АО «СталкерСофт»
123458, Российская Федерация, Москва
Ул.Маршала Прошлякова, дом 30
+7 (499) 271-3154
www.communigate.ru

Руководство администратора

«CommuniGate Pro AntiSpam Plugin based on Kaspersky SDK»
(ПО CommuniGate Pro Kaspersky AS Plugin; также – Плагин)

Обзор Плагина

ПО CommuniGate Pro Kaspersky AS Plugin запускается как Внешний Фильтр и высчитывает спам-рейтинг для каждого обработанного сообщения. В отличии от утилит со статически определенными шаблонами спам сообщений, Плагин KAS динамически получает новые шаблоны из Сети Лаборатории, которая обеспечивает высокую точность в определении новых спам сообщений.

Рейтинг определяется в пределах от 0 до 100; чем выше рейтинг сообщения, тем с большей вероятностью это сообщение является спамом. Сведения о рейтинге добавляются в заголовок сообщения, таким образом оно может быть обработано Правилами Сервера, Домена или Аккаунта.

По-умолчанию добавляемый заголовок выглядит так:

X-Junk-Score: 92 [XXXX]
X-KAS-Score: 92 [XXXX]
X-Alert: possible spam!
X-Color: red
Кроме цифрового значения рейтинга в поле заголовка содержится «штрих-код» для упрощения автоматической обработки сообщений: чем больше символов «X» в «штрих-коде», тем выше рейтинг. Ниже приведены соответствия цифрового значения рейтинга и «штрих-кода» по умолчанию:

Цифровое значение рейтинга	Штрих-код
0	[]
1-39	[X]
40-80	[XX]
81-90	[XXX]
91-95	[XXXX]
96-99	[XXXXX]
100	[XXXXXX]

Каждый день в полночь Плагин генерирует отчет о количестве обработанных сообщений и их рейтинги. По умолчанию отчет отправляется на ардес postmaster из главного домена CommuniGate.

До установки, обратите внимание:

- Для функционирования ПО CommuniGate Pro Kaspersky AS Plugin требуется версия ПО CommuniGate Pro 6.2.4 или выше.
- ПО CommuniGate Pro Kaspersky AS Plugin доступно только для некоторых платформ, поддерживаемых ПО CommuniGate Pro.
  Убедитесь в доступности ПО CommuniGate Pro Kaspersky AS Plugin для той платформы, на которой работает Ваш CommuniGate Pro сервер.
- Для работы Плагина требуется два ключа:
  - Внутренний Ключ Лаборатории Касперского
  - Цифровой лицензионный ключ CommuniGate Pro.

Установка в Linux-совместимых операционных системах:

- Загрузите архив Плагина CGPKAS-*platform-processor-version*.tar.gz.
- Войдите под учетной записью супер-пользователя (root).
- Перенесите архив в директорию /var/CommuniGate/, которая является *Базовой Директорией* CommuniGate Pro.
- Распакуйте архив командой gtar (или командами gunzip и tar):
  gunzip CGPKAS-*.tar.gz
  tar -xf CGPKAS-*.tar
  . Будет создана директория CGPKAS внутри /var/CommuniGate/.
- Установите Внутренний Ключ Лаборатории Касперского:
  cp 12345ABC.key /var/CommuniGate/CGPKAS/licenses/
- Проведите **Тестирование Плагина.**

Установка в MS Windows-совместимых операционных системах:

- Загрузите архив Плагина CGPKAS-Windows-x86_64.zip.
- Перенесите архив в *Базовую директорию* CommuniGate Pro C:\CommuniGate Files\
- Распакуйте Плагин любой утилитой "unzip":
  pkunzip CGPKAS-*.zip
  Директория CGPKAS будет создана внутри *Базовой директории*.
- Установите Внутренний Ключ Касперского:
  copy 12345ABC.key C:\CommuniGate Files\CGPKAS\licenses\
- Проведите **Тестирование Плагина.**

Тестирование Плагина.

На Linux-совместимых системах:

- Смените текущую директорию на *Базовую директорию* CommuniGate Pro:
  cd /var/CommuniGate
- Запустите приложение CGPKAS из его директории:
  CGPKAS/CGPKAS
  Оно сообщит текущую версию Плагина, версию движка, время последнего обновления базы спама, и некоторую другую информацию.
- Введите:
  1 FILE CGPKAS/test.msg
  Плагин должен ответить записью ADDHEADER с последующим выводом строки заголовка сообщения с некоторым выставленным рейтингом.
- Завершите работу приложения нажав Ctrl-D.

