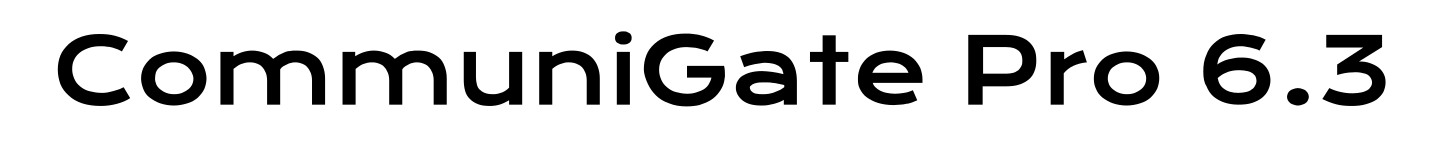
**Внешний помощник CGP-KAV для**



Руководство пользователя

|  |  |
| --- | --- |
| Версия продукта : | 1.0.0 |
| Версия документации : | 1.0 |
| Дата : | 03.10.2024 |

**Содержание**

[Предисловие 3](#__RefHeading___Toc2753_4160107288)

[Требования 3](#__RefHeading___Toc2755_4160107288)

[Примечания 3](#__RefHeading___Toc2757_4160107288)

[Сокращения 3](#__RefHeading___Toc2759_4160107288)

[Установка Помощника CGP-KAV 4](#__RefHeading___Toc2761_4160107288)

[Установка из дистрибутива 4](#__RefHeading___Toc2899_4160107288)

[CommuniGate Pro 4](#__RefHeading___Toc2763_4160107288)

[Настройка внешнего помощника 4](#__RefHeading___Toc2901_4160107288)

[Настройка SMTP-правил 4](#__RefHeading___Toc2903_4160107288)

[Включение Внешнего помощника 5](#__RefHeading___Toc2905_4160107288)

[Выключение Внешнего помощника 5](#__RefHeading___Toc2905_4160107288_Copy_1)

[Утилита диагностики 5](#__RefHeading___Toc2907_4160107288)

[Настройка Внешнего помощника CGP-KAV 5](#__RefHeading___Toc2765_4160107288)

[Основные настройки 5](#__RefHeading___Toc2767_4160107288)

[Настройки Anti-Virus 6](#__RefHeading___Toc2769_4160107288)

[Отладка внешнего помощника CGP-KAV 7](#__RefHeading___Toc2771_4160107288)

[Заголовки результатов сканирования 7](#__RefHeading___Toc2773_4160107288)

[Kaspersky Anti-Virus Engine 7](#__RefHeading___Toc2775_4160107288)

[Угроза не обнаружена 7](#__RefHeading___Toc2909_4160107288)

[Угроза обнаружена 7](#__RefHeading___Toc2911_4160107288)

[Ошибка 7](#__RefHeading___Toc2913_4160107288)

[Расширенные настройки 8](#__RefHeading___Toc2777_4160107288)

[Kaspersky Anti-Virus Engine 8](#__RefHeading___Toc2779_4160107288)

[Настройки сетевых proxy сканера 8](#__RefHeading___Toc2915_4160107288)

[Настройки сетевых proxy сервиса обновления 8](#__RefHeading___Toc2917_4160107288)

[Настройки KAV Scanner Engine 9](#__RefHeading___Toc2919_4160107288)

[Обновление лицензионных ключей KAS 13](#__RefHeading___Toc1596_3575718543)

[Настройки производительности 13](#__RefHeading___Toc2781_4160107288)

[Рекомендации Лаборатории Касперского по настройке KAV 13](#__RefHeading___Toc2783_4160107288)

[Установка в очередь CGPro и рабочие потоки внешнего помощника 15](#__RefHeading___Toc2785_4160107288)

# Предисловие

В этом документе описано, как устанавливать, настраивать и запускать Внешний помощник CGP-KAV для CommuniGate Pro, необходимый для проверки электронных писем с помощью Анти-Вируса Касперского. В электронные письма будут добавлены SMTP-заголовки с результатами проверок. Это позволит автоматически фильтровать электронные письма с помощью SMTP-правил CommuniGate Pro.

