# AVG Email Server Edition 2011

## Руководство пользователя

**Версия документа 2011.01 (22. 9. 2010)**

# Содержимое

# 1. Введение

Руководство пользователя содержит полные сведения о системе **AVG Email Server Edition 2011**.

**Поздравляем с приобретением AVG Email Server Edition 2011!**

**AVG Email Server Edition 2011** является одним из представителей линейки продуктов AVG, удостоенных различных наград, который создан для обеспечения вашего спокойствия и полной безопасности компьютера. Как и другие продукты, система **AVG Email Server Edition 2011** была полностью переработана для обеспечения традиционно высокой безопасности продуктов AVG, а также имеет новый более удобный и эффективный интерфейс.

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

***Примечание.*** *Данная документация содержит описание функций выпуска E-mail Server Edition. Информацию о других функциях AVG см. в руководстве пользователя выпуска Internet Security, которое содержит все необходимые сведения. Руководство можно загрузить на веб-сайте http://www.avg.com.*

# 2. Требования для установки AVG

## 2.1. Поддерживаемые операционные системы

**AVG Email Server Edition 2011** обеспечивает защиту серверов электронной почты, на которых используются следующие операционные системы.

- Windows 2008 Server Edition (x86 и x64)
- Windows 2003 Server (x86, x64) с пакетом обновления 1

## 2.2. Поддерживаемые серверы эл. почты

Поддерживаются следующие серверы электронной почты.

- Версия сервера MS Exchange 2003
- Версия сервера MS Exchange 2007
- Версия сервера MS Exchange 2010
- AVG для почтового сервера Kerio Версия 6.7.2 или выше.

## 2.3. Требования к оборудованию

Ниже описаны минимальные требования к оборудованию для **AVG Email Server Edition 2011**.

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

Ниже описаны рекомендуемые требования к оборудованию для **AVG Email Server Edition 2011**.

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

## 2.4. Удаление предыдущих версий

Если установлена более ранняя версия сервера AVG Email Server, то перед установкой программы **AVG Email Server Edition 2011** ее необходимо удалить вручную. Необходимо вручную удалить предыдущую версию с помощью

стандартной функции Windows.

- В меню Пуск выберите ***Конфигурация/Панель управления/Установка и удаление программ***, а затем выберите необходимую программу в списке установленных. Будьте внимательны и выберите правильную программу AVG для удаления. Необходимо удалить программу Email Server Edition перед удалением AVG File Server Edition.

- После удаления Email Server Edition можно удалить предыдущую версию AVG File Server Edition. Это можно сделать с помощью меню Пуск. Выберите ***Пуск/Все программы/AVG/Удалить AVG***

- Если ранее использовалась версия AVG 8.x или выше, не забудьте также удалить отдельные модули сервера.

  ***Примечание.*** *Во время процесса удаления потребуется перезапустить службу хранилища.*

  ***Модуль Exchange***. Запустите файл setupes.exe с помощью параметра /uninstall из папки, в которой был установлен модуль.

  *Например: C:\AVG4ES2K\setupes.exe /uninstall*

  ***Модуль Lotus Domino/Notes***. Запустите файл setupln.exe с помощью параметра /uninstall из папки, в которой был установлен модуль.

  *Например: C:\AVG4LN\setupln.exe /uninstall*

## 2.5. Пакеты обновления MS Exchange

Для сервера MS Exchange 2003 Server не требуются пакеты обновления. Однако в целях обеспечения максимального уровня защиты рекомендуется устанавливать все доступные пакеты обновления и исправления.

**Пакет обновления для сервера MS Exchange 2003 Server (необязательно):**

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

В начале процесса установки будут проверены версии всех системных библиотек. Если потребуется установить более новые библиотеки, программа установки переименует устаревшие библиотеки и добавит в их имена файлов расширение . delete. Они будут удалены после перезагрузки системы.

**Пакет обновления для сервера MS Exchange 2007 Server (необязательно):**

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

# 3. Процесс установки AVG

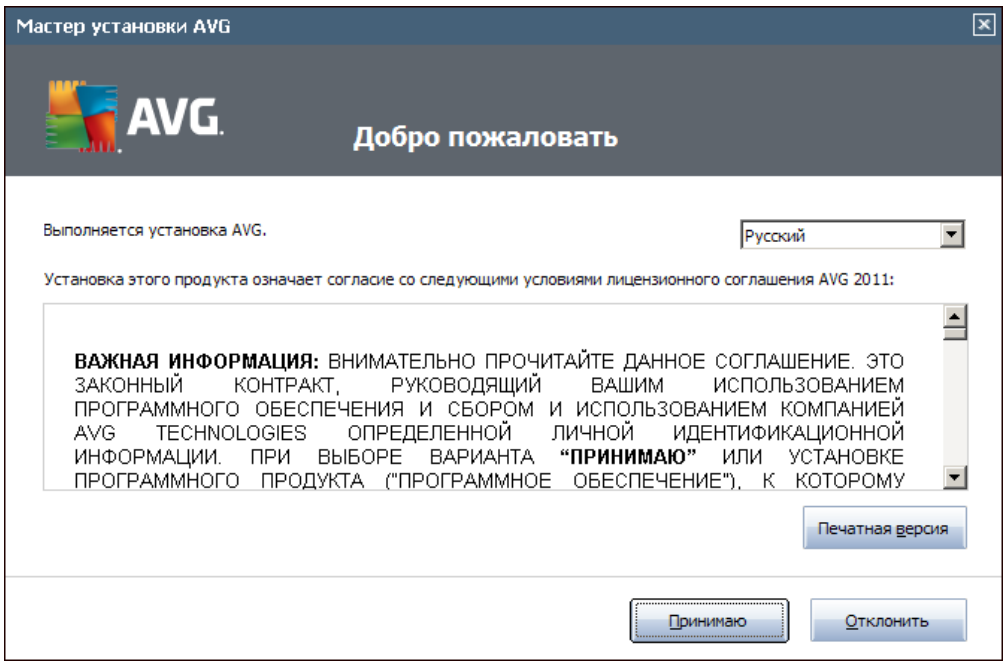
Чтобы установить приложение AVG на компьютер, необходимо загрузить последний файл установки. Можно использовать файл установки на компакт-диске, включенном в коробочную версию, но этот файл может устареть. Поэтому рекомендуется загружать последние файлы установки в Интернете. Файл можно загрузить на веб-сайте AVG (по адресу: http://www.avg.com/download?prd=msw)

***Примечание.*** *Доступно два пакета установки продукта - для 32-разрядных (с обозначением x86) и 64-разрядных операционных систем (с обозначением x64). Выберите пакет установки, соответствующий вашей операционной системе..*

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

После загрузки и сохранения файла установки на жестком диске можно запустить процесс установки. Установка - это последовательность диалоговых окон с кратким описанием необходимых действий на каждом этапе. Далее приводится описание каждого диалогового окна.

## 3.1. Запуск установки




При запуске процесса установки открывается окно ***Добро пожаловать***. В данном окне необходимо выбрать язык, который будет использоваться во время процесса установки, а также для отображения лицензионного соглашения. Нажмите кнопку ***Печатная версия***, чтобы открыть текст лицензии в новом окне. Затем нажмите кнопку ***Принять***, чтобы подтвердить выбор и перейти к следующему

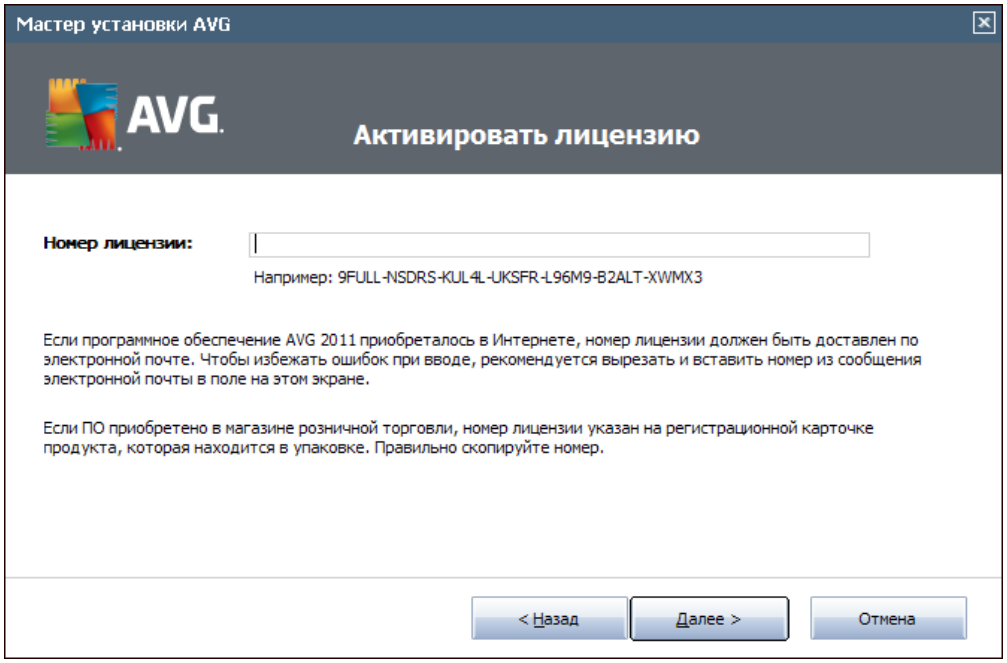
диалоговому окну.

***Внимание!*** *Позже во время установки также можно будет выбрать дополнительные языки для интерфейса приложения.*

## 3.2. Активировать лицензию

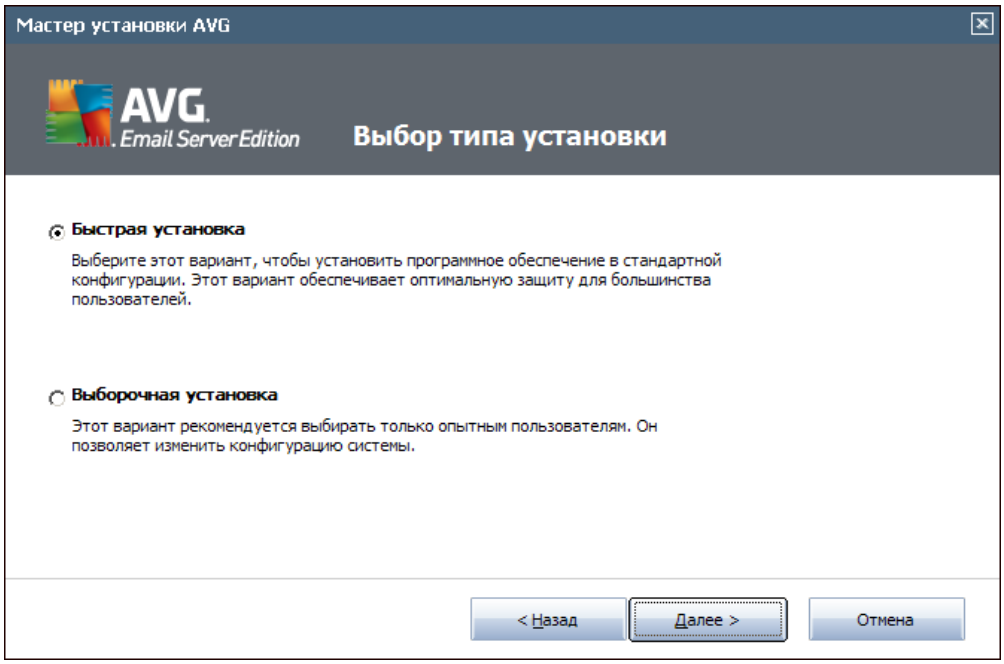
В диалоговом окне ***Активация лицензии*** необходимо указать номер лицензии.

Введите номер лицензии в текстовом поле ***Номер лицензии***. Номер лицензии будет указан в подтверждающем сообщении электронной почты, которое высылается после оформления покупки AVG через Интернет. Необходимо правильно ввести номер. Номер лицензии в цифровом виде (приведенный в сообщении электронной почты) можно вставить с использованием стандартного метода копирования и вставки.




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

## 3.3. Выбор типа установки

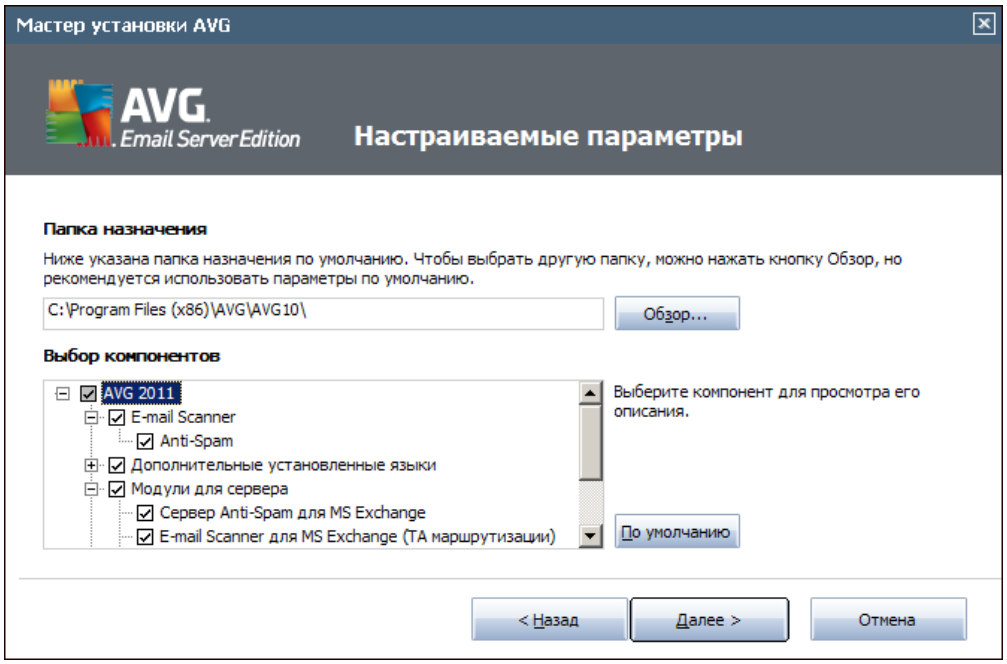



В диалоговом окне ***Выбор типа установки*** можно выбрать один из двух типов установки: ***Быстрая установка*** и ***Выборочная установка***.

Для большинства пользователей рекомендуется выбирать вариант ***Быстрая установка***. В этом случае установка AVG выполняется в полностью автоматическом режиме с параметрами, предварительно заданными поставщиком программного обеспечения. Данный вариант установки обеспечивает максимальный уровень защиты наряду с оптимальным уровнем использования ресурсов. Если в дальнейшем потребуется изменить конфигурацию, это всегда можно будет сделать напрямую в приложении AVG.

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

## 3.4. Выборочная установка - Пользовательские параметры




С помощью диалогового окна ***Папка назначения*** можно указать местоположение для установки продукта AVG. По умолчанию установка AVG выполняется в папку Program Files, которая расположена на диске C:. Чтобы изменить это местоположение, используйте кнопку ***Обзор***, после нажатия которой отобразится структура дисков, в которой можно выбрать соответствующую папку.

Диалоговое окно ***Выбор компонентов*** содержит обзор всех компонентов AVG, которые могут быть установлены. Если значения параметров по умолчанию не подходят, можно добавить или удалить определенные компоненты.

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

- ***Клиент удаленного администрирования AVG***. Если AVG будет подключаться к AVG DataCenter (выпуски AVG Network Edition), необходимо выбрать этот параметр.

  ***Примечание.*** *Удаленное управление поддерживают только серверные компоненты, доступные в списке.*

- ***Диспетчер параметров*** - это инструмент, предназначенный для сетевых администраторов и позволяющий копировать, редактировать и распределять конфигурацию AVG. Конфигурацию можно сохранить на портативном устройстве (флэш-накопитель USB и т. д.), а затем применить вручную или другим способом к выбранным станциям.

- ***Дополнительные установленные языки***. Можно выбрать языки

интерфейса AVG, которые необходимо установить. Установите флажок ***Дополнительные установленные языки***, а затем выберите необходимые языки в соответствующем меню.

Ниже приведен краткий обзор отдельных компонентов сервера (***надстройки сервера***).

- ***Сервер Anti-Spam для MS Exchange***

  Выполняет проверку всех входящих сообщений эл. почты и отмечает нежелательные сообщения как спам. Данный компонент использует несколько способов анализа для обработки каждого сообщения электронной почты, обеспечивая максимальную защиту от спама.

- ***E-mail Scanner для MS Exchange (TA маршрутизации)***

  Выполняет проверку всех входящих, исходящих и внутренних сообщений эл. почты, проходящих через роль сервера-концентратора MS Exchange.

  Этот компонент доступен для MS Exchange 2007/2010 и может быть установлен только для роли концентратора.

- ***E-mail Scanner для MS Exchange (TA SMTP)***

  Выполняет проверку всех сообщений эл. почты, проходящих через интерфейс SMTP сервера MS Exchange.

  Этот компонент доступен только для MS Exchange 2007/2010 и может быть установлен для ролей пограничного сервера и концентратора.