На системе MS Windows:

- Смените текущую директорию на *Базовую директорию* CommuniGate Pro:
  cd "C:\CommuniGate Files"
- Запустите приложение CGPKAS.exe из его директории:
  CGPKAS\CGPKAS.exe
  Оно сообщит текущую версию Плагина, версию движка, время последнего обновления базы спама, и некоторую другую информацию.

  Обратите внимание: Если Плагин не запускается, укажите полный путь, включая букву диска:
  "C:\CommuniGate Files\CGPKAS\CGPKAS.exe"

- Введите:
  1 FILE CGPKAS\test.msg
  Плагин должен ответить записью ADDHEADER с последующим выводом строки заголовка сообщения с некоторым выставленным рейтингом.
- Завершите работу приложения нажав Ctrl-Z.

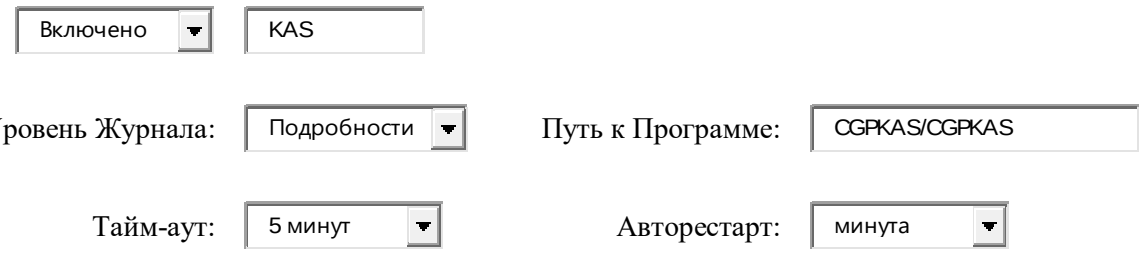
Обратите внимание: Без Внутреннего Ключа Лаборатории Касперского Плагин выдаст ошибку и прекратит работу. Но, тем не менее, тестирование без Внутреннего Ключа Лаборатории Касперского имеет смысл для проверки зависимостей Плагина от системных библиотек.

Интеграция Плагина в CommuniGate Pro

Шаг #1: Создайте Помошника как описано ниже:
Пожалуйста, ознакомьтесь с разделом Внешние помошники в мануале CommuniGate Pro.

Откройте страницу Общие в разделе Установки в Административном веб-интерфейсе CommuniGate Pro и перейдите в раздел Помощники. Создайте Помощника для Плагина:

Фильтрация данных

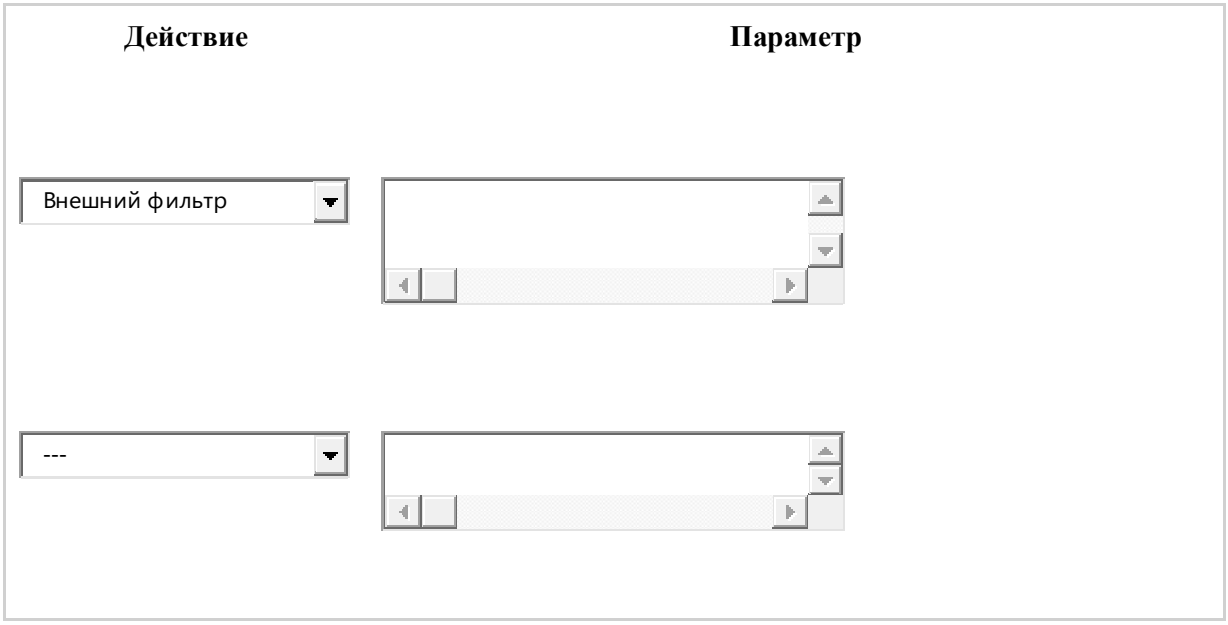


Обратите внимание: Для Windows путь к Программе должен быть полным, например "C:\CommuniGate Files\CGPKAS\CGPKAS.exe"

