Спамооборона

Серверное решение для фильтрации спама

Руководство администратора

Яndex

so.yandex.ru

Правообладателем исключительных прав на настоящую документацию «Руководство администратора» (далее — «документация») является ООО «ЯНДЕКС». Документация предназначена исключительно для целей ознакомления и/или использования по прямому назначению в качестве руководства для эксплуатации программы для ЭВМ «Спамооборона» (© 2005 ООО «ЯНДЕКС»). Ни документация, ни какая бы то ни было ее часть не могут быть использованы для иных целей, а также воспроизведены, копированы, распространены, переведены и/или иным образом переработаны без письменного разрешения правообладателя.

© 2005 ООО «ЯНДЕКС»
Адрес: г. Москва, ул. Губкина, д.3
Адрес для уведомлений: 119991, г. Москва, ул. Вавилова, д.40
Телефон: +7 (095) 974-35-55, факс: +7 (095) 974-35-65
www.yandex.ru

Издание, распространение и техническая поддержка программы для ЭВМ «Спамооборона» осуществляется эксклюзивным дистрибьютором — ЗАО «ДиалогНаука».

117105, Москва, ул. Нагатинская, д.1, бизнес-центр «Ферейн», офис 810.
Телефон: +7 (095) 980-67-76
Телефон/факс: +7 (095) 980-67-75
Эл. почта (отдел продаж): sales@dialognauka.ru
Эл. почта (отдел по работе с партнерами): dealers@dialognauka.ru

Редакция документа от **15.12.2005**. Содержание соответствует программе **версии 1.5 (бета)**.

Содержание

1. ЧТО НУЖНО ДЛЯ УСТАНОВКИ «СПАМООБОРОНЫ» 5

1.1 Аппаратные требования 5
1.2 Поддерживаемые операционные системы 5
1.3 Поддерживаемые почтовые серверы (MTA) 6
1.4 Необходимые пакеты сторонних производителей 6
1.5 Перед установкой 7

2. УСТАНОВКА И УДАЛЕНИЕ «СПАМООБОРОНЫ» 9

2.1 Состав дистрибутива 9
2.2 Порядок установки 9
2.3 Установочный сценарий 9
2.4 Активация продукта 15
2.5 Получение обновлений базы знаний 16
2.6 Интеграция с MTA 19
2.7 Заполнение списка пользователей 22
2.8 Запуск «Спамооборoны» 23
2.9 Результаты проверки письма 23
2.10 Удаление «Спамооборoны» 24
2.11 Замена версии «Спамооборoны» на более новую 25

3. ВОЗМОЖНОСТИ НАСТРОЙКИ СИСТЕМЫ 27

3.1 «Белый список» 27
3.2 Доверенные сети 28
3.3 Отказ от приема спама 28
3.4 Персональные настройки отказа от нежелательных писем 29
3.5 Безусловная доставка 30
3.6 Флаг результата проверки 30
3.7 Получение обновлений 30

4. СОВЕТЫ ПО ЭКСПЛУАТАЦИИ 33

4.1 Что делать при пропуске спама 33
4.2 Что делать при ложных срабатываниях 34
4.3 Что делать при большом потоке почты 35

5. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА 36

ПРИЛОЖЕНИЕ 1. АДМИНИСТРАТИВНЫЙ СЦЕНАРИЙ ADM_SO 37

1.1 REQUEST STATUS 37
1.2 STARTUP SPAMOOBORONA 38
1.3 STOP SPAMOOBORONA 38
1.4 RELOAD CONFIG FILES 38
1.5 DATABASE SETUP 39
1.6 SPAMOOBORONA PARAMETERS 40
1.7 WHITE/BLACK LIST DNS CHECK 43
1.8 WHITELIST SETUP 43
1.9 UPDATES SETUP 45
1.10 REJECT VALUES TABLE 49

ПРИЛОЖЕНИЕ 2. ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ИХ РЕШЕНИЕ 51

1. Что нужно для установки «Спамообороны»

Для установки «Спамообороны» необходимо иметь квалификацию системного администратора Unix: иметь опыт настройки одного из поддерживаемых почтовых серверов (Sendmail, Qmail, Postfix, CommuniGatePro или Exim), а также сервера доменных имён (DNS) ISC BIND (named). Кроме того, будут полезны знакомство с администрированием сервера MySQL и навыки редактирования зон DNS.

1.1 Аппаратные требования

Минимальные требования (пропускная способность — одно письмо в секунду):

- Процессор Intel Pentium III с частотой не менее 500 МГц;
- Оперативная память — не менее 512 МБ;
- Свободное дисковое пространство — не менее 100 Мб (400 Мб при работе с локальной копией базы знаний).

Рекомендованной конфигурацией является: Intel Pentium 4, 1,5 ГГц, 1Гб ОЗУ. Такой сервер сможет обрабатывать до 15 писем в секунду. Фактическая производительность «Спамообороны» зависит от многих факторов, в том числе от содержания писем.

В большинстве случаев «Спамооборона» не требует выделенного сервера.

Измерения производились с использованием локальных баз знаний и MTA sendmail.

1.2 Поддерживаемые операционные системы

«Спамооборона» поддерживает следующие операционные системы (ОС):

- FreeBSD/i386 4.9 и выше;
- FreeBSD/i386 5.4;
- FreeBSD/i386 6.0 (с библиотеками compat_freebsd5x);
- Linux Debian 3.1/i386 с ядром версии 2.6;
- Linux Fedora Core release 4/i386 (установка на release 3 также возможна, но потребуется установка сервера MySQL версии 4.1, отличной от штатной для release 3 версии MySQL 3.23).

Внимание: использование сочетания Linux Fedora Core release 3 и MySQL версии 4.1 может привести к необходимости обновления некоторых системных библиотек.

Если вы используете операционную систему, которой нет среди вышеперечисленных, обратитесь в Службу технической поддержки — мы постараемся учесть ваш запрос при развитии программы.

1.3 Поддерживаемые почтовые серверы (MTA)

Mail Transfer Agent (MTA) — программное обеспечение для межсерверного обмена электронной почтой по протоколу SMTP. Здесь и далее под почтовыми серверами и системами подразумевается MTA.

«Спамооборона» работает со следующими MTA:

- Sendmail версии 8.11.x и старше (собранный с поддержкой milter API) — http://www.sendmail.org;
- Qmail версии 1.0.3 (с установленным патчем QMAILQUEUE http://www.qmail.org/qmailqueue-patch) или NetQmail 1.0.5 — http://www.qmail.org;
- CommuniGate Pro версии 4.x — http://www.stalker.com/CommuniGatePro.
- Postfix версии 2.2 и выше — http://www.postfix.org.

  Возможно использование с MTA Postfix 2.1, в этом случае в файле конфигурации master.cf потребуется убрать параметр -a.

- Exim версии 4 и выше — http://www.exim.org

  Потребуется перекомпиляция MTA Exim с использованием local_scan.c, входящего в комплект Спамообороны.

Если вы используете MTA, которого нет среди вышеперечисленных, обратитесь в Службу технической поддержки — мы постараемся учесть ваш запрос при развитии программы.

1.4 Необходимые пакеты сторонних производителей

Для корректной работы «Спамообороны» на сервере должны быть установлены следующие дополнительные свободно распространяемые программные пакеты:

- MySQL Server — http://www.mysql.org;

  Сервер MySQL требуется только при использовании локальной копии БД метрик писем (шинглов). Следует использовать сервер MySQL версии 4.1 с параметром –old-passwords. Подробнее о режимах доступа к обновлениям см. п. 2.5.

- Bind9 — http://www.isc.org/index.pl?/sw/bind/bind9.php;

  во FreeBSD используется Bind, входящий в состав системы.

- Rbldnsd — http://www.corpit.ru/mjt/rbldnsd/

Rbldnsd требуется только в том случае, когда используются DNS-запросы к локальной копии «черного списка», получаемой по rsync. Подробнее о локальных и удалённых данных см. п. 2.5.

- Perl — http://www.perl.org;

  Требуются модули DBI, DBD::Mysql.

- Dialog — http://invisible-island.net/dialog/

  во FreeBSD используется dialog, входящий в состав системы.

Пожалуйста, установите и настройте эти программы до инсталляции «Спамообороны».

Сценарий install.sh попытается самостоятельно установить эти пакеты, если не обнаружит их на вашем сервере, но это не всегда возможно сделать автоматически.

1.5 Перед установкой

Для установки «Спамообороны» требуются права пользователя `root` в операционной системе и аналогичные права на сервере MySQL.

Перед началом установки продукта необходимо выполнить следующие действия:

- Проверить наличие установленных пакетов:
  - Для FreeBSD 4/5:
    - expat; libiconv; gettext
    - mysql-server-4.1.x (если используется локальная копия БД шинглов, см. п. 1.4);
    - popt; rsync; rbldnsd (если используется локальная копия «чёрного списка», см. п. 1.4);

    «Спамооборона» не предназначена для эксплуатации в виртуальных средах, таких как jail во FreeBSD.
  - Для Linux Debian:
    - bind9; libexpat1; gettext; wget; bzip2; pmake; dialog; dnsutils, lockfile;
    - mysql-server-4.1 (если используется локальная копия БД шинглов, см. п. 1.4);
    - libpopt0; rsync; rbldnsd (если используется локальная копия «чёрного списка», см. п. 1.4);
  - Для Linux Fedora Core:
    - bind; gettext; wget; bzip2; pmake; dialog; lockfile; compat-libstdc++;

- mysql-server (или mysql-server-standard для FC release3) (если используется локальная копия БД шинглов, см. п. 1.4);
- rsync; rbldnsd (если используется локальная копия «чёрного списка», см. п. 1.4);

Сценарий install.sh попытается самостоятельно установить эти пакеты, если не обнаружит их на вашем сервере, но это не всегда возможно сделать автоматически.

- Убедиться, что сервер MySQL запущен (если используется локальная копия БД шинглов, см п. 1.4).
- Убедиться, что ваш почтовый сервер находится в рабочем состоянии (принимает и отправляет почту).

  Устанавливайте «Спамооборону» в период наименьшего потока почтовых сообщений.

- Сохранить резервные копии конфигурационных файлов почтовой системы.

  Прежнюю конфигурацию почтовой системы будет легко восстановить — инсталлятор сохранит резервную копию файла макроконфигурации Sendmail .mc с расширением .so-bak. Конфигурации других MTA установочный сценарий не изменяет.

- Убедиться, что через сервер со «Спамообороной» проходит весь почтовый поток. Если вы принимаете почту через несколько серверов, то желательно, чтобы «Спамооборона» была установлена на все внешние серверы.

  Если через сервер с установленной «Спамообороной» проходит не весь почтовый поток, часть корреспонденции может избежать фильтрации. Если вы используете несколько MX (Mail eXchanger – сервер входящей почты) – например, используете почтовый сервер своего провайдера в качестве вторичного MX, то получаемая им почта должна в дальнейшем попадать на сервер с установленной «Спамообороной». Если «Спамооборона» установлена на несколько серверов в цепочке доставки почты, имеет смысл на каждом последующем сервере вписывать предыдущие в переменную general.non-check-wl, чтобы не тратить ресурсы на повторные проверки (см. п. 3.2).

2. Установка и удаление «Спамообороны»

2.1 Состав дистрибутива

В состав дистрибутива входит установочный пакет «Спамообороны», лицензионное соглашение, настоящее руководство, сценарий установки, настройки, обновления и удаления `install.sh`, а также пакет служебных данных «Спамообороны».

На компакт-диске «Спамообороны» записаны версии продукта для всех поддерживаемых операционных систем и MTA.

2.2 Порядок установки

1) Проверьте права доступа и наличие необходимых пакетов (см п. 1.4 и 1.5).
2) Установите пакет «Спамооборона», используя сценарий `install.sh`.
3) Получите лицензионный ключ и выполните активацию продукта.
4) Загрузите базу знаний с сервера компании «Яндекс».
5) Завершите настройку, воспользовавшись административным сценарием `adm_so`.
6) Выполните интеграцию «Спамообороны» с почтовой системой.
7) Заполните список ящиков, для которых осуществляется фильтрация.

2.3 Установочный сценарий

Первым этапом установки «Спамообороны» является запуск установочного сценария. Запустите сценарий `install.sh` и выберите пункт меню «Install».

Резервные копии системных файлов, таких как resolv.conf, named.conf, сценарий сохраняет с расширением .so-bak

Рис. 1.