- ***E-mail Scanner для MS Exchange (VSAPI)***

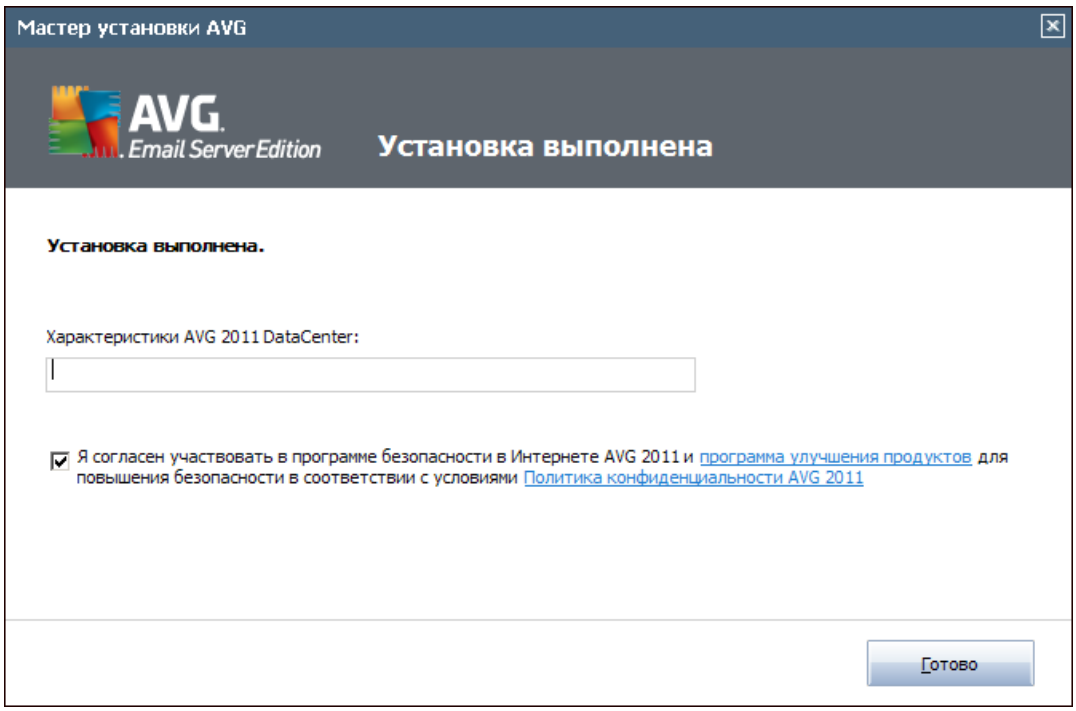
  Выполняет проверку всех сообщений эл. почты, хранящихся в почтовых ящиках пользователей. При обнаружении вирусов сообщения перемещаются в вирусное хранилище или удаляются.

***Примечание.*** *Набор параметров для сервера MS Exchange зависит от версии сервера.*

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

## 3.5. Завершение установки

Если при выборе модулей был выбран модуль ***Компонент Удаленное администрирование***, на последнем экране можно определить строку подключения для подключения к базе данных AVG DataCenter.




Приложение AVG установлено и работает правильно. Программа работает в виде фонового процесса в автоматическом режиме.

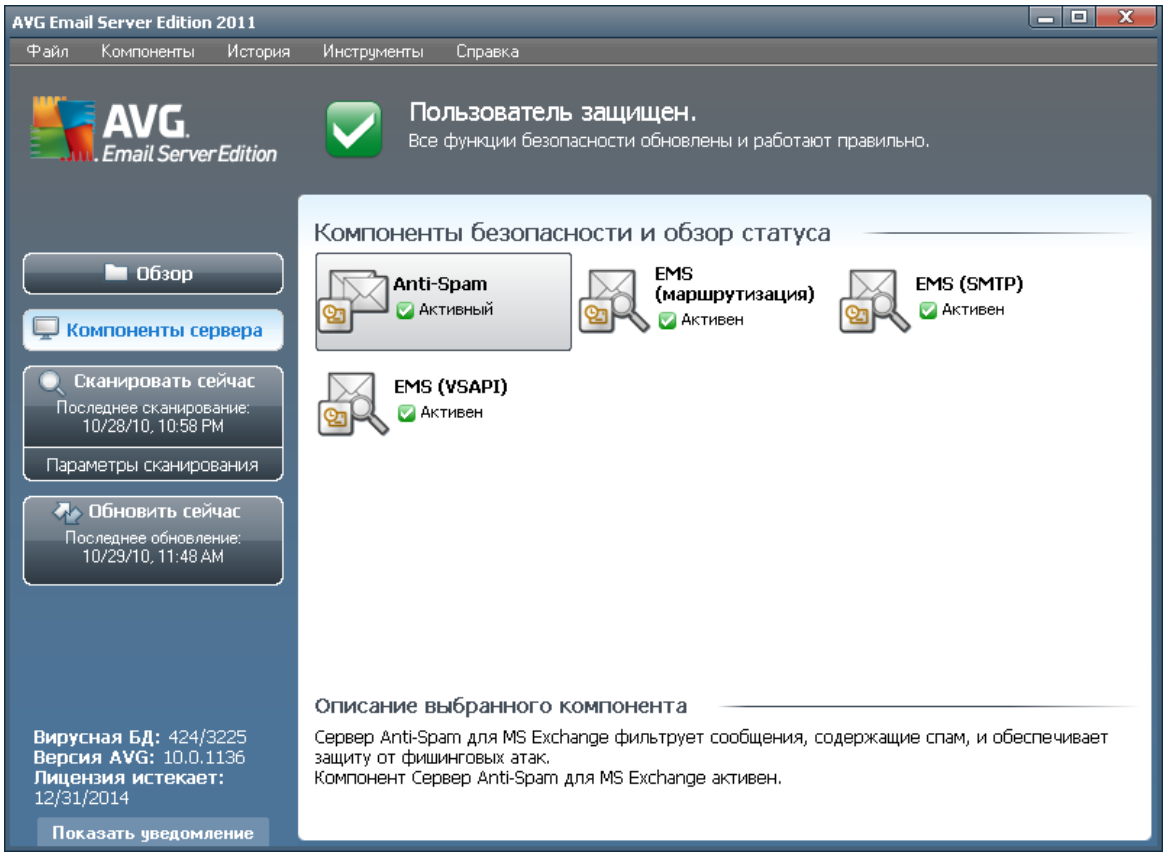
Чтобы настроить защиту сервера эл. почты, см. соответствующую главу.

- ***E-mail Scanner для сервера MS Exchange 2007/2010***
- ***E-mail Scanner для MS Exchange Server 2003***
- ***AVG для почтового сервера Kerio***

# 4. E-mail Scanner для MS Exchange Server 2007/2010

## 4.1. Обзор

Варианты конфигурации AVG для MS Exchange Server 2007 полностью интегрированы с AVG Email Server Edition 2011 в качестве серверных компонентов.




Ниже приведен краткий обзор отдельных компонентов сервера.

- ***Anti-Spam - Сервер Anti-Spam для MS Exchange***

  Выполняет проверку всех входящих сообщений эл. почты и отмечает нежелательные сообщения как спам. Данный компонент использует несколько способов анализа для обработки каждого сообщения электронной почты, обеспечивая максимальную защиту от спама.

- ***EMS (маршрутизация) - E-mail Scanner для MS Exchange (TA маршрутизации)***

  Выполняет проверку всех входящих, исходящих и внутренних сообщений эл. почты, проходящих через роль сервера-концентратора MS Exchange.

Этот компонент доступен для MS Exchange 2007/2010 и может быть установлен только для роли концентратора.

- ***EMS (SMTP) - E-mail Scanner для MS Exchange (TA SMTP)***

  Выполняет проверку всех сообщений эл. почты, проходящих через интерфейс SMTP сервера MS Exchange.

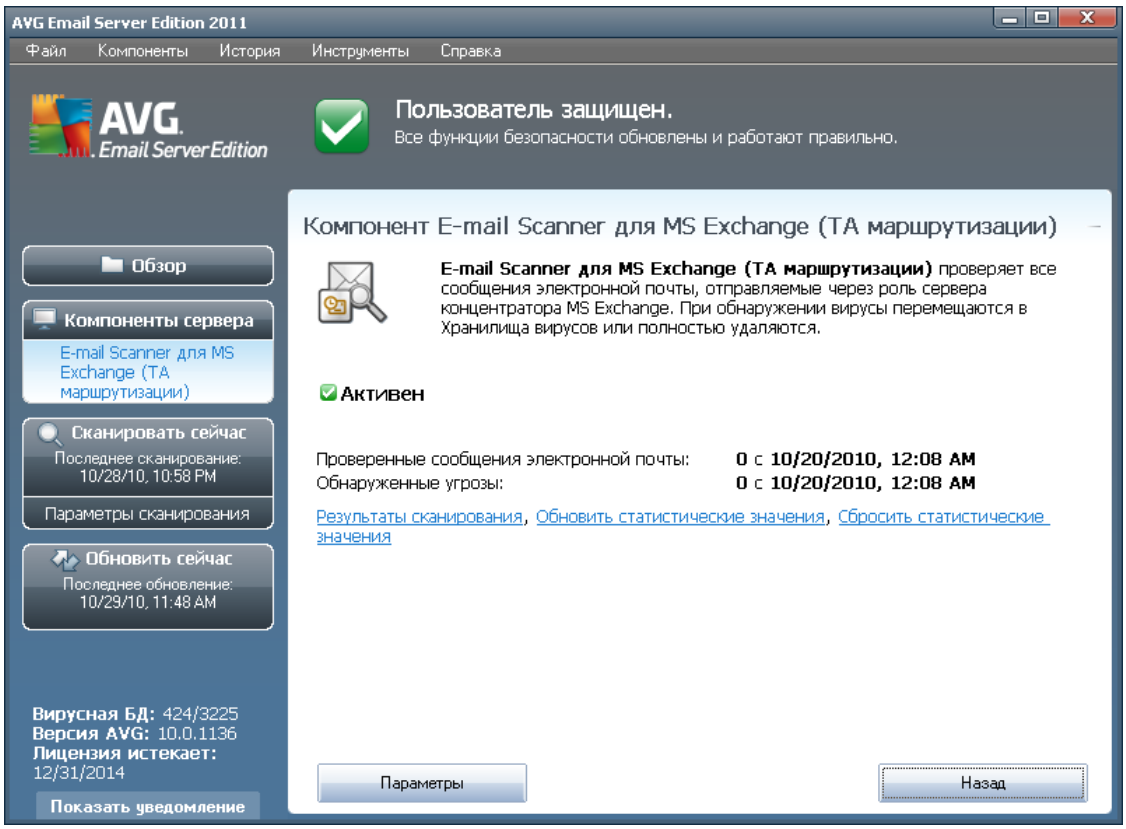
  Этот компонент доступен только для MS Exchange 2007/2010 и может быть установлен для ролей пограничного сервера и концентратора.

- ***EMS (VSAPI) - E-mail Scanner для MS Exchange (VSAPI)***

  Выполняет проверку всех сообщений эл. почты, хранящихся в почтовых ящиках пользователей. При обнаружении вирусов сообщения перемещаются в вирусное хранилище или удаляются.

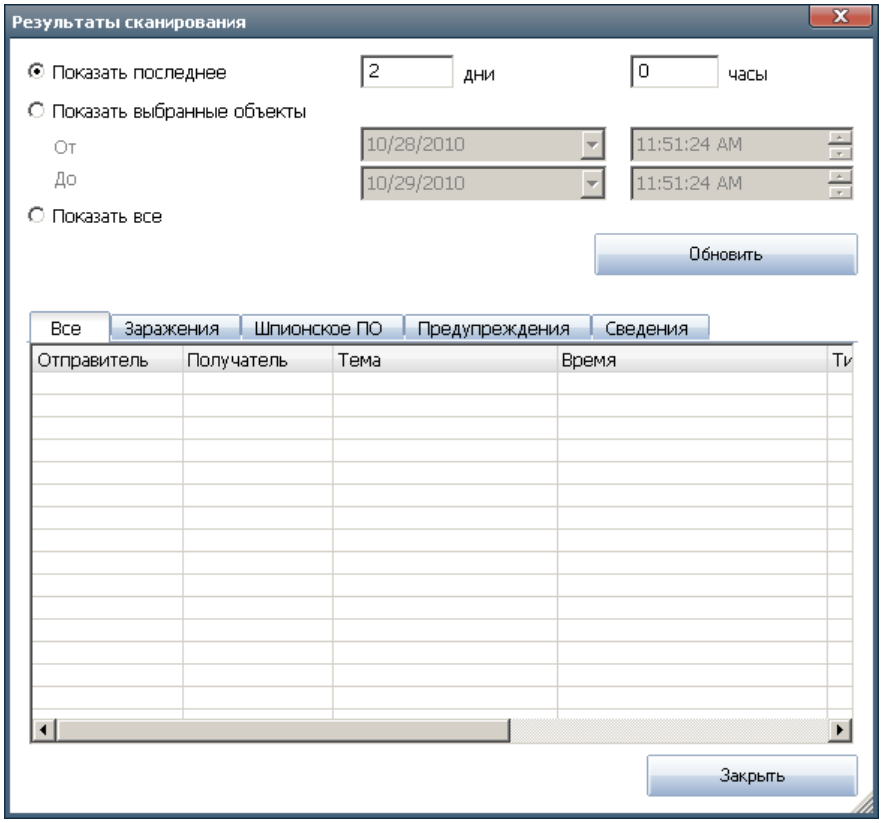
***Важно.*** *При установке и использовании VSAPI в сочетании с другим агентом транспорта в роли сервера-концентратора Exchange ваши сообщения эл. почты будут сканироваться дважды. Чтобы этого избежать, ознакомьтесь с разделом* ***Техническое примечание*** *ниже для получения дополнительных сведений.*

Дважды щелкните компонент, чтобы открыть его интерфейс. Во всех компонентах, кроме Anti-Spam, используются одинаковые кнопки управления и ссылки.



- ***Результаты сканирования***

  Открытие нового диалогового окна, в котором можно просмотреть результаты сканирования.




  В этом окне можно просмотреть сообщения на различных вкладках, соответствующих уровню серьезности. Для получения информации об изменении уровней серьезности и параметров отчетности см. разделы, посвященные настройке отдельных компонентов.

  По умолчанию отображаются результаты сканирования за последние два дня. Период отображаемых сообщений можно изменить с помощью следующих параметров.

  - ***Показать последние***. Вставка необходимых значений дней и часов.
  - ***Показать выбранное***. Выбор интервала времени и даты.
  - ***Показать все***. Отображение результатов за весь период времени.

  Чтобы обновить результаты, нажмите кнопку ***Обновить***.

- ***Обновить статистические данные***. Обновление статистических данных, отображенных выше.

- ***Сбросить статистические данные***. Сброс статистических данных.

Доступны следующие кнопки.

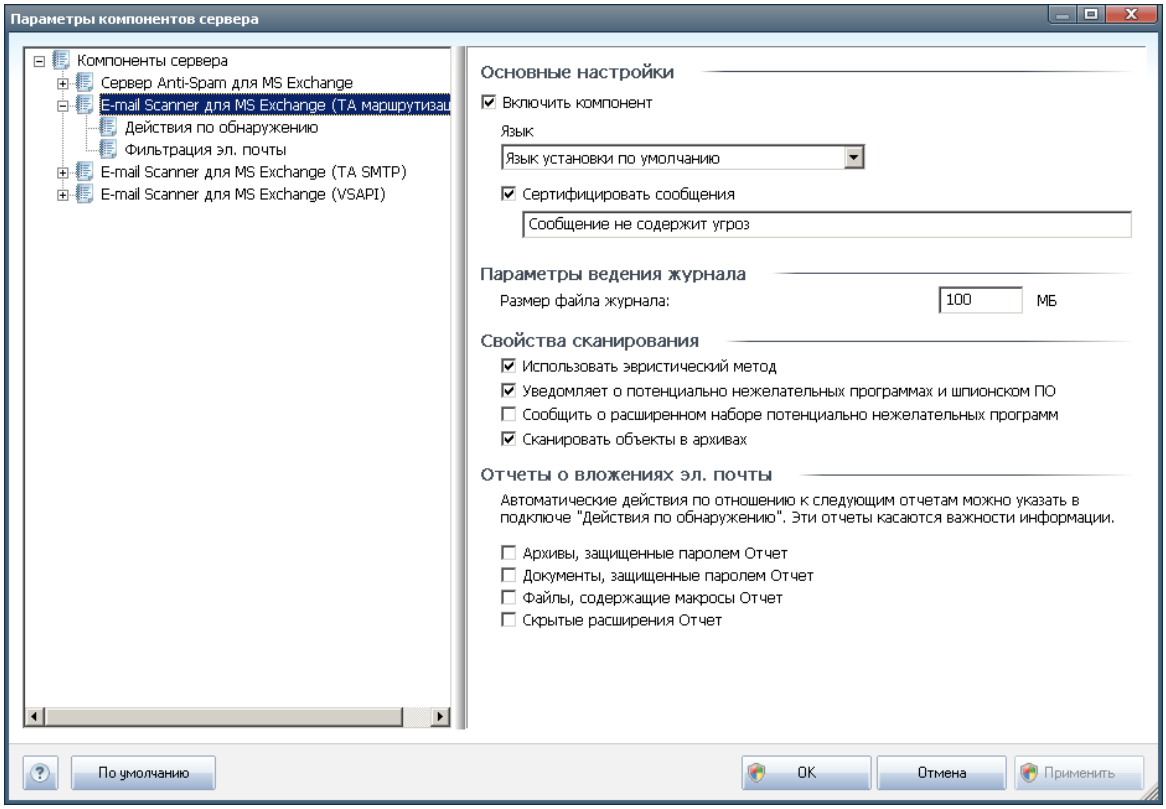
- ***Параметры***. Позволяет открыть окно параметров компонента.
- ***Назад***. Нажмите эту кнопку, чтобы вернуться к окну обзора компонентов сервера.

