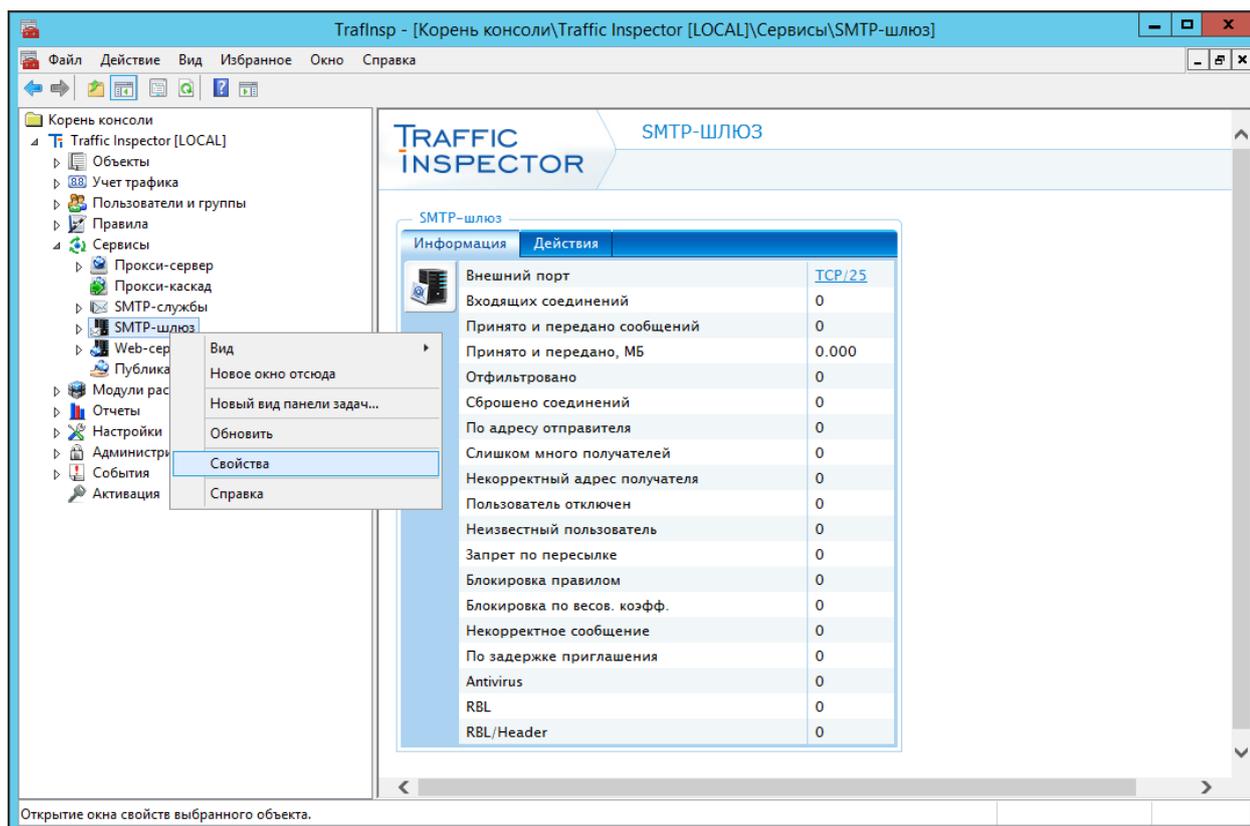


# НАСТРОЙКА ПОЧТОВОГО ШЛЮЗА TRAFFIC INSPECTOR

SMTP-шлюз используется в том случае, если в сети имеется свой почтовый сервер. Совместно со службой отправки сообщений он применяется для приема входящей почты снаружи с целью ее фильтрации и тарификации. Если почтовый сервер находится внутри сети, то использование SMTP-шлюза заменяет задачу наружной публикации SMTP-сервера.

## 1. Настройка SMTP-шлюза

1.1 Откройте окно свойств **SMTP-шлюза**. Сделать это можно из блока **SMTP-шлюз** в одноименном разделе консоли администратора.



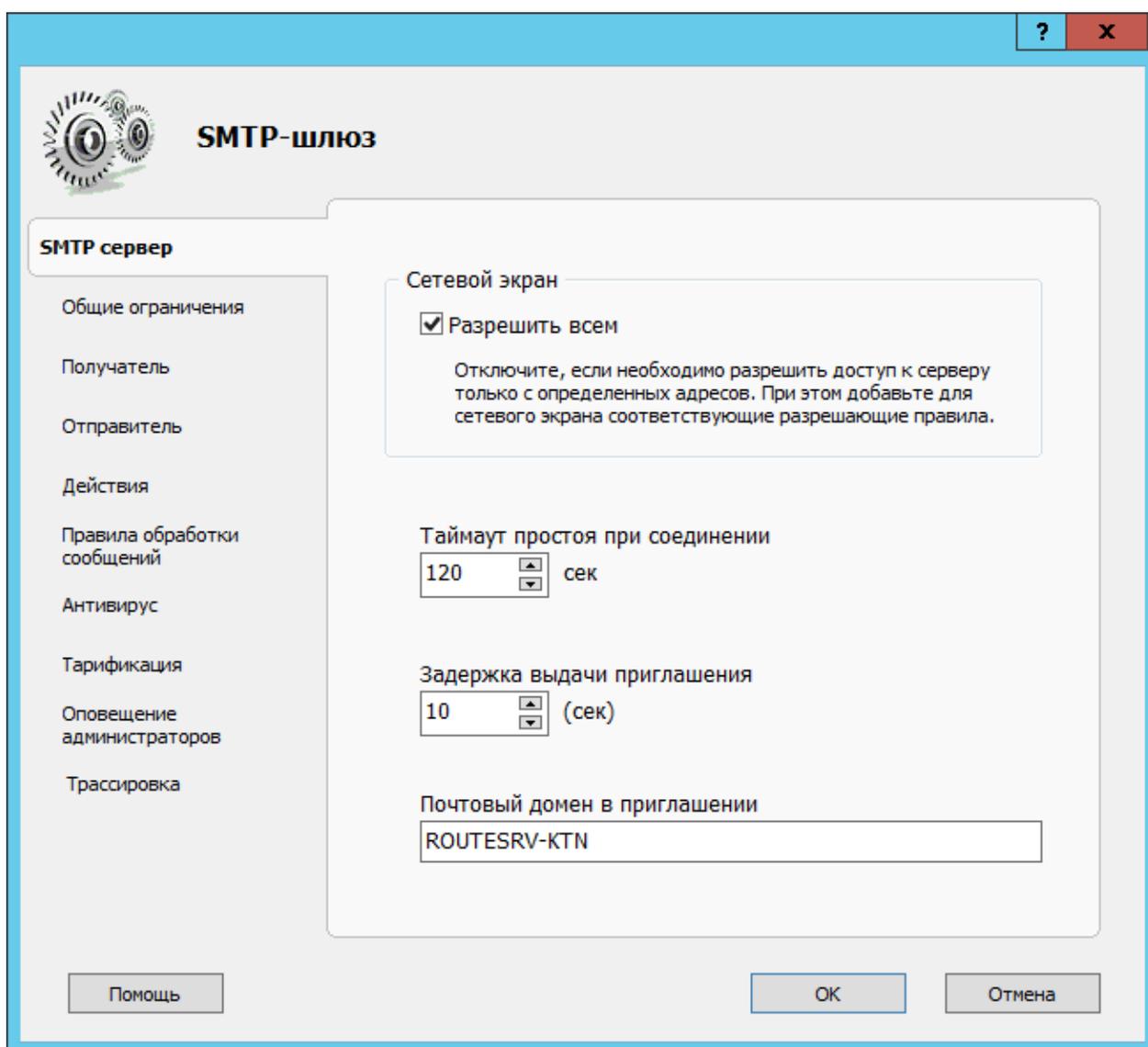
1.2 На вкладке **«SMTP сервер»** включите или выключите доступ на порт сервера (порт задается в конфигураторе при включении **«SMTP-шлюза»**).