Шаг #2: Создание Правила Сканирования

Для вызова Помощника KAS Вам необходимо создать Общесерверное Правило с действием "Внешний Фильтр KAS". Правило сканирования будет применено Плагином к сообщению, и спам рейтинг будет добавлен к заголовку сообщения.
Обратите внимание: Это должно быть Общесерверное правило, а не Общедоменное Правило или Правило Аккаунта.

Рекомендованные правила сканирования сообщений:



Это правило пропускает сообщения от адреса MAILER-DAEMON (такие как сообщения о недоставке, и другие служебные сообщения), а также сообщения отправленные с Клиентских IP Адресов и аутентифицированных отправителей и включая только сообщения для локальных аккаунтов и списков рассылки.

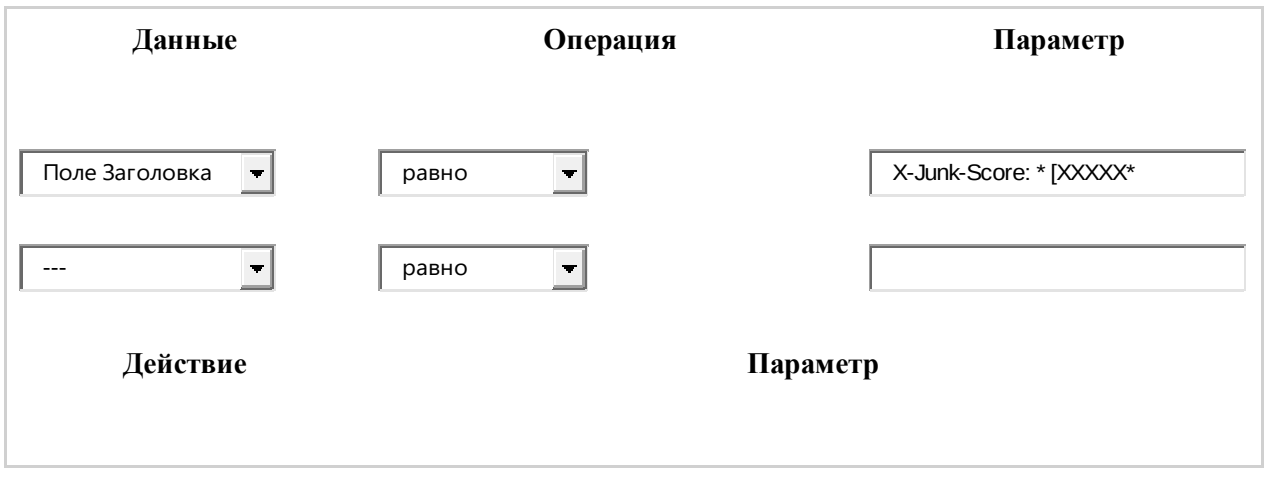
Примечание: Не лицензированная установка Плагина ограничена обработкой 5 сообщений в час. Если трафик сообщений превышает этот лимит, Плагин будет пропускать эти сообщения без выставления рейтинга.