Дополнительная информация о настройке параметров отдельных компонентов приведена в разделах ниже.

## 4.2. E-mail Scanner для MS Exchange (TA маршрутизации)

Чтобы открыть параметры компонента ***E-mail Scanner для MS Exchange (TA маршрутизации)***, нажмите кнопку ***Параметры*** в интерфейсе компонента.

В списке ***Компоненты сервера*** выберите пункт ***E-mail Scanner для MS Exchange (TA маршрутизации)***.




Раздел ***Основные параметры*** содержит следующие элементы.

- ***Включить компонент***. Снимите флажок, чтобы полностью отключить компонент.

- ***Язык***. Выберите предпочтительный язык компонента.

- ***Сертифицировать сообщения***. Установите этот флажок, если требуется добавлять примечание о сертификации во все сканируемые сообщения. Текст сообщения можно указать в расположенном рядом поле.

Раздел ***Параметры ведения журнала***.

- ***Размер файла журнала***. Выберите предпочтительный размер файла журнала. Значение по умолчанию: 100 МБ.

Раздел ***Свойства сканирования***.

- ***Использовать эвристический анализ***. Установите этот флажок, чтобы включить метод эвристического анализа при сканировании.

- ***Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО***. Установите этот флажок, чтобы включить в отчет сведения о наличии потенциально нежелательных программ и шпионского ПО.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ***. 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, а также безвредные, но нежелательные программы (различные панели инструментов и т. п.). Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности и комфорта при работе, однако из-за него могут также блокироваться некоторые законные программы, поэтому по умолчанию параметр отключен. Примечание. Данная функция обнаружения является дополнением к предыдущему параметру, поэтому, чтобы обеспечить защиту от основных типов шпионского ПО, не снимайте флажок, установленный напротив предыдущего параметра.

- ***Сканировать объекты в архивах***. Установите этот флажок, чтобы выполнять проверку объектов в архивных файлах (zip, rar и т. д.).

Раздел ***Отчеты о вложениях эл. почты*** позволяет выбрать объекты, которые требуется указывать в отчетах во время сканирования. Если флажок установлен, каждое сообщение эл. почты с таким объектом будет содержать метку [ИНФОРМАЦИЯ] в поле темы. Такая конфигурация установлена по умолчанию, и ее можно легко изменить в разделе ***Действия по обнаружению***, часть ***Информация*** (см. ниже).

Доступны следующие параметры.

- ***Архивы, защищенные паролем.***

- ***Документы, защищенные паролем.***

- ***Файлы, содержащие макросы.***
- ***Скрытые расширения.***

Также в структуре дерева доступны следующие подэлементы.

- ***Действия по обнаружению.***
- ***Фильтрация электронной почты.***

## 4.3. E-mail Scanner для MS Exchange (TA SMTP)

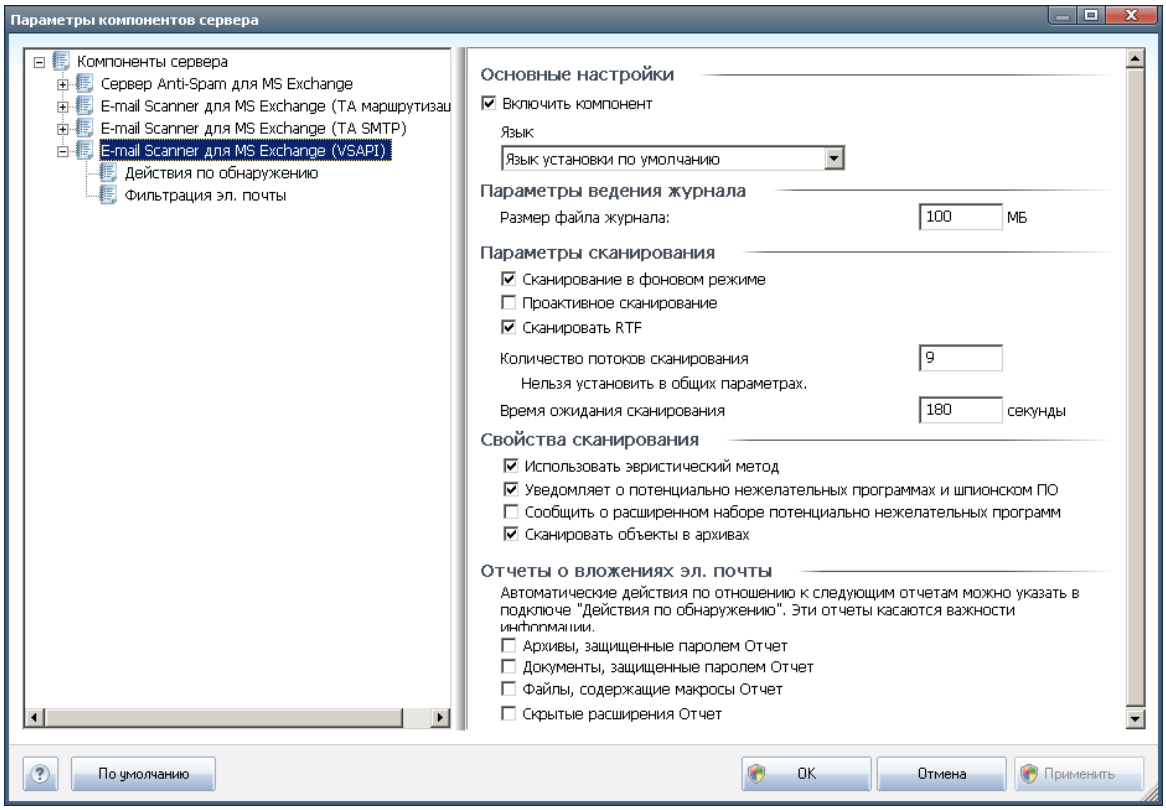
Конфигурация компонента ***E-mail Scanner для MS Exchange (агент транспорта SMTP)*** идентична конфигурации агента транспорта маршрутизации. Дополнительную информацию см. в разделе ***E-mail Scanner для MS Exchange (агент транспорта маршрутизации)*** выше.

Также в структуре дерева доступны следующие подэлементы.

- ***Действия по обнаружению.***
- ***Фильтрация электронной почты.***

## 4.4. E-mail Scanner для MS Exchange (VSAPI)

Этот элемент содержит параметры компонента ***E-mail Scanner для MS Exchange (VSAPI)***.




Раздел ***Основные параметры*** содержит следующие элементы.

- ***Включить компонент***. Снимите флажок, чтобы полностью отключить компонент.
- ***Язык***. Выберите предпочтительный язык компонента.

Раздел ***Параметры ведения журнала***.

- ***Размер файла журнала***. Выберите предпочтительный размер файла журнала. Значение по умолчанию: 100 МБ.

Раздел ***Параметры сканирования***.

- ***Сканирование в фоновом режиме***. Включение или отключение сканирования в фоновом режиме. Сканирование в фоновом режиме является одной из функций интерфейса приложения VSAPI 2.0/2.5. Данная функция обеспечивает сканирование баз данных службы обмена сообщениями Exchange. При обнаружении в папках почтовых ящиков пользователей объектов, которые не были просканированы с использованием последней

вирусной базы данных AVG, эти объекты отправляются на сканирование одним из компонентов AVG, предназначенных для серверов Exchange. Одновременно запускается сканирование и поиск непроверенных объектов.

Использование для каждой базы данных потоков с более низким приоритетом гарантирует, что другие задачи (например, сохранение сообщений электронной почты в базе данных Microsoft Exchange) будут выполняться в первую очередь.

- ***Проактивное сканирование (входящие сообщения)***

  Можно включить или отключить функцию проактивного сканирования VSAPI 2.0/2.5. Такое сканирование выполняется, когда объект добавляется в папку, но клиент не отправляет запрос.

  При отправке сообщений в хранилище Exchange они входят в глобальную очередь сканирования с низким приоритетом (максимум 30 элементов). Они сканируются по принципу FIFO (первый входит, первый выходит). При обращении к элементу, который все еще находится в очереди, ему назначается высокий приоритет.

  ***Примечание.*** *Избыточные сообщения будут храниться без сканирования.*

***Примечание.*** *Даже при отключении параметров* ***Сканирование в фоновом режиме*** *и* ***Проактивное сканирование*** *сканер доступа будет по-прежнему работать при попытке пользователя загрузить сообщение в клиенте MS Outlook.*

- ***Сканировать RTF***. Указание необходимости сканирования файлов в формате RTF.
- ***Количество потоков сканирования***. По умолчанию процесс сканирования разделен на потоки для увеличения общей эффективности сканирования путем указания уровней параллельности. В данном поле можно изменить количество потоков.

  По умолчанию количество потоков рассчитывается следующим образом: 2 умножается на количество процессоров + 1.

  Минимальное количество потоков рассчитывается следующим образом: (количество процессоров + 1) делится на 2.

  Максимальное количество потоков рассчитывается следующим образом: количество процессоров умножается на 5 + 1.

  Если указанное значение равно или меньше/больше минимального или максимального, будет использоваться значение по умолчанию.

- ***Время ожидания сканирования***. Максимальный непрерывный интервал (в секундах) для одного потока, определенный для доступа к сканируемому сообщению (по умолчанию установлено значение 180 секунд).

Раздел ***Свойства сканирования***.

- ***Использовать эвристический анализ***. Установите этот флажок, чтобы включить метод эвристического анализа при сканировании.

- ***Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО***. Установите этот флажок, чтобы включить в отчет сведения о наличии потенциально нежелательных программ и шпионского ПО.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ***. 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, а также безвредные, но нежелательные программы (различные панели инструментов и т. п.). Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности и комфорта при работе, однако из-за него могут также блокироваться некоторые законные программы, поэтому по умолчанию параметр отключен. Примечание. Данная функция обнаружения является дополнением к предыдущему параметру, поэтому, чтобы обеспечить защиту от основных типов шпионского ПО, не снимайте флажок, установленный напротив предыдущего параметра.

- ***Сканировать объекты в архивах***. Установите этот флажок, чтобы выполнять проверку объектов в архивных файлах (zip, rar и т. д.).

Раздел ***Отчеты о вложениях эл. почты*** позволяет выбрать объекты, которые требуется указывать в отчетах во время сканирования. Конфигурацию по умолчанию можно легко изменить в разделе ***Действия по обнаружению***, часть ***Информация*** (см. ниже).

Доступны следующие параметры.

- ***Архивы, защищенные паролем.***

- ***Документы, защищенные паролем.***

- ***Файлы, содержащие макросы.***

- ***Скрытые расширения.***

Обычно некоторые из этих элементов представляют собой пользовательские расширения служб интерфейса приложений Microsoft VSAPI 2.0/2.5. Для получения подробной информации об интерфейсе VSAPI 2.0/2.5 воспользуйтесь следующими ссылками (а также ссылками на соответствующих страницах).

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - сведения о взаимодействии Exchange и антивирусного программного обеспечения.

- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 - сведения о дополнительных функциях VSAPI 2.5 сервера Exchange 2003.

Также в структуре дерева доступны следующие подэлементы.

- ***Действия по обнаружению.***
- ***Фильтрация электронной почты.***

## 4.5. Техническое примечание

Данные сведения относятся к ситуации, когда на сервере, выступающем в роли сервера-концентратора Exchange, одновременно устанавливаются и используются VSAPI и агент транспорта. В этом случае сообщения эл. почты сканируются дважды (сначала сканером доступа VSAPI, а затем агентом транспорта маршрутизации).

По причине принципа работы интерфейса VSAPI в результатах сканирования могут возникать несоответствия. Кроме того, он будет оказывать чрезмерную нагрузку на систему. Поэтому, во избежание повторного сканирования рекомендуется использовать небольшое исправление (см. ниже), чтобы мгновенно разрешить данную проблему.

***Примечание.*** *Настройка реестра должна производиться только опытными пользователями. Перед редактированием реестра рекомендуется выполнить резервное копирование реестра и узнать, как восстановить резервную копию на случай возникновения проблемы.*

Откройте редактор реестра (в ОС Windows выберите ***Пуск/Выполнить***, введите команду ***regedit*** и нажмите клавишу "Enter"). Перейдите к следующей ветви:

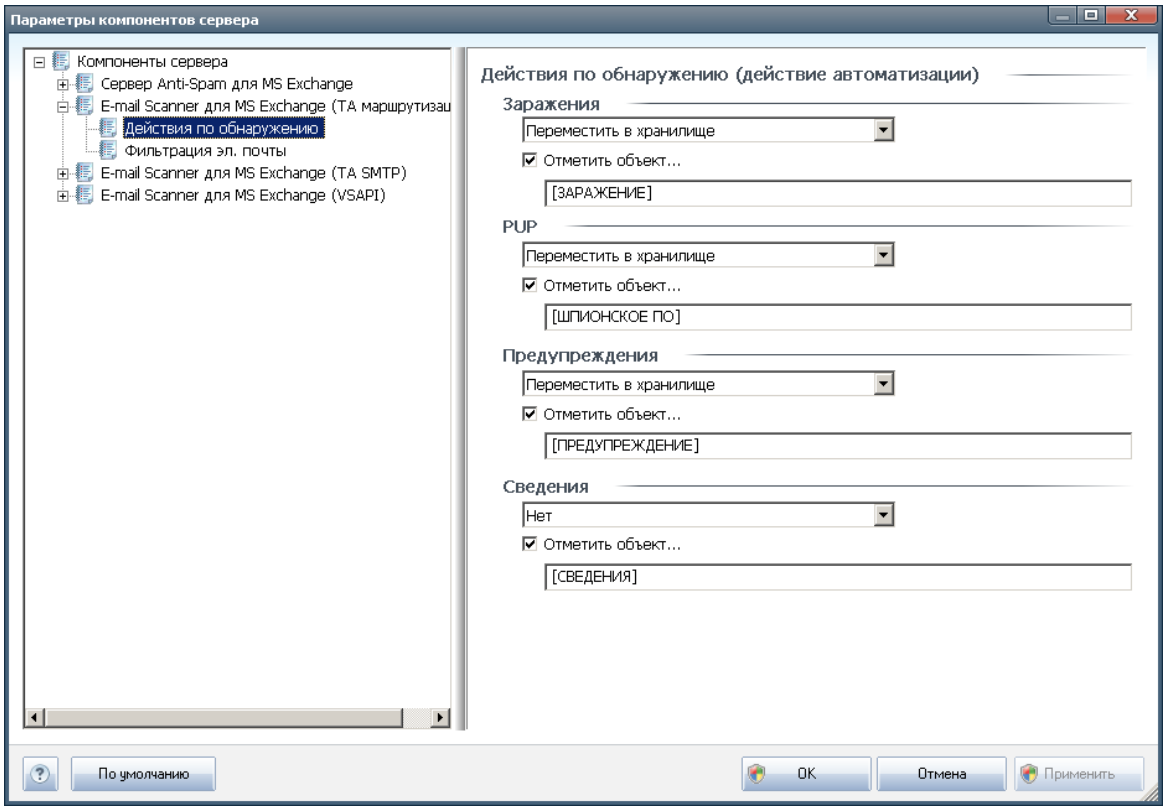
***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan***

Щелкните правой кнопкой мыши в правой части окна и выберите в контекстном меню ***Создать/Параметр DWORD (32 бита)***. Назовите новый параметр ***TransportExclusion***. После создания щелкните его дважды, а затем измените его значение на ***1***.

Чтобы изменения вступили в силу на сервере MS Exchange, установите для ***ReloadNow*** значение 1. Для этого дважды щелкните данный параметр и измените его значение.

Это приведет к отключению сканирования исходящих сообщений сканером доступа VSAPI. Изменение вступит в силу в течение нескольких минут.

## 4.6. Действия по обнаружению




В подэлементе ***Действия по обнаружению*** можно выбрать автоматические действия, которые необходимо выполнить при сканировании.

Доступны действия для следующих элементов.