Здесь же задайте таймаут соединения, то есть время простоя, при котором входящее TCP-соединение будет закрыто (по умолчанию 120 секунд). Также можно настроить задержку выдачи приглашения. Это мера, обеспечивающая дополнительную фильтрацию спама. Приглашение SMTP-сервера отправляет не сразу, а через указанное количество секунд (по

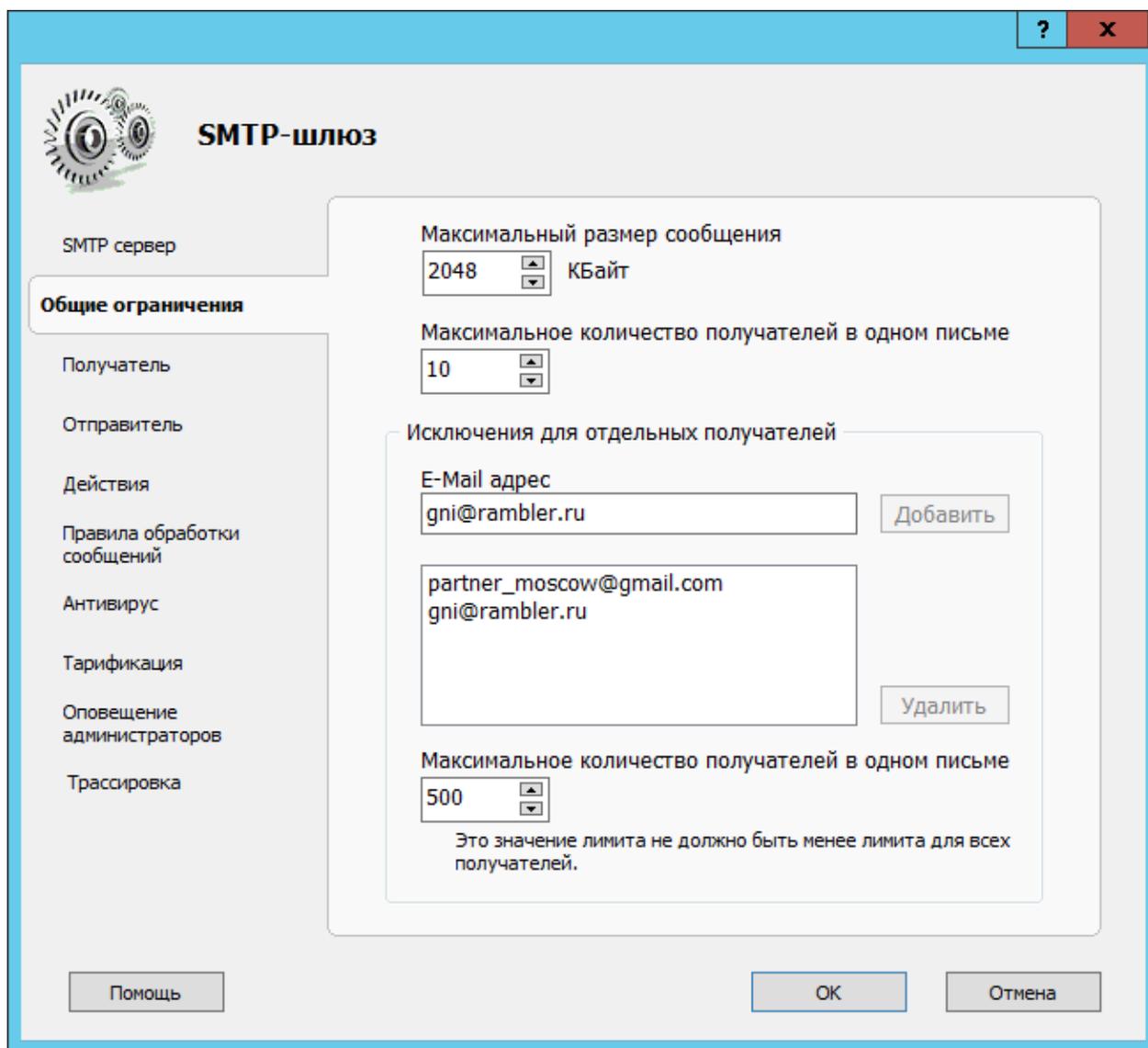
умолчанию 10 секунд) после установления TCP-соединения с отправителем. Если же отправитель начал отправку сообщения, не дожидаясь получения приглашения, то такое соединение будет прервано. Для отключения этой функции задайте задержку, равную 0.

На этой же вкладке пропишите имя домена (или доменное имя хоста), которое будет использоваться в ответе на команды HELO и EHLO. По умолчанию Traffic Inspector подставляет имя сервера

В первом случае будет автоматически создано правило, разрешающее трафик на данный порт с любых внешних сетей. Во втором случае необходимо будет вручную создать одно или несколько разрешающих правил сетевого экрана, которые разрешат трафик только с определенных IP-адресов или IP-сетей (подробнее о правила сетевого экрана см. в п. Правила внешнего сетевого экрана). Доступ с других адресов будет заблокирован.

