

# Антиспамовое решение «Спамооборона», версия 1.5.0

## Описание продукта.

### 1. Введение

**Спамооборона** – это программный продукт по защите электронной почты от нежелательной корреспонденции (спама), устанавливаемый на почтовых серверах на платформе UNIX и предназначенный для корпоративных пользователей.

Разработчик – компания Яндекс.

Технология разработана и проверена на публичном сервисе Яндекс.Почта, одном из лучших в плане защиты от спама.

### 2. Технические характеристики

Качество фильтрации:

Свыше 90% (по результатам тестирования 93-98%)

Характеристики продукта:

- низкая ресурсоемкость
- высокая производительность
- возможность занесения спамого веса письма в его тему
- управление прочими настройками записи в заголовок письма или журнал
- автоматизация труда администратора в процессе эксплуатации, за счет возможности автоматического заполнения пользовательских данных
- единый диалоговый интерфейс установки/удаления/настройки
- пороги «отказ/спам/не спам»
- персонализация белых списков и порогов отказа
- специальная unlimited ISP версия для провайдеров

Главные преимущества продукта:

- полный анализ письма
- качественная фильтрация как иностранного, так и русскоязычного спама.

Поддерживаемые платформы:

- FreeBSD/i386 4.9 и выше
- FreeBSD/i386 5.3 и выше
- FreeBSD/i386 6.0 (с библиотеками compat\_freebsd5x)
- Linux Debian 3.1/i386 (ядро 2.6)
- Linux Fedora Core 3, 4/i386
- Linux RedHat Enterprise Server/Advanced Server 4/i386
- Linux Slackware 10.2/i386
- Linux SuSe 10/i386
- ASPLinux 11/i386

(RPM дистрибутив для Linux Fedora Core может быть использован для установки на прочих Linux-системах с ядром 2.6 и glibc 2.3.5 и выше)

Поддерживаемые почтовые сервера:

- SendMail 8.11 и выше (собранный с поддержкой militer API)
- NetQmail 1.0.5 или QMail версии 1.0.3 (с установленным патчем QmailQueue)
- CommuniGate Pro версии 4.x
- Postfix 2.1 и выше
- Exim 4 и выше (используя local\_scan. c)

Минимальные аппаратные требования:

Intel Pentium III 500MHz, 512Mb RAM, 100Mb HDD (400Mb в случае локальных баз)

Рекомендованная конфигурация (до 15 писем/сек):

Intel Pentium IV 1,5GHz 1Gb RAM 500Mb HDD

Продукты и пакеты сторонних производителей, необходимые для работы:

- libmysqlclient
- MySQL Server 4.1.x (опционально - в случае локальной базы шинглов)
- rblndsd (опционально - в случае локальной базы черных списков)
- Bind9
- Perl
- Dialog

Подробно системные требования, описание технических характеристик и информация, где можно найти необходимые пакеты сторонних производителей, указаны в документации и могут быть получены по указанному в конце документа адресу.

### **3. Описание**

Продукт является по сути экспертным модулем, главная задача которого – качественное распознавание спама, путем разметки писем флагом спам/не спам.

Продукт не является полнофункциональным почтовым сервером, в функции которого входят прием почты, пересылка или доставка сообщений в почтовые ящики конечных пользователей.

Функции по пересылке почтовых сообщений выполняет почтовая система (MTA), установленная на сервере.

Принятие решений о дальнейшей судьбе писем, определенных как спам, оставляется за почтовой системой пользователя (то есть, почтовым сервером и почтовые клиентами на местах) и настраивается любым удобным пользователю способом согласно требований политики безопасности компании пользователя.

Продукт состоит из:

- устанавливаемой на сервере пользователя клиентской части
- функционирующей на сайте компании-разработчика серверной части, обеспечивающей выпуск обновлений и обработку запросов в случае удаленного доступа к базам данных на сервере

Устанавливаемая на сервере пользователя часть продукта включает:

- средство администрирования
- *опционально* – локальную копию текущей базы данных “шинглов” – ключей-характеристик писем
- *опционально* - локальную копию базы данных “черных списков” – адресов источников спама
- локальную базу данных или файлы пользовательских данных, включающих список защищаемых почтовых адресов, белый список, таблицу порогов отказов
- механизм обновления данных
- сервисы фильтрации почты
- сервис лицензирования
- файлы конфигурации
- дополнительные утилиты

а также корректирует некоторые системные файлы, с целью регистрации продукта и его интеграции с текущей конфигурацией сервера.