- ***Зараженные объекты.***
- ***Потенциально нежелательные программы (PUP).***
- ***Предупреждения.***
- ***Информация.***

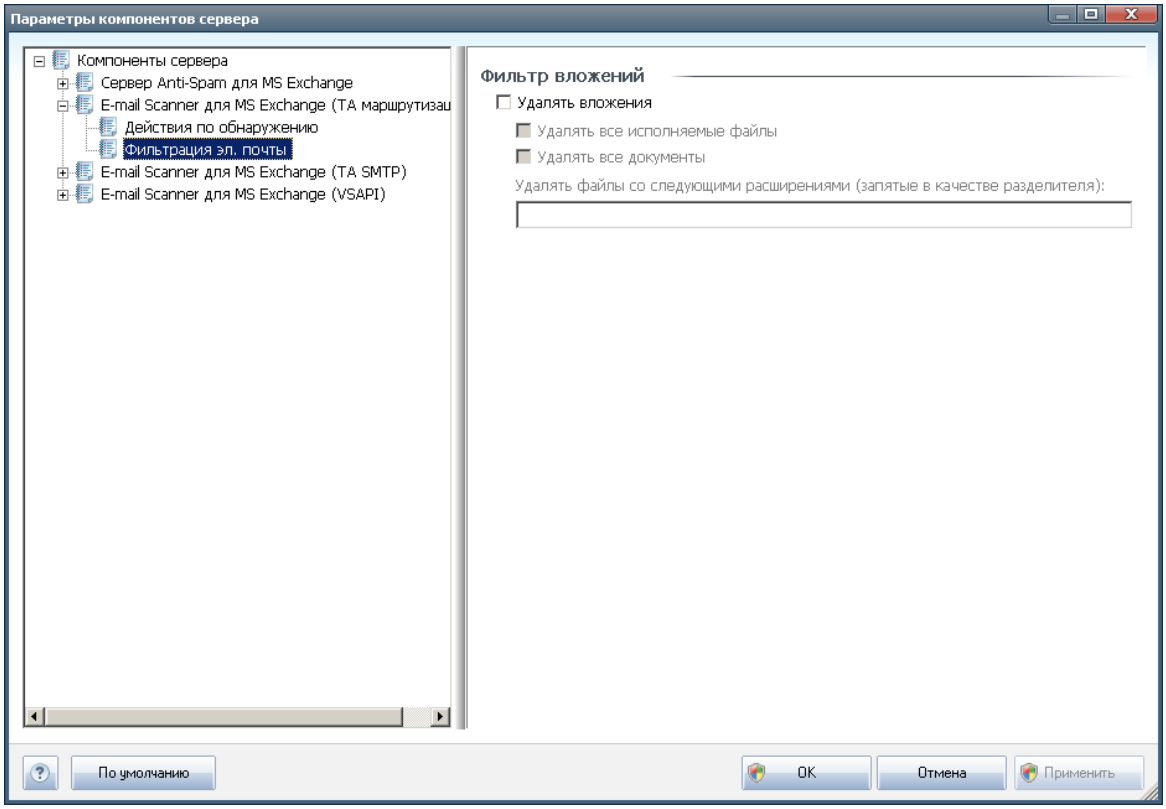
Используйте раскрывающееся меню, чтобы выбрать действие для каждого элемента.

- ***Нет***. Никакое действие не будет выполняться.
- ***Переместить в хранилище***. Угроза будет перемещена в хранилище вирусов.
- ***Удалить***. Угроза будет удалена.

Чтобы настроить текст темы для сообщений, содержащих определенные объекты или угрозы, установите флажок ***Отметить объект...*** и введите значение.

***Примечание.*** *Последняя указанная функция недоступна для компонента E-mail Scanner для MS Exchange VSAPI.*

## 4.7. Фильтрация электронной почты



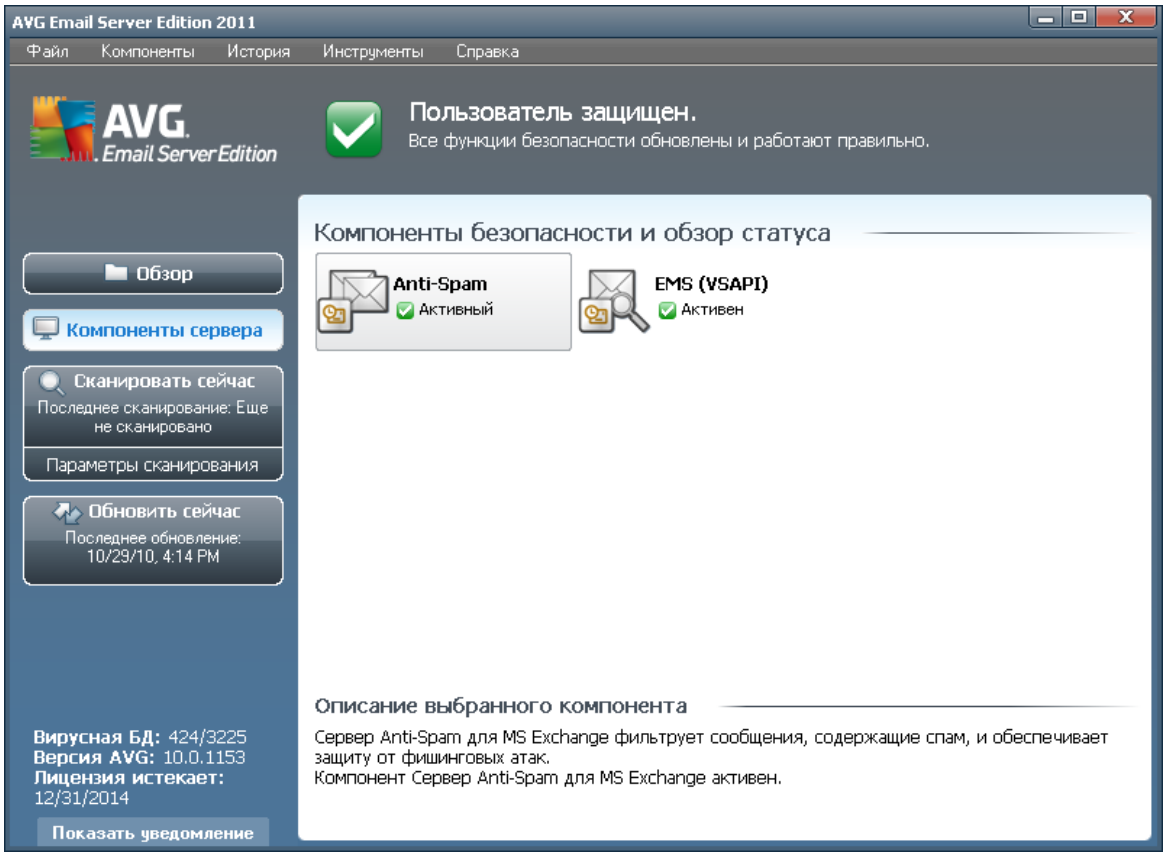

В элементе ***Фильтрация электронной почты*** при необходимости можно настроить автоматическое удаление вложений. Доступны следующие параметры.

- ***Удалять вложения***. Установите флажок, чтобы включить данную функцию.
- ***Удалять все исполняемые файлы***. Удаление всех исполняемых файлов.
- ***Удалять все документы***. Удаление всех файлов документов.
- ***Удалять файлы с расширениями, разделенными запятыми***. Введите в поле расширения файлов, которые будут автоматически удаляться. Разделяйте расширения запятой.

# 5. E-mail Scanner для MS Exchange Server 2003

## 5.1. Обзор

Параметры конфигурации E-mail Scanner для MS Exchange Server 2003 полностью интегрированы с AVG Email Server Edition 2011 в качестве серверного компонента.




Серверные компоненты включают в себя следующие.

Ниже приведен краткий обзор отдельных компонентов сервера.

- ***Anti-Spam - Сервер Anti-Spam для MS Exchange***

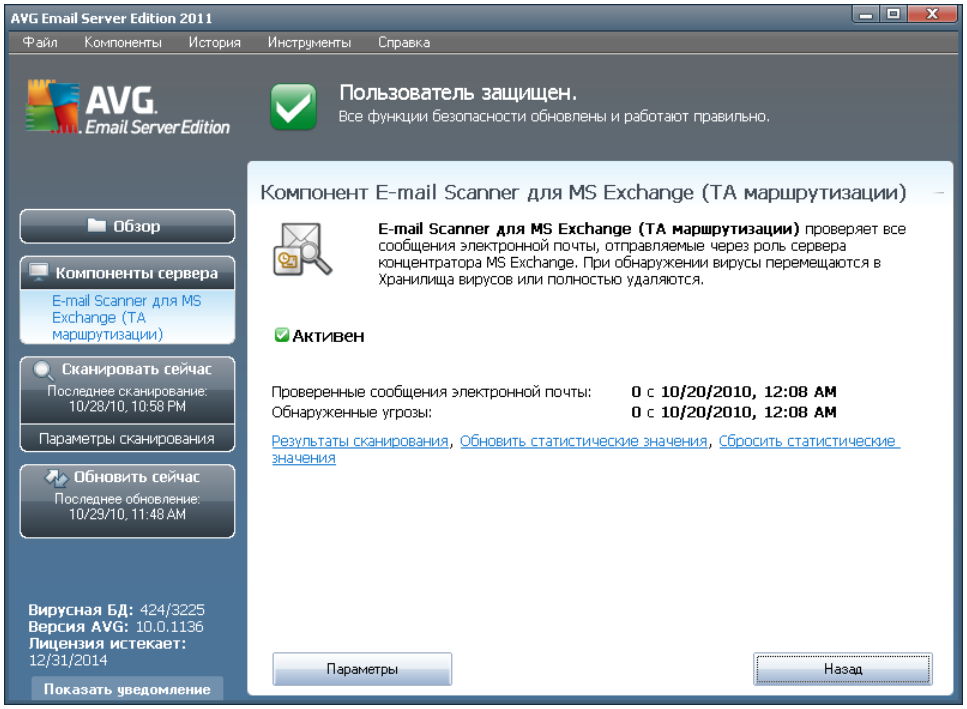
  Выполняет проверку всех входящих сообщений эл. почты и отмечает нежелательные сообщения как СПАМ. Данный компонент использует несколько способов анализа для обработки каждого сообщения электронной почты, обеспечивая максимальную защиту от спама.

- ***EMS (VSAPI) - E-mail Scanner для MS Exchange (VSAPI)***

  Выполняет проверку всех сообщений эл. почты, хранящихся в почтовых ящиках пользователей. При обнаружении вирусов сообщения перемещаются

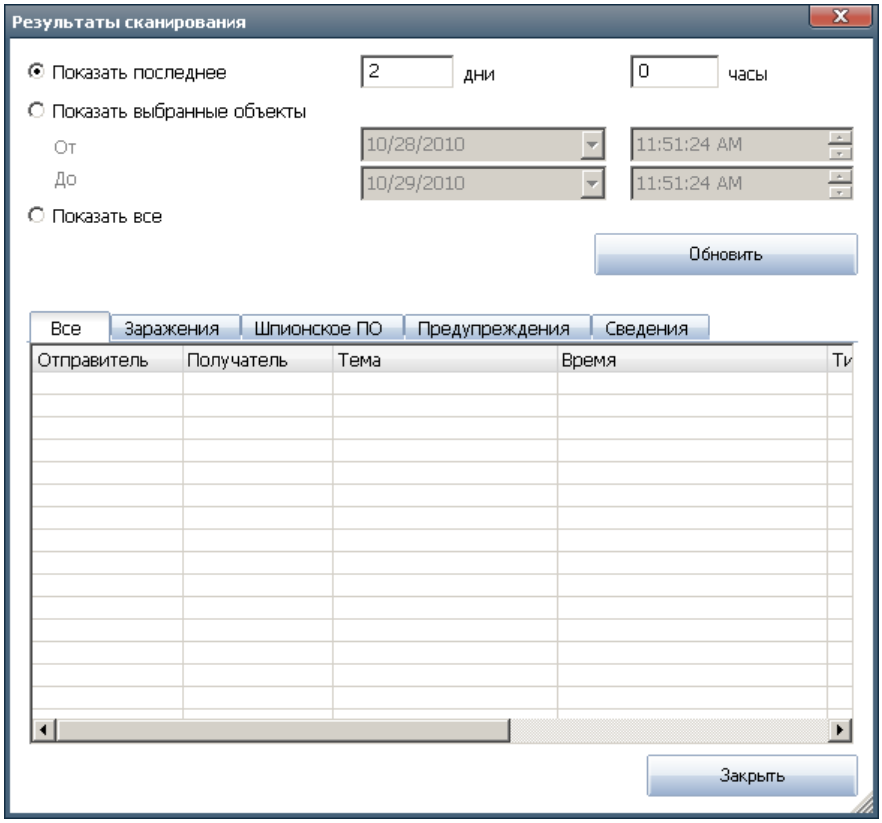
в вирусное хранилище или удаляются.

Дважды щелкните компонент, чтобы открыть его интерфейс. Во всех компонентах, кроме Anti-Spam, используются одинаковые кнопки управления и ссылки.




- ***Результаты сканирования***

  Открытие нового диалогового окна, в котором можно просмотреть результаты сканирования.




В этом окне можно просмотреть сообщения на различных вкладках, соответствующих уровню серьезности. Для получения информации об изменении уровней серьезности и параметров отчетности см. разделы, посвященные настройке отдельных компонентов.

По умолчанию отображаются результаты сканирования за последние два дня. Период отображаемых сообщений можно изменить с помощью следующих параметров.

- ***Показать последние***. Вставка необходимых значений дней и часов.
- ***Показать выбранное***. Выбор интервала времени и даты.
- ***Показать все***. Отображение результатов за весь период времени.

Чтобы обновить результаты, нажмите кнопку ***Обновить***.

- ***Обновить статистические данные***. Обновление статистических данных, отображенных выше.
- ***Сбросить статистические данные***. Сброс статистических данных.

Доступны следующие кнопки.

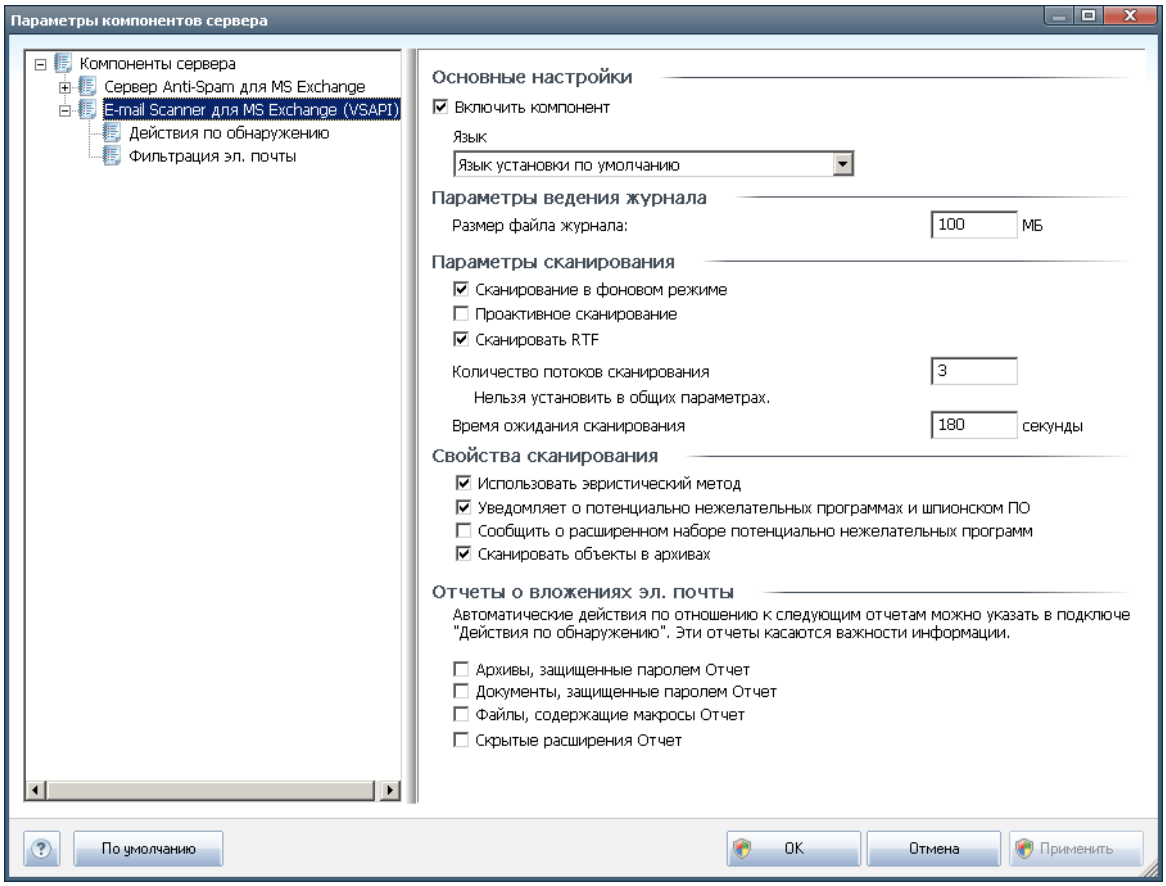
- ***Параметры***. Позволяет открыть окно параметров компонента.

- ***Назад***. Нажмите эту кнопку, чтобы вернуться к окну обзора компонентов сервера.

Дополнительная информация о настройке параметров отдельных компонентов приведена в разделах ниже.

## 5.2. E-mail Scanner для MS Exchange (VSAPI)

Этот элемент содержит параметры компонента ***E-mail Scanner для MS Exchange (VSAPI)***.




Раздел ***Основные параметры*** содержит следующие элементы.

- ***Включить компонент***. Снимите флажок, чтобы полностью отключить компонент.

- ***Язык***. Выберите предпочтительный язык компонента.

Раздел ***Параметры ведения журнала***.

- ***Размер файла журнала***. Выберите предпочтительный размер файла журнала. Значение по умолчанию: 100 МБ.

Раздел ***Параметры сканирования***.

- ***Сканирование в фоновом режиме***. Включение или отключение сканирования в фоновом режиме. Сканирование в фоновом режиме является одной из функций интерфейса приложения VSAPI 2.0/2.5. Данная функция обеспечивает сканирование баз данных службы обмена сообщениями Exchange. При обнаружении в папках почтовых ящиков пользователей объектов, которые не были просканированы с использованием последней вирусной базы данных AVG, эти объекты отправляются на сканирование одним из компонентов AVG, предназначенных для серверов Exchange. Одновременно запускается сканирование и поиск непроверенных объектов.