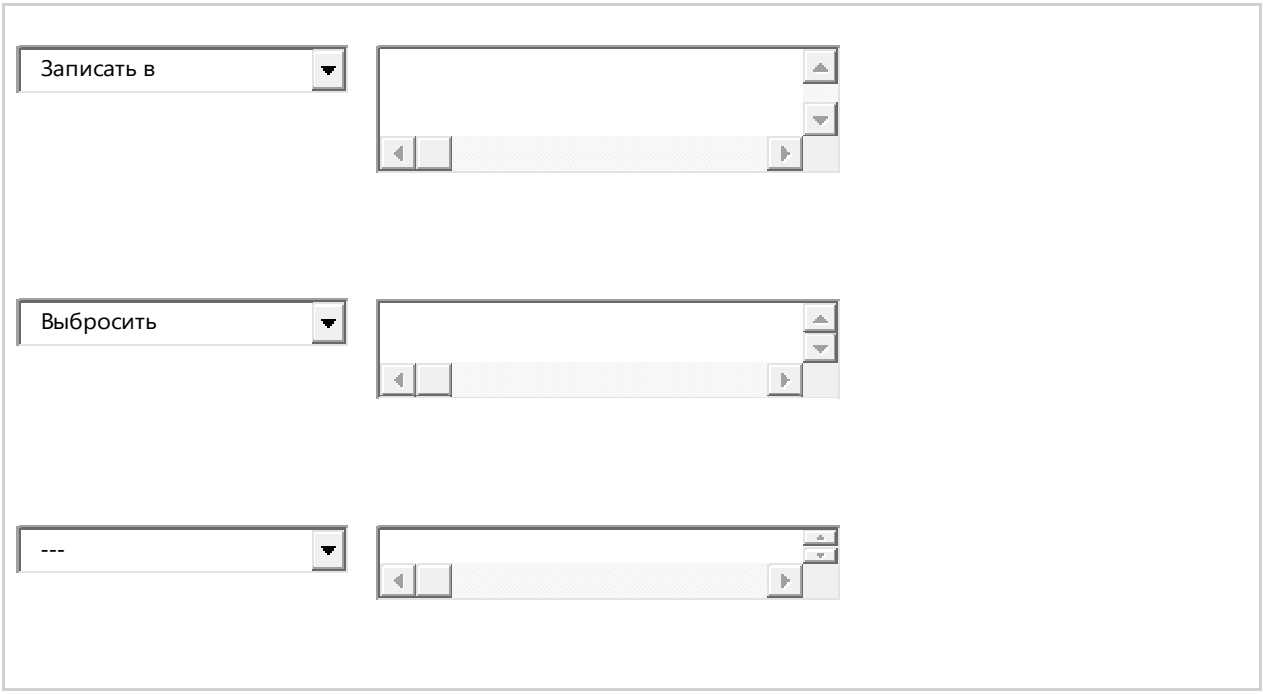
Шаг #3: Обработка Сообщений после выставления Рейтинга

Плагин сам по себе не блокирует спам сообщения, он лишь присваивает таким сообщениям определенный рейтинг. Для непосредственной блокировки спама, Вам необходимо создать Правило, которое будет блокировать сообщения на основе их спам-рейтинга. Существует несколько возможных сценариев:

Сценарий #1: подходит небольшим организациям, где Вы можете назначить ответственным одного человека (например, Postmaster) для ежедневного просмотра спам сообщений для проверки на ложные срабатывания, и если такое ложное срабатывание находится - перенаправлять эти сообщения соответствующим получателям.

Создайте Общесерверное Правило следующего содержания:

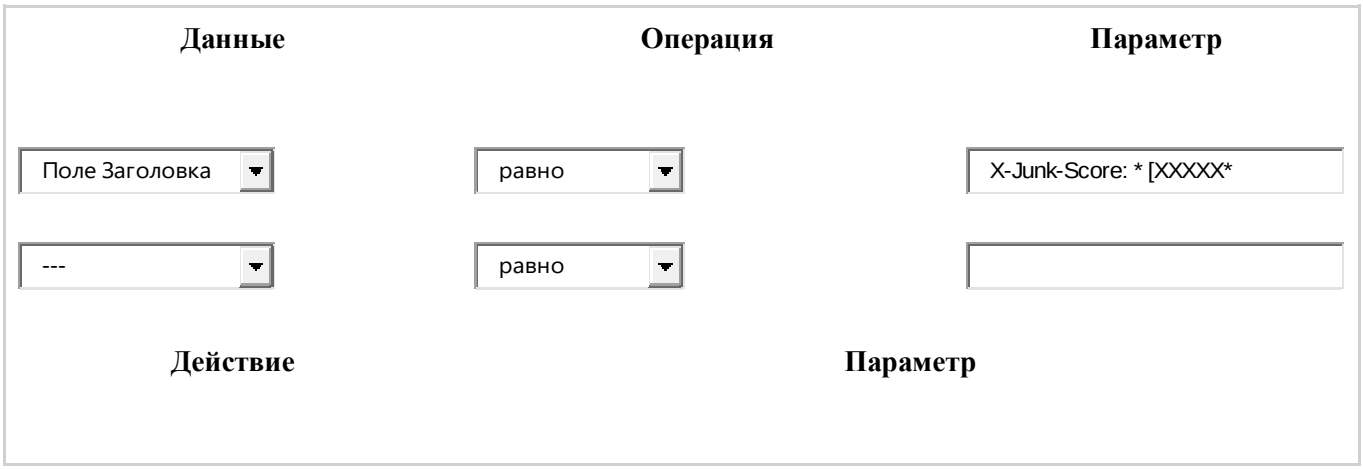


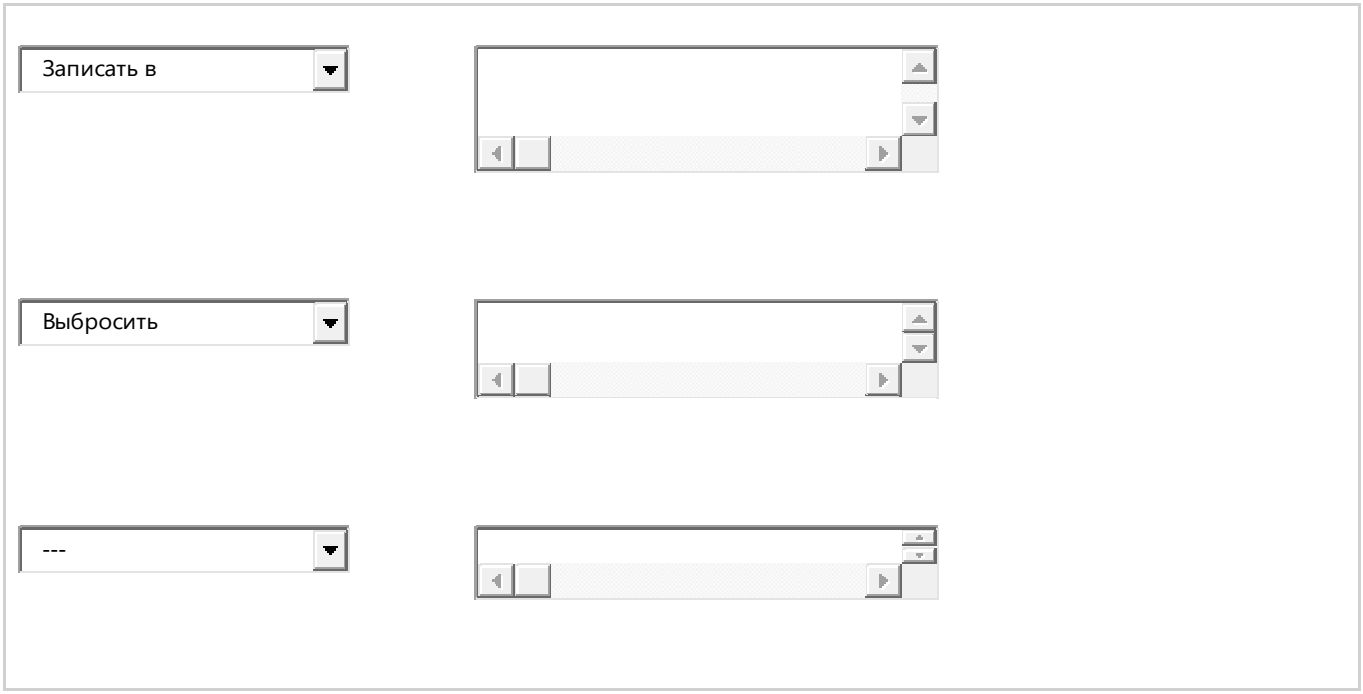


Это Правило переносит входящие сообщения с рейтингом 96 и выше в ящик «spam_box» аккаунта postmaster@domain.com. Действие «Выбросить» требуется для предотвращения отправки сообщения первоначальному получателю (ящик INBOX). Обратите внимание, в примере выше символ «*» в выражении [XXXXX* необходим, чтобы отфильтровать все сообщения с рейтингом ниже 5 X. Без этого символа правило будет фильтровать только сообщения с рейтингом 5 X.
Обратите внимание: Приоритет Общесерверных правил должен быть ниже, чем приоритет Правил Сканирования.

Сценарий #2: подходящий для больших организаций и Интернет Провайдеров. Сценарий позволяет пользователям сами решать, что делать со спамом.

Создайте Общедоменное правило или несколько Правил Аккаунта для Аккаунтов, которым необходима фильтрация, со следующим содержаием:





Это Правило переносит входящие сообщения с рейтингом 96 и выше в ящик «Junk» аккаунта первоначального получателя. Пользователь должен сам проверять свой ящик «Junk» и очищать его. Действие «Выбросить» требуется для предотвращения отправки сообщения первоначальному получателю (ящик INBOX). Обратите внимание, в примере выше символ «*» в выражении [XXXXX* необходим, чтобы отфильтровать все сообщения с рейтингом ниже 5 X. Без этого символа правило будет фильтровать только сообщения с рейтингом 5 X.