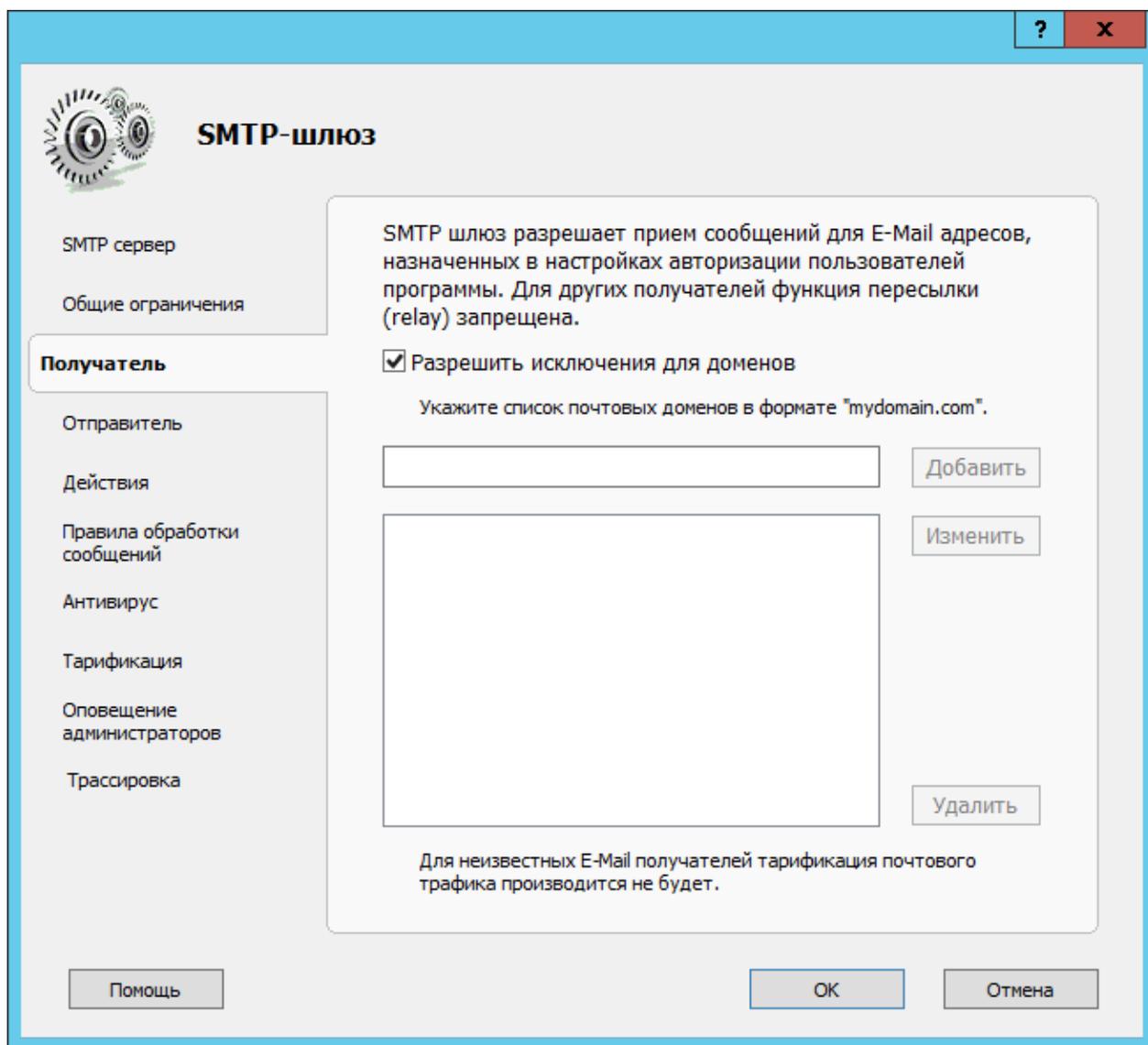


1.3 На вкладке **«Общие ограничения»** задайте максимально возможный размер сообщений в килобайтах (по умолчанию 2048) и максимально возможное число получателей в одном письме (по умолчанию 50). При необходимости создайте список исключений – адресов электронной почты получателей, для которых перечисленные выше ограничения не будут действовать. Также можно отдельно указать максимальное количество получателей в одном письме, которое будет действовать на все письма без исключений (по умолчанию 500). Данные ограничения позволяют предотвратить получение различных нежелательных сообщений – спама, рассылок вредоносного программного обеспечения и пр.