  Использование для каждой базы данных потоков с более низким приоритетом гарантирует, что другие задачи (например, сохранение сообщений электронной почты в базе данных Microsoft Exchange) будут выполняться в первую очередь.

- ***Проактивное сканирование (входящие сообщения)***

  Можно включить или отключить функцию проактивного сканирования VSAPI 2.0/2.5. Такое сканирование выполняется, когда объект добавляется в папку, но клиент не отправляет запрос.

  При отправке сообщений в хранилище Exchange они входят в глобальную очередь сканирования с низким приоритетом (максимум 30 элементов). Они сканируются по принципу FIFO (первый входит, первый выходит). При обращении к элементу, который все еще находится в очереди, ему назначается высокий приоритет.

  ***Примечание.*** *Избыточные сообщения будут храниться без сканирования.*

***Примечание.*** *Даже при отключении параметров* ***Сканирование в фоновом режиме*** *и* ***Проактивное сканирование*** *сканер доступа будет по-прежнему работать при попытке пользователя загрузить сообщение в клиенте MS Outlook.*

- ***Сканировать RTF.*** Указание необходимости сканирования файлов в формате RTF.
- ***Количество потоков сканирования.*** По умолчанию процесс сканирования разделен на потоки для увеличения общей эффективности сканирования путем указания уровней параллельности. В данном поле можно изменить количество потоков.

  По умолчанию количество потоков рассчитывается следующим образом: 2 умножается на количество процессоров + 1.

  Минимальное количество потоков рассчитывается следующим образом: (количество процессоров + 1) делится на 2.

  Максимальное количество потоков рассчитывается следующим образом: количество процессоров умножается на 5 + 1.

  Если указанное значение равно или меньше/больше минимального или

максимального, будет использоваться значение по умолчанию.

- ***Время ожидания сканирования***. Максимальный непрерывный интервал (в секундах) для одного потока, определенный для доступа к сканируемому сообщению (по умолчанию установлено значение 180 секунд).

Раздел ***Свойства сканирования***.

- ***Использовать эвристический анализ***. Установите этот флажок, чтобы включить метод эвристического анализа при сканировании.

- ***Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО***. Установите этот флажок, чтобы включить в отчет сведения о наличии потенциально нежелательных программ и шпионского ПО.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ***. 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, а также безвредные, но нежелательные программы (различные панели инструментов и т. п.). Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности и комфорта при работе, однако из-за него могут также блокироваться некоторые законные программы, поэтому по умолчанию параметр отключен. Примечание. Данная функция обнаружения является дополнением к предыдущему параметру, поэтому, чтобы обеспечить защиту от основных типов шпионского ПО, не снимайте флажок, установленный напротив предыдущего параметра.

- ***Сканировать объекты в архивах***. Установите этот флажок, чтобы выполнять проверку объектов в архивных файлах (zip, rar и т. д.).

Раздел ***Отчеты о вложениях эл. почты*** позволяет выбрать объекты, которые требуется указывать в отчетах во время сканирования. Конфигурацию по умолчанию можно легко изменить в разделе ***Действия по обнаружению***, часть ***Информация*** (см. ниже).

Доступны следующие параметры.

- ***Архивы, защищенные паролем.***

- ***Документы, защищенные паролем.***

- ***Файлы, содержащие макросы.***

- ***Скрытые расширения.***

Обычно все эти элементы представляют собой пользовательские расширения служб интерфейса приложений Microsoft VSAPI 2.0/2.5. Для получения подробной информации об интерфейсе VSAPI 2.0/2.5 воспользуйтесь следующими ссылками (а также ссылками на соответствующих страницах).

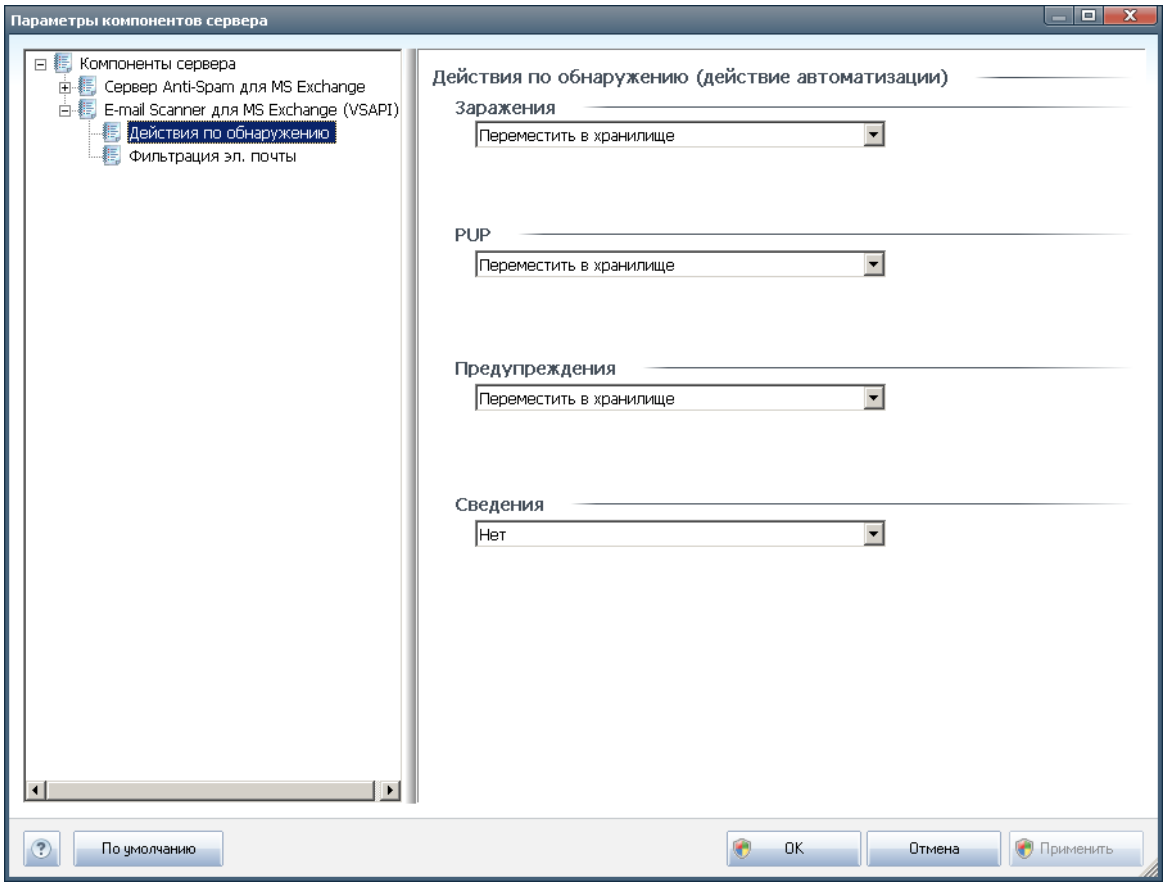
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - сведения о взаимодействии Exchange и антивирусного программного обеспечения.

- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 - сведения о дополнительных функциях VSAPI 2.5 сервера Exchange 2003.

Также в структуре дерева доступны следующие подэлементы.

- ***Действия по обнаружению.***
- ***Фильтрация электронной почты.***

## 5.3. Действия по обнаружению




В подэлементе ***Действия по обнаружению*** можно выбрать автоматические действия, которые необходимо выполнить при сканировании.

Доступны действия для следующих элементов.

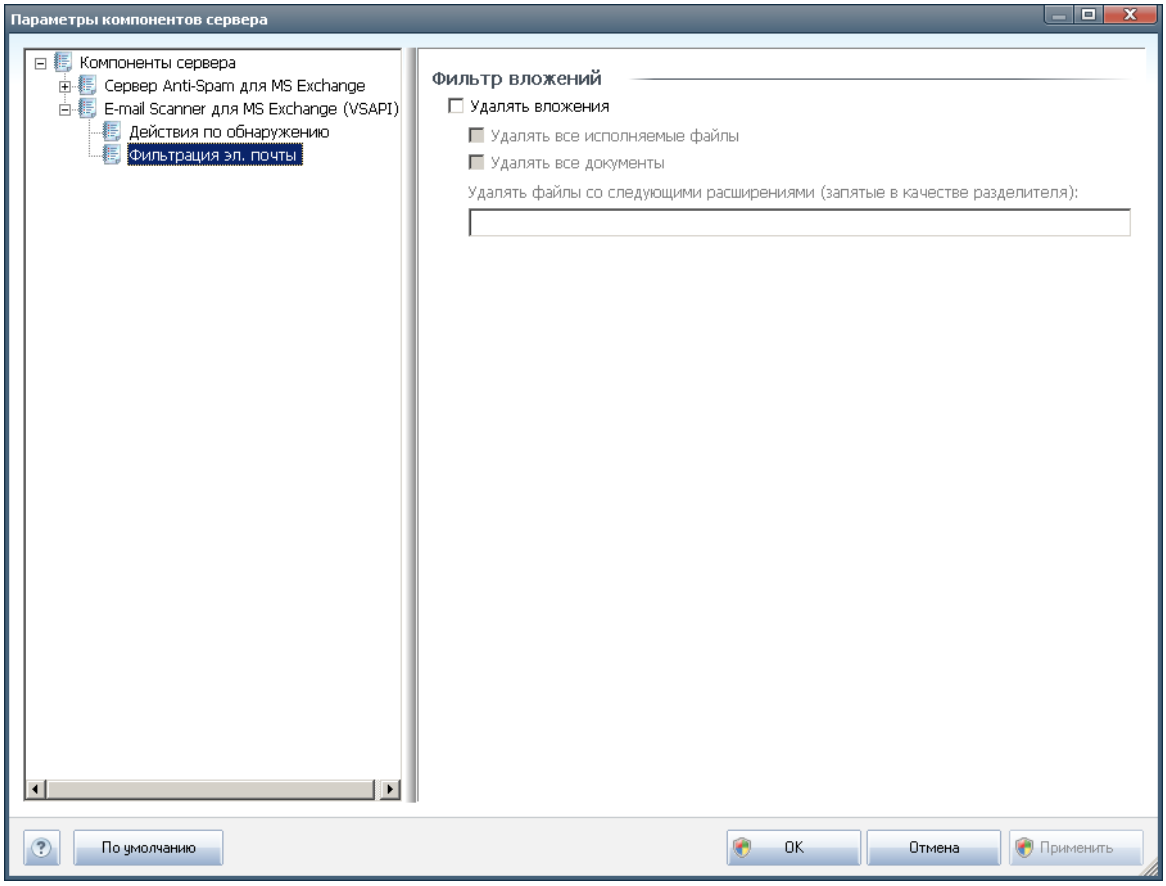
- ***Зараженные объекты.***
- ***Потенциально нежелательные программы (PUP).***

- ***Предупреждения.***
- ***Информация.***

Используйте раскрывающееся меню, чтобы выбрать действие для каждого элемента.

- ***Нет***. Никакое действие не будет выполняться.
- ***Переместить в хранилище***. Угроза будет перемещена в хранилище вирусов.
- ***Удалить***. Угроза будет удалена.

## 5.4. Фильтрация электронной почты




В элементе ***Фильтрация электронной почты*** при необходимости можно настроить автоматическое удаление вложений. Доступны следующие параметры.

- ***Удалять вложения***. Установите флажок, чтобы включить данную функцию.
- ***Удалять все исполняемые файлы***. Удаление всех исполняемых файлов.

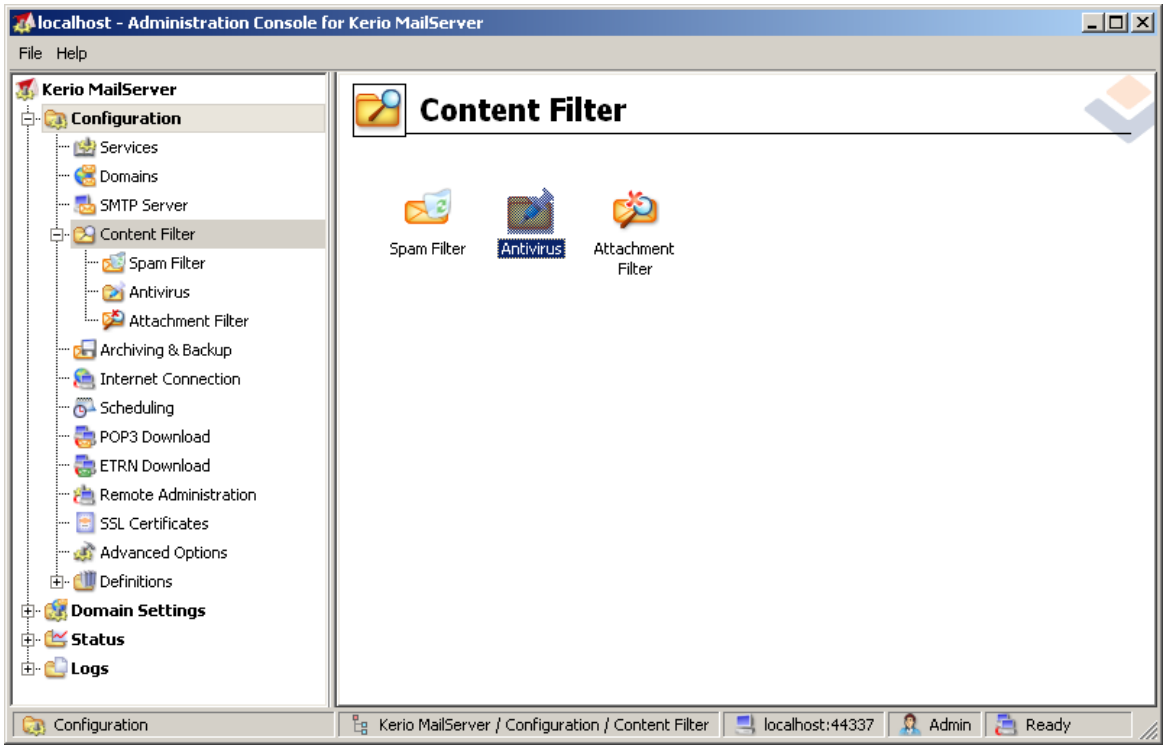
- ***Удалять все документы***. Удаление всех файлов документов.

- ***Удалять файлы с расширениями, разделенными запятыми***. Введите в поле расширения файлов, которые будут автоматически удаляться. Разделяйте расширения запятой.

# 6. AVG для почтового сервера Kerio

## 6.1. Конфигурация

Механизм защиты компонента Anti-Virus интегрирован непосредственно в почтовый сервер Kerio MailServer. Чтобы активировать защиту электронной почты почтового сервера Kerio, обеспечиваемую модулем сканирования AVG, запустите консоль администратора Kerio. В дереве управления, расположенном в левой части окна приложения, выберите подветвь Фильтр содержимого ветви Конфигурация.

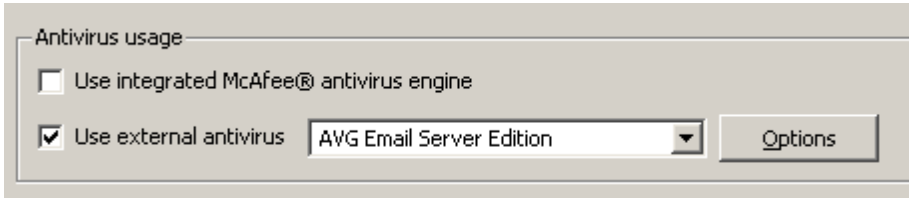



При щелчке элемента Фильтр содержимого отобразится диалоговое окно с тремя пунктами.

- ***Фильтр спама***
- ***Anti-Virus*** (см. раздел ***Anti-Virus***)
- ***Фильтр вложений*** (см. раздел ***Фильтр вложений***)

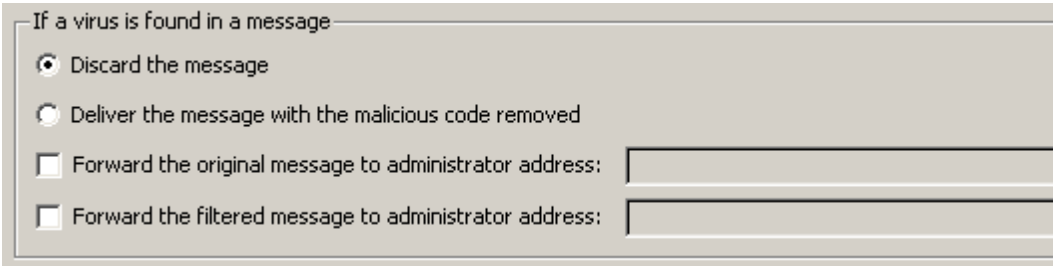
### 6.1.1. Антивирусное ПО

Чтобы активировать программу AVG для почтового сервера Kerio, установите флажок Использовать стороннее антивирусное ПО, и выберите в меню сторонних программ, доступном в блоке использования антивирусного ПО окна конфигурации, пункт AVG Email Server Edition.




В следующем разделе можно указать действия, которые должны предприниматься в отношении зараженных или отфильтрованных сообщений.