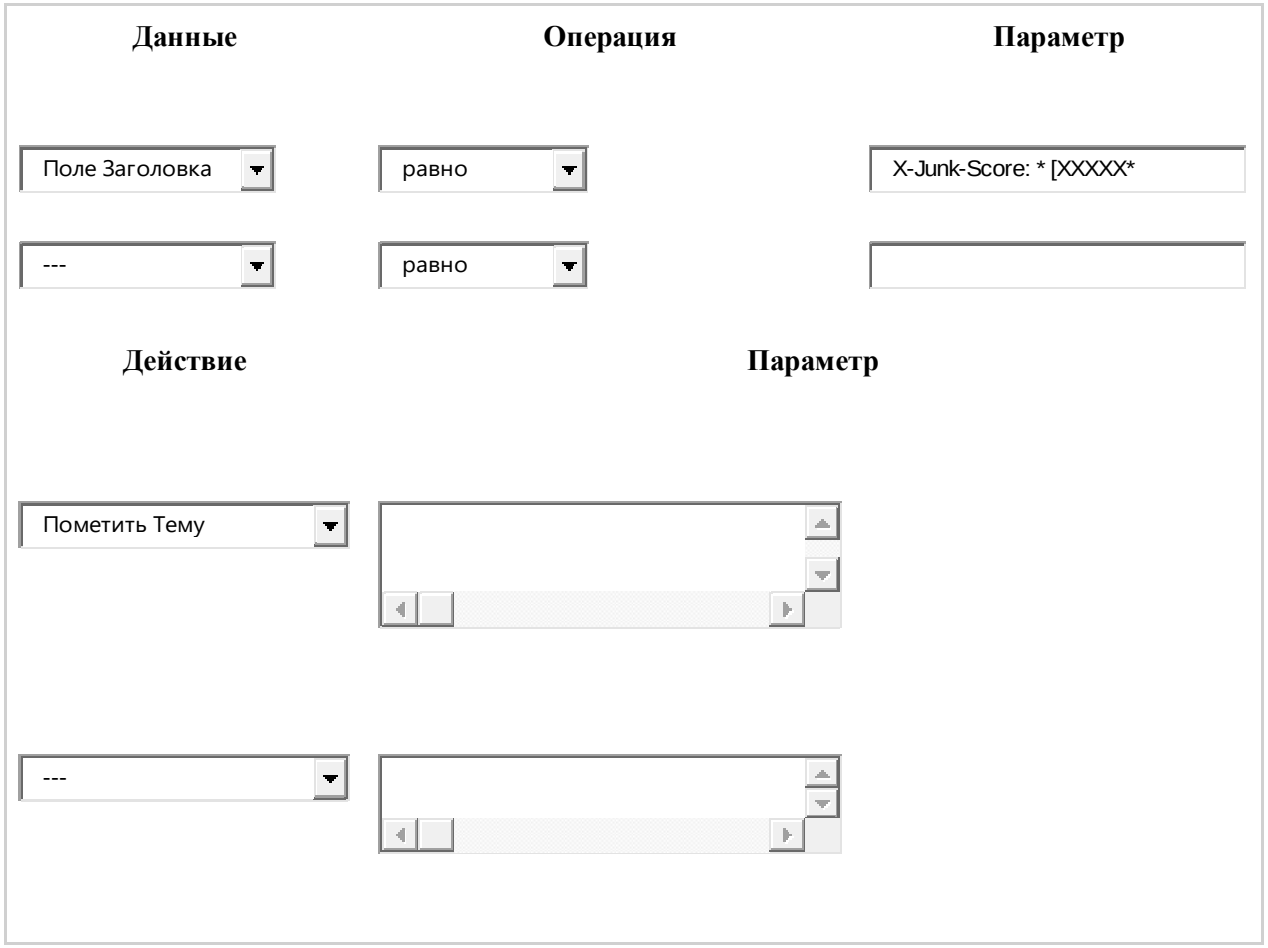
В качестве альтернативы, Вы можете использовать упрощенные Правила «Управление Спамом» на уровне домена или аккаунта:

Управление Спамом

Высокая вероятность:	Средняя вероятность:	Низкая вероятность:
Пометить как Спам		

Сценарий #3: подходящий для больших организаций и Интернет Провайдеров, пользователи которых имею доступ только к ящику INBOX (например пользователи POP3).

Создайте Общедоменное правило или несколько Правил Аккаунта для Аккаунтов, которым необходима фильтрация, со следующим содержаием:



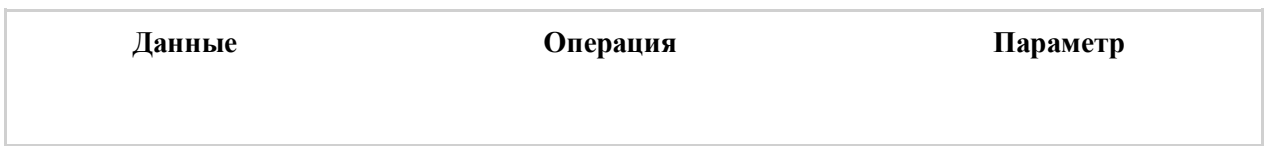
Это правило помечает спам сообщения префиксом [SPAM] в теме сообщения.