Проверьте параметры установки и выберите нужный вам вариант (выбранные параметры установки будут указаны в квадратных скобках):

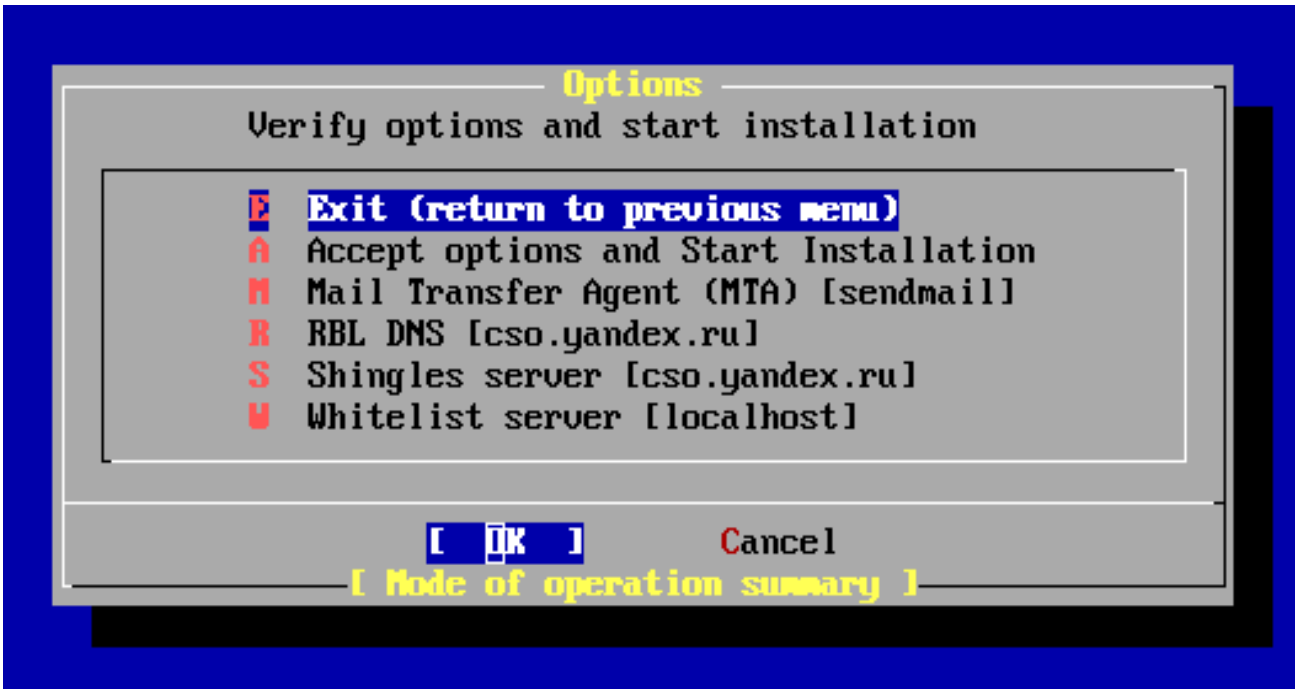


Рис. 2.

Рекомендуемый режим работы «Спамообороны» — с использованием удалённого сервера RBL DNS (установлен по умолчанию) и метрик писем (шинглов) на сервере cso.yandex.ru

(также установлен по умолчанию).

> «Шингл» — это специальным образом рассчитываемая метрика письма, позволяющая выявлять массовые рассылки. Алгоритм расчета шинглов основан на определении уникальных характеристик схожих сообщений.
>
> RBL (Realtime Block List) DNS — это список адресов IP открытых почтовых релеев, прокси-серверов и плохо администрируемых сетей, из которых рассылается спам. В своей работе «Спамооборона» использует несколько RBL, в т.ч. и собственный список, создаваемый на основе работы службы Яндекс.Почта.

Вы можете изменить настройки шинглов и RBL DNS с помощью пунктов меню Options:

- *«RBL DNS»* . Ответьте «Yes» для работы с удаленным сервером RBL; ответив «No», вы укажете «Спамообороне», что она должна работать с локальной копией RBL с помощью rbldnsd и BIND, при этом обновление таблиц RBL будет происходить по протоколу rsync:

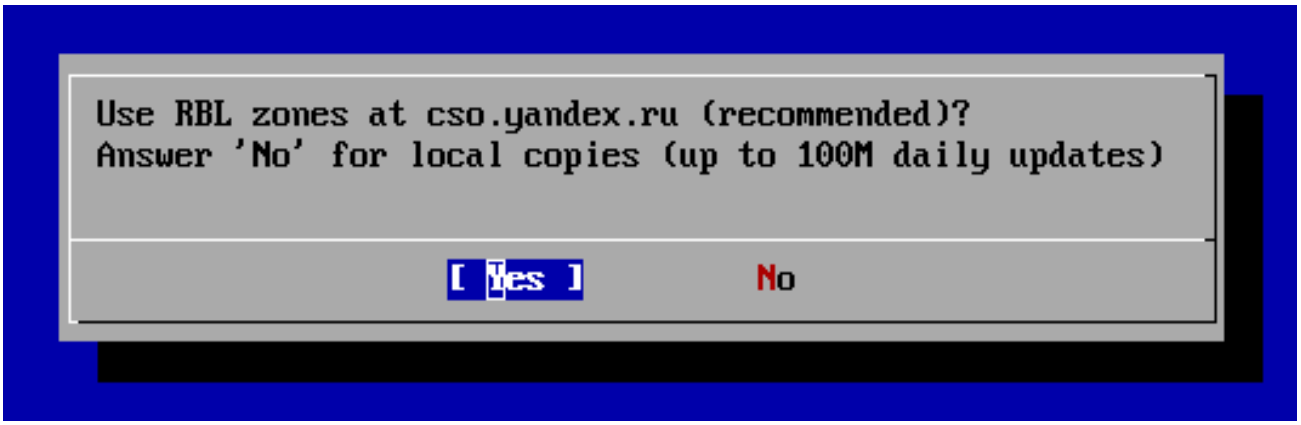


Рис. 3.

> Использование локальной копии RBL зон сокращает время обработки запроса, однако требует регулярной загрузки обновлений локальной копии черных списков, что может создать существенную дополнительную нагрузку по трафику (вплоть до 100Мб ежедневно).
>
> До того как выбирать режим доступа к RBL, определитесь, какой вариант для вас является предпочтительным (см. п. 3.7).
>
> После установки обязательно проверьте содержимое файлов /etc/resolv.conf и /etc/namedb/named.conf (/etc/named.conf в Linux) локального сервера DNS на предмет корректности внесенных «Спамообороной» изменений.

- *«Shingles server»* Ответьте “Yes” для работы с удаленным MySQL-сервером cso.yandex.ru; ответив “No”, вы укажете «Спамообороне», что она должна обращаться

к локальной копии БД шинглов. Обновление шинглов будет происходить по протоколу rsync:

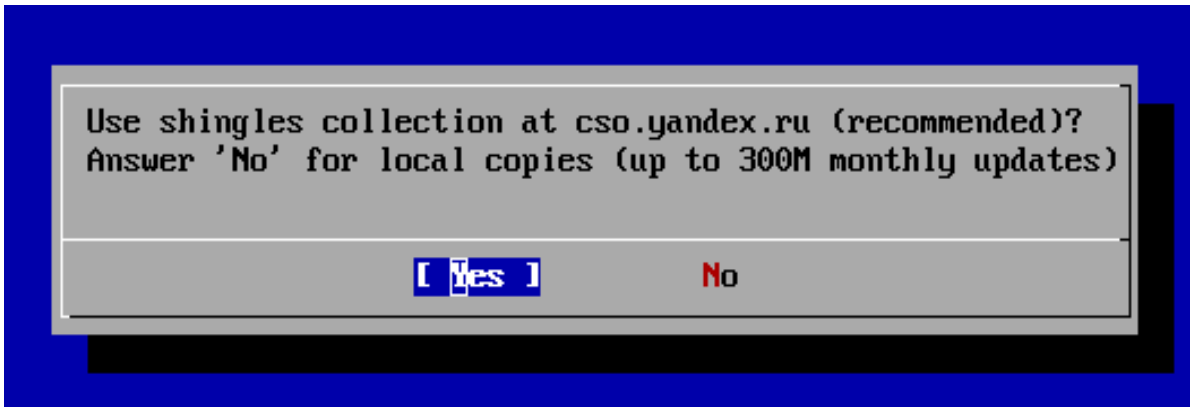


Рис. 4.

Использование локальной копии БД шинглов сокращает время обработки запроса, однако требует регулярной загрузки обновлений локальной копии БД. Проверка «он-лайн» может оказаться более эффективной за счет более оперативного обновления информации в основной базе. Кроме того, локальная копия БД означает загрузку 3Мб обновлений в сутки, а также 20Мб дополнительно с интервалом в 1-4 недели.

В процессе работы с шинглами «Спамооборона» отправляет копии подсчитанных шинглов на сервер для накопления статистической информации по перехвату спама. Шинглы являются контрольными суммами, из которых невозможно восстановить оригинальное содержание или путь следования письма. Отправка шинглов не нарушает информационную безопасность и конфиденциальность почтового сервера.

После выбора пункта меню «Accept options and Start installation» начинается непосредственно установка. В процессе установки появятся следующие диалоговые окна:

- *«Enter real Internet address which will be granted to access updates».* Укажите внешний адрес IP сервера, на котором предполагается использование «Спамообороны». Если сервер расположен в локальной сети, внешним адресом может быть адрес NAT-сервера, а не самого сервера «Спамообороны». Именно этот адрес IP должен получить доступ к обновлениям базы знаний на сервере cso.yandex.ru:

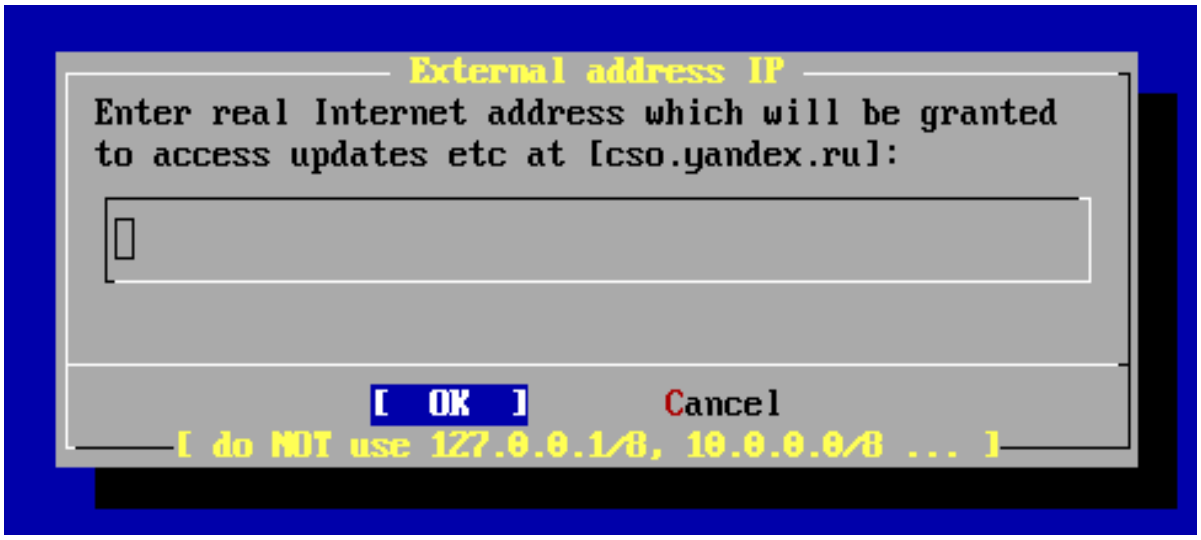


Рис. 6.

- *«Those domains will be supported:».* Сценарий выведет список доменов. Проследите, чтобы в данном списке были указаны все ваши домены, для которых должна осуществляться фильтрация спама:

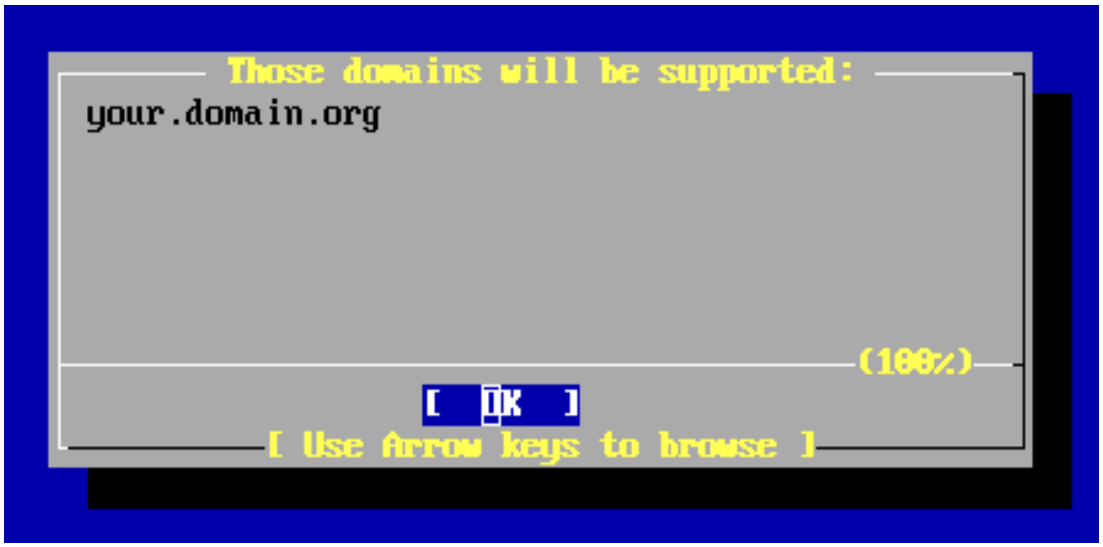


Рис. 7.

