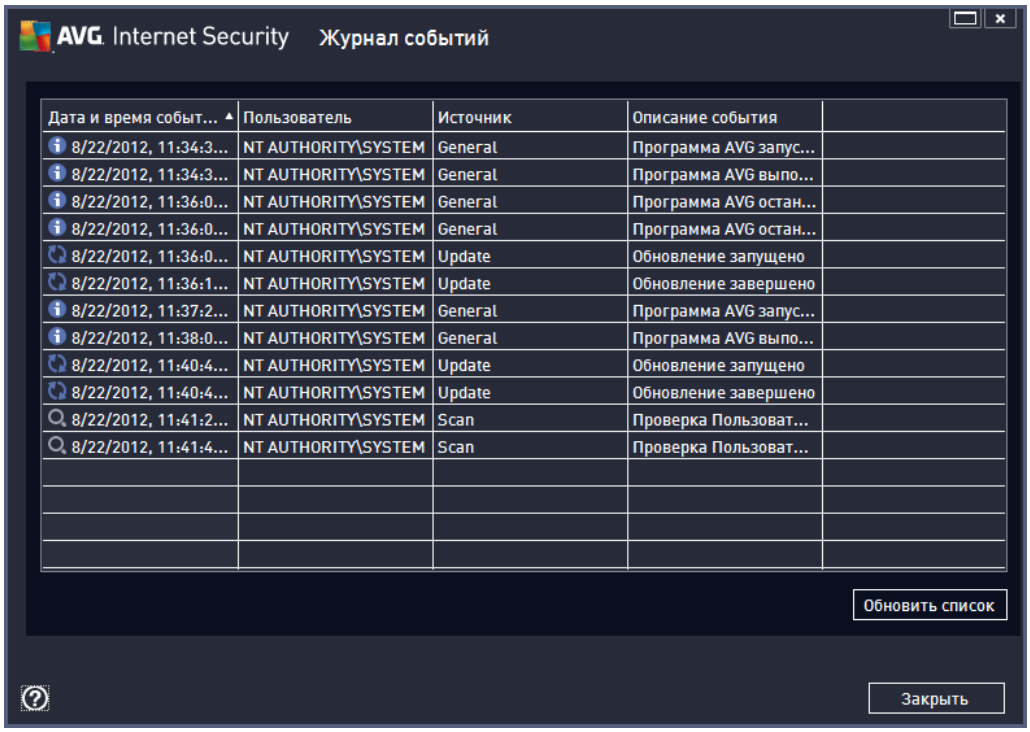
По каждому обнаруженному объекту предоставляется следующая информация.

- ***Название объекта*** — описание (*возможно даже имя*) обнаруженного объекта и его источник (*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.

Кнопки управления

- ***Обновить*** — обновление списка объектов, обнаруженных с помощью ***Online Shield***
- ***Экспорт*** — передать весь список обнаруженных объектов в файл.
- — возврат к стандартному главному окну AVG *(обзор компонентов)* с помощью стрелки в левом верхнем углу диалогового окна.

13.5. Журнал событий



Диалоговое окно ***Журнал событий*** доступно из меню ***Настройки / История / Журнал событий*** в верхней строке навигации на главном окне **AVG Internet Security 2013**. В этом окне можно посмотреть перечень важных событий, произошедших во время работы **AVG Internet Security 2013**. В диалоговом окне показаны сведения о таких событиях: информация об обновлении приложений AVG; сведения о времени начала и конца, а также остановки сканирования (*в том числе об автоматических проверках*); данные об обнаружении вирусов (*постоянной защитой или в ходе сканирования*), в том числе о месте их обнаружения, а также о других важных событиях.

Для каждого события отображаются следующие сведения.

- ***Дата и время события*** — указывает точную дату и время события.
- ***Имя пользователя*** — указывает имя пользователя, зарегистрированного в системе на момент события.
- ***Источник*** — содержит информацию об исходном компоненте или другом элементе системы AVG, который запустил событие
- ***Описание события*** — краткое описание произошедшего события