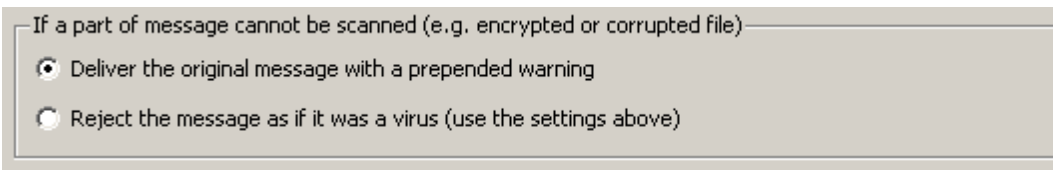
- ***Если в сообщении найден вирус***




В данном блоке указывается действие, которое будет выполняться при обнаружении вируса в сообщении, или если сообщение было отфильтровано фильтром вложений.

  - ***Удалить сообщение***. Если выбрано данное действие, зараженные или отфильтрованные сообщения будут удалены.
  - ***Доставить сообщение, но удалить вредоносный код***. Если выбрано данное действие, сообщение будет доставлено получателю без потенциально вредоносного вложения.
  - ***Переслать исходное сообщение на адрес администратора***. Если выбрано данное действие, зараженное сообщение будет перенаправлено на адрес, указанный в текстовом поле для адреса.
  - ***Переслать отфильтрованное сообщение на адрес администратора*** . Если выбрано данное действие, отфильтрованное сообщение будет перенаправлено на адрес, указанный в текстовом поле для адреса.

- ***Если не удалось сканировать сообщение полностью (например, файл зашифрован или поврежден)***



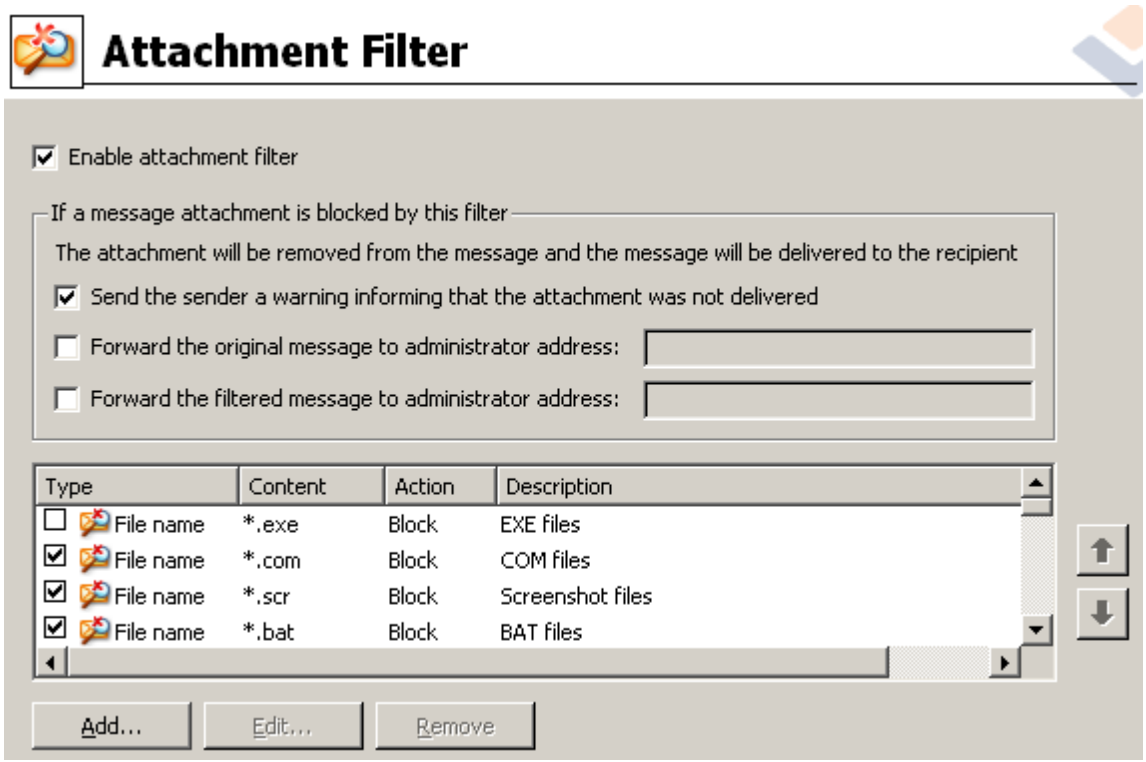

В данном блоке указывается действие, которое будет выполняться, если не удастся сканировать сообщение или вложение полностью.

- ***Доставить исходное сообщение с подготовленным предупреждением***. Если выбрано данное действие, сообщение (или вложение) будет доставлено без проверки. Пользователь будет предупрежден о возможном наличии вирусов в сообщении.

- ***Отклонить сообщение как вирус***. Если выбрано данное действие, система определит сообщение как вирус (т. е. сообщение будет отклонено или доставлено без вложения). Данное действие обеспечивает безопасность, однако отправка архивов, защищенных паролем, будет невозможна.

### 6.1.2. Фильтр вложений

В меню Фильтр вложений содержится список различных определений вложений.




Чтобы включить/отключить фильтрацию вложений почтовых сообщений, установите флажок Включить фильтр вложений. Дополнительно можно изменить следующие параметры.

- ***Уведомить отправителя об отсутствии вложения в сообщении***

  Отправитель получит предупреждение от почтового сервера Kerio об отправке сообщения с вирусом или заблокированным вложением.

- ***Переслать исходное сообщение на адрес администратора***

  Сообщение будет переадресовано (без изменений - с зараженным или

запрещенным вложением) на определенный адрес электронной почты независимо от того, является этот адрес локальным или внешним.

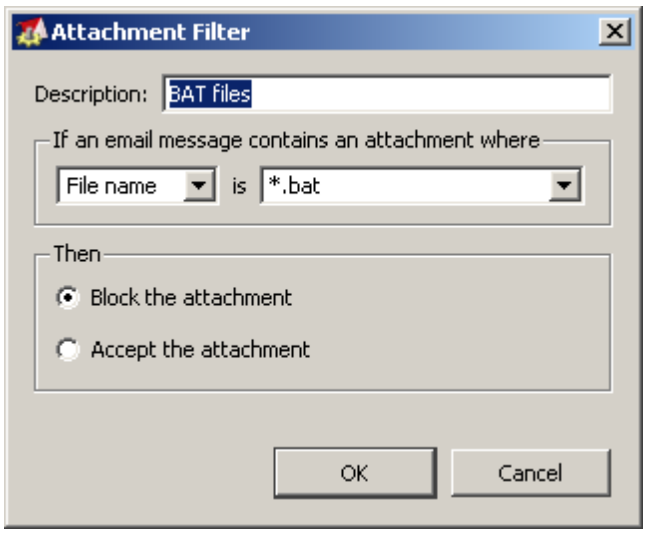
- ***Переслать отфильтрованное сообщение на адрес администратора***

  Сообщение без зараженного или запрещенного вложения будет (без учета действий, выбранных ниже) перенаправлено на указанный адрес электронной почты. Данное действие можно выполнить для проверки работоспособности антивирусного ПО и/или фильтра вложений.

В списке расширений каждый элемент имеет четыре поля.

- ***Тип***. Характеристика типа вложения, определенная расширением в поле Содержимое. Возможные варианты - Имя файла или тип MIME. В данном поле можно установить соответствующий флажок, чтобы включить/ исключить элемент из списка объектов фильтрации вложений.
- ***Содержимое***. Расширение для фильтрации. Для ввода можно использовать подстановочные знаки операционной системы (например, строка "*.doc.*" будет обозначать любой файл с расширением .doc, что также можно использовать и с другими расширениями).
- ***Действие***. Действие, которое будет выполняться в отношении определенного вложения. Возможные действия: Принять (принять вложение) и Блокировать (данное действие будет выполнено в соответствии со списком исключенных вложений).
- ***Описание***. Описание вложения.

Для удаления элемента из списка нажмите кнопку Удалить. Для добавления элемента в список нажмите кнопку ***Добавить...***. Чтобы изменить существующую запись, нажмите кнопку ***Изменить...***. Откроется следующее окно.




- В поле Описание можно указать краткое описание вложения для

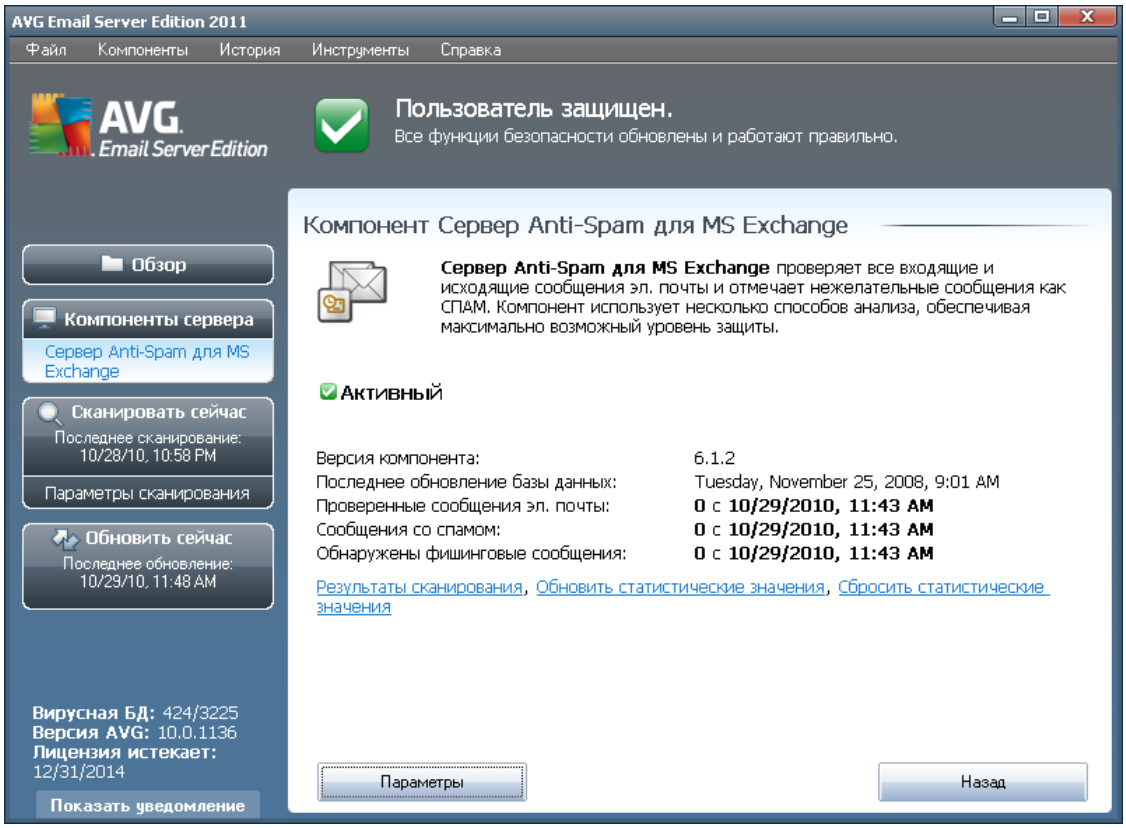
фильтрации.

- В поле Если сообщение электронной почты содержит вложение, в котором... можно выбрать тип вложения (Имя файла или тип MIME). Также можно выбрать определенное расширение в списке расширений или ввести расширение с подстановочным знаком.

В поле Дальше можно указать, требуется ли блокировать определенное вложение.

# 7. Конфигурация компонента Anti-Spam

## 7.1. Интерфейс Anti-Spam

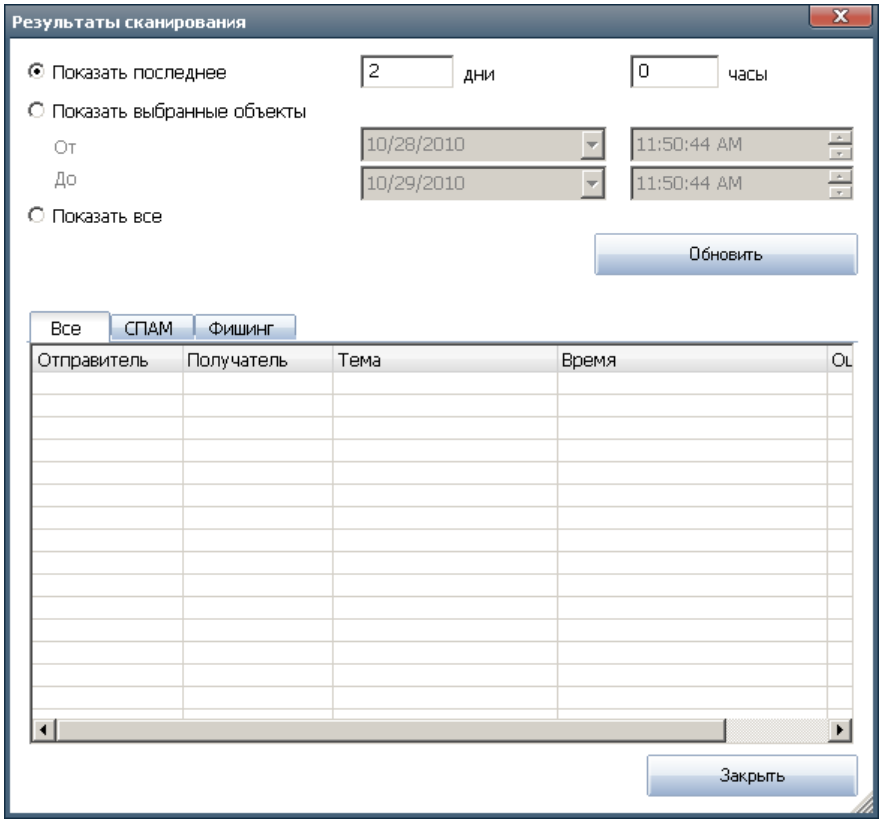



Диалоговое окно компонента сервера ***Anti-Spam***расположено в разделе ***Компоненты сервера*** (меню слева). В данном окне содержатся общие сведения о функциях компонента сервера, его текущем состоянии (*Севрер Anti-Spam для MS Exchange активен.*), а также некоторые статистические сведения.

Доступны следующие ссылки.

- ***Результаты сканирования***

  Открытие нового диалогового окна, в котором можно просмотреть результаты сканирования, выполненного компонентом Anti-Spam.




В этом окне можно просмотреть сообщения, определенные как спам (нежелательная почта) или средства фишинга (предназначены для кражи персональных данных, сведений о банковских счетах и т. п.). По умолчанию отображаются результаты сканирования за последние два дня. Период отображаемых сообщений можно изменить с помощью следующих параметров.

- ***Показать последние***. Вставка необходимых значений дней и часов.
- ***Показать выбранное***. Выбор интервала времени и даты.
- ***Показать все***. Отображение результатов за весь период времени.

Чтобы обновить результаты, нажмите кнопку ***Обновить***.

- ***Обновить статистические данные***. Обновление статистических данных, отображенных выше.
- ***Сбросить статистические данные***. Сброс статистических данных.

Доступны следующие кнопки.

- ***Параметры***. Позволяет открыть окно Параметры Anti-Spam.
- ***Назад***. Нажмите эту кнопку, чтобы вернуться к окну обзора компонентов

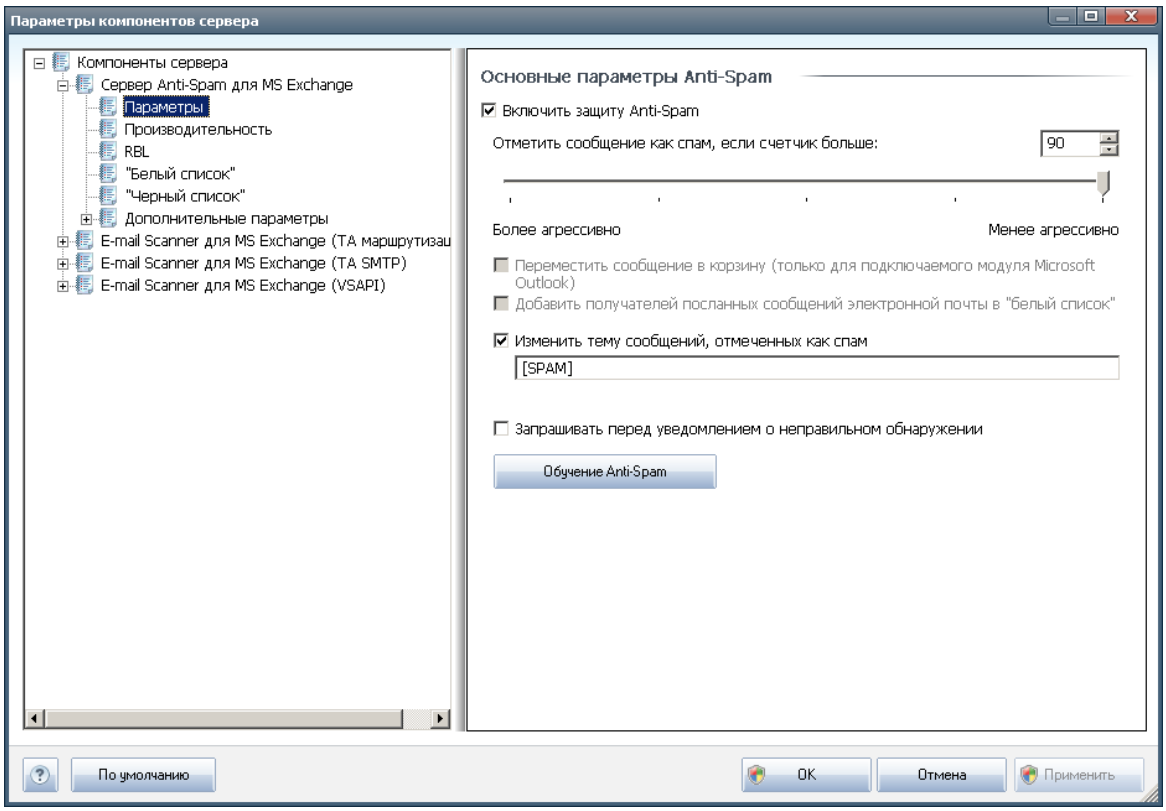
сервера.