Если список неполон, введите все нужные домены (по одному на строку), ответив «Yes» на вопрос «Do you want to edit the domain list?»:

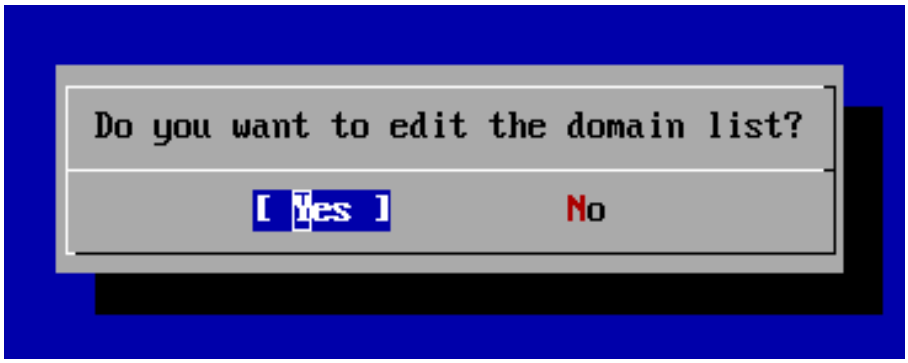


Рис. 8.

Завершите редактирование списка выходом из текстового редактора (вызывается редактор, указанный в переменной окружения EDITOR, либо vi, если переменная окружения не установлена). После окончания установки (но до получения ключа) вы сможете отредактировать список обслуживаемых доменов в файле `PREFIX/spam.ini` (что такое PREFIX — см. ниже).

Обратите внимание, список не должен быть пустым.

Если список доменов настолько велик, что его неудобно весь вводить с помощью диалога, то можно позднее добавить в конфигурационный файл «Спамообороны» PREFIX/spam.ini строку security.localdomains: <имя файла со списком доменов>

Формат файла-списка – текстовый, по одному домену на строку.

- *«Now choose where to add sp-milter call»* . Этот запрос появится только в случае установки «Спамообороны» для Sendmail, если в вашей системе более одного конфигурационного файла Sendmail и ни в одном из них нет строки вызова «Спамообороны» (sp-milter):

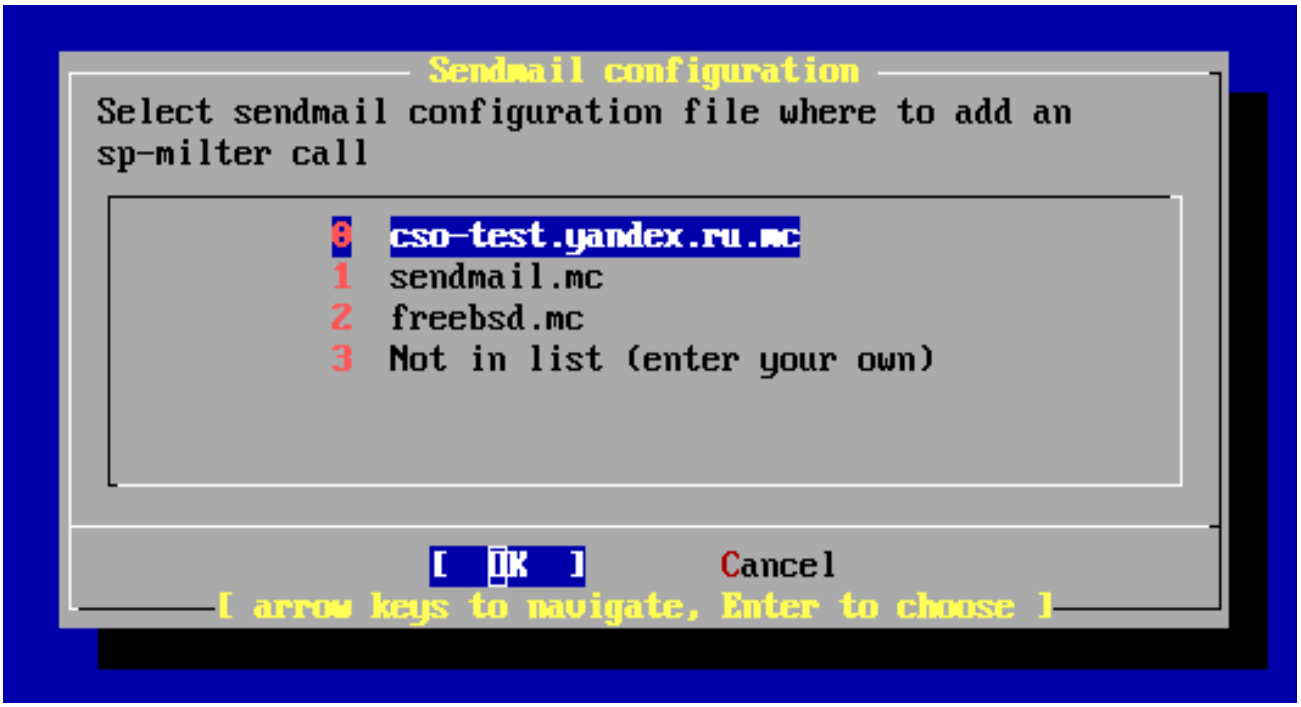


Рис. 9.

Будьте внимательны, выберите именно тот файл, который используется в вашей системе. По умолчанию сценарий установки выбирает файл с именем сервера, а если его нет, с именем sendmail.mc. Вы можете ввести собственный вариант (например, если вы храните файл конфигурации не в директории `/etc/mail`).

Служебной директорией, содержащей конфигурационные файлы «Спамообороны», для FreeBSD является `/usr/local/etc/spamooborona`, для Linux — `/etc/spamooborona`. Далее по тексту эта директория будет обозначаться `PREFIX`.

2.4 Активация продукта

Для продолжения установки «Спамообороны» и получения доступа к обновлениям необходимо выполнить активацию продукта, то есть получить серийный номер и лицензионный ключ.

После оплаты лицензии программы вам выдается уникальный серийный номер. Для получения лицензионного ключа вам необходимо зайти на сайт компании «ДиалогНаука» по адресу http://www.dialognauka.ru/so. После регистрации на сайте на странице «Спамооборона – регистрация продукта» заполните форму: введите серийный номер, передайте на сервер файл конфигурации `spam.ini`, который находится в каталоге `PREFIX`. Если вы воспользовались отдель-

ным файлом-списком доменов (добавили в spam.ini строку security.localdomains: <имя файла списка доменов>), тогда этот файл также нужно отправить на сервер.

На указанный при регистрации адрес электронной почты вам будет выслан персональный ключевой файл. Запишите его в каталог `PREFIX` (см. п. 2.3).

Ключ также может быть запрошен для ознакомительной версии «Спамооборoны». При этом отправка серийного номера не потребуется. Ознакомительная версия продукта будет работать в течение 30 дней без каких-либо функциональных ограничений.

2.5 Получение обновлений базы знаний

Метод получения доступа к обновляемым данным «Спамооборoны» — БД шинглов и спискам DNSBL (RBL DNS) — выбирается в процессе ответа на вопросы установочного сценария `install.sh`. Обновляются не только БД шинглов и списки DNSBL, но и набор эвристик. Выбор режима доступа к набору эвристик не предусмотрен, т.к. «Спамооборона» всегда работает с локальной копией коллекцией эвристик.

«Спамооборона» использует программу rsync для обновления локальных копий RBL DNS и БД шинглов, HTTPS для обновления набора эвристик и планировщик cron для организации регулярных обновлений.

- Пример записей в `/etc/crontab` для FreeBSD:
  - получение локальной копии RBL

```
5 * * * *  root /usr/bin/lockf -st 0 /var/tmp/rsync.dnsbl.lock
/usr/local/sbin/cron_rbl
```

  - получение локальной копии БД шинглов

```
35 * * * *      root /usr/bin/lockf -st 0 /var/tmp/rsync.so-
dump.lock /usr/local/sbin/cron_db
```

  - получение коллекции правил фильтрации

```
*/20 * * * *    root /usr/local/sbin/cron_rul
```

- Пример записей для Linux:
  - получение локальной копии RBL

```
5 * * * *  root /etc/spamooborona/cron_rbl
```

  - получение локальной копии БД шинглов

```
35 * * * *      root /etc/spamooborona/cron_db
```

  - получение коллекции правил фильтрации

```
*/20 * * * *    root /etc/spamooborona/cron_rul
```

При успешной загрузке копии RBL с сервера компании «Яндекс», в каталоге `/var/db/rbldnsd` (`/var/lib/rbldns` в ОС Linux) должны появиться несколько файлов зон dnsbl с префиксом rbldns.

> Если вы хотите получить обновление RBL быстрее, чем это произойдет автоматически по расписанию планировщика cron, выполните пункт «Updates setup/RBL tables/Update RBL tables now» административного сценария PREFIX/adm_so.

Если локальная копия БД шинглов была получена успешно, в каталоге `/var/db/so-dump` появятся архивированные файлы дампов базы с расширением `*.bz2`, а также файл их автоматического обновления `Makefile.dist`. Сохраните `Makefile.dist` под именем `Makefile` и отредактируйте его, если это необходимо. Если настройки доступа к БД MySQL не совпадают с настройками по умолчанию (загрузка дампов БД по умолчанию выполняется от имени пользователя MySQL root с пустым паролем) — присвойте нужные значения переменным окружения SHINGLES_USER, SHINGLES_PASS, SHINGLES_HOST, SHINGLES_PORT, SHINGLES_SOCKET. После завершения изменений выполните команду `make`.

> Если вы хотите получить обновление БД шинглов быстрее, чем это произойдет автоматически по расписанию cron, то выполните пункт «Updates setup/Shingles/Update shingles now» административного сценария PREFIX/adm_so. Сценарий PREFIX/scripts/upd_shingles.sh использует те права доступа к MySQL, которые установлены для базы шинглов.

Если обновления с сервера компании «Яндекс» не доставляются, обратитесь в Службу технической поддержки «Спамооборoны».

Если вы хотите изменить логин или пароль для доступа к базе данных «Спамооборoны», отредактируйте файл `PREFIX/adm_so.conf`. В нем укажите параметры для присоединения к БД в следующих переменных:

```
DB_HOST=<имя хоста БД шинглов, по умолчанию — cso.yandex.ru>;
DB_USER=<логин к БД шинглов, по умолчанию — серийный номер>;
DB_PASS=<пароль к БД шинглов, по умолчанию — ключ доступа>;
```

Административный сценарий `adm_so` (см. ниже) поместит эти настройки в файл конфигурации доступа к базам «Спамооборoны» (`/usr/local/etc/reply.conf`).

Если вы работаете с локальной копией БД шинглов, то создайте в MySQL пользователя с тем именем и паролем, которые были только что указаны в конфигурационном файле. Дайте этому пользователю все права на работу с БД «safeguarddb».

Для проверки корректности установки «Спамооборoны» и ее дальнейшей настройки

можно воспользоваться административным сценарием adm_so (сценарий располагается в `PREFIX/adm_so`). Подробнее работа с adm_so описана в Приложении 1.

Выберите пункт «Database setup/Create config».

Для всех MTA кроме CommuniGate Pro выполните также команду «Startup spamoobo-rona». Если запуск прошел успешно, приступайте к настройке MTA.

2.6 Интеграция с MTA

2.6.1 Sendmail

Настройка Sendmail для работы со «Спамообороной» осуществляется автоматически в процессе выполнения установочного сценария `install.sh`. Сценарии запуска «Спамообороны» для FreeBSD и Linux называются `/usr/local/etc/rc.d/sp-milter.sh` и `/etc/init.d/sp-milter` соответственно.

2.6.2 Qmail

Сценарии запуска «Спамообороны» для FreeBSD и Linux называются `/usr/local/etc/rc.d/sp-qmaild.sh` и `/etc/init.d/sp-qmaild` соответственно.

«Спамооборона» для Qmail состоит из агента, который работает с почтовым сервером Qmail через QMAILQUEUE, и демона, который получает корреспонденцию от агента, обрабатывает ее и затем передает Qmail для доставки.