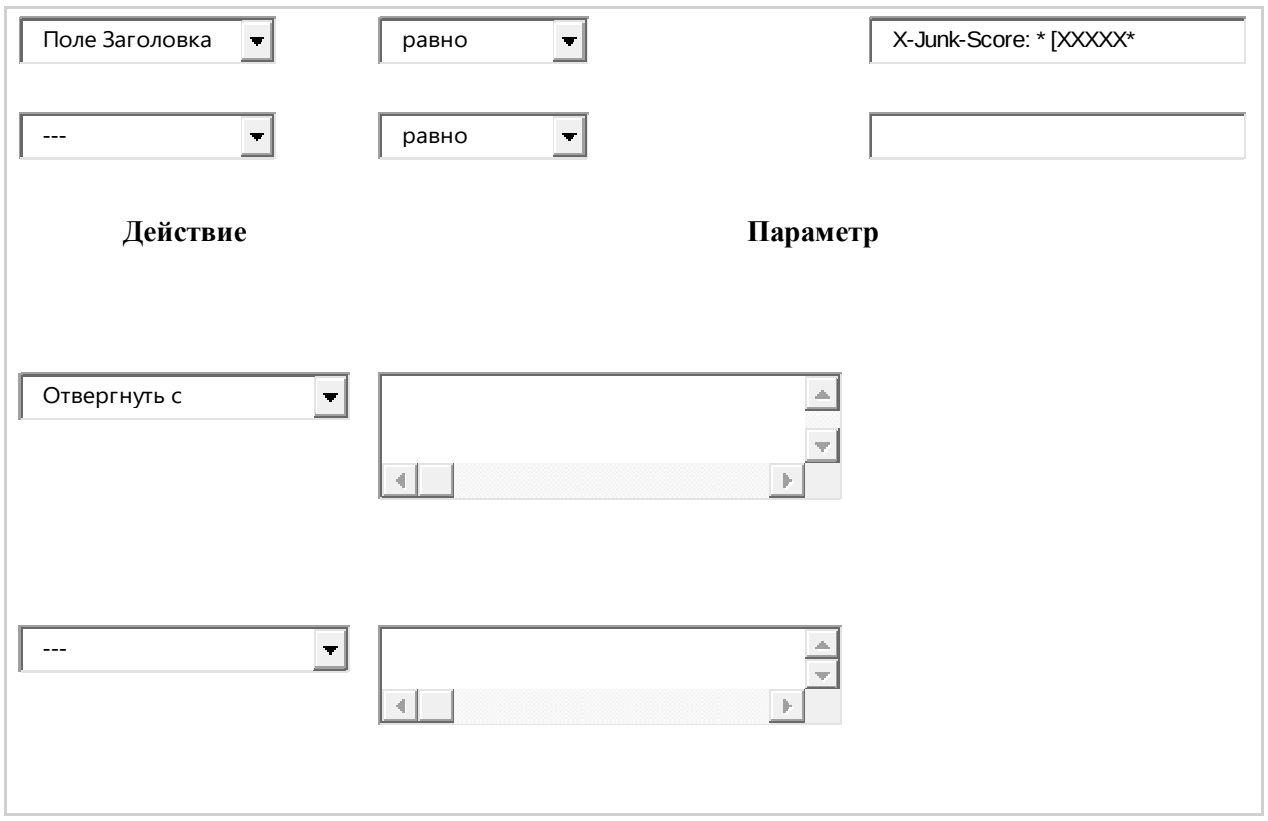
Сценарий #4: подходит для компаний с относительно небольшим входящим трафиком. Доступен для серверов CommuniGate Pro версии 5.1 и выше.

В CommuniGate Pro версии 5.1 и выше, Вы можете добавлять сообщения в очередь синхронно. Используйте Веб Интерфейс Администратора, чтобы сконфигурировать компонент Очереди. Откройте страницу Очередь в разделе Установки -> Почта: Снимите галочку с опции «Добавлять в очередь асинхронно»:

Более детальную информацию смотрите в Мануале CommuniGate.

Создайте Общесерверное Правило следующего содержания:





При синхронной постановке в очередь, если сообщение отвергается Общесерверным правилом, оно отвергается еще на уровне SMTP с кодом ошибки 5xx, вместо полноценной операции приёма и отклонения с ответом.