Кнопки управления

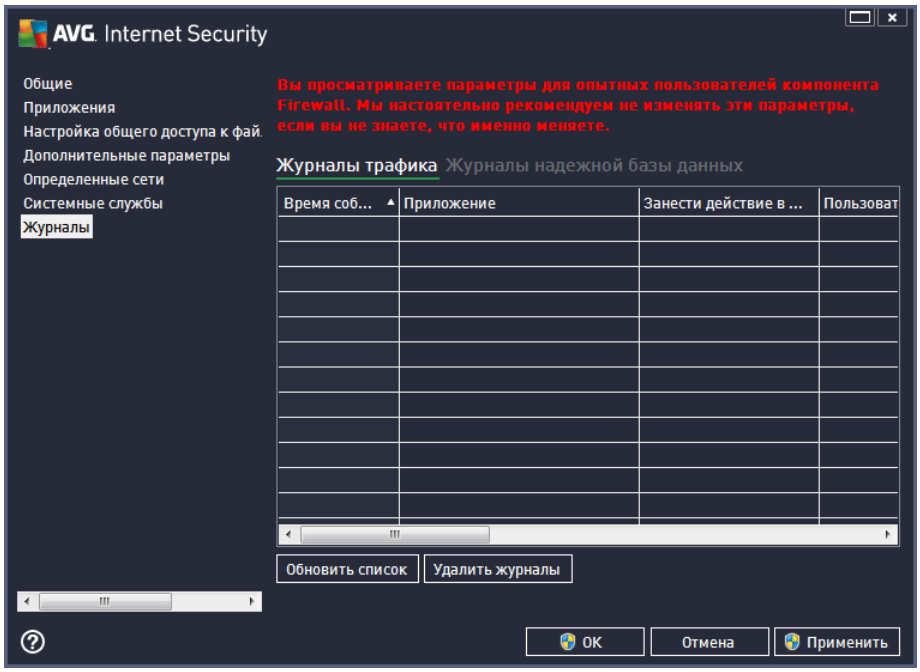
- ***Обновить список*** — нажатие этой кнопки обновляет все записи в списке событий.
- ***Закрыть*** — используйте эту кнопку для возврата в **AVG Internet Security 2013**

главное окно.

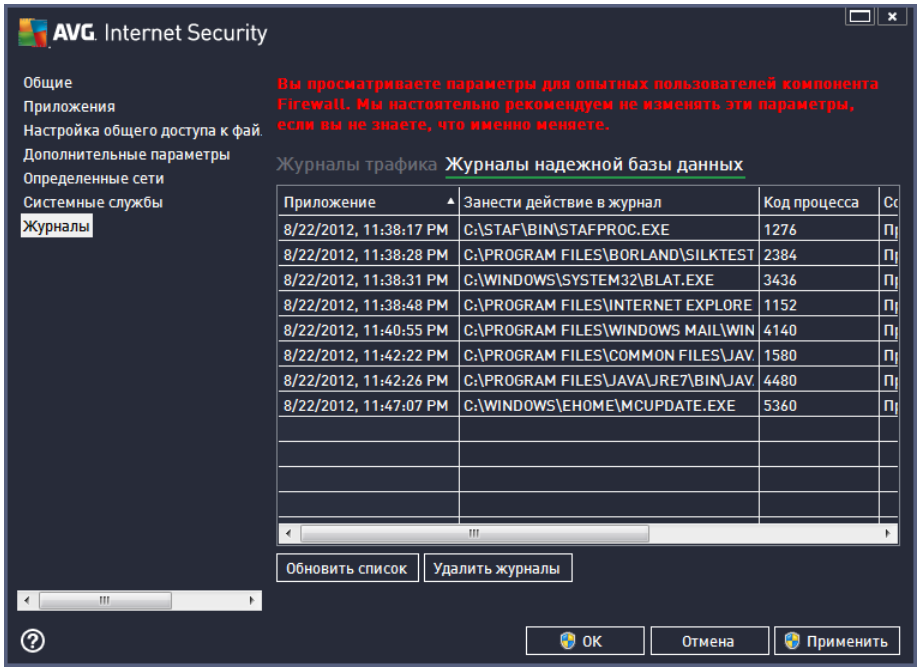
13.6. Журнал Firewall

В диалоговом окне ***Журналы*** можно просмотреть список всех занесенных в журнал действий и событий компонента Firewall, а также подробное описание соответствующих параметров.

- ***Журналы трафика*** — на этой вкладке содержатся сведения о действиях всех приложений, которые выполняли попытки подключиться к сети. Каждая запись содержит данные о времени события, названии приложения, соответствующем действии в журнале, идентификаторе, направлении подключения, типе протокола, номерах удаленных и локальных портов, а также сведения о локальных и удаленных IP-адресах.



- ***Журналы надежной базы данных***: *надежная база данных* — это внутренняя база данных AVG, содержащая сведения о сертифицированных и надежных приложениях, которым всегда разрешен доступ в Интернет. Если новое приложение первый раз пытается подключиться к сети (*т. е. для него еще не создано правило брандмауэра*), необходимо выбрать — 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 данные об этом приложении, отобразится запрос в отдельном окне, в котором необходимо определить, разрешить ли доступ в сеть для данного приложения.



Кнопки управления

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

- ***Удалить журналы*** — нажмите, чтобы удалить все записи в таблице.