## Требования

CommuniGate Pro: 6.3.39 и новее

OS: Linux amd64

## Примечания

Технологиям Kaspersky необходим доступ к Kaspersky Security Network для обновления базы данных вирусных сигнатур. Некоторые функции сканирования, используемые для повышения точности, могут требовать отправки данных в Kaspersky Security Network. Вам необходимо открыть сетевой доступ по протоколам HTTP и HTTPS (80-TCP, 443-TCP) на следующие хосты:

\*.kaspersky-labs.com

\*.kaspersky.com

## Сокращения

KAV: Анти-Вирус Касперского

KSN: Kaspersky Security Network CGPro: CommuniGate Pro

# Установка Помощника CGP-KAV

В этом разделе описано, как устанавливать Внешний помощник CGP-KAV

*cgpro\_home* - это путь к директории установленного CGPro.

### Установка из дистрибутива

Скачайте последнюю версию пакета для вашей системы по адресу: <https://www.communigatepro.ru/pub/plugins/Kaspersky/>

# cd *cgpro\_home*

# sudo tar xf *path/to/CGP-KAV*-Linux-amd64\_vX.Y.Z.tar.bz2

# sudo chown -R root:mail *cgpro\_home*/CGP-KAV

## CommuniGate Pro

Чтобы внешний помощник CGP-KAV обрабатывал почту, необходимо объявить этот новый помощник и создать SMTP-правило для вызова помощника на основе почтового потока.

### **Настройка внешнего помощника**

Чтобы добавить внешнего помощника CGP-KAV, в интерфейсе администрирования CGPro перейдите в

Установки → Общее → Помощники

Создайте новый помощник в разделе Фильтрация данных:

|  |  |  |  |
| --- | --- | --- | --- |
| **Выключено** | AntiVirus |  | |
| **Уровень журнала** | Все | **Путь к Программе** | CGP-KAV/CGP-kAV |
| **Тайм-аут** | 2мин | **Авторестарт** | 15сек |

### **Настройка SMTP-правил**

В данном примере показано, как сканировать все письма, направляемые через модуль LOCAL, который будет доставлять письма в почтовые ящики пользователей. Такие настройки означают, что любое письмо, отправленное даже от вас самих на ваш собственный почтовый ящик, будет направлено во Внешний помощник CGP-KAV.

Перейдите в раздел Установки → Почта → Правила

Добавьте новое правило с названием AntiVirus и нажмите Изменить

Добавьте в правило следующие параметры :

**Данные Операция Параметр**

Любой Маршрут равно LOCAL(\*

–--

**Действие Параметр**

Внешний Фильтр AntiVirus

---

**Лицензии**

Убедитесь, что лицензии для внешнего помощника CGP-KAV добавлены в CGPro. Для этого откройте раздел интерфейса администратора CGPro Главное → Лицензия

Если лицензионные ключи помощников CGP-KAV добавлены, в списке будут записи, содержащие “Kaspersky AnviVirus”.

### **Включение Внешнего помощника**

В интерфейсе администрирования CGPro перейдите в раздел Настройки → Общее → Помощники и измените для Фильтра данных AntiVirus со значения Выключено на Включено.

### **Выключение Внешнего помощника**

В интерфейсе администрирования CGPro перейдите в раздел Настройки → Общее → Помощники и измените для Фильтра данных AntiVirus со значения Включено на Выключено. Обратите внимание, что движку KAV нужно порядка 15-30 секунд на корректное завершение работы.

### **Утилита диагностики**

Теперь можно убедиться, что движок помощника CGP-KAV работает в вашей системе так, как ожидается, с помощью утилиты диагностики. Утилита диагностики может быть так же использована в случае проблем с запуском внешнего помощника через CGPro. Пожалуйста, обратитесь к разделу Отладка внешнего помощника CGP-KAV для получения более подробной информации.