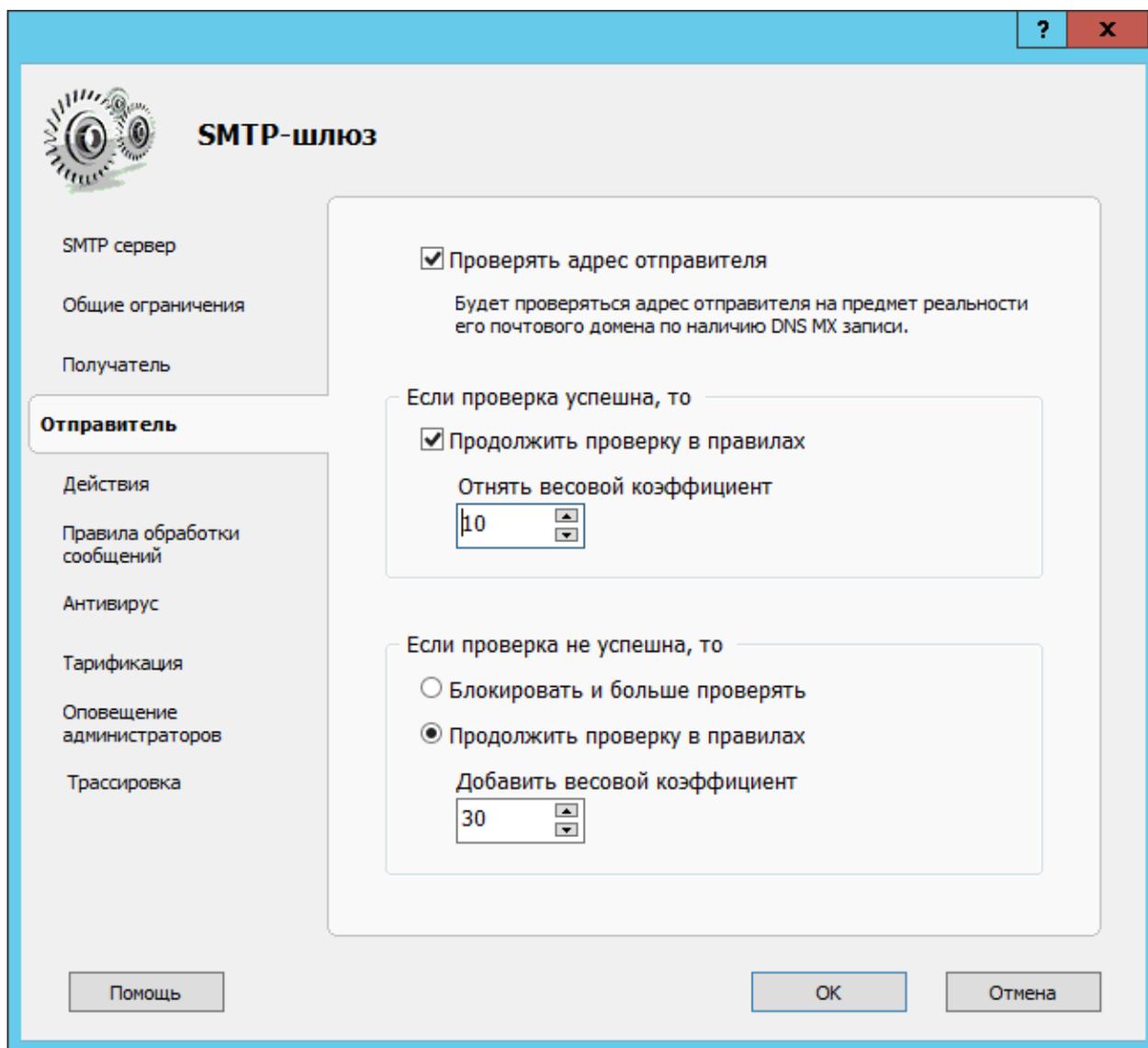


1.4 По умолчанию «SMTP-шлюз» принимает сообщения только для тех адресов, которые прописаны в настройках авторизации пользователей программы, а все остальные сообщения блокируются. При этом весь почтовый трафик будет соотнесен конкретным пользователем и учтен в биллинге. Если в сообщении несколько получателей, то каждый получатель будет обрабатываться отдельно. Если прием на адрес какого-либо отдельного получателя запрещен, то он будет исключен из списка получателей сообщения. Если исключаются все получатели, то сообщение фильтруется.

При необходимости можно указать домены, на который будет возможен прием почты независимо от того, прописан адрес получателя в программе или нет. В этом случае почтовый трафик будет учитываться только для тех сообщений, адрес получателей которых имеется у пользователей программы. Для настройки этой функции сформируйте список почтовых доменов (в формате domain.com) на вкладке «Получатель».



1.5 При необходимости на вкладке **«Отправитель»** включите проверку сообщений по отправителю. Под проверкой подразумевается проверка реальности почтового домена отправителя на предмет наличия у него DNS MX-записи. При включении настройте действия, которые будет выполнять Traffic Inspector по результатам обработки письмами, которые прошли и не прошли проверку. Для успешных сообщений включите или выключите дальнейшую обработку сообщения правилами и, при необходимости, укажите число, на которое будет уменьшен их рейтинг. Для не прошедших проверку писем включите их блокировку или укажите число, на которое будет увеличен их рейтинг.



1.6 На вкладке «**Действия**» укажите **рейтинг**, при котором сообщение будет признано нежелательным и заблокировано (рейтинг сообщения вычисляется в ходе его обработки SMTP-шлюзом и дополнительными модулями, в ходе которых он может как увеличиваться, так и уменьшаться), а также задайте код и текст отклика отправителю (по умолчанию используется код 554 и текст **Access denied**). Изменение кода на другой может изменить характер поведения отправителя почты при срабатывании блокировки.

Здесь же, при необходимости, задайте действия, которые будет выполнять «SMTP-шлюз» с сообщениями, рейтинг которых больше указанного значения. Это могут быть следующие действия:

Добавление к письмам произвольных заголовков. При создании заголовков можно использовать параметр подстановки %WEIGH% (весовой коэффициент на момент пометки сообщения).

Перенаправление на указанный адрес. Следует учесть, что это сообщение будет отправляться обычным порядком через ту же службу отправки сообщений, поэтому адрес должен нормально восприниматься SMTP-сервером организации. Авторизация для этого адреса в программе не требуется, тарифицироваться данная почта будет для тех получателей, на чей адрес она пришла. При редиректе тема сообщения заменяется на список адресов получателей.

Изменение темы сообщения согласно указанному шаблону. В шаблоне можно использоваться следующие параметры подстановки:

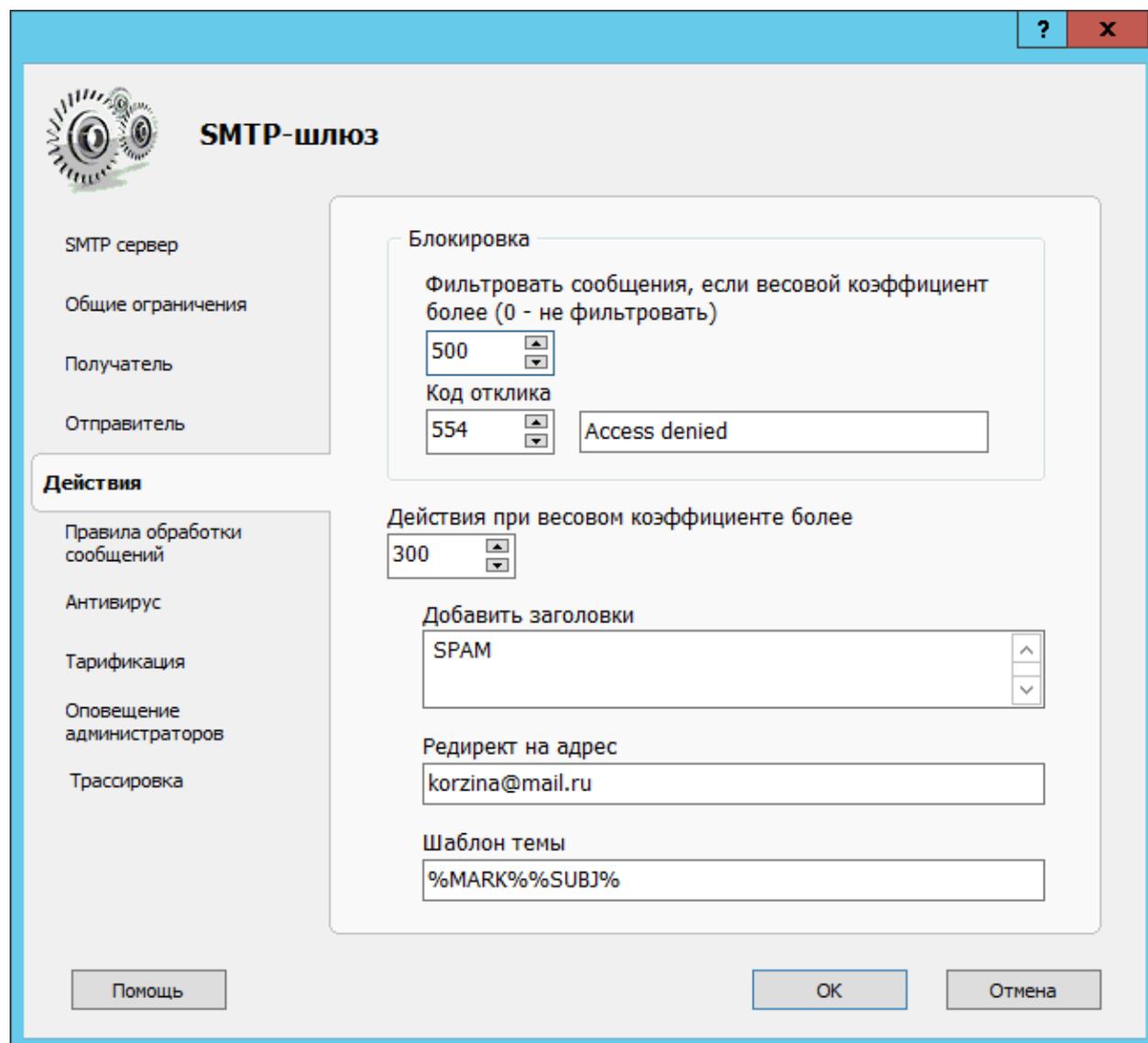
%WEIGHT% – весовой коэффициент на момент пометки сообщения.

%MARK% – ранее сформированная пометка темы другим правилом.

%SUBJ% – исходная тема сообщения.

Редирект же можно использовать для пересылки всех потенциально нежелательных сообщений в почтовый ящик – "отстойник".

В нашем примере при значении весового коэффициента больше 300 в заголовок писем будет добавляться слово SPAM и они будут отправляться на почтовый ящик korzina@mail.ru, при значении весового коэффициента более 500 письма будут блокироваться.

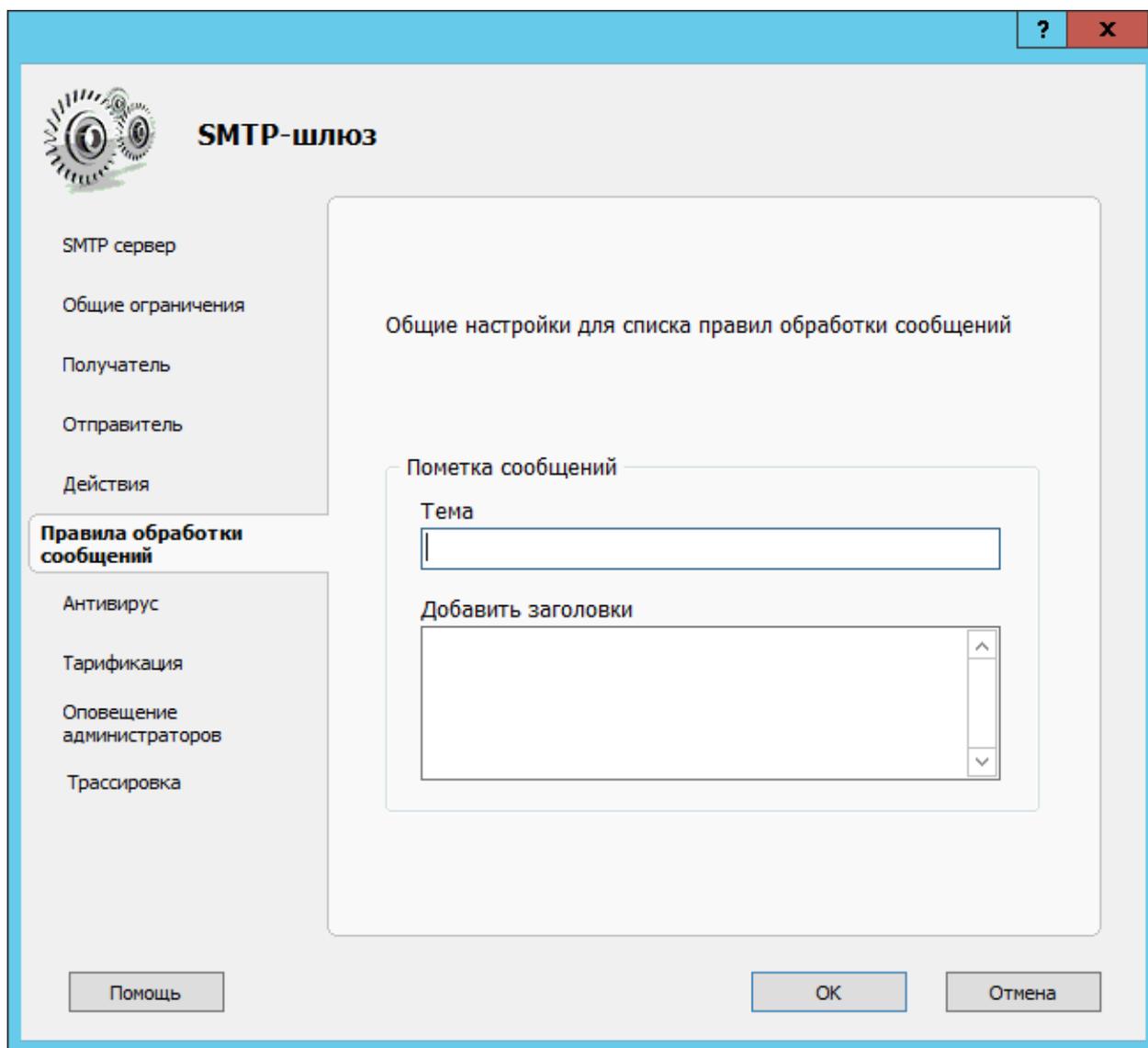


The screenshot shows the "SMTP-шлюз" (SMTP Gateway) configuration window. The window has a blue title bar with a question mark and a close button. On the left, there is a sidebar with a gear icon and several menu items: "SMTP сервер", "Общие ограничения", "Получатель", "Отправитель", "Действия", "Правила обработки сообщений", "Антивирус", "Тарификация", "Оповещение администраторов", and "Трассировка". The main area is titled "SMTP-шлюз" and contains the following settings:

- Блокировка**: "Фильтровать сообщения, если весовой коэффициент более (0 - не фильтровать)". The "Weight" dropdown is set to 500. The "Response code" dropdown is set to 554, and the "Response text" field contains "Access denied".
- Действия при весовом коэффициенте более**: The "Weight" dropdown is set to 300.
- Добавить заголовки**: A text box contains "SPAM".
- Редирект на адрес**: A text box contains "korzina@mail.ru".
- Шаблон темы**: A text box contains "%MARK%%SUBJ%".

At the bottom of the window, there are three buttons: "Помощь" (Help), "ОК", and "Отмена" (Cancel).

1.7 На вкладке «**Правила обработки**» сообщений задайте настройки по умолчанию для правил обработки сообщений. Для этого введите шаблон, согласно которому будет изменяться тема сообщения.



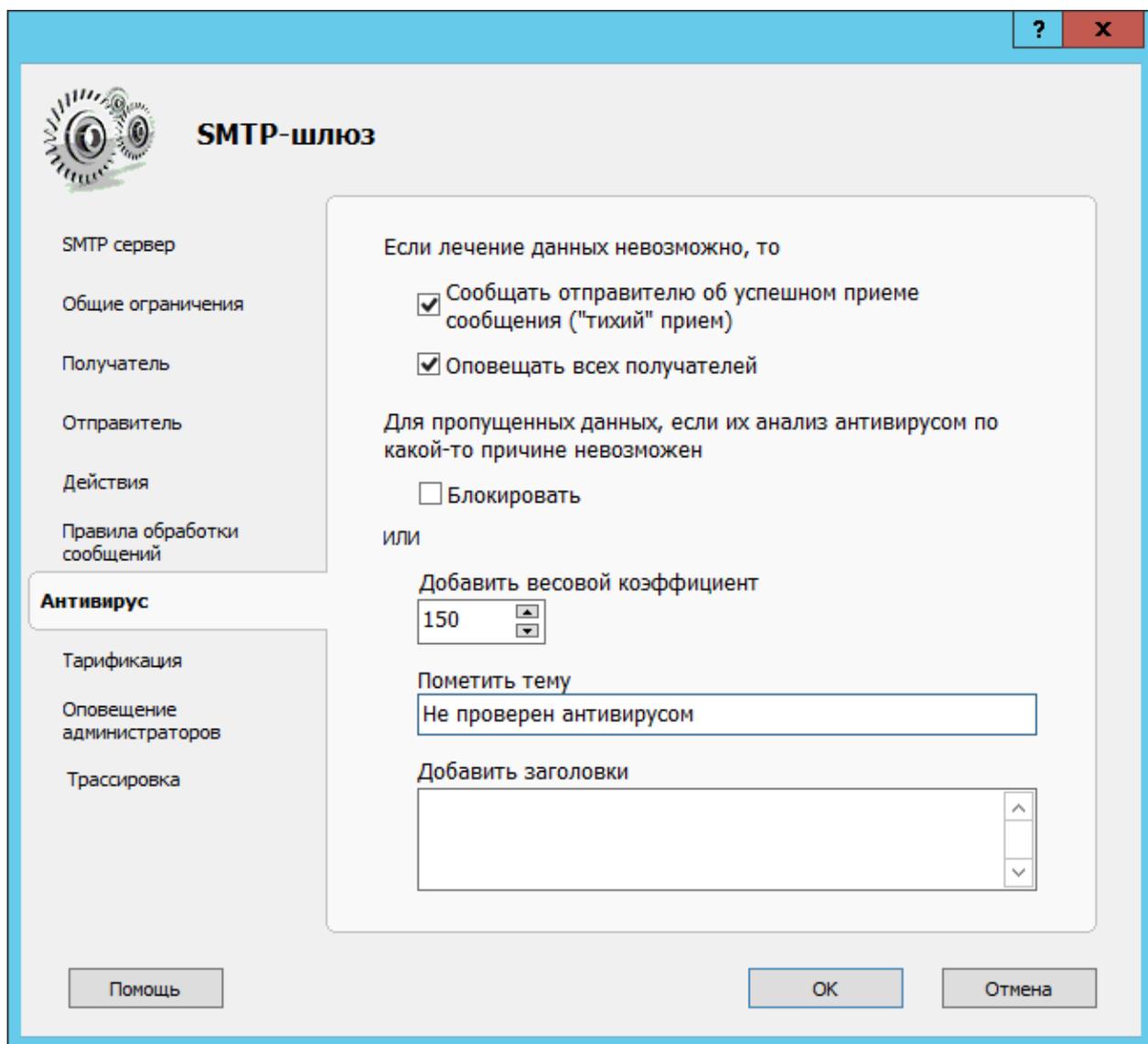
1.8 На вкладке **«Антивирус»** настройте действия, которые будет выполнять SMTP-шлюз для инфицированных сообщений, лечение которых невозможно. Для этого включите или выключите "тихий" прием. При включении такое письмо принимается и отправляющей стороне возвращается код успешного приема сообщения. В противном случае отправляющей стороне возвращается код ошибки. Также включите или выключите оповещение получателей. При включении инфицированное сообщение будет заблокировано, а всем его получателям будет отправлено автоматически сформированное письмо с отчетом о найденных вирусах.

На этой же вкладке, при необходимости, настройте действие, выполняющееся с письмами, которые по тем или иным причинам не могут быть проверены антивирусом. Это может быть блокировка сообщения или выполнение одного или нескольких обработок:

Добавление к рейтингу сообщения указанного числа.

Добавление к теме сообщения указанной метки (в метке можно использовать параметр подстановки %MARK% –ранее сформированная пометка темы другим правилом).

Добавление к сообщению одного или нескольких произвольных заголовков.



1.9 На вкладке **«Тарификация»** включите или выключите следующие параметры тарификации.