14. Обновления AVG

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

Учитывая количество новых угроз и скорость, с которой они распространяются, очень важно регулярно обновлять **AVG Internet Security 2013**. Наилучшим решением является сохранение параметров по умолчанию, которые предусматривают автоматическое обновление. Помните, что если не обновлять вирусную базу данных **AVG Internet Security 2013**, программа не сможет обнаруживать новые угрозы.

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

14.1. Запуск обновления

Для обеспечения максимальной защиты программа **AVG Internet Security 2013** по умолчанию проверяет наличие обновлений вирусной базы данных каждые четыре часа. Так как обновления AVG выпускаются не по расписанию, а в связи с появлением некоторого числа новых угроз, крайне важно регулярно обновлять вирусную базу данных AVG.

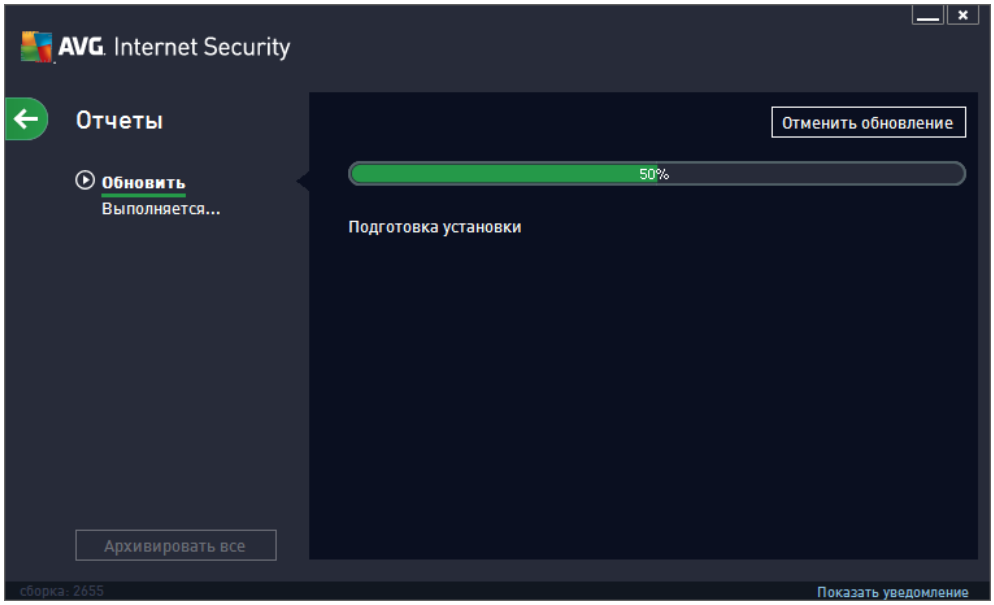
При необходимости вы можете уменьшить количество запусков обновления, установив свои параметры запуска обновления. Тем не менее, настоятельно рекомендуется запускать обновление как минимум раз в день. Данную конфигурацию можно настроить в разделе Дополнительные параметры/Расписания в следующих окнах.

- Расписание обновления определений
- Расписание обновления программы
- Расписание обновления компонента Anti-Spam

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

14.2. Ход обновления

После подтверждения начала обновления программа AVG сначала проверит наличие новых доступных файлов обновления. Если файлы имеются, **AVG Internet Security 2013** начнет их загрузку и выполнит запуск обновления самостоятельно. В процессе обновления откроется интерфейс ***Отчеты***, где можно просмотреть выполняемый процесс в графическом представлении, а также ознакомиться с соответствующими статистическими параметрами *(размер файла обновления, полученные данные, скорость загрузки, время выполнения и т. п.)*.



14.3. Уровни обновлений

AVG Internet Security 2013 предлагает два уровня обновлений на выбор.

- ***Обновление определений*** содержит изменения, необходимые для обеспечения надежной защиты от вирусов, нежелательных сообщений электронной почты и вредоносного ПО. Как правило, сюда не включены изменения кода, а только обновления базы данных определений. Обновление необходимо выполнять сразу после его выпуска.

- ***Обновление программы*** — содержит различные изменения, исправления и улучшения программы.

При планировании обновления можно настроить определенные параметры для обеих уровней обновлений.