Для установки и настройки Qmail мы рекомендуем воспользоваться инструкцией «Life with Qmail» (http://ops.iip.net/lwq.html). После установки и настройки по этой инструкции необходимо выполнить следующие действия:

1) Откройте файл `/etc/tcp.smtp`. Добавьте вызов агента «Спамообороны» через QMAILQUEUE в строках, описывающих случаи, в которых требуется фильтрация корреспонденции, например (путь будет `/usr/local/sbin` для FreeBSD, `/usr/sbin` для Linux):

```
1. 127.:allow,RELAYCLIENT="",QMAILQUEUE="/путь/к/sp-qmail"
2. :allow,QMAILQUEUE="/путь/к/sp-qmail"
```

2) Выполните команду `qmailctl cdb`, чтобы изменения вступили в силу.
3) Если запуск агента «Спамообороны» неудачен, уберите вызов «softlimit» в файле `/var/qmail/supervise/qmail-smtpd/run`, в строке запуска smtp-демона. Он устанавливает лимит памяти для работы внешних фильтров в 2Мб, что может быть недостаточно для работы агента «Спамообороны».
4) Убедитесь, что каталог `/var/tmp/qmail` доступен на запись пользователю, от имени которого работает `tcpserver`.

Если вы выполняли установку Qmail каким-либо другим способом, то после редактиро-

вания файла /etc/tcp.smtp обновите cdb-файл, например командой:

```
tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
```

Если программы qmail-queue и qmail-inject в вашей системе находятся не в каталоге /var/qmail/bin/, то укажите в файле PREFIX/spam.ini полные пути к этим программам:

```
general.qmail-queue: </путь/к/qmail-queue>
general.qmail-inject: </путь/к/qmail-inject>
```

Установочный сценарий install.sh проверит наличие этих программ и предложит ввести пути к ним, если не обнаружит их на стандартном месте.

! В почтовых системах с большой нагрузкой рекомендуется увеличить максимальное количество доступных файловых дескрипторов в системе, поскольку Qmail расходует по 3 дескриптора на одно письмо.

2.6.3 Postfix

«Спамооборона» для Postfix состоит из агента, который работает с почтовым сервером через интерфейс «content filter», и демона, который получает корреспонденцию от агента, обрабатывает ее и затем передает обратно серверу Postfix для доставки.

Сценарии запуска демона «Спамообороны» для FreeBSD и Linux называются /usr/local/etc/rc.d/sp-postfixd.sh и /etc/init.d/sp-postfixd.sh соответственно.

Чтобы Postfix стал вызывать агента «Спамоброны» для проверки писем, отредактируйте файл master.cf (этот файл обычно находится в том каталоге, куда вы установили Postfix):

- Найдите строку

```
"smtp      inet  …"
```

- Допишите к ней продолжение:

```
-o content_filter=so-postfix
```

этим вы направите поток писем агенту «Спамообороны».

- В конце файла добавьте строки:

```
localhost:1025  inet n    -    n    -    -    smtpd
     -o content_filter=
```

На этом порту Postfix будет принимать уже проверенную «Спамообороной» почту. Здесь указано что письма принимаются без проверки, т.к. второй раз она не нужна.

```
so-postfix      unix -    n    n    -    5    pipe
     flags=q user=<so username> argv=<full path>/sp-postfix
     -d /var/tmp/postfix -p /var/run/sp-postfixd.sock
```

```
-a ${client_address} -f ${sender} -- ${recipient}
```

Это описание фильтра, здесь <so username> - логин пользователя, от имени которого будет запускаться агент. Этот пользователь уже должен быть заведён в системе.

<full path> - это путь к выполняемому файлу программы-агента «Спамообороны». Обычно это /usr/local/sbin для FeeBSD и /usr/sbin для Linux.

Вы можете указать любой удобный вам каталог для временных файлов «Спамообороны» вместо /var/tmp/postfix. Установите такие права доступа к выбранному каталогу, чтобы посторонние пользователи не могли прочитать чужую почту. Позаботьтесь о том, чтобы для временных файлов было достаточно места.

2.6.4 CommuniGate Pro

Настройка MTA CommuniGate Pro проводится с помощью веб-интерфейса этой программы. Зайдите в раздел «Settings -> General -> Helpers» (рис.10.) и добавьте в таблицу новый «content-filter» с параметрами (путь будет `/usr/local/sbin` для FreeBSD, `/usr/sbin` для Linux):

```
Use Filter: spamooborona
Log: Problems
Path: /путь/к/sp-extfilter [-s] -i <PREFIX/spam.ini>
```

Описание параметра «-s» см. в пункте 2.10.

```
Time-Out: 30 seconds
Auto-Restart: minute
```

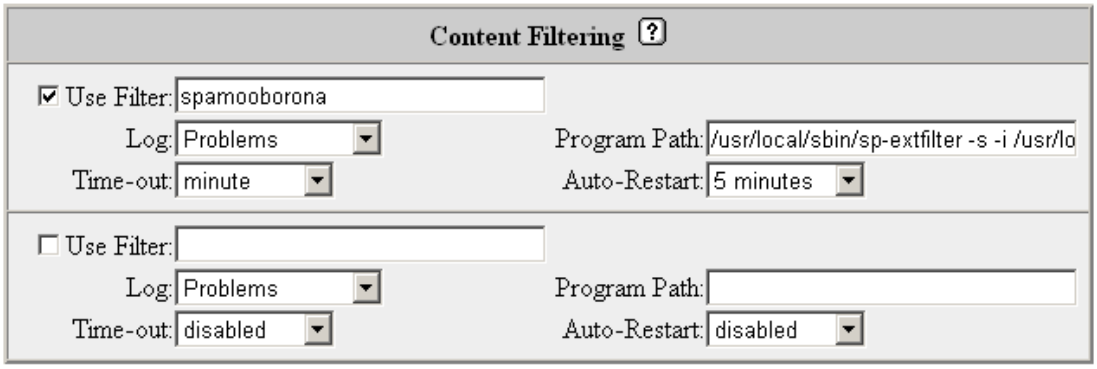


Рис. 10.

В разделе «Settings -> Rules» (рис.11.) создайте новое правило:

```
Action: external filter
Parameters: spamooborona
```

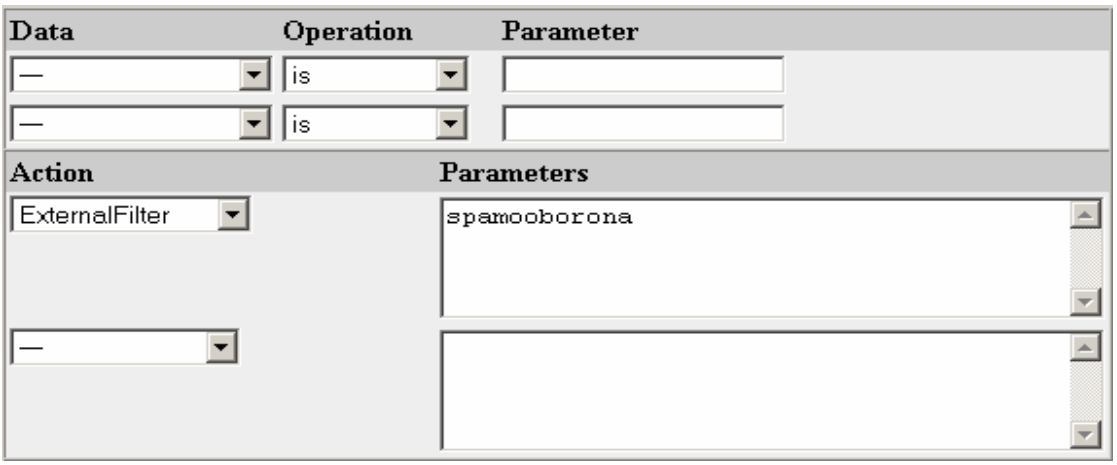


Рис. 11.

2.6.5 Exim

«Спамооборона» для Exim представляет собой демон, который получает корреспонденцию от агента, встраиваемого в Exim через интерфейс LocalScan, обрабатывает ее и затем возвращает результат обратно серверу Exim для доставки или отказа в приеме.

Интеграция «Спамообороны» с Exim заключается в пересборке Exim с модулем local_scan.c, который поставляется в составе «Спамообороны». Подробнее о том, как собрать Exim с возможностью LocalScan, написано по адресу:

http://www.exim.org/exim-html-4.50/doc/html/spec_41.html#CHAP41)

2.7 Заполнение списка пользователей

«Спамооборона» обрабатывает почту только для тех ящиков, адреса которых занесены в список обслуживаемых (файл /var/yamail/mailboxes). Для заполнения и редактирования списка адресов воспользуйтесь административным сценарием adm_so — раздел «Spamooborona parameters/Maintain mailboxes list» (см. Приложение 1, п. 1.6.4).

Количество защищаемых ящиков ограничено лицензией (для коммерческой версии), ознакомительная версия «Спамообороны» не имеет ограничения на число ящиков.

> ! Если вы заполняете список защищаемых ящиков, непосредственно заполняя файл /var/yamail/mailboxes, следите, чтобы их количество не превышало лицензионный лимит. Если количество почтовых ящиков увеличивается — обращайтесь за дополнительными лицензиями заблаговременно.

При покупке лицензии на неограниченное число ящиков необходимость поддерживать

список защищаемых адресов отсутствует.

2.8 Запуск «Спамооборoны»

При использовании CommuniGate Pro специального запуска не требуется, так как этот MTA запускает все установленные в нем фильтры самостоятельно.

Для остальных MTA первый запуск «Спамооборoны» выполняется административным сценарием adm_so — через пункт «Startup Spamooborona». При перезагрузке ОС «Спамооборoна» запускается системой автоматически.

2.9 Результаты проверки письма

В случае успешной установки «Спамооборoна» начинает размечать обрабатываемую корреспонденцию, добавляя в каждое письмо следующие служебные строки заголовка:

- X-Spam-Flag:
  может принимать значения: YES — для писем, определенных как спам; NO — для «чистой» корреспонденции; DLVR — для легальных рассылок (экспериментальный режим); SKIP — для писем на необслуживаемые ящики или для всех писем после истечения срока действия лицензии.
- X-Spam-Yversion:
  Показывает номер установленной версии «Спамооборoны».
- X-Spam-Status:
  Необязательный заголовок, может быть включен для добавления строки «статуса», в которой отображается количество набранных баллов и перечень сработавших правил фильтрации. Для Sendmail, Qmail, Postfix и Exim включение этого заголовка возможно с помощью сценария adm_so — пункт «Spamooborona parameters/Change statusline mode». Чтобы эти изменения вступили в силу, необходимо перезапустить «Спамооборoну». Чтобы включить этот заголовок для CommuniGate Pro, требуется добавить ключ «`-s`» в строку описания вызова программы `sp-extfilter`. Заголовок статуса может понадобиться для отладочных целей перед обращением в Службу технической поддержки.

Обработка выявленного спама может выполняться, например, в клиентских почтовых приложениях настройкой фильтров по значению заголовка X-Spam-Flag, а также на сервере

правилами sieve (сервер IMAP производства Cyrus), procmail или другими средствами предварительной обработки почты.