Пропорциональное разделение трафика, потраченного на прием сообщения, между всеми получателями пропорционально. При выключении этого параметра каждому получателю будет засчитан весь трафика в полном объеме.

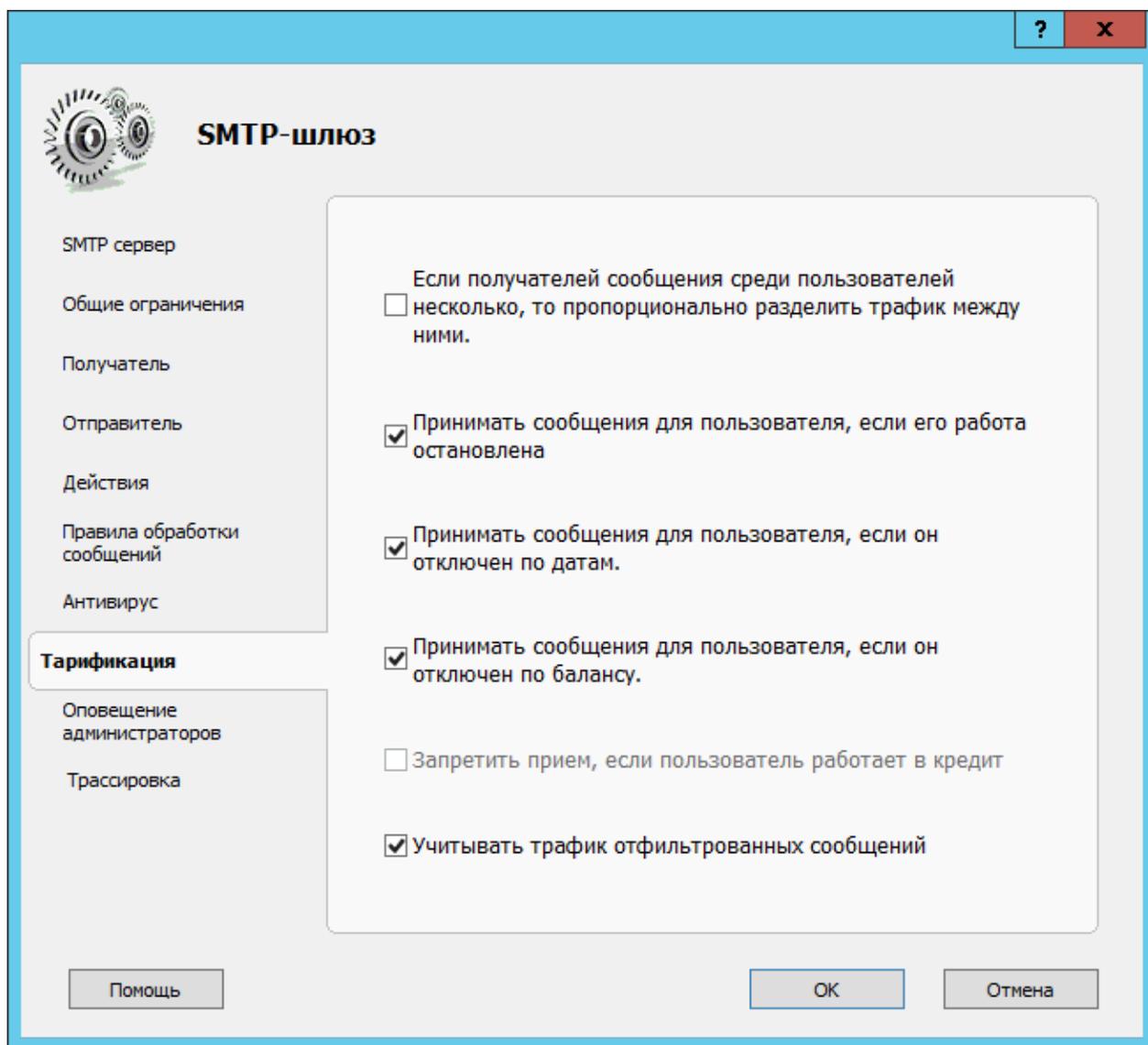
Прием сообщений для пользователей, работа которых приостановлена.

Прием сообщений для пользователей, отключенных по датам.

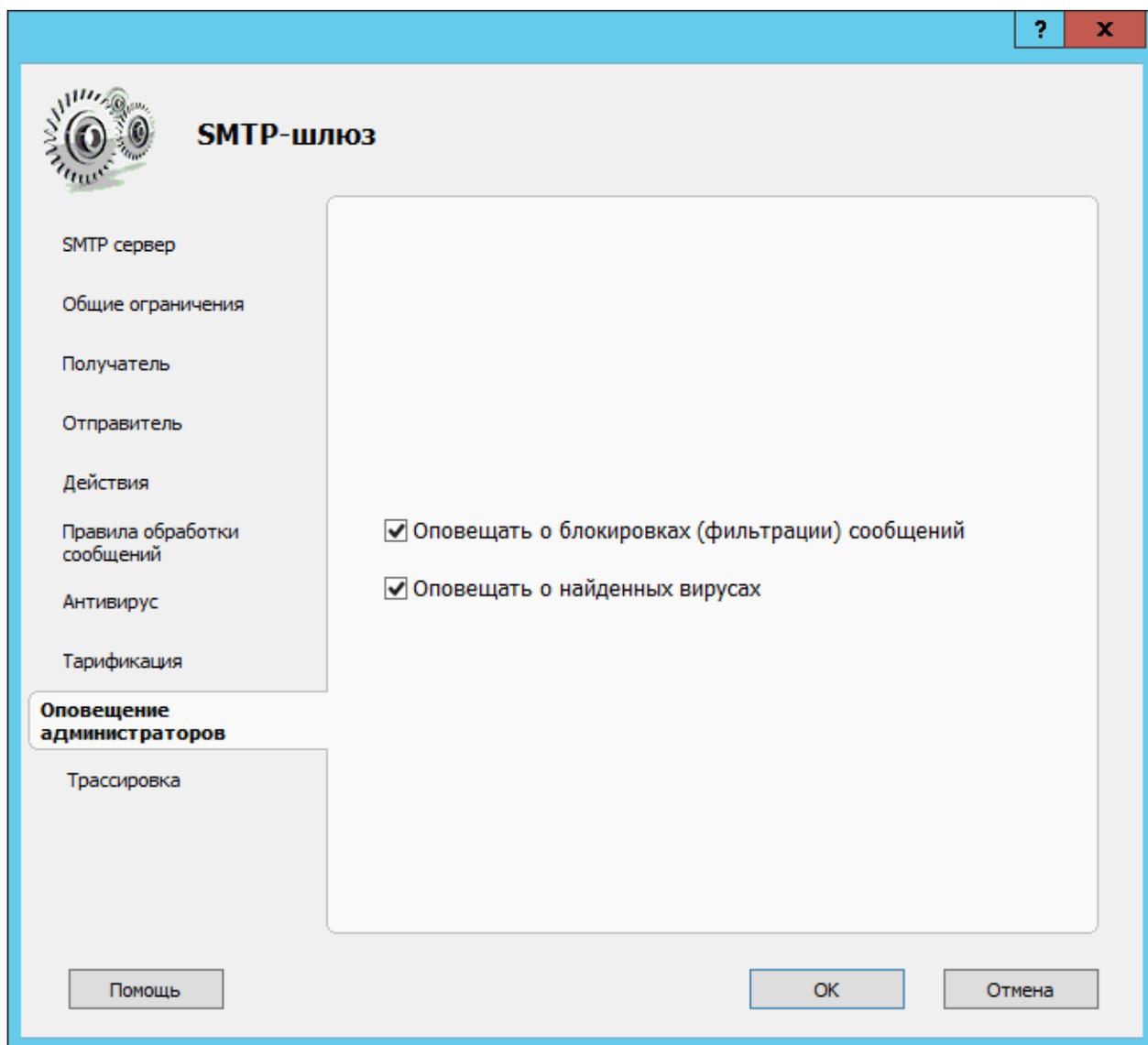
Прием сообщений для пользователей, отключенных из-за отрицательного баланса.

