

Kaspersky® Anti-Spam

Kaspersky Anti-Spam 3.0 – продукт для защиты пользователей почтовых систем компаний и интернет-провайдеров от массовой незапрошенной корреспонденции – спама.

Обмен электронной почтой неизбежно приводит к тому, что адреса пользователей попадают в базы данных злоумышленников. В результате на эти адреса приходит масса непрошенной анонимной корреспонденции. Компании сталкиваются с ощутимыми потерями рабочего времени сотрудников, вынужденных ежедневно удалять из своих почтовых ящиков десятки и сотни нежелательных писем. А также – с оплатой лишнего трафика, перегрузкой инфраструктуры почтовых систем, повышенным риском вирусных и мошеннических атак посредством электронной почты.

Используя интеллектуальные технологии распознавания спама, основанные на опыте защиты крупнейших почтовых систем, Kaspersky Anti-Spam 3.0 помогает пользователям почтовой системы избавиться от получения нежелательных массовых рассылок.

Основные преимущества

Передовые технологии защиты от спама. Продукт использует собственную интеллектуальную технологию для распознавания нежелательной корреспонденции. Она включает комплексный набор методик определения спама: подключаемые черные списки (DNSBL), проверки по SPF и SURBL, анализ формальных атрибутов сообщения, лингвистические эвристики, обновляемые в режиме реального времени сигнатуры и распознавание графического спама.

Скорость реакции на новые спамерские рассылки. Спам-лаборатория «Лаборатории Касперского» работает в круглосуточном режиме, ежеминутно добавляя в базы обнаруженные новые образцы спама и новые правила лингвистического анализа. Технология UDS (Urgent Detection System), реализованная в Kaspersky Anti-Spam 3.0, позволяет приложению получать данные о последних спамерских рассылках уже через секунду после их обнаружения – при этом не увеличивая трафик.

Комфортная работа администратора. Веб-интерфейс Kaspersky Anti-Spam 3.0 позволяет администратору продукта управлять им и настраивать его из любой точки. Интуитивно понятные элементы управления облегчают освоение возможностей приложения. А новый модуль статистики делает простым и быстрым процесс анализа уровня почтовых потоков и доли спама в нем.

Производительность и масштабируемость. Новое фильтрующее ядро Kaspersky Anti-Spam 3.0 потребляет ресурсы системы в 4-5 раз меньше предшественника, а объем загружаемых из Сети баз обновлений сокращен в 3,5 раза. Kaspersky Anti-Spam 3.0 успешно защищает как небольшие сети малых предприятий, так и огромные почтовые системы – такие как Mail.Ru, где ежедневно фильтруется до 70 млн. сообщений объемом до 500 ГБ.



Функции Защита от спама

Списки. Письмо проверяется на вхождение IP-адреса отправителя в черные списки, которые ведут провайдеры и различные общественные организации (так называемые DNSBL – DNS-based Blackhole List). Администратор Kaspersky Anti-Spam 3.0 может также вести свои белые списки («списки друзей»), от которых почта принимается всегда, минуя этапы анализа.

SPF и SURBL. В процессе фильтрации может учитываться авторизация отправителя по технологии SPF (Sender Policy Framework). В дополнение к DNSBL, блокирующим спамерские IP-адреса, используется технология SURBL (Spam URI Realtime Block List), выявляющая спамерские URL в теле сообщения.

Анализ формальных признаков письма. Модификация адреса отправителя, слишком много получателей или их отсутствие, отсутствие IP-адреса в системе интернет-адресов DNS и т.п. – все это является признаками спамерского сообщения. Осуществляется анализ по размеру и формату сообщения.

Лингвистические эвристики. Проверяется наличие в письме признаков спамерского содержания: определенного набора и распределения по письму специфических словосочетаний. Причем сервер фильтрации анализирует не только текст самого письма, но и вложения.

Сигнатурный анализ. По каждому спамерскому письму может быть автоматически создана так называемая лексическая сигнатура, позволяющая распознать это письмо даже с небольшими модификациями. Такие сигнатуры добавляются в базы лингвистической лаборатории.

Обнаружение графического спама. Процесс создания и добавления графических сигнатур схож с процессом создания обычных образцов спама, но в данном случае работа ведется с изображениями, используемыми спамерами как в теле письма, так и в виде вложения.

UDS-запросы в режиме реального времени. Если некое письмо не получило однозначной оценки (спам, не-спам), выполняется запрос к UDS-серверу. Он содержит данные о самых последних рассылках; информация о новом спае добавляется в тот же момент, когда он обнаружен спам-аналитиком.

Администрирование

Тонкая настройка. Администратор может настраивать строгость фильтрации, белые и черные списки отправителей, подключать/отключать действие тех или иных правил фильтрации, включать блокирование почты с кодировками восточных языков.

Управление группами пользователей. Администратор продукта может задавать определенные группы пользователей – причем как списком адресов, так и с помощью масок доменов (например, *@???.domain.com). Для каждой группы могут быть заданы различные настройки и правила фильтрации и различная бизнес-логика обработки сообщений.

Бизнес-логика фильтрации. Можно настроить различные действия приложения по отношению к детектированному спаю. Письмо может быть автоматически удалено, отправителю может быть отправлен отказ в приеме сообщения, письмо или его копия может быть перенаправлено в карантинную папку. К теме или служебным заголовкам письма может быть добавлена заданная администратором метка, чтобы письмо доставлялось получателю и фильтровалось на уровне почтового клиента.

Обновление баз. Обновление основных баз производится по расписанию, заданному администратором (по умолчанию, каждые 20 минут). При этом при необходимости приложение в режиме реального времени обращается к серверу UDS-обновлений с запросом относительно подозрительных сообщений.

Подробные отчеты. Администратор может контролировать работу приложения, состояние защиты от спама и статус лицензий, используя наглядные HTML-отчеты или просматривая лог-файлы Linux. Возможен экспорт в формат CSV или Excel. Доступны отчеты об общем почтовом трафике и различных долях спама в нем за заданный период.

Системные требования

Аппаратные требования

- процессор Intel Pentium III 500 МГц или выше (рекомендуется Intel Pentium IV 2,4 МГц);
- не менее 512 МБ свободной оперативной памяти (рекомендуется 1 ГБ).

Программные требования

Почтовые системы:

- Sendmail 8.13.5 с поддержкой Milter API
- Postfix 2.2.2
- Qmail 1.03
- Exim 4.50

- Communicate Pro 4.3.7

Операционные системы:

- RedHat Linux 9.0
- RedHat Fedora Core 3
- RedHat Enterprise Linux Advanced Server 3
- SuSe Linux Enterprise Server 9.0
- SuSe Linux Professional 9.2
- Mandrake Linux version 10.1
- Debian GNU/Linux version 3.1
- FreeBSD version 4.10
- FreeBSD version 5.4

Необходимы установленные утилиты bzip2, which, интерпретатор языка Perl.

Язык локализации продукта: английский, русский (только документация).

Версия продукта: 3.0

Для получения любой дополнительной информации, пожалуйста, обращайтесь:

Россия, 123060, Москва,
1-й Волоколамский проезд, д.10, стр. 1

Телефон/факс: +7 495 797 8700

info@kaspersky.com;
www.kaspersky.ru;
www.viruslist.ru

© ЗАО «Лаборатория Касперского»
Антивирус Касперского — зарегистрированная торговая марка ЗАО «Лаборатория Касперского».

Все другие названия являются торговыми марками соответствующих владельцев.