Таким образом, продукт может быть установлен в одной из следующих конфигураций:

- локальная база “шинглов” + локальная база “черных списков”  
используется, когда компания не экономит на трафике или в случае крайне большого потока корреспонденции
- локальная база “шинглов” + удаленный доступ к базе “черных списков” на сервере компании-разработчика  
основной рекомендованный вариант, среднемесячный объем обновлений – около 150 Мб
- удаленный доступ к базе “шинглов” на сервере компании-разработчика + локальная база “черных списков”  
не оправдан в силу большого трафика обновлений базы “черных списков”
- удаленный доступ к базе “шинглов” на сервере компании-разработчика + удаленный доступ к базе “черных списков” на сервере компании-разработчика  
оправдан в случае небольшого потока корреспонденции

Изменить конфигурацию на альтернативную после установки продукта можно в любой момент путем выбора соответствующей директивы в сценарии установки.

После установления соединения с интерфейсом МТА «Спамооборона» получает от почтового клиента письмо, анализирует его и:

- в случае, если адрес не входит в список защищаемых - возвращает почтовому клиенту без анализа с пометкой “пропущено”
- в случае, если адрес в списке пользователей, включен режим отбраковки явного спама, и письмо признается явным спамом – отвергается, с уведомлением отправителя о недоставке (по умолчанию отключен)
- в остальных случаях - анализирует письмо и возвращает его почтовому серверу с пометкой спам/не спам

Во время анализа письмо последовательно проверяется набором правил фильтрации (около 3000), каждое из которых, при выполнении его условий, добавляет свой вес в общий спамовый вес письма.

Принятие решения производится путем сравнения полученного веса письма с порогами «отказ / спам / не спам».

Пометка «пропущено без анализа/спам/не спам» ставится в специально добавляемом в заголовок письма поле, также как информация о версии решения и набранном итоговом весе письма.

Коллекция правил фильтрации поставляется компанией-разработчиком в закрытом для просмотра виде и поддерживается в актуальном состоянии разработчиком.

Часть правил являются «отбеливающими», доступны для просмотра и коррекции и отвечают за признание письма не спамом, вычитая свой вес из совокупного веса письма.

Тривиальным примером правил фильтрации может являться наличие некоторого запрещенного слова, примером отбеливающих – признаки службы рассылок, например [Subscribe.ru](http://Subscribe.ru).

Большинство же правил являются композицией и предназначены для определения всевозможных уловок спамеров.

Особая группа правил использует базу шинглов, специальных контрольных сумм, собираемых по спамерским письмам, которые являются характеристикой массовости рассылки письма, и черные списки адресов, для которых известна практика рассылки спама.

Метод построения шинглов является ноу-хау компании-разработчика, он позволяет не просто получать слепок спамового письма, но отождествлять все письма-клоны, получаемые из оригинала путем незначительной модификации.

Базу черных списков составляют как некоторые публичные черные списки, так и собственный черный список компании-разработчика, постоянно пополняемый и поддерживаемый в актуальном состоянии.

Таким образом, нет ни одного решающего критерия, все методы вносят свой вес, и даже принятие письма от запрещенного адресата не приводит к его немедленной маркировке как спам, а только при наличии других характеристик спамового характера письма.

Актуальность информации и своевременный выпуск обновлений обеспечивается специальными автоматизированными службами сбора, анализа и проверки данных, а также службой реагирования на запросы пользователей Яндекс.Почты с целью повышения качества фильтрации и предотвращения ложных срабатываний.

За счет сбора информации на территории России данное решение особенно выгодно отличается от конкурентов путем отличного качества фильтрации русскоязычного спама, при этом не в ущерб качеству фильтрации иностранного.

Все это обеспечивает заявленное, пожалуй, лучшее на данный момент качество фильтрации.

Среди остальных характеристик продукта:

- Возможность изменения порогов «отказ/ спам /не спам»
- Возможность добавления пометки “спам” а также веса в теме письма
- Механизм импорта/автозаполнения списка пользователей из почтового журнала
- Персонализация порогов отказа, то есть создание личных порогов для выбранных одиночных адресов или целых доменов

- Механизм белого списка
- Персонализация белого списка, то есть возможность назначить индивидуальные отбеливающие веса для отдельных адресов или доменов
- Механизм импорта/автозаполнения белого списка из почтового журнала

Администрирование системы производится через удобный диалоговый интерфейс.

При установке продукт прописывает в системе ряд своих параметров, в том числе устанавливающих расписание получения обновлений, что далее используется механизмом обновления и может быть изменено в любой момент системным администратором компании пользователя согласно политике безопасности компании пользователя с целью большей оперативности или большей экономии трафика.

#### **4. Лицензирование**

Лицензирование производится по числу защищаемых почтовых адресов. Каждый адрес-синоним считается как отдельный почтовый адрес.

Адреса, подлежащие защите, прописываются / импортируются в список пользователей.

Обновление данных, используемых при фильтрации, производится только после получения лицензионного ключа при активации продукта.

#### **5. Дополнительная информация**

Детальное описание продукта:

<http://www.dialognauka.ru/so>

Полная документация:

<http://www.antivir.ru/statdir/stat.php?id=SOadminguide15>

Свободно распространяемая полнофункциональная ознакомительная версия:

<http://www.antivir.ru/download.phtml?id=7>