При любом сценарии не рекомендуется отвергать сообщения без сохранения их, так как всегда существует возможность ложного срабатывания. Крайне не рекомендуется автоматически отвергать спам сообщения (кроме синхронного режима, используемого в сценарии 4), потому что обратный адрес зачастую сфабрикован и сообщение о отвергнутом сообщении может прийти человеку, который не отправлял данное сообщение. При отвержении писем в синхронном режиме, хост отправитель получит ошибку еще на уровне SMTP, и никакого ответного сообщения от Вашего сервера отправлено не будет.

Рекомендуемый порог (значение рейтинга, при котором сообщение расценивается как спам) - 96. Если слишком большое количество спам сообщений проходит фильтр, снизьте порог до 90. Если же наоборот, происходит слишком много ложных срабатываний, повысьте порог до 100.

Файл конфигурации Плагина

При старте Плагин зачитывает содержимое файла CGPKAS.cfg из текущей директории. Формат данных в этом файле описан здесь http://www.communigate.ru/CommuniGatePro/Data.html. Описание элементов данных находится в самом файле CGPKAS.cfg. Стандартный файл CGPKAS.cfg доступен здесь.

Стандартный файл CGPKAS.cfg имеет следующее содержимое:

```
Header="X-Junk-Score: ^1 [^2]";
```

Эта строка определяет заголовок с рейтингом, который будет добавлен в сообщение. Комбинация ^1 заменяется числовым рейтингом сообщения.
Комбинация ^2 заменяется «штрих-кодом» с рейтингом сообщения.
Чтобы создать заголовок с несколькими строчками, используйте комбинацию \e для переноса строки. Убедитесь, что каждая строка соответствует требованиям RFC. Лучше всего начинать каждую строку с префикса «X-». Пример: Header="X-Score: ^1\eX-Bar-Score: ^2"

AlertLevel=96;

Эта строка определяет рейтинг, который инициирует добавление предупреждающего заголовка AlertHeader в сообщение, а в ежедневные отчеты об источниках и получателях спама, будет добавлена информация об этих сообщениях.

AlertHeader="X-Alert: possible spam!\eX-Color: red";

Эта строка определяет заголовок с рейтингом, который будет добавлен в сообщение, если его рейтинг равер или выше значения AlertLevel. Комбинация «X-Color: red» меняет цвет сообщения при просмотре через Пользовательский Веб Интерфейс CommuniGate Pro.
Обратите внимание: Для обработки спам сообщений, Вы можете использовать факт наличия заголовка AlertHeader вместо проверки рейтинга сообщения, но этот метод не слишком гибкий, в случае если пользователи хотят использовать различные пороговые рейтинги.

SubmittedDirectory = "Submitted";

Эта строка определяет директорию Submitted в CommuniGate Pro, которая требуется для приёма отчетов через модуль PIPE. Это может быть относительный или абсолютный путь, например "/var/CommuniGate/Submitted"

OnLicenseLimitReached=Pass;

Эта строка определяет поведения Плагина при превышении лимита сообщений, который определен лицензией. Когда он установлен в значение «Delay», Плагин будет задерживать модуль обработки Очереди CommuniGate Pro, а в значении «Pass», Плагин будет пропускать сообщения без обработки и выставления рейтинга. Такие необработанные сообщения не будут иметь заголовка X-KAS-Score. Кроме того, в записи лога CommuniGate Pro будут записи о превышении лимита лицензии.

Обращение в Спам-лабораторию

Технические требования для приема сообщений о ложных срабатываниях в Лабораторию Касперского:

- Для анализа спам-писем «Лаборатории Касперского» необходим оригинал сообщения в rfc822 MIME формате с полными техническими заголовками. Прикрепите образец спама в формате MSG или EML.
- Для анализа подходят только те спам-письма, которые были получены в течение последних 48 часов. Ваш запрос поступит в очередь на обработку в автоматическом режиме, ответа спам-аналитиков с данного адреса не предусмотрено.

Сообщения должны отправляться по следующим адресам:

notspam@kaspersky.com - для ложно-положительных срабатываний
spam@kaspersky.com - для ложно-отрицательных срабатываний

Использования Microsoft Outlook для отправки отзыва:

1. Запустите Outlook.
2. Создайте новое сообщение нажатием на кнопку «Новое сообщение».
3. Перетащите сообщение, которое было неверно классифицировано в окно с новым письмом, чтобы добавить его как вложение.
4. Отправьте созданное сообщение с вложением на один из адресов для отзывов, перечисленных выше.

Использования Веб Почты CommuniGate для отправки отзыва

1. Откройте сообщение, которое было неверно классифицировано в отдельном окне.
2. Нажмите кнопку «Переслать» для создания сообщения с отзывом.
3. В поле «Кому» введите один из адресов для отзывов, перечисленных выше.
4. Нажмите на кнопку «Отправить».