# cd *cgpro\_home/CGP-KAV*

# sudo ./diagnose

# Настройка Внешнего помощника CGP-KAV

Этот раздел описывает параметры конфигурирования, которые находятся в

*cgpro\_home*/CGP-KAV/kav.conf

Конфигурационный файл регистрозависимый.

## Основные настройки

Основные настройки определены в блоке **[main]**.

Необходимо указать помощнику путь к инсталляции CGPro :

**cgpro\_home = /var/CommuniGate**

Политика отказов позволяет определить, как будет действовать Внешний помощник в случае сбоев при вызове движка KAV. Если политика фильтрации определена как отклонение сообщения, любая ошибка сканирования заставит Внешнего помощника отложить сообщение в очереди CGPro. Любая другая ошибка, кроме ключевого слова reject, будет указывать помощнику на то, что письмо должно быть доставлено (политика pass). В этом случае к письму добавляется заголовок ошибки (X-KAV-Error). Параметр политики отказа :

**failure\_policy = reject|pass**

Рабочие потоки позволяют настроить количество потоков, обрабатывающих очередь сообщений движками KAV.

**worker\_threads = 4**

Следующая настройка позволяет отсрочить запуск Внешнего помощника, чтобы убедиться, что CGPro доступен для получения лицензий :

**delay\_start = 0**

## Настройки Anti-Virus

Настройки антивируса определяются в разделе **[antivirus]**.

Вы можете добавить собственные заголовки результатов в электронные письма после того, как они были успешно просканированы KAV:

**KAV\_Header\_Status = X-KAV-Status KAV\_Header\_Extended = X-KAV-Extended**

**KAV\_Header\_Error = X-KAV-Error**

Заголовок KAV\_Header\_Extended будет содержать идентификатор вируса в случае его обнаружения. Подробности см. в разделе Заголовки результатов сканирования.

Следующие параметры раздела **[antivirus]** относятся к настройкам Kaspersyk Anti-Virus и перезаписывают значения в файле *cgpro\_home/*CGP-KAV*/*KAV/etc/kavhttpd.xml

Вы можете задать период времени в секундах, по истечении которого внешний помощник будет проверять наличие обновлений в базе вирусных сигнатур KAV перед сканированием нового сообщения электронной почты. Значение по умолчанию - 360 минут (6 часов):

**UpdatePeriodMinutes = 360**

Вы можете настроить количество процессов и потоков сканера, которые будут запущены службой KAV при запуске внешнего помощника. Более подробная информация и советы по настройке этих параметров приведены в разделе Настройки производительности. Значения по умолчанию:

**ScannersCount = 2** // ограничивается системой (ulimit -u)

**ThreadsCount = 2** // максимум 32

Вы можете задать таймаут сессии (SessionTimeout) в миллисекундах, по истечении которого сканирование будет прервано и выдаст ошибку таймаута. В зависимости от политики отказа (reject или pass) в главном разделе конфигурации, письмо будет выпущено с заголовком ошибки или отложено для другой попытки. По умолчанию для сканирования сообщений установлено значение 10 000 миллисекунд (10 секунд):

**SessionTimeout = 10000**

Время, необходимое для сканирования письма, зависит от вычислительных возможностей вашего оборудования, размера писем и загруженности системы в момент вызова сканирования. Вы можете настроить этот параметр в зависимости от типа SMTP-потока, который вы хотите направить в KAV для сканирования.