- Расписание обновления определений

- Расписание обновления программы

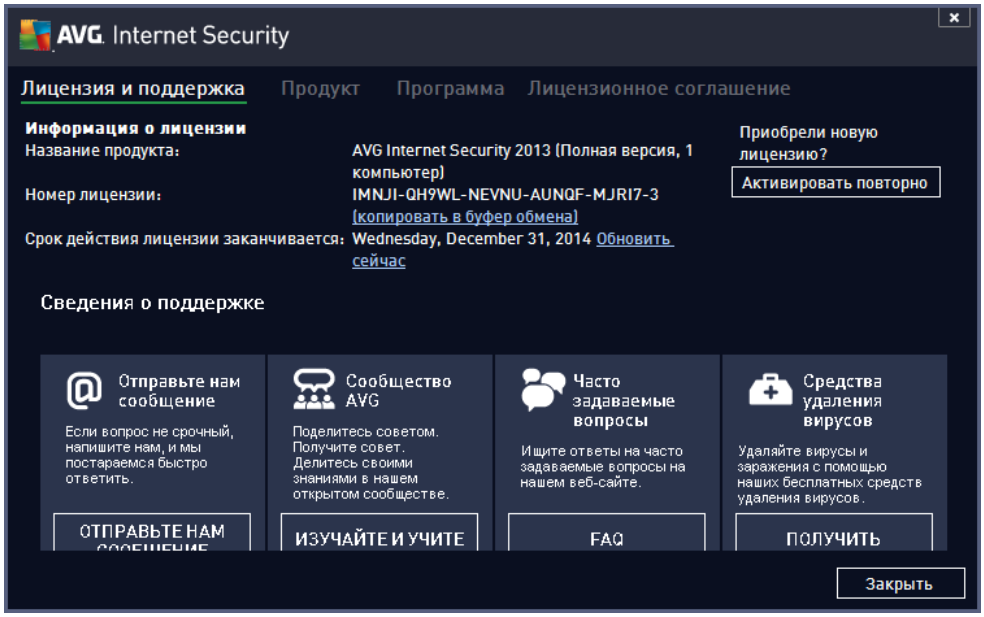
Примечание. *Если запланированное обновление программы и запланированное сканирование придутся на одно и то же время, сканирование будет прервано, так как процесс обновления имеет более высокий приоритет.*

15. Часто задаваемые вопросы и техническая поддержка

При возникновении вопросов при продаже или технических проблем, связанных с использованием приложения **AVG Internet Security 2013**, справочную информацию можно получить несколькими способами. Выберите один из следующих вариантов.

- ***Поддержка***. С помощью меню приложения AVG можно перейти на страницу службы поддержки пользователей на веб-сайте AVG (http://www.avg.com/). Выберите пункт главного меню ***Справка / Поддержка*** для перехода на веб-сайт AVG с доступными средствами поддержки. Далее следуйте приведенным на веб-странице инструкциям.

- ***Поддержка (ссылка в главном меню)***. Меню приложения AVG (*в верхней части основного пользовательского интерфейса*) содержит ссылку ***Поддержка***, при нажатии на которую открывается новое диалоговое окно со всей необходимой информацией для решения проблемы. В этом окне содержится основная информация об установленной программе AVG (*программа/версия базы данных*), сведения о лицензии и список ссылок для быстрого перехода в соответствующий раздел поддержки.



- ***Устранение неполадок в файле справки***. Новый раздел ***Устранение неполадок*** можно найти в файле справки **AVG Internet Security 2013** *(чтобы открыть файл справки, нажмите клавишу F1 в любом диалоговом окне приложения)*. Данный раздел содержит список наиболее часто возникающих ситуаций, в которых пользователю может понадобиться профессиональная помощь по техническим вопросам. Выберите ситуацию, которая наиболее полно описывает возникшую проблему, и щелкните на ней, чтобы открыть подробные инструкции для решения этой проблемы.

- ***Центр поддержки веб-сайта AVG***. Также можно поискать решение возникшей проблемы на веб-сайте AVG (http://www.avg.com/). В разделе ***Центр поддержки*** можно найти структурированный по тематическим группам обзор, содержащий вопросы как технического характера, так и связанные с продажами.

- ***Часто задаваемые вопросы***. На веб-сайте компании AVG (http://www.avg.com/)

также можно ознакомиться с хорошо структурированным специальным разделом часто задаваемых вопросов. Данный раздел доступен из пункта меню ***Центр поддержки/Часто задаваемые вопросы***. Все вопросы удобно разделены на категории, относящиеся к продажам, техническим неполадкам и вирусам.

- ***Сведения о вирусах и угрозах***. Отдельная часть веб-сайта AVG (http://www.avg.com/) посвящена проблемам вирусов *(перейти на эту веб-страницу можно с помощью главного меню через пункт «Справка / О вирусах и угрозах»)*. Для перехода на страницу с подробным обзором сетевых угроз выберите в меню пункт ***Центр поддержки / Сведения о вирусах и угрозах***. Здесь можно найти инструкции по удалению вирусов и шпионского ПО, а также советы о том, как защититься.

- ***Дискуссионный форум***. Проблему также можно обсудить на форуме для пользователей AVG, доступном по адресу http://forums.avg.com.