2.10 Удаление «Спамооборoны»

Сценарий `install.sh` позволяет также произвести автоматизированное удаление «Спамооборoны». Вам будет предложено автоматическое удаление либо список пакетов к удалению, из которого вы сможете выбрать, какие из пакетов следует удалить:

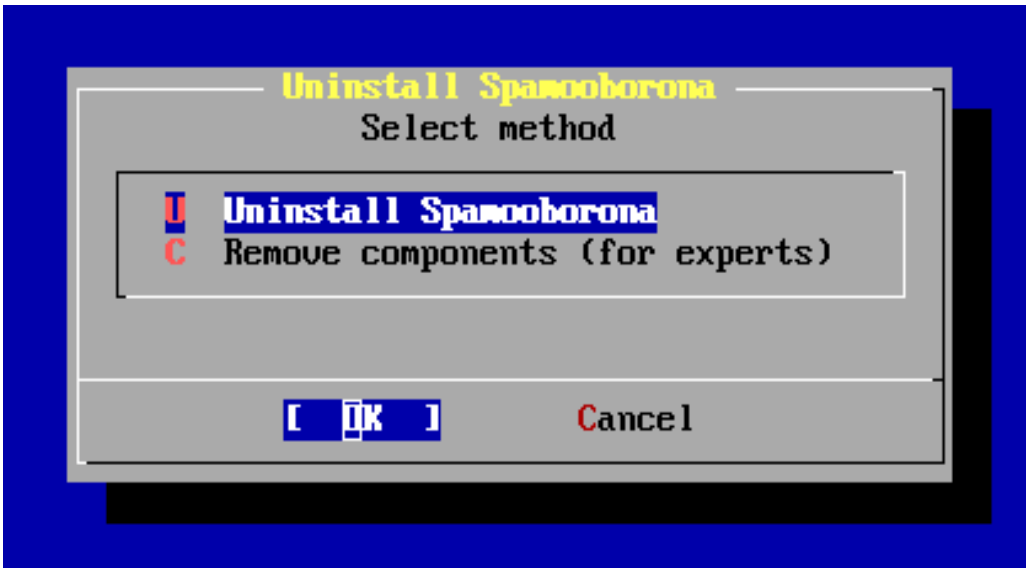


Рис. 12

По умолчанию в этом списке отмечены к удалению «Спамооборона» и пакет её служебных данных, остальные пункты по желанию выбираются вручную:

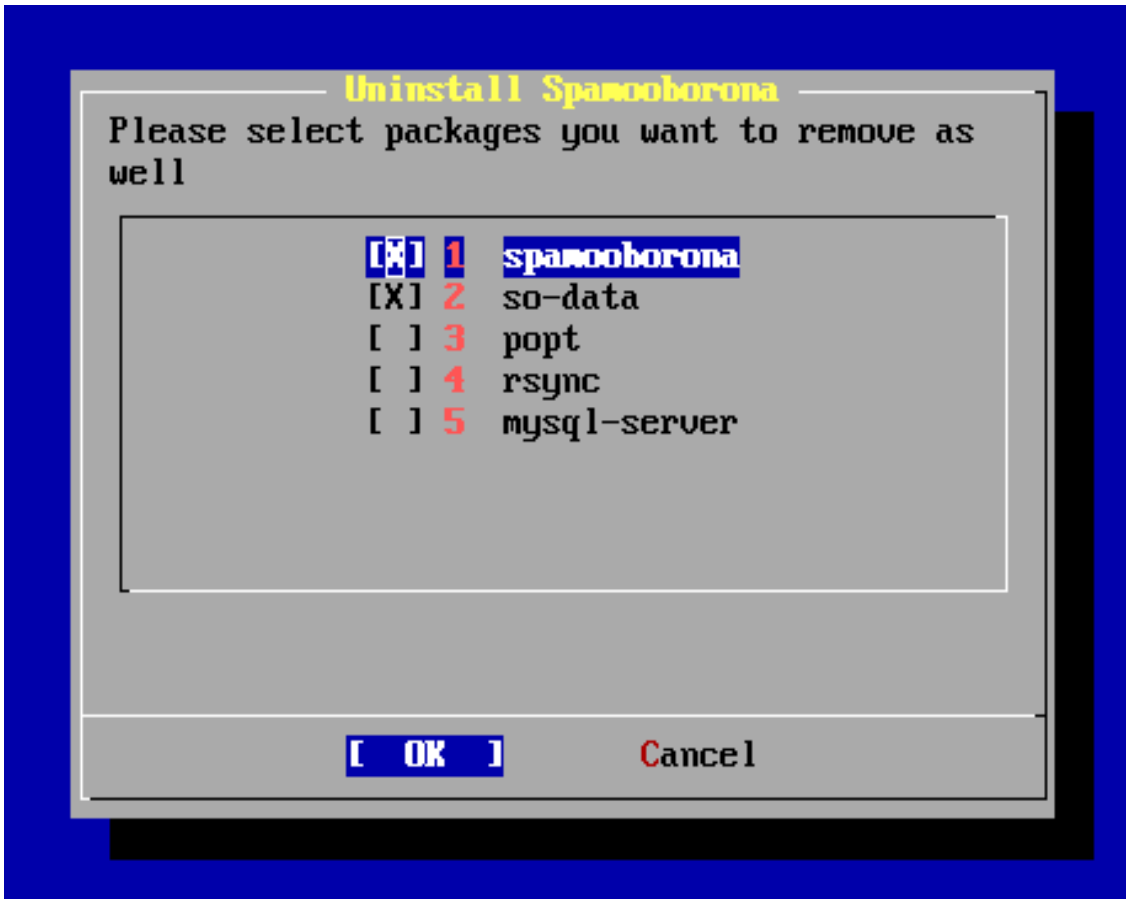


Рис. 13

2.11 Замена версии «Спамооборoны» на более новую

Пункт меню «Update» предназначен для замены пакета «Спамооборoны» более новым, полученным от производителя (например, загруженным с официального сайта программы — so.yandex.ru). Запустите сценарий `install.sh` в директории, где записан новый пакет «Спамооборoны», и подтвердите обновление (рис. 14). Сценарий удалит старый пакет «Спамооборoны» и установит новый, сохранив файлы конфигурации `spam.ini` и `local_domains.conf`. Сценарий не проверяет, является ли устанавливаемый пакет в действительности более новым. Эту функцию реализуют утилиты работы с пакетами, применяемые в используемой операционной системе.

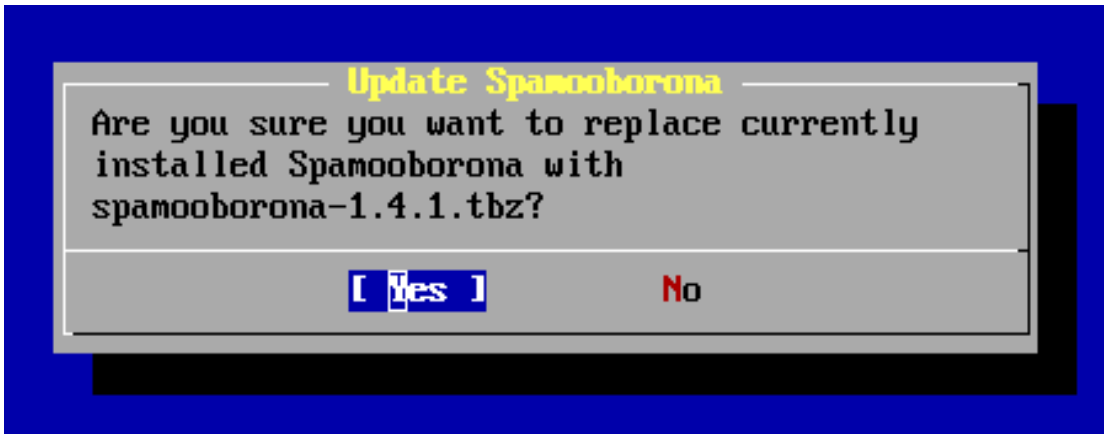

Update Spamooborona
Are you sure you want to replace currently
installed Spamooborona with
spamooborona-1.4.1.tbz?
[Yes]
No

Рис. 14.

3. Возможности настройки системы

«Спамооборона» проводит комплексный анализ всех возможных данных о письме, используя тысячи его характеристик. Эти характеристики выявляются набором эвристик, на основе которых составлены правила фильтрации. Каждое правило имеет определенный весовой коэффициент, положительный либо отрицательный (компенсирующий). Если суммарный положительный вес сработавших правил превышает порог, определенный параметром `spam.score`, письмо маркируется как спам. Существует ряд возможностей влиять на процесс принятия решения.

3.1 «Белый список»

«Белый список» формируется на основе отправленных локальными пользователями писем по журналу работы MTA. В файле белого списка «Спамообороны» /var/yamail/whitelist сохраняются пары адресов: локальный адрес — внешний корреспондент. При получении письма извне проверяется наличие адреса внешнего корреспондента в «белом списке». Существует три режима проверки:

0 — «белый список» не применяется

1 — используется общий список,

2 — используются персональные списки.

Если адрес внешнего корреспондента найден в «белом списке», и включен режим 1, сработает правило `FROM_IN_WL` (отправитель в белом списке), компенсирующий вес которого администратор системы может назначить самостоятельно. Если в «белом списке» найдена доменная часть адреса электронной почты внешнего корреспондента, сработает правило `DOMAIN_IN_WL`.

Если включен режим 2, и адрес внешнего корреспондента найден в «белом списке» получателя, сработает правило `FROM_IN_PERSONAL_WL` (отправитель в персональном «белом списке»), а если в «белом списке» получателя присутствует доменная часть адреса электронной почты отправителя, — соответственно, правило `DOMAIN_IN_PERSONAL_WL`.

> i В случае, когда одно письмо имеет несколько адресатов (несколько SMTP команд RCPT TO на одно тело письма), то правила «белого списка» сработают, если в «белом списке» найден хотя бы один адресат.

По умолчанию всем этим правилам назначен вес «-10». Изменить его можно в файле

/var/yamail/wl.rul.

Общий список (режим 1) используется в качестве режима по умолчанию.

Администратор системы может самостоятельно добавлять пары адресов в «белый список» при помощи пункта меню «Whitelist setup/Append manually» сценария adm_so. Посмотреть список целиком можно через меню «Whitelist setup/Browse whitelist» или непосредственно в файле /var/yamail/whitelist. Чтобы изменить режим работы, необходимо воспользоваться разделом «Whitelist setup/Change whitelist mode» сценария adm_so. Редактирование «белого списка» администратор при желании производит самостоятельно.

3.2 Доверенные сети

«Спамооборона» допускает наличие сетей, почта из которых будет доставляться адресатам без проверки. Для этой цели в конфигурационном файле `PREFIX/spam.ini` в параметре «`non-check-wl`» в формате `<сеть> <маска>` администратор должен указать одну или несколько (до 10) сетей, по одной в каждой строке.

Рекомендуется включить в этот список все сети вашей организации, это исключит излишнюю нагрузку на сервер, в частности, проверку исходящей почты. Обратите внимание: в этом списке ни в коем случае не должны присутствовать серверы, принимающие почту из «внешнего мира» (например, резервные MX), на которых ***не*** установлена «Спамооборона», — это приведет к получению спама.

3.3 Отказ от приема спама

В конфигурации, выбранной по умолчанию, «Спамооборона» доставляет все письма, независимо от количества набранных баллов. Если вы хотите отвергать часть корреспонденции, набравшей большое количество баллов, укажите в файле `PREFIX/spam.ini` недопустимый вес «`general.RejectValue: <вес>`». Недопустимый вес не должен быть меньше порогового веса спама «`spam.score`». Рекомендованное значение недопустимого веса «`RejectValue`» — 40.

Если набранный письмом вес выше допустимого, почтовый сервер отвергнет его, выдав сообщение об ошибке с кодом 550 и текстом «Message rejected under suspicion of spam».

Вы можете указать собственный текст в строке «general.RejectString» (латиницей). Рекомендуется добавлять в это сообщение адрес электронной почты администратора почтовой системы.

Существует возможность выбрасывать письмо, вместо того чтобы отвергать его с выдачей сообщения об ошибке, — для этого задайте значение параметра «`general.Discard: 1`». В этом случае недопустимый вес, указанный в «`general.RejectValue`», будет порогом, начиная с которого письма будут выбрасываться.

> Функции reject и discard работают в версиях «Спамооборoны» для Sendmail, CommunuGate Pro. Функция reject также работает в версии «Спамооборoны» для Exim.
>
> Не используйте функцию reject в случае, если «Спамооборoна» установлена не на сервере, непосредственно принимающем почту из «внешнего мира». В этом случае «внешний» по отношению к «Спамооборoне» сервер будет отправлять квитанции о недоставке, скорее всего по поддельным адресам. Поток этих квитанций может вызвать недовольство администраторов почтовых узлов, которые будут их получать. Информацию о проблеме автоответчиков можно прочитать на странице http://www.spamcop.net/fomserve/cache/329.html.

3.4 Персональные настройки отказа от нежелательных писем

Пункт «Reject values/Append table» сценария adm_so позволяет назначить отдельным адресам электронной почты персональное значение порога Reject, отличное от общего «`general.RejectValue`», указанного в файле конфигурации. В случае, когда задан режим Discard, это значение будет трактоваться как порог отбрасывания письма. Значения порогов хранятся в файле /var/yamail/rejects.

Вы можете в качестве адреса указать только имя домена, в этом случае «Спамооборoна» будет определять порог отказа в следующем порядке:

1. Если найдена запись о пороге для адресата, то используется порог из этой записи.
2. Иначе, если найдена запись о пороге для домена адресата, то используется порог из этой записи.
3. Иначе используется общий порог, установленный в `spam.ini`.

> Функция работает в версиях «Спамооборoны» для Sendmail , CommunuGate Pro и Exim.
>
> В случае, когда одно письмо имеет несколько адресатов (несколько SMTP команд RCPT TO на одно тело письма), будет использован самый высокий из заданных порогов отказа от нежелательных писем.

3.5 Безусловная доставка

Нулевое значение порога reject в файле персональных порогов reject позволяет осуществлять доставку всей корреспонденции в выбранные ящики, например, abuse@domain.ru или postmaster@domain.ru, независимо от результата проверки «Спамообороной». См. также п. 1.10 Приложения 1.