Порт, на котором запускается KAV SDK можно задать через параметр

**ConnectionString = localhost:7776**

## Отладка внешнего помощника CGP-KAV

Для того чтобы внешний помощник мог вести полные журналы, необходимо активировать запись полных журналов в модуле сбора сообщений:

Почта → Очередь → Установка в очередь → Уровень журнала : Всё

Чтобы отладить внутренние функции внешнего помощника, вы можете активировать режим verbose для различных модулей в секции **[debug]** конфигурационного файла kav.conf:

**DebugExternal = 0** // выводит инофрмацию об ограничениях лицензии (значения 0,1)

**DebugFilterDaemon = 0** // выводит информацию о взаимодейтсвии с KAS (значения 0,1)

**DebugThreading = 0**  // отчёты о работе потоков (значения 0,1)

**DebugConfig = 0** // выводит актуальные конфиги помощника (значения 0,1)

**DebugCGateInput = 0** // выводит запросы, приходящие от CGate (значения 0,1)

# Заголовки результатов сканирования

В этом разделе представлен обзор заголовков, добавляемых в письма, проверяемые внешним помощником CGP-KAV.

## Kaspersky Anti-Virus Engine

### Угроза не обнаружена

**X-KAV-Status: CLEAN** добавляется в просканированное письмо при отсутствии угрозы.

### Угроза обнаружена

**X-KAV-Status: DETECT** добавляется в сканируемое письмо при обнаружении угрозы

**X-KAV-Extended: <virus\_id>** добавляется в сканируемое письмо при обнаружении угрозы

### Ошибка

**X-KAV-Error : <message>** добавляется к письму при возникновении ошибки.

# Расширенные настройки

Расширенные настройки позволяют настроить сетевой прокси-доступ для сервисов KAV и получить доступ к тонкой настройке движка KAV.

Пара опций в этих файлах управляется самим внешним помощником. Не изменяйте эти опции, иначе это может нарушить работу механизма перезаписи файлов конфигурации при следующем перезапуске внешнего помощника. Опции, которые будут переписаны, всегда устанавливаются в 0 в конфигурационных файлах шаблона, их легко определить.

## Kaspersky Anti-Virus Engine

Файлы конфигурации KAV Engine: *cgpro\_home*/CGP-KAV/KAV/kavhttpd/etc/kavhttpd.xml

**Прим.** Параметры kav.conf из раздела [antivirus] перезаписывают соответствующие параметры файла kavhttpd.xml

### Настройки сетевых proxy сканера

Отредактируйте файл конфигурации сканера KAV и измените этот раздел в соответствии с параметрами вашего сетевого прокси-сервера:

**<UseHTTPProxy>0</UseHTTPProxy> <!-- Specifies whether KAV HTTPD uses proxy when making requests to KSN: 0 (not used) or 1 (used) -->**

**<HTTPProxy>**

**<url></url> <!-- Address of the proxy -->**

**<port></port> <!-- Port of the proxy -->**

**<user></user> <!-- User name for the proxy authentication -->**

**<pass></pass> <!-- Password for the proxy authentication -->**

**</HTTPProxy>**

### Настройки сетевых proxy сервиса обновления

Настройки сетевых proxy задаются в разделе ProxySettings файла *cgpro\_home*/CGP-KAV/KAV/kavhttpd/etc/kavhttpd.xml

**<ProxySettings>**

**<UseProxy>0</UseProxy>**

**<ProxyUrl>proxy.somehost.com</ProxyUrl>**

**<ProxyPort>80</ProxyPort>**

**<ProxyLogin>ProxyUser</ProxyLogin>**

**<ProxyPassword>ExamplePassword</ProxyPassword>**

**<ProxyRequiresAuthorization>0</ProxyRequiresAuthorization>**

**<NtlmAuthorization>1</NtlmAuthorization>**

**</ProxySettings>**

### Настройки KAV Scanner Engine

Настройки KAV Scanner Engine определяются в разделе ServerSettings файла:

*cgpro\_home*/CGP-KAV/KAV/kavhttpd/etc/kavhttpd/kavhttpd.xml

**<ServerSettings>**

**<Flags>KAV\_SHT\_ENGINE\_KLAV | KAV\_SHT\_ENGINE\_KLAVEMU | KAV\_SHT\_ENGINE\_WMUF</Flags>**

**</ServerSettings>**

Подробнее о доступных флагах инициализации сервиса KAV:

|  |  |
| --- | --- |
| KAV\_SHT\_ENGINE\_KLAV | Битовый флаг, разрешающий загрузку нового основного антивирусного движка (KLAV). |
| KAV\_SHT\_ENGINE\_KLAVEMU | Битовый флаг, разрешающий загрузку продвинутого эвристического антивирусного движка (эмулятора KLAV).  Этот флаг следует установить, если вы собираетесь использовать расширенный эвристический режим сканирования. |
| KAV\_SHT\_ENGINE\_WMUF | Включение компонента фильтрации WMUF. Компонент использует базу данных WMUF. |
| KAV\_SHT\_ENGINE\_KSN | Включение использования Cloud Protection для проверки репутации файлов и URL-адресов.  Обратите внимание, что для включения проверки репутации URL-адресов необходимо установить флаги  должны быть установлены флаги KAV\_SHT\_ENGINE\_WMUF и KAV\_SHT\_ENGINE\_KSN.  Для включения проверки репутации файлов достаточно флага KAV\_SHT\_ENGINE\_KSN.  Обратите внимание, что, установив флаг KAV\_SHT\_ENGINE\_KSN, вы соглашаетесь на передачу файла с данными в "Лабораторию Касперского". |

**<KAVScanningSettings>**

**<Flags>KAV\_O\_M\_PACKED | KAV\_O\_M\_ARCHIVED | KAV\_O\_M\_MAILPLAIN | KAV\_O\_M\_COMPOSITE\_SCAN\_KSN | KAV\_O\_M\_HEURISTIC\_LEVEL\_DETAIL</Flags>**

**<Mode>KAV\_SKIP</Mode>**

**</KAVScanningSettings>**

Информация о возможных параметрах инициализации KAV Engine:

|  |  |
| --- | --- |
| KAV\_O\_M\_PACKED | Включение сканирования сжатых исполняемых файлов. |
| KAV\_O\_M\_ARCHIVED | Сканирование заархивированных файлов включено.  KAV Engine автоматически добавит флаг KAV\_O\_M\_PACKED к маске сканирования, если вы установили флаг KAV\_O\_M\_ARCHIVED. Включение сканирования архивных файлов также автоматически включает сканирование упакованных исполняемых файлов, но не наоборот. |
| KAV\_O\_M\_BACKUP | Включение сохранения копий зараженных объектов в резервном хранилище. Копии сохраняются до того, как оригинальные объекты будут вылечены или удалены.  При обнаружении составного зараженного объекта (например, архива, упакованного объекта, сообщения электронной почты, базы данных электронной почты) в резервное хранилище сохраняется копия всего объекта, а не только его зараженной части.  Когда одна из этих функций вызывается с этим флагом и обнаруживает зараженный объект, она автоматически помещает оригинальную копию зараженного файла в резервное хранилище, и только после этого выполняются дальнейшие операции, такие как лечение или удаление. Операции соответствуют выбранному режиму очистки. |
| KAV\_O\_M\_MAILPLAIN | Сканирование сообщений электронной почты включено.  Установка этого параметра сканирования обеспечивает поддержку следующих форматов файлов обычных сообщений электронной почты:  - Текстовые сообщения в формате RFC 822  - Файлы сообщений Microsoft Outlook (MSG)   * + - Любые файлы, закодированные с использованием текстовых кодировок UUE/XXE/base64, например архивы UUE. |
| KAV\_O\_M\_HEURISTIC\_ LEVEL\_SHALLOW | Включение расширенного эвристического анализатора кода. Этот анализатор основан на улучшенной технологии обнаружения; уровень сканирования будет более низким.  Уровень детализации продвинутого эвристического анализатора обеспечивает баланс между качеством сканирования и потреблением ресурсов операционной системы, а также продолжительностью сканирования. Чем выше уровень продвинутой эвристики, тем больше системных ресурсов требуется, и тем дольше длится сканирование. |
| KAV\_O\_M\_HEURISTIC\_ LEVEL\_MEDIUM | Включение расширенного эвристического анализатора кода. Этот анализатор основан на улучшенной технологии обнаружения; уровень сканирования будет средним.  Уровень детализации продвинутого эвристического анализатора обеспечивает баланс между качеством сканирования и потреблением ресурсов операционной системы, а также продолжительностью сканирования. Чем выше уровень продвинутой эвристики, тем больше системных ресурсов требуется, и тем дольше длится сканирование. |
| KAV\_O\_M\_HEURISTIC\_ LEVEL\_DETAIL | Включение расширенного эвристического анализатора кода. Этот анализатор основан на улучшенной технологии обнаружения; уровень сканирования будет более детальным.  Уровень детализации продвинутого эвристического анализатора обеспечивает баланс между качеством сканирования и потреблением ресурсов операционной системы, а также продолжительностью сканирования. Чем выше уровень продвинутой эвристики, тем больше системных ресурсов требуется, и тем дольше длится сканирование. |
| KAV\_O\_M\_HEURISTIC\_ LEVEL\_MAXIMUM | Этот флаг позволяет включить режим тщательного эвристического анализа в KAV Engine, который дает возможность вашему приложению получить еще более сложную эвристическую эмуляцию файлов и других объектов, которые вы сканируете.  Включение этого режима сканирования обеспечивает более высокую эффективность обнаружения за счет максимально возможной глубины эвристической эмуляции.  Чрезвычайно тщательная эвристическая эмуляция обеспечивается за счет снижения скорости сканирования. Использование этого режима сканирования может привести к значительному снижению скорости сканирования. |
| KAV\_O\_M\_URL | Обеспечивает сканирование каждого запрашиваемого адреса URL.  Когда веб-страница открывается в браузере, ее веб-адрес проверяется по базе данных Web Malicious Url Filtering (WMUF). Сюда входят веб-адреса, запрашиваемые из приложения браузера, и URL-адреса веб-страниц, запрашиваемые в открываемой веб-странице. Если при использовании открывается веб-страница, содержащая скрипт или iFrame, запрашивающий другой веб-адрес, по базе WMUF проверяется как адрес исходной веб-страницы, так и встроенные URL-адреса. |
| KAV\_O\_M\_COMPOSITE\_ SCAN\_KSN | Позволяет проверять многократно упакованные файлы с помощью облачного сервиса Kaspersky.  Многопакетные файлы, например архивные файлы или самораспаковывающиеся архивы, упакованные несколько раз, или файлы со встроенными объектами OLE могут быть проверены в облачном сервисе Kaspersky KSN.  Если KAV обнаруживает объект, сканируемый по локальной базе данных, KAV повторно сканирует его в облаке, даже если флаг KAV\_O\_M\_COMPOSITE\_SCAN\_KSN выключен. Повторное сканирование объекта в облачном сервисе обеспечивает защиту от ложных обнаружений.  Когда статус сканирования объекта с помощью локальной базы данных равен KAV\_S\_R\_CLEAN, KAV проверяет, был ли использован флаг KAV\_O\_M\_COMPOSITE\_SCAN\_KSN. Если флаг не использовался, проверки в облаке не выполняются. Если флаг был использован, KAV SDK повторно сканирует объект с помощью KSN. |

|  |  |
| --- | --- |
|  | Этот флаг должен использоваться с любой комбинацией следующих флагов:  - KAV\_O\_M\_PACKED  - KAV\_O\_M\_ARCHIVED  - KAV\_O\_M\_MAILBASES  - KAV\_O\_M\_MAILPLAIN  Если ни один из перечисленных флагов не указан,  KAV\_O\_M\_COMPOSITE\_SCAN\_KSN игнорируется.  Обратите внимание, что при включении KAV\_O\_M\_COMPOSITE\_SCAN\_KSN и  KAV\_SHT\_ENGINE\_KSN, вы соглашаетесь на передачу файла данных в Лабораторию Касперского. |
| KAV\_O\_M\_RECOGNIZE\_ FILE\_FORMAT | Включить распознавание формата файлов. |
| KAV\_O\_M\_RECOGNIZE\_ NESTED\_FILES\_FORMA T | Включить распознавание формата для вложенных файлов. |

Доступные режимы инициализации KAV Engine:

|  |  |
| --- | --- |
| KAV\_SKIP | Если при сканировании объекта обнаружено вредоносное ПО, KAV Engine не будет предпринимать никаких попыток лечения или удаления вредоносного объекта. Текущая задача сканирования будет пропущена. |

## Обновление лицензионных ключей KAS

Периодически внутренние ключи движков KAV нуждаются в обновлении. В этом случае АО «СБК» предоставит вам ключи и инструкции по их обновлению.

# Настройки производительности

## Рекомендации Лаборатории Касперского по настройке KAV

Для повышения производительности движка KAV рекомендуется установить значения ThreadsCount и ScannersCount равными количеству логических ядер в системе. Производительность снизится, если вы добавите больше потоков или сканеров, чем доступно логических ядер. В случае если оба параметра имеют разные значения, KAV Engine будет использовать минимальное из них.

Согласно статистике Лаборатории Касперского в 2018 году, если вы сканируете письма размером менее 5 МБ, вы покрываете 98% вредоносных программ, присутствующих в почтовом потоке.

Чтобы повысить производительность, можно исключить объекты, отфильтровав определенные типы файлов. Поскольку некоторые типы файлов не являются вредоносными по своей сути, есть возможность разрешить определенным типам файлов обходить механизм сканирования на основании их расширения.

Существует также ряд объектов с низким уровнем опасности, например видеопотоки, музыкальные файлы и изображения. Возможно, будет полезно избежать сканирования таких файлов.

По информации специалистов Лаборатории Касперского, было обнаружено несколько уязвимостей, например, в различных графических просмотрщиках и редакторах, обрабатывающих изображения, поэтому есть шанс, что вредоносное изображение воспользуется существующей уязвимостью. Однако, на данный момент было найдено всего несколько PoC-образцов подобных атак, и реальное заражение системы с помощью вредоносных изображений или видеофайлов - очень редкий случай по сравнению с другими типами объектов, используемых вредоносным ПО для распространения через Интернет.

Эти типы содержимого можно исключить:

text/plain; text/css; image/bmp;

image/gif;

image/png; image/jpg; audio/mp3;

Аналитики Лаборатории Касперского настоятельно рекомендуют сканирование следующих типов содержимого:

text/html application/octet-stream application/x-javascript

application/x-shockwave-flash

**Примечание для администраторов CGPro:** Внешний помощник CGP-KAV будет проверять любое письмо, отправленное на обработку CGPro. Правило SMTP, вызывающее помощника, отвечает за выбор SMTP-потока, направляемого помощнику. Предыдущие фильтры могут использоваться для обнаружения и маркировки писем по типу содержимого, чтобы иметь возможность исключить/включить их в SMTP-правило, вызывающее внешний помощник CGP-KAV.

## Установка в очередь CGPro и рабочие потоки внешнего помощника

Теоретически количество **worker\_threads** должно соответствовать количеству потоков обработчиков почты CGPro, определенному в:

Почта → Очередь → Установка в очередь → Обработчики

Теоретическое количество писем в секунду, которое может обработать Kaspersky External-Helper, составляет worker\_threads+5. Время, необходимое для проверки писем Kav, может уменьшить этот теоретический предел.

+5 относится к дополнительной работе, которую External-Helper может выполнить в течение секунды. Она ограничена 5 статическим сном в 0,2 секунды, чтобы сохранить использование процессора в ожидании, пока доступные рабочие потоки закончат свою работу.