## 7.2. Принципы работы Anti-Spam

Спам обозначает незапрашиваемые сообщения электронной почты, в частности рекламные рассылки о продуктах и услугах, которые массово рассылаются на большое количество адресов электронной почты одновременно, заполняя почтовые ящики получателей. Спам не является законной коммерческой рассылкой, на которую пользователи давали свое согласие. Спам не только досаждает, но также может содержать вирусы, сообщения оскорбительного характера или быть инструментом мошенников.

Компонент ***Anti-Spam*** проверяет все входящие сообщения электронной почты и помечает нежелательные сообщения электронной почты как СПАМ. Данный компонент использует несколько способов анализа для обработки каждого сообщения электронной почты, обеспечивая максимальную защиту от спама.

## 7.3. Параметры Anti-Spam




В диалоговом окне ***Основные параметры Anti-Spam*** можно установить флажок ***Включить защиту Anti-Spam***, чтобы разрешить/запретить компоненту Anti-Spam сканирование сообщений электронной почты.

В данном диалоговом окне также можно выбрать степень точности определения

рейтинга. Фильтр ***Anti-Spam*** определяет рейтинг каждого сообщения (*то есть насколько содержимое сообщения соответствует критериям СПАМА*) на основе нескольких способов динамического сканирования. Для настройки параметра ***Пометить сообщение как спам, если его рейтинг превышает или равен*** введите необходимо значение (*от 50 до 90*) или переместите ползунок влево или вправо.

Ниже представлен общий обзор пороговых значений рейтинга.

- ***Значение 90***. Будет доставлено большинство сообщений электронной почты (сообщения не будут помечены как спам). Будет производиться фильтрация спама, который легче всего обнаружить, однако значительное количество спама будет продолжать поступать в почтовый ящик.

- ***Значения в диапазоне 80-89***. Будет производиться фильтрация сообщений электронной почты, которые возможно являются спамом. Некоторые сообщения, которые не являются спамом, могут быть неверно помечены как спам.

- ***Значения в диапазоне 60–79***. Значения в данном диапазоне обеспечивают довольно высокий уровень защиты. Будет производиться фильтрация сообщений электронной почты, которые скорее всего являются спамом. Сообщения, которые не являются спамом, могут быть определены как спам.

- ***Значения в диапазоне 50–59***. Значения в данном диапазоне обеспечивают очень высокую степень защиты. Сообщения, которые не являются спамом, могут быть определены как настоящий спам. Обычно не рекомендуется использовать пороговые значения из данного диапазона.

Затем можно определить действия, предпринимаемые в отношении обнаруженных нежелательных сообщений электронной почты (спама).

- ***Изменить тему сообщений, отмеченных как спам***. Установите данный флажок, если необходимо, чтобы все сообщения, определенные как спам, были отмечены специальным словом или символом в поле темы сообщения. Необходимый текст можно ввести в активированном текстовое поле.

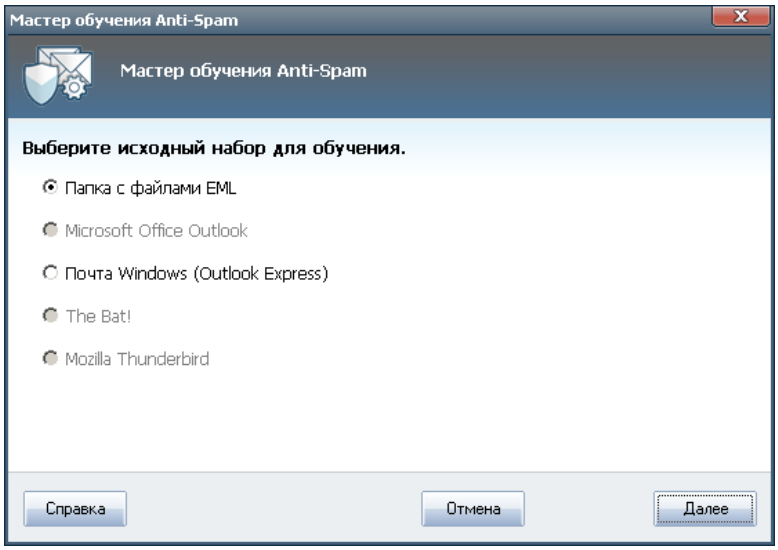
- ***Запрашивать перед уведомлением о неправильном обнаружении***. Данный флажок можно установить, если в процессе установки вы согласились участвовать в программе улучшения продуктов, т. е. разрешили отправку сведений об обнаруженных угрозах в компанию AVG. Благодаря данной программе мы можем собирать актуальные сведения о последних угрозах от пользователей по всему миру и таким образом улучшать защиту каждого пользователя. Отправка отчетов осуществляется автоматически. Однако в случае установки данного флажка перед отправкой отчетов об обнаруженном спаме в компанию AVG вы будете получать запрос, позволяющий подтвердить, что сообщение, о котором вы сообщаете, действительно является спамом.

  ***Примечание.*** *Данный параметр не применим для AVG Email Server Edition 2011.*

Кнопка ***Обучение Anti-Spam*** позволяет открыть ***Мастер обучения Anti-Spam***, подробно описанный в следующей главе.

### 7.3.1. Мастер обучения Anti-Spam

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




Необходимо выбрать один из приведенных ниже вариантов.

- ***Определенный клиент электронной почты***. Если используется один из указанных клиентов электронной почты (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), выберите соответствующие параметр.

- ***Папка с файлами EML*** - при использовании другой почтовой программы сначала необходимо сохранить сообщения в специальной папке (в формате *eml*) или узнать точное расположение папки с сообщениями используемого клиента электронной почты. Затем необходимо выбрать пункт ***Папка с файлами EML***, чтобы на следующем шаге указать необходимую папку

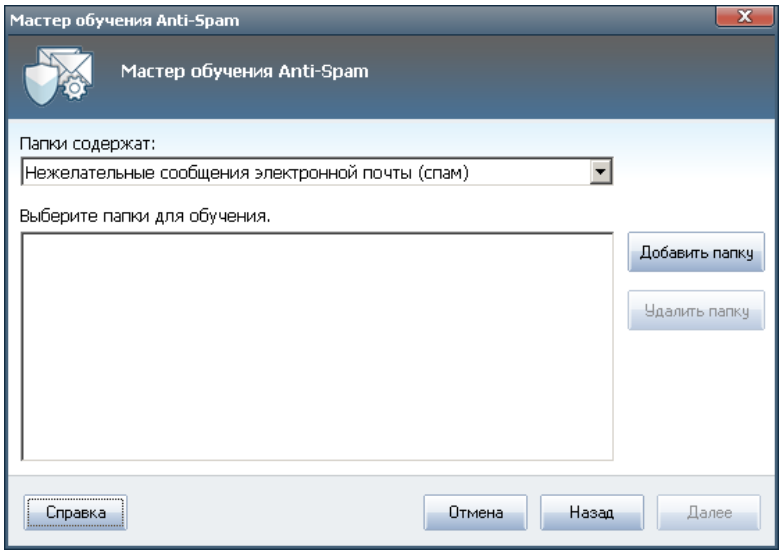
Чтобы упростить и ускорить процесс обучения, можно заранее отсортировать сообщения электронной почты в папке так, чтобы папка, которая используется для обучения, содержала только учебные сообщения (желательные или нежелательные). Однако в этом нет необходимости, так как данный мастер позволяет выполнить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

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

### 7.3.2. Выбор папки с сообщениями

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

#### Папки с файлами EML



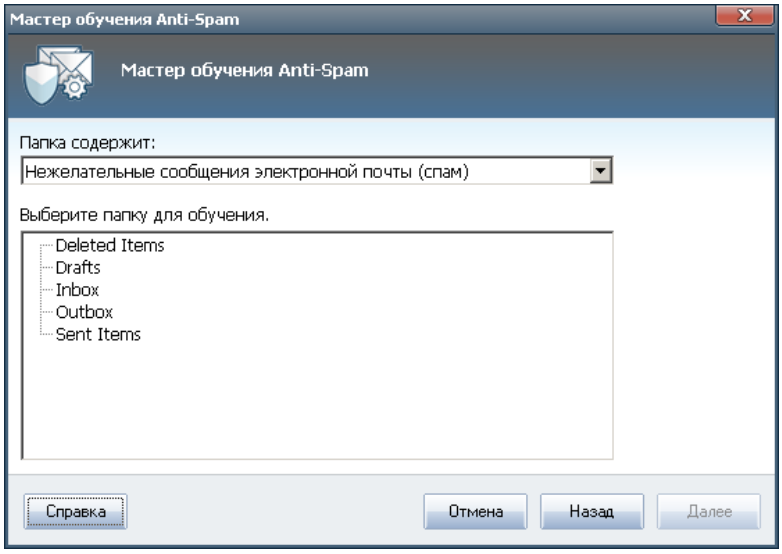

В данном диалоговом окне нужно указать папку с сообщениями, которые необходимо использовать для обучения. Нажмите ***Добавить папку***, чтобы указать местоположение папки с файлами .eml (*сохраненные сообщения электронной почты*). Выбранная папка будет отображена в диалоговом окне.

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

По завершении щелкните ***Далее*** и перейдите к ***параметрам фильтрации сообщений***.

#### Определенный клиент электронной почты

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

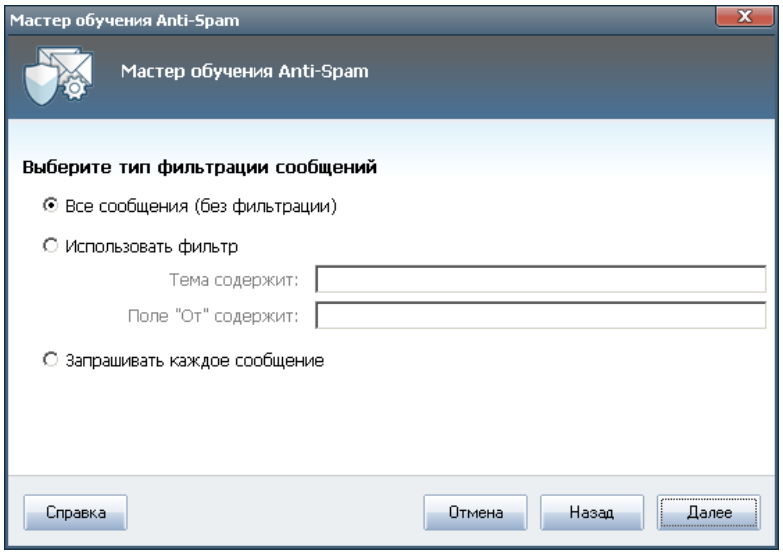



***Примечание.*** *При использование Microsoft Office Outlook будет предложено сначала выбрать профиль MS Office Outlook.*

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

По завершении щелкните ***Далее*** и перейдите к ***параметрам фильтрации сообщений***.

### 7.3.3. Параметры фильтрации сообщений




В данном окне можно настроить фильтрацию сообщений электронной почты.

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

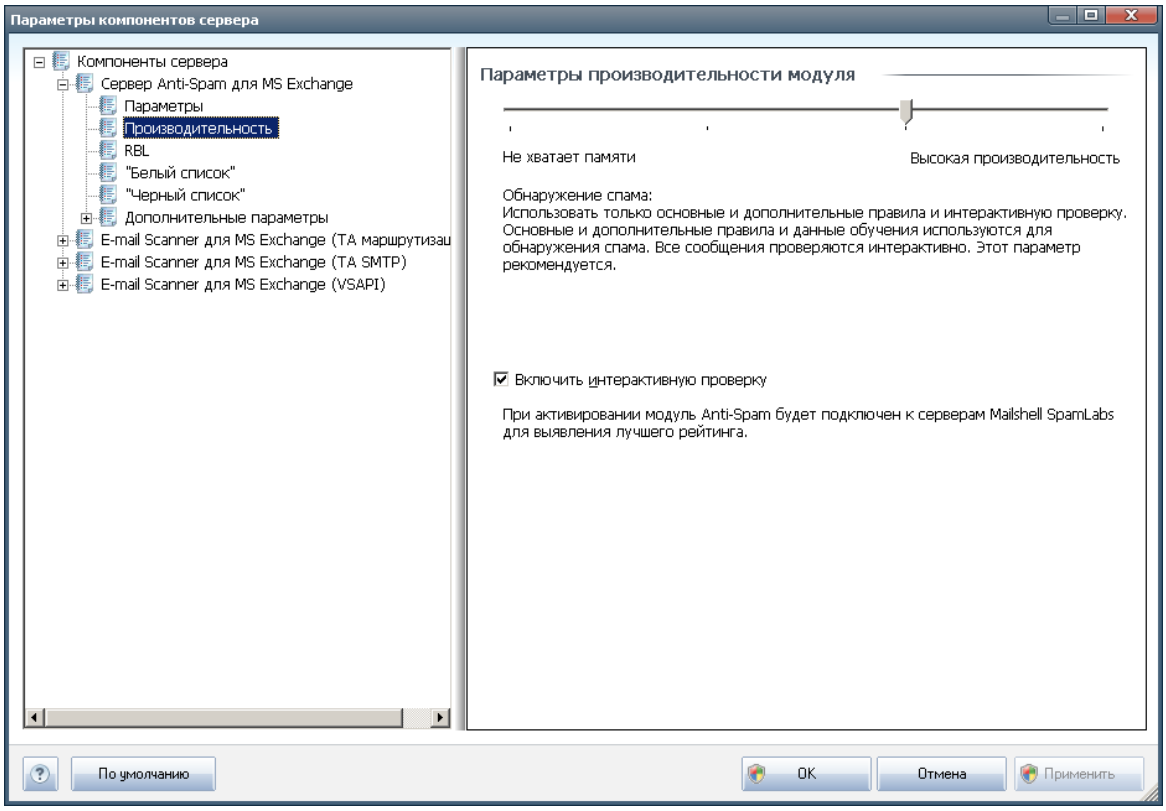
Если сообщения, находящиеся в папке, неизвестны и необходимо, чтобы мастер отображал запрос о каждом отдельном сообщении (чтобы определить, использовать его для обучения или нет), выберите параметр ***Запрашивать каждое сообщение***.

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

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

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

## 7.4. Производительность




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

- ***Малая загрузка памяти***. В процессе сканирования будет определяться только спам, правила использоваться не будут. Для определения будут использоваться только данные обучения. Данный режим рекомендуется использовать только на компьютерах с действительно низкой конфигурацией.

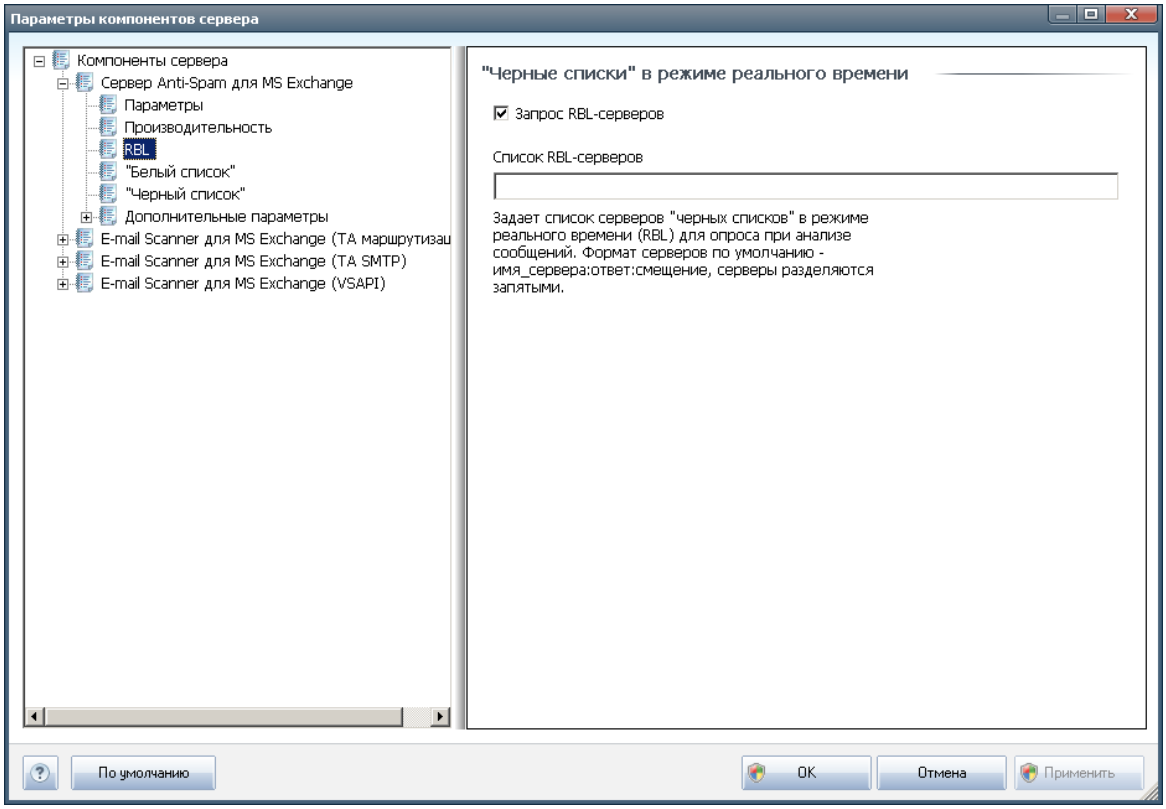
- ***Высокая производительность***. При работе в данном режиме программа использует большой объем памяти компьютера. Для определения спама при сканировании будут использоваться следующие функции: правила и кэш базы данных спама, основные и дополнительные правила, IP-адреса и базы данных распространителей спама.