Запрет приема сообщений для пользователей, работающих в кредит.

Запись трафика, потраченных на загрузку отфильтрованных впоследствии сообщений, на баланс их получателей.

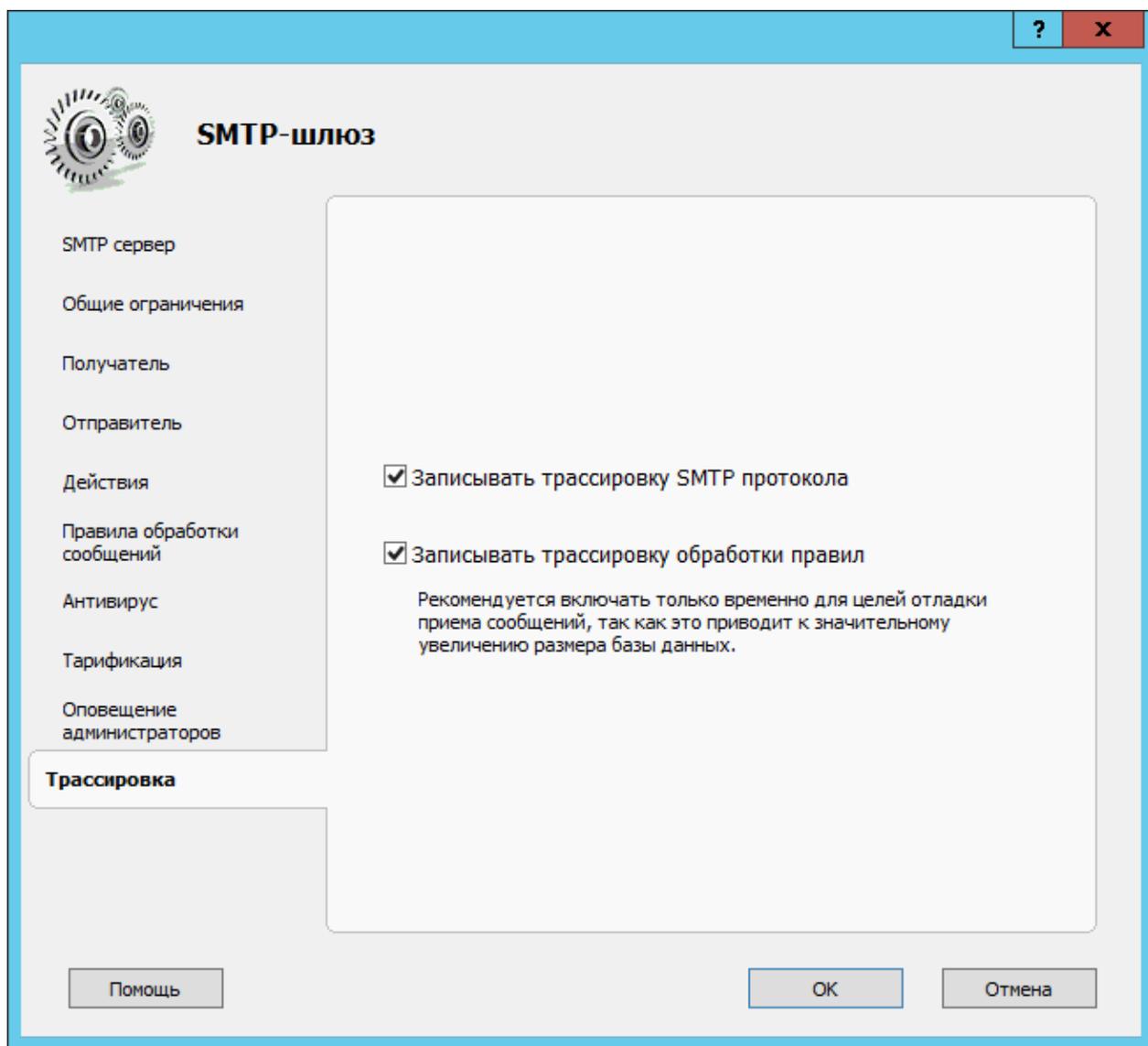


1.10 На вкладке **«Оповещение администраторов»** включите или выключите отправку оповещений администратору о блокировке сообщений и об обнаружении в них вирусов. Замечание! Отправка осуществляется с помощью службы отправки, которая предварительно должна быть настроена.



1.11 Если есть необходимость ведения подробной записи действий SMTP-шлюза в отдельном журнале, то на вкладке «Трассировка» включите запись трассировки SMTP-протокола. Это может быть полезно для отладки взаимодействия с различными SMTP-серверами. Здесь же можно включить запись трассировки обработки правил. Это может пригодиться для отладки работы логики правил.

Замечание! Трассировку рекомендуется включать только временно с целью выполнения отладки приема сообщений, поскольку она значительно увеличивает размер базы данных.



Сохраните внесенные изменения.