3.6 Флаг результата проверки

При работе с Sendmail имеется возможность отображать результат проверки письма не только в виде служебного заголовка X-Spam-Flag, но и произвольной меткой в начале поля темы (Subject), которую можно задать посредством административного сценария `adm_so` (см. Приложение 1, п. 1.6). Кроме того, этот, а также другие параметры запуска «Спамообороны» могут быть записаны в файле конфигурации:

- В ОС Linux — `/etc/spamooborona/spamooborona.conf`
- В ОС FreeBSD — `/etc/rc.conf`.

Как минимум, в этом файле должна присутствовать следующая строка, иначе «Спамооборона» не запустится:

```
spmilter_enable="YES"
```

Строка, которая включает маркировку темы письма, выглядит так:

```
spmilter_subject="[SPAM]"
```

где «[SPAM]» — любой текст в 7-битной кодировке (латиница).

> Имейте в виду — максимальная длина строки в заголовке письма ограничена правилами RFC.

3.7 Получение обновлений

Обширный набор знаний «Самообороны» создает запас прочности, достаточный для выявления новых видов спама. Однако для достижения наилучшего качества фильтрации необходимо использовать актуальную базу знаний. Это можно делать двумя способами: автоматически загружать обновления на свой сервер и работать с локальной копией базы знаний «Спамообороны», либо обращаться при проверке письма с запросами к базе знаний, расположенной на сервере компании «Яндекс». Первый способ позволяет достичь максимальной производительности

«Спамообороны» при интенсивном потоке писем (несколько в секунду), второй — сбережет интернет-трафик в условиях низкой нагрузки за счёт объёма обновлений.

При работе с локальными данными администратор может самостоятельно скорректировать частоту проверки обновлений, отредактировав файл `/etc/crontab`. Доставка необходимых для обновления файлов и перезапуск процесса фильтрации осуществляются автоматически. При этом размеры и регулярность обновлений составляют:

- список зон для rbldnsd — ежечасное обновление, размер обновления 0,1-5Мб;
- база данных шинглов — ежечасное обновление, размер обновления около 100Кб;
- база данных источников спама — еженедельное обновление, размер обновления порядка 20Мб;
- эвристические алгоритмы — ежедневное обновление, размер обновления около 150Кб.

Если при установке «Спамообороны» был выбран режим работы с удаленным сервером MySQL cso.yandex.ru, при проверке каждого письма будет передаваться в среднем 1 Кб в сторону сервера cso.yandex.ru и 0,7Кб обратно. При работе с удаленным сервером RBL cso.yandex.ru генерируется трафик в пределах 0,2Кб на письмо.

> Выбирая режим доступа к базе знаний «Спамообороны», имейте в виду, что поделить объем суточных обновлений на средний трафик письма и оценить поток, при котором загрузка локальных копий данных нецелесообразна — простой, но не совсем правильный способ. Помните о пиковых нагрузках почтового сервера, во время которых «Спамооборона» не должна становиться «узким местом», с одной стороны, и о том, что локальные копии данных неизбежно будут содержать частично устаревшие данные, с другой стороны. Т.е. качество фильтрации при работе с локальными копиями данных несколько ниже за счёт снижения оперативности поступления данных.

3.7.1 Изменение режима доступа к базе знаний

Режим доступа к обновляемой базе знаний «Спамообороны» может быть изменен при помощи пункта меню «Configure» сценария установки. Это меню аналогично меню установки (см. п. 2.3):

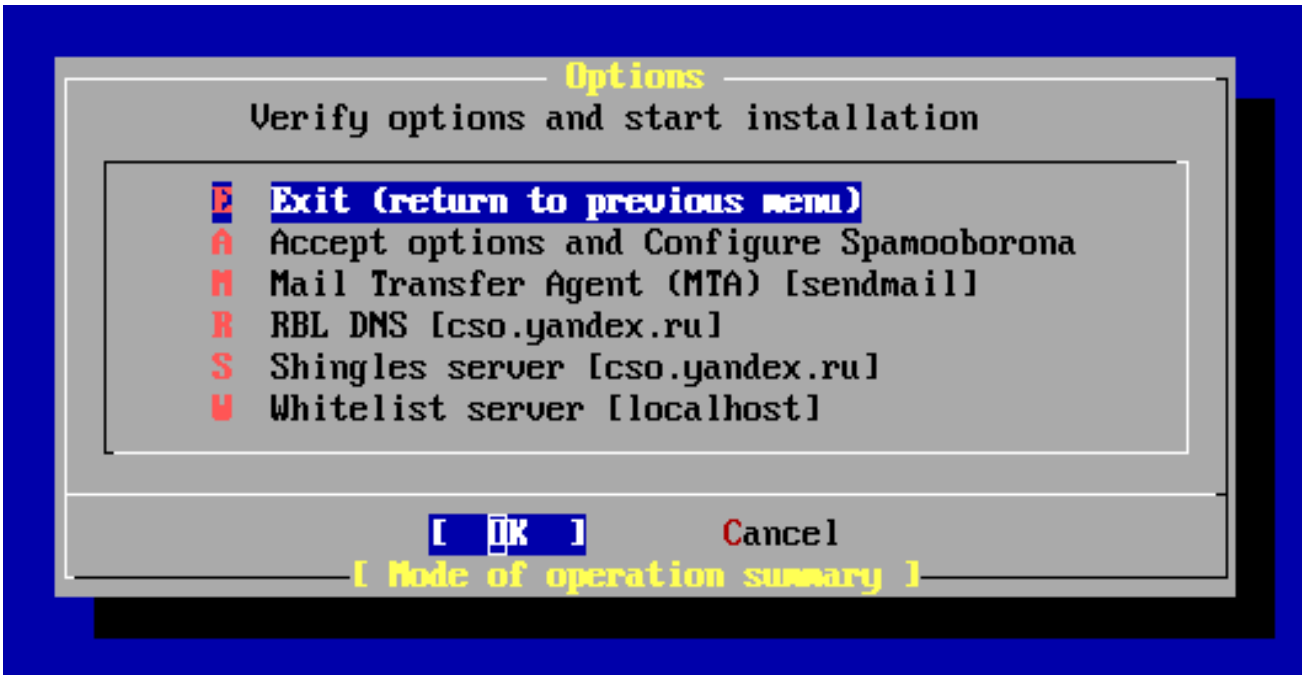

Options
Verify options and start installation
E Exit (return to previous menu)
A Accept options and Configure Spamooborona
M Mail Transfer Agent (MTA) [sendmail]
R RBL DNS [cso.yandex.ru]
S Shingles server [cso.yandex.ru]
W Whitelist server [localhost]
[OK]
Cancel
[Mode of operation summary]

Рис. 15.

4. Советы по эксплуатации

4.1 Что делать при пропуске спама

«Спамооборона» — устойчивая система, которая может эффективно работать даже при неполном наборе данных или некорректных настройках. Постоянный уровень полноты фильтрации спама ниже 90% в большинстве случаев означает неверную настройку «Спамооборoны». При этом целесообразно проверить соединение с БД шинглов, работоспособность «черного списка» и при необходимости скорректировать список доверенных источников почты trusted_zone (см. п. 4.1.2).

Полнота фильтрации — процент поступающего спама, который был выявлен фильтром.

4.1.1 Проверка соединения с БД шинглов

Выполните пункт «Database Setup/Test DB Connection» сценария adm_so. В случае правильных настроек вы увидите такое сообщение:

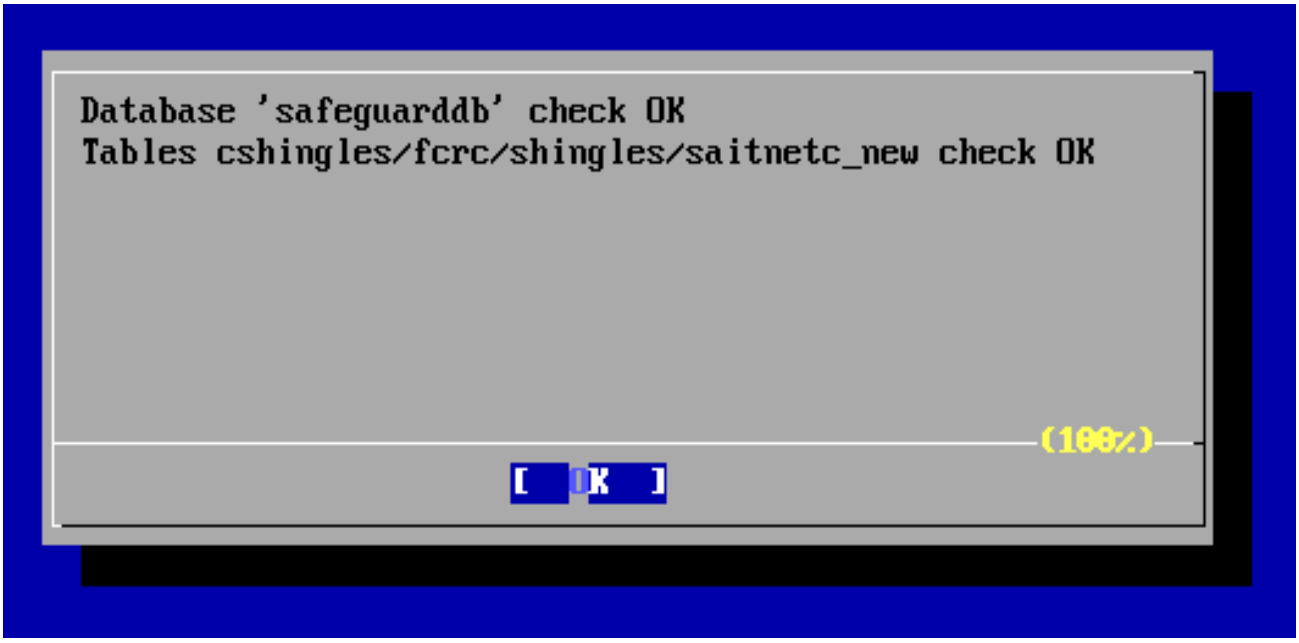


Рис. 16.

В противном случае будет показано сообщение об ошибке.

4.1.2 Настройка trusted zone

Создайте файл `/var/yamail/trusted_zone` и перечислите в нём почтовые серверы организаций, в подлинности которых вы абсолютно уверены, — например, адрес сервера своего провайдера. Адреса вносятся в формате CIDR по одному адресу в строке. Опираясь на составленный список адресов серверов, «Спамооборона» будет отделять заголовки, добавленные доверенными почтовыми серверами, от заголовков других серверов по маршруту следования письма, что положительно скажется на качестве фильтрации.

Этот список не отключает проверки, но описывает список сетей, сведениям из которых можно полностью доверять; правильно заполненный список `trusted_zone` повышает полноту фильтрации и снижает вероятность ложного срабатывания «Спамоброны».

4.1.3 Пересылка образцов спама

Вы можете помочь улучшению базы знаний, применяемой в «Спамообороне», пересылая не отфильтровавшийся спам на адрес so-report@yandex-team.ru. Поскольку обработка информации при отсутствии полных служебных заголовков невозможна, пересылайте письма как вложения (forward as attachment), так как в этом случае оригинал письма не подвергается искажениям. Обратите внимание, почтовый клиент Outlook из пакета Microsoft Office удаляет служебные заголовки при пересылке, поэтому в данном случае необходимо вручную скопировать заголовки из свойств пересылаемого письма и вставить в текст.

4.2 Что делать при ложных срабатываниях

Причину ошибочного определения спама необходимо рассматривать в каждом случае отдельно. Ложные срабатывания могут возникать, прежде всего, на рассылках коммерческих предложений и подобных сообщениях, которые похожи на спам по группе признаков.

Используйте «белые списки» «Спамооборoны» (п. 3.1). При необходимости задайте самостоятельно вес для правил `FROM_IN_WL`, `DOMAIN_IN_WL` и `FROM_IN_PERSONAL_WL`, `DOMAIN_IN_PERSONAL_WL`, пополняйте таблицу адресов «белого списка».

Заполните файл `/var/yamail/trusted_zone` (см. выше п. 4.1.2).

В случае значительного количества ложных срабатываний обратитесь в Службу технической поддержки «Спамооборoны».

4.3 Что делать при большом потоке почты

Какой именно поток писем является «большим» для вашего почтового сервера, заранее сказать нельзя. Признаком того, что нагрузка на «Спамооборону» на вашем сервере высока, является значительное время обработки писем (более секунды на письмо).

Узнать время обработки одного письма можно по журналу MTA (обычно `/var/log/maillog`), куда «Спамооборона» записывает строки вида:

```
spamstop[<pid>]: (spamstop time) took 0.284722 sec, 0.234375 CPU
sec.
```

Попробуйте последить за изменением времени обработки в зависимости от увеличения и уменьшения потока почты. Если вы обнаруживаете прямую связь, и при этом время обработки писем заметно возрастает, то, скорее всего, загруженность «Спамообороны» на вашем сервере близка к предельной.