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

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

## 7.5. RBL

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




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

Сервер RBL (*"черный список" в режиме реального времени*) - это сервер DNS с расширенной базой данных известных отправителей спама. Если данная функция включена, все сообщения электронной почты будут при проверке сопоставлены с базой данных сервера RBL и отмечены как спам в случае совпадения с одной из записей в базе данных.

Базы данных серверов RBL содержат наиболее свежие идентификационные отметки спама, благодаря чему обеспечивается наилучшее и наиболее точное обнаружение спама. Данная функция будет особенно полезна пользователям, получающим большое количество спама, который не распознается правильно модулем Anti-Spam.

***Список серверов RBL*** позволяет указать местоположения серверов RBL. По

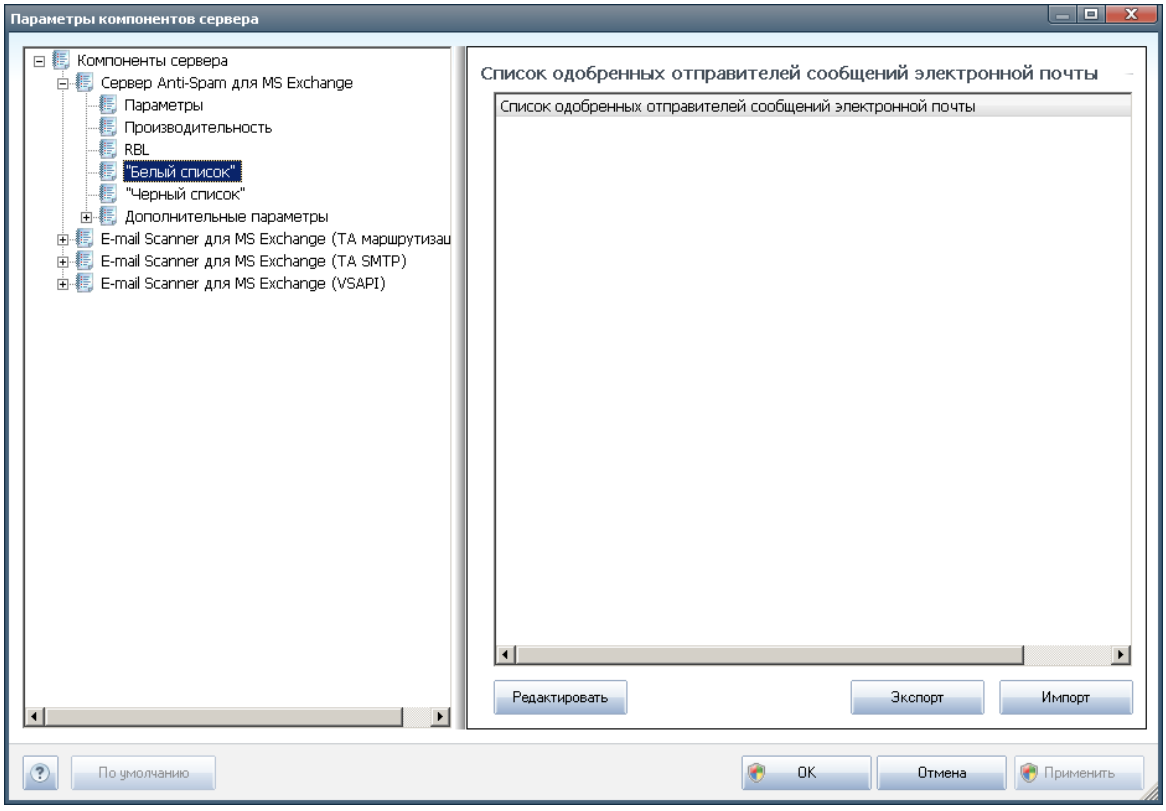
умолчанию указано два адреса серверов RBL. Рекомендуется использовать значение по умолчанию. Изменять значение следует только опытным пользователям (если это действительно необходимо).

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

***Отправка личных данных на сервер не выполняется.***

## 7.6. Белый список

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




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

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

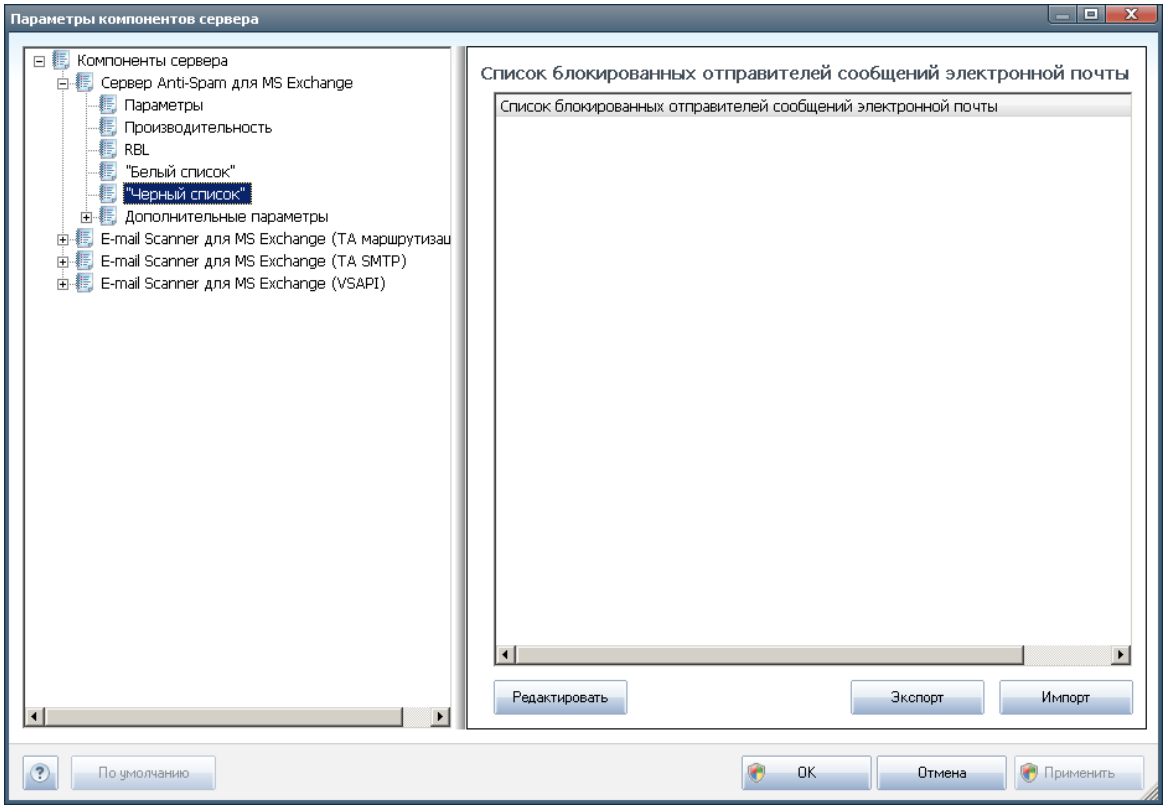
- ***Редактировать***. *При нажатии этой кнопки откроется диалоговое окно, в котором можно вручную ввести список адресов (также можно использовать способ "копировать/вставить"*). Можно вставлять только один элемент (отправитель, имя домена) в каждую строку.

- ***Импорт***. Нажмите данную кнопку, чтобы импортировать существующие адреса эл. почты. Файл ввода может быть текстовым файлом (в формате простого текста с одним элементом содержимого в строке - адрес, имя домена) или файлом WAB. Также можно выполнить импорт из адресной книги Windows или приложения Microsoft Office Outlook.

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

## 7.7. Черный список

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




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

будут расцениваться как спам.

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

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

- ***Импорт***. Нажмите данную кнопку, чтобы импортировать существующие адреса эл. почты. Файл ввода может быть текстовым файлом (в формате простого текста с одним элементом содержимого в строке - адрес, имя домена) или файлом WAB. Также можно выполнить импорт из адресной книги Windows или приложения Microsoft Office Outlook.

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

## 7.8. Дополнительные параметры

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

Чтобы изменить дополнительные параметры компонента Anti-Spam, следуйте инструкциям, приведенным непосредственно в интерфейсе пользователя. В каждом диалоговом окне указана одна определенная функция, которую можно редактировать. Описание функции приведено в диалоговом окне.

- ***Кэш***. Отпечаток, репутация домена, LegitRepute.

- ***Обучение***. Максимальное количества слов, порог автоматического обучения, вес.

- ***Фильтрация***. Список языков, список стран, одобренные IP-адреса, блокируемые IP-адреса, блокируемые страны, блокируемые кодировки, ложные отправители.

- ***RBL***. Серверы RBL, множественные совпадения, порог, время ожидания, максимальное количество IP-адресов.

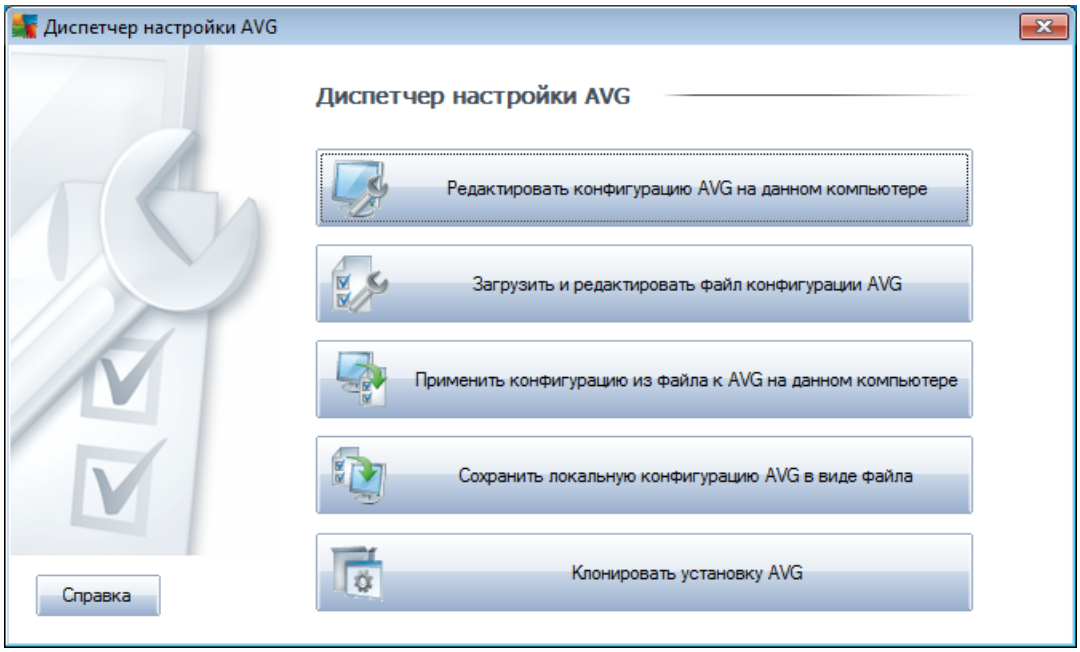
- ***Подключение к Интернету***. Время ожидания, прокси-сервер, проверка подлинности прокси-сервера.

# 8. Диспетчер параметров AVG

***Диспетчер параметров AVG*** - это инструмент, предназначенный в основном для небольших сетей и позволяющий копировать, редактировать и распределять конфигурацию AVG. Конфигурацию можно сохранить на портативном устройстве (флэш-накопитель USB и т. п.), а затем применить вручную к выбранным станциям.

Данный инструмент включен в пакет установки программы AVG и доступен для запуска в меню Пуск ОС Windows:

***Все программы/AVG 2011/Диспетчер параметров AVG***




- ***Изменить конфигурацию AVG на данном компьютере***

  Данная кнопка позволяет открыть диалоговое окно, содержащие расширенные параметры локальной версии программы AVG. Все произведенные в нем изменения будут применены к локальной версии программы AVG.

- ***Загрузить и изменить файл конфигурации AVG***

  Нажмите данную кнопку для редактирования файла конфигурации AVG (.pck) при его наличии. После подтверждения изменений нажмите кнопку ***OK*** или ***Применить***, и файл будет заменен файлом с новыми параметрами.

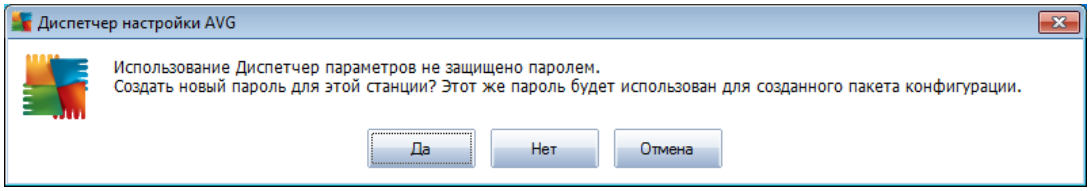
- ***Применить конфигурацию из файла к программе AVG на данном компьютере***

  Данная кнопка позволяет открыть файл конфигурации AVG (.pck) и

применить содержащуюся в нем конфигурацию к локальной версии программы AVG.

- ***Сохранить конфигурацию локальной версии AVG в файл***

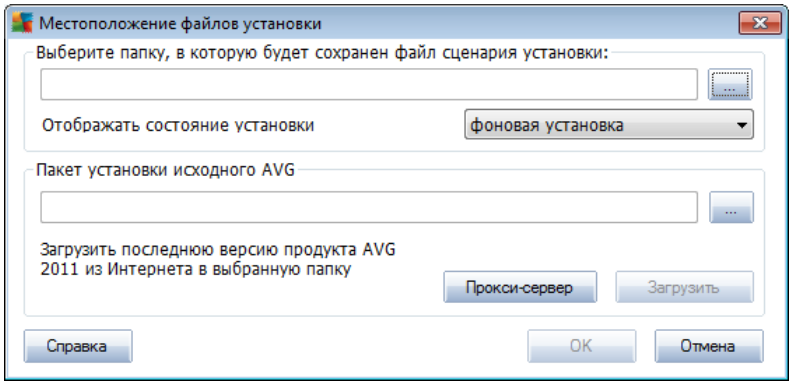
  Данная кнопка позволяет сохранить файл конфигурации локальной версии программы AVG (.pck). Если для разрешенных действий не установлен пароль, может отобразиться следующее диалоговое окно.




  Выберите ответ ***Да***, чтобы установить пароль для доступа разрешенных элементов, а затем указать необходимые сведения и подтвердить выбор. Выберите ответ ***Нет***, чтобы отказаться от создания пароля и перейти к сохранению конфигурации локальной версии программы AVG в файл.

- ***Клонировать установку AVG***

  Данный параметр позволяет создать точную копию локальной установки программы AVG путем создания пакета установки с пользовательскими параметрами. Выберите папку, в которую будет сохранен сценарий установки, чтобы продолжить.




  Затем в раскрывающемся меню выберите один из следующих параметров.

  - ***Фоновая установка***. Во время процесса установки информация отображаться не будет.
  - ***Показывать только состояние процесса установки***. Для установки не потребуется участие пользователя, однако он сможет следить за состоянием процесса установки.
  - ***Показывать мастер установки***. Будут отображены все шаги установки, участие пользователя необходимо для подтверждения

шагов.

Нажмите кнопку ***Загрузить***, чтобы загрузить последнюю версию пакета установки AVG с веб-сайта AVG в выбранную папку, или поместите пакет установки программы AVG в эту папку вручную.

Нажмите кнопку ***Прокси-сервер***, чтобы определить параметры прокси-сервера, если это требуется для успешного сетевого подключения.

При нажатии кнопки ***OK*** начнется процесс клонирования. Процесс не займет много времени. Также может отобразиться диалоговое окно с запросом на создание пароля для разрешенных элементов (см. выше). По завершении процесса клонирования в выбранной папке появится файл ***AvgSetup.bat***, а также другие файлы установки. Если запустить файл ***AvgSetup.bat***, будет выполнена установка программы AVG в соответствии с описанными выше параметрами.

# 9. Часто задаваемые вопросы и техническая поддержка

При возникновении каких-либо проблем с продуктом AVG, делового или технического характера, см. раздел веб-сайта AVG ***Часто задаваемые вопросы***, который находится по адресу: http://www.avg.com.

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