На время обработки писем влияют три фактора:

- время ответа БД шинглов;
- время отклика на запросы к «черному списку» DNS;
- вычислительные мощности почтового сервера.

Если работу «Спамообороны» задерживает время выполнения запросов к БД или RBL DNS, и вы используете удаленный доступ к базе знаний — попробуйте перенастроить «Спамооборону» на работу с локальной копией данных.

Если БД отвечает быстро, но все равно накапливаются очереди писем, время их обработки постепенно нарастает и, кроме того, в файлах журналов почтового сервера появляются сообщения вида «Please try again later» — это признак проблемы, связанной с обработкой чрезмерно большого количества конвейеров (threads) «Спамообороны». Максимальное количество стабильно работающих параллельных конвейеров индивидуально для каждого сервера, его значение можно определить лишь опытным путем. Для этого попробуйте задавать разные значения параметра «`general.threads`» в файле `PREFIX/spam.ini`.

Если вы имеете распределенную сетевую инфраструктуру, внесите свои сети в список `non-check-wl` (п. 3.2). Это снизит нагрузку на сервер «Спамообороны».

Кроме того, вы можете сбалансировать работу сервера, нарастив его вычислительные мощности.

5. Техническая поддержка

Техническая поддержка «Спамообороны» осуществляется компанией «ДиалогНаука» по электронной почте и телефону в рабочие дни с 9:00 до 19:00:

- e-mail: so-support@dialognauka.ru;
- телефон: (095) 980-6776.

Подробную информацию о продукте вы можете найти на сайте компании «ДиалогНаука» по адресу http://www.dialognauka.ru/so или на сайте «Спамообороны» http://so.yandex.ru.

Приложение 1. Административный сценарий adm_so

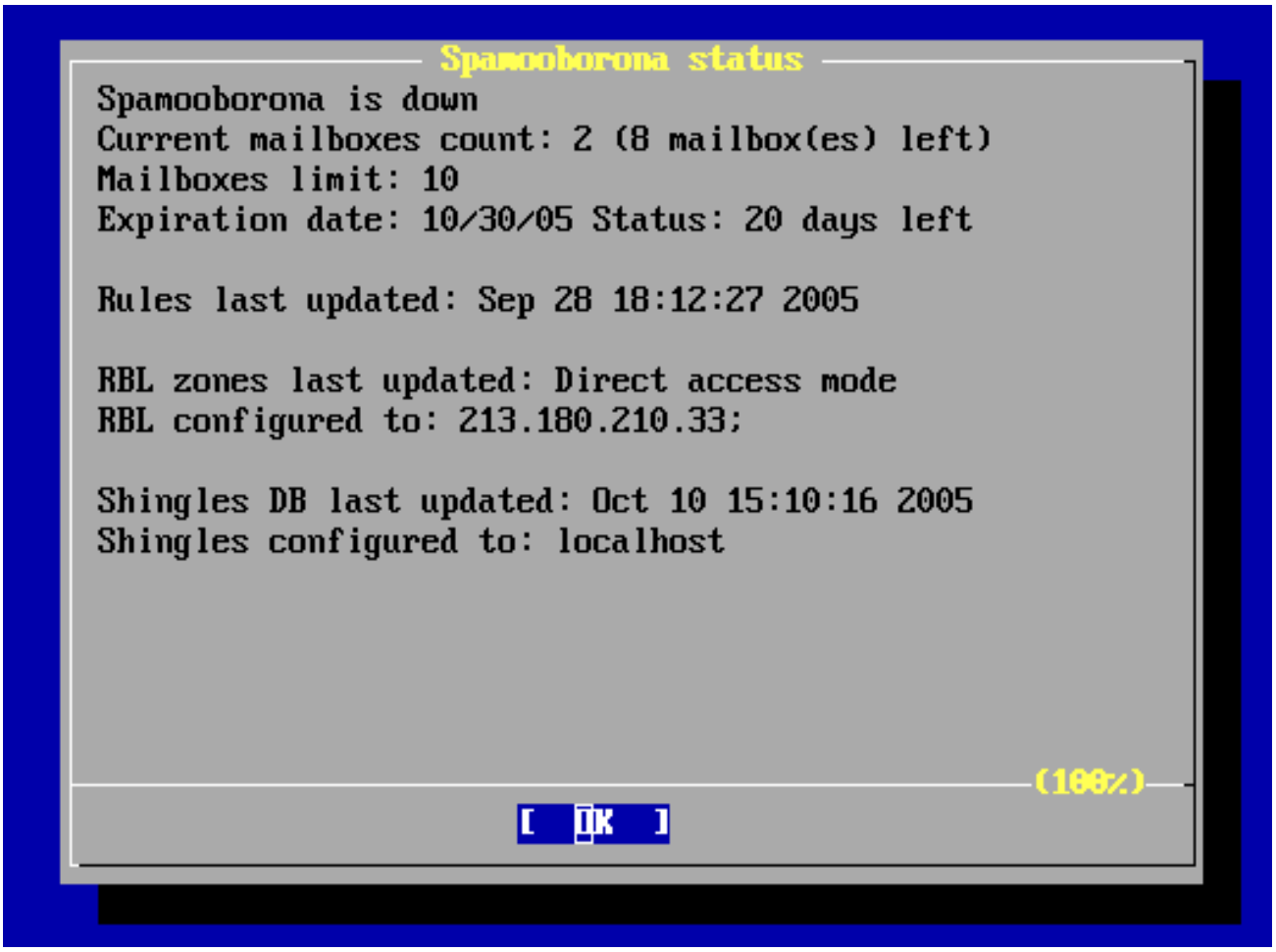
Административный сценарий adm_so располагается в каталоге `PREFIX` (`/usr/local/etc/spamooborona/` для FreeBSD или `/etc/spamooborona/` для Linux). Помните, что все действия должны выполняться от имени пользователя `root`. Пункты 2-4 не выполняются для CommuniGate Pro.

1.1 Request status

Выбор пункта «Request status» позволяет проверить текущее состояние демона «Спамооборoны». На экран будет выведена также информация о лимите ящиков, дате окончания срока действия лицензии, режиме и времени последнего получения обновлений правил фильтрации, RBL-зон и шинглов.

Если при очередных обновлениях был получен файл обработки шинглов Makefile.dist более новый, чем тот, который у вас используется, об этом также будет выведено предупреждение. В этом случае следует скопировать полученный Makefile.dist в Makefile и проверить его на со-

ответствие вашей системе. Это действие аналогично выполняемому при установке «Спамообороны» (см. п. 2.5).



1.2 Startup spamooborona

Выбор пункта «Startup spamooborona» запускает демон «Спамообороны», если он еще не был запущен. О результатах попытки запуска выдается специальное сообщение.

1.3 Stop spamooborona

Выбор пункта «Stop spamooborona» осуществляет остановку демона «Спамообороны».

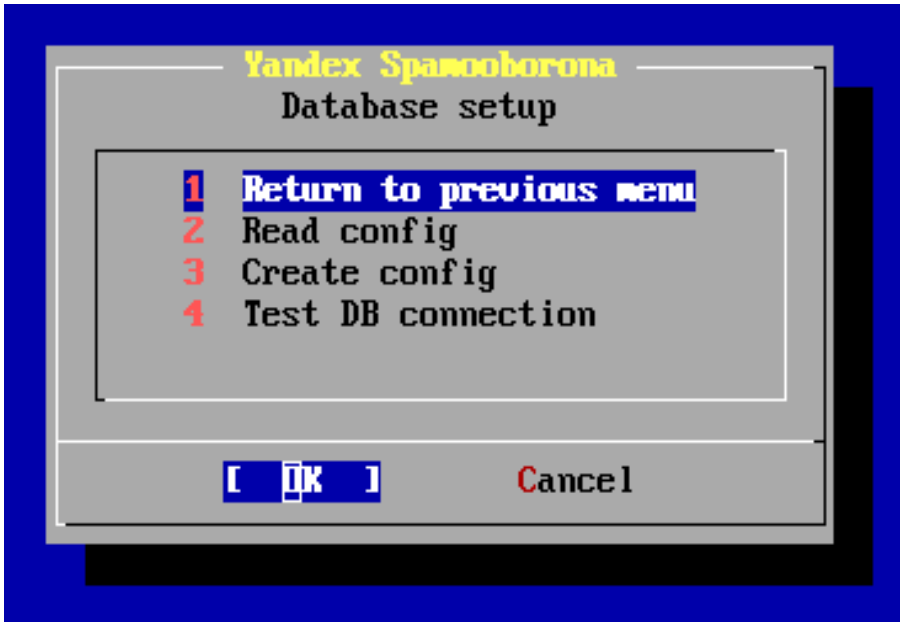
1.4 Reload config files

Выбор пункта «Reload config files» посылает демону сигнал о необходимости перечитать свои конфигурационные файлы (`PREFIX/spam.ini` и коллекцию правил фильтрации). Переза-

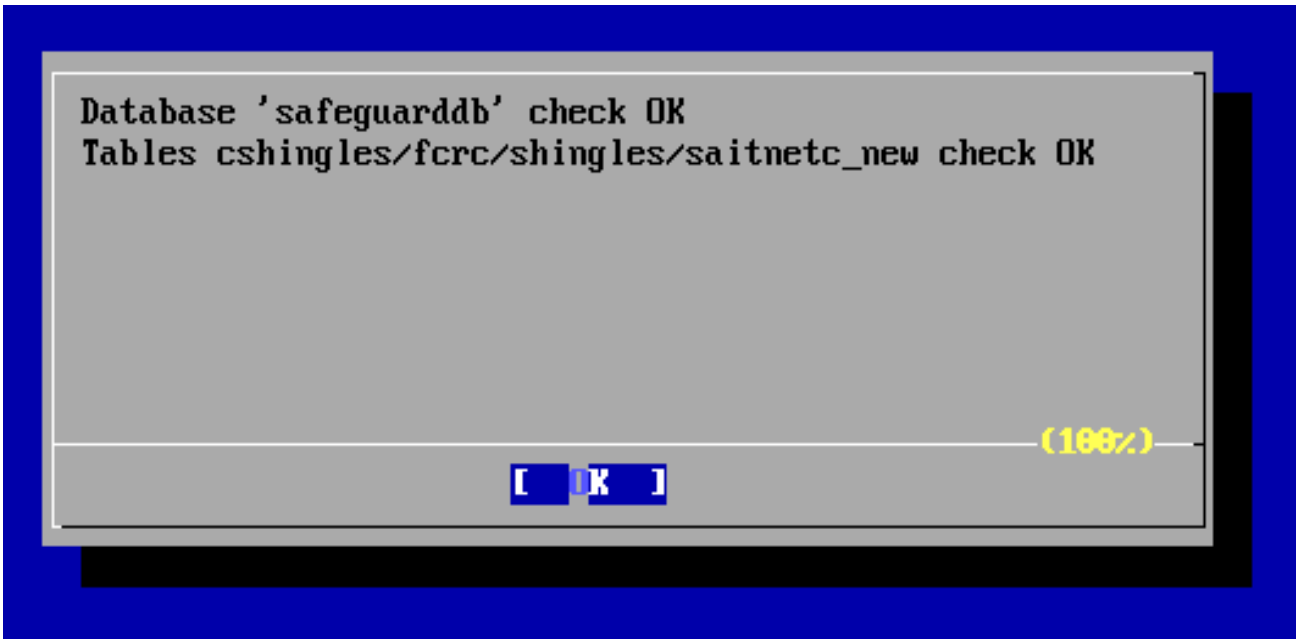
грузка осуществится перед обработкой следующего после получения сигнала письма. Эту возможность удобно использовать для активизации изменений в `spam.ini` без перезапуска «Спамообороны».

1.5 Database setup

Выбор пункта «Database setup» позволяет проверить корректность настроек доступа к базам данных «Спамообороны» и на основе занесенных в PREXIF/adm_so.conf параметров создать конфигурационный файл (см. п. 2.5).



- «Read config» осуществляет просмотр текущего файла конфигурации БД;
- «Create config» отвечает за создание файла конфигурации БД на основе параметров, указанных в файлах `PREFIX/adm_so.conf` и в самом `PREFIX/adm_so`;
- «Test DB connection» осуществляет проверку с соединения с базой шинглов «Спамообороны». В случае успеха выводится сообщение вида:



1.6 Spamooborona parameters

Раздел административного сценария adm_so «Spamooborona parameters» дает возможность управлять рядом настроек «Спамообороны».

- «Browse parameters file» позволяет просмотреть содержимое конфигурационного

файла `PREFIX/spam.ini`.

- «Change whitelist mode» изменяет режим работы «белого списка»:

  0 – проверка по «белому списку» выключена;

  1 – режим общего «белого списка»;

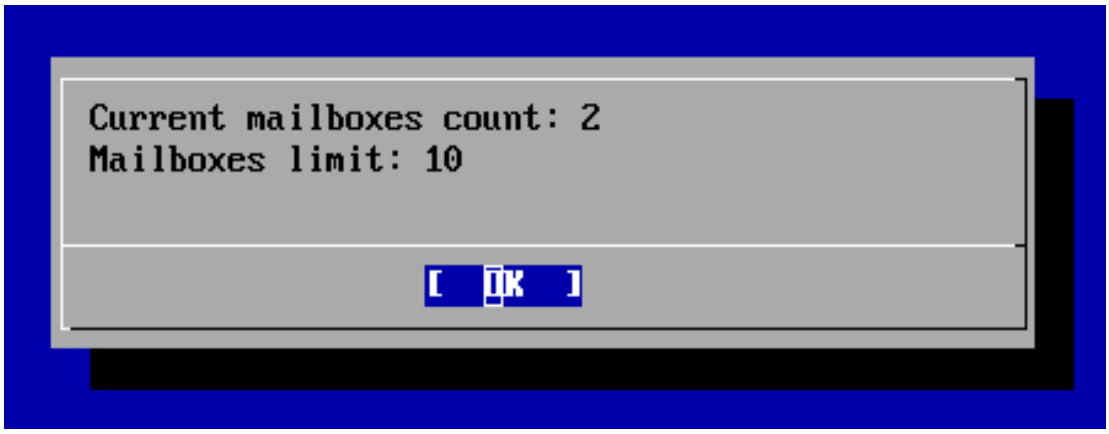
  2 – режим персональных «белых списков».

  Чтобы активизировать изменение режима «белого списка», нужно, чтобы система перечитала конфигурационные файлы. Выполните «Reload Config Files» или «Stop spamooborona» – «Startup spamooborona».
- «Change statusline mode» разрешает/запрещает добавление заголовка статуса в обработанные письма. В заголовке статуса содержится количество набранных баллов и список сработавших правил фильтрации. По умолчанию заголовок статуса не выводится. Обратите внимание, команда работает для Sendmail и Qmail, добавление строки статуса для CommuniGate Pro описано в п. 2.9.
- «Spam mark in subject» позволяет задать или выключить маркировку спама в теме письма (в настоящий момент только для MTA sendmail).

1.6.1 Maintain mailboxes list

Подраздел «Maintain mailboxes list» позволяет выполнять типовые операции со списком почтовых ящиков, которые обслуживаются «Спамообороной».

- «Checkup mailboxes limit» позволяет проверить текущее количество обслуживаемых системой ящиков, а также количество, которое допускается вашей лицензией.



- «Browse mailboxes list» выводит список защищаемых почтовых ящиков.
- «Append from file» позволяет импортировать список ящиков из текстового файла. При подготовке такого файла допускается написание одного или нескольких разделенных пробелом почтовых адресов в строке. При импорте производится проверка корректности синтаксиса адреса e-mail.
- «Append manually» позволяет вручную добавлять в список по одному ящику.
- «Delete mailbox record» удаляет запись о ящике.

1.7 White/black list DNS check

В случае когда «Спамооборона» настроена на получение локальной копии «черного списка» и работу с ним через rbldnsd, пункт «White/black list DNS check» позволяет проверить корректность настройки BIND (сервера DNS).

1.8 Whitelist setup

Подраздел «Whitelist setup» предоставляет администратору средства управления «белым списком» (см. п. 3.1).

- «Check mode» позволяет проверить текущий режим «белого списка». Если установлен режим 1 или 2, но правила `FROM_IN_WL/DOMAIN_IN_WL` или `FROM_IN_PERSONAL_WL/DOMAIN_IN_PERSONAL_WL` не определены, будет выдано предупреждение.
- «Change whitelist mode» производит изменение режима работы «белого списка»:

0 – проверка по белому списку выключена;

1 – режим общего белого списка;

2 – режим персональных белых списков.

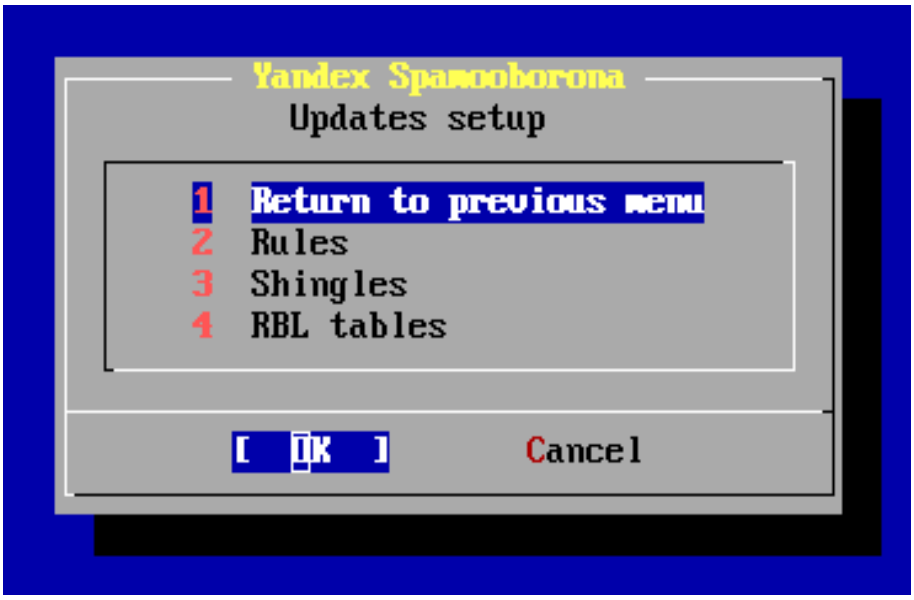
Чтобы активизировать изменение режима «белого списка», нужно перечитать конфигурационные файлы, выполнив либо «Reload Config Files», либо «Stop spamooborona» и «Startup spamooborona».

- «Test whitelist database» проверяет соединение с БД локальных данных.
- «Check local domains list» осуществляет проверку копии списка локальных доменов. Эта копия списка используется при анализе журналов MTA. В «белый список» будут попадать только корреспонденты пользователей из перечисленных доменов. После установки «Спамообороны» в список локальных доменов заносятся те, которые были указаны как обслуживаемые «Спамообороной». Если список доменов для заполнения «белого списка» отличается от списка обслуживаемых доменов, отредактируйте файл конфигурации белого списка `PREFIX/scripts/local_domains.conf`.
- «Update whitelist from maillog» запускает сценарий разбора журналов MTA для автоматического заполнения «белого списка». При самом первом запуске просматривается весь архив логов, при последующих запусках — только последний закрытый лог.
- «Append manually» позволяет выполнить ручное добавление в «белый список» пары корреспондент-получатель (удаленный адрес – локальный адрес). Можно указать только удаленный адрес, который может быть использован в режиме работы с общим «белым списком» (режим 1). Также допустимо указывать для удаленного адреса только домен. Подробнее см. п. 3.1 руководства администратора.
- «Delete» выполняет удаление пары корреспондент-получатель.
- «Browse whitelist» позволяет просмотреть содержимое «белого списка».
- «Export to file» выполняет сохранение содержимого таблицы «белого списка» в текстовый файл. Формат файла – одна строка на одну запись таблицы.
- «Import file» выполняет чтение адресов из текстового файла и последующее автоматическое заполнение таблицы «белого списка». Формат файла – одна строка на одну запись таблицы, в строке один или два адреса, причем первым указывается удаленный адрес, а вторым – локальный.

- «Mail log parser» запускает и останавливает процесс автоматического разбора журнала почтового сервера с последующим внесением записей в «белый список».

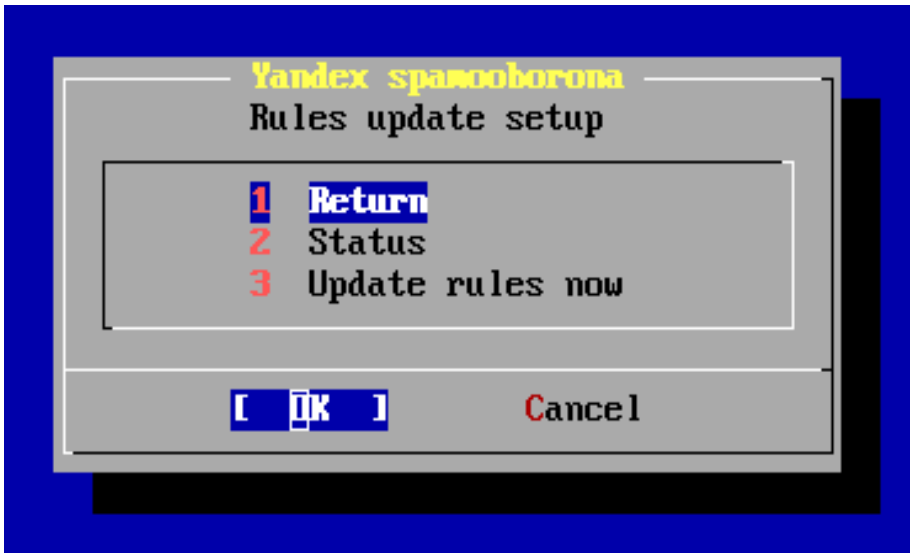
1.9 Updates Setup

Подраздел «Updates Setup» предназначен для контроля над процессом обновления базы знаний «Спамооборoны», в которую входят обновления коллекции правил фильтрации, БД шинглов и таблиц RBL.

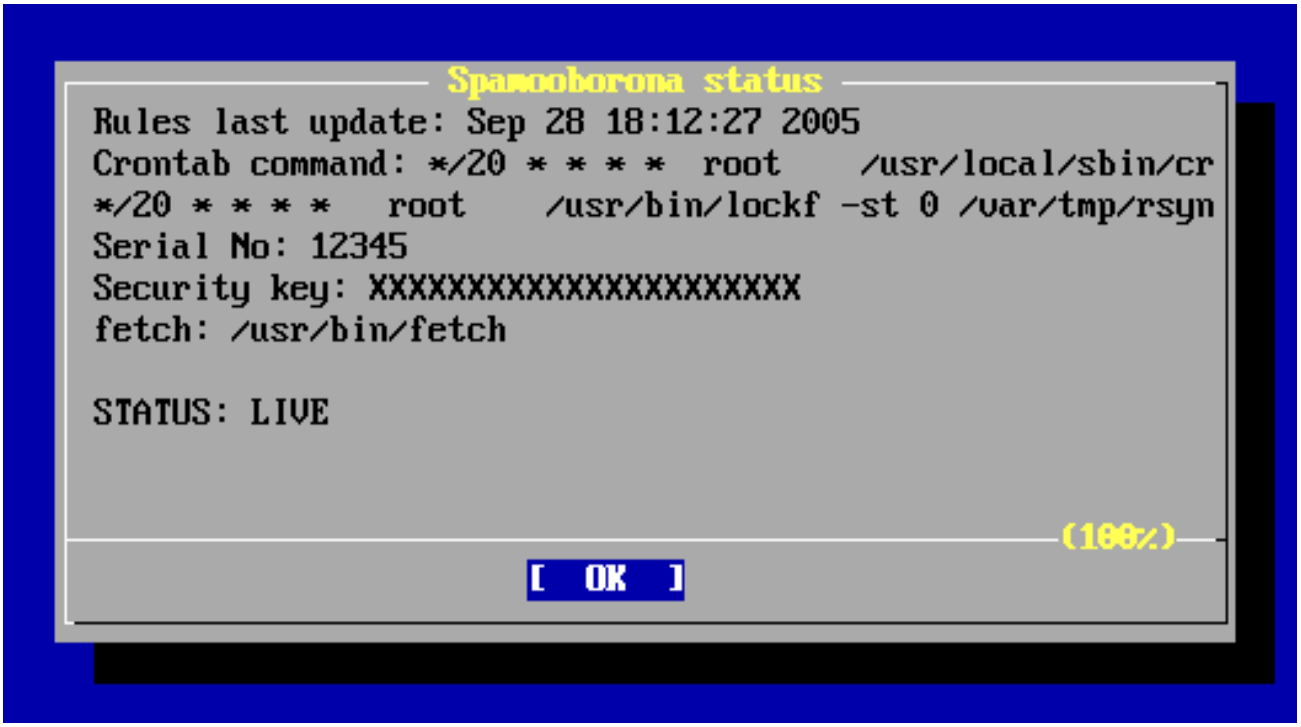


1.9.1 Rules

Подраздел «Rules» предназначен для работы с коллекцией правил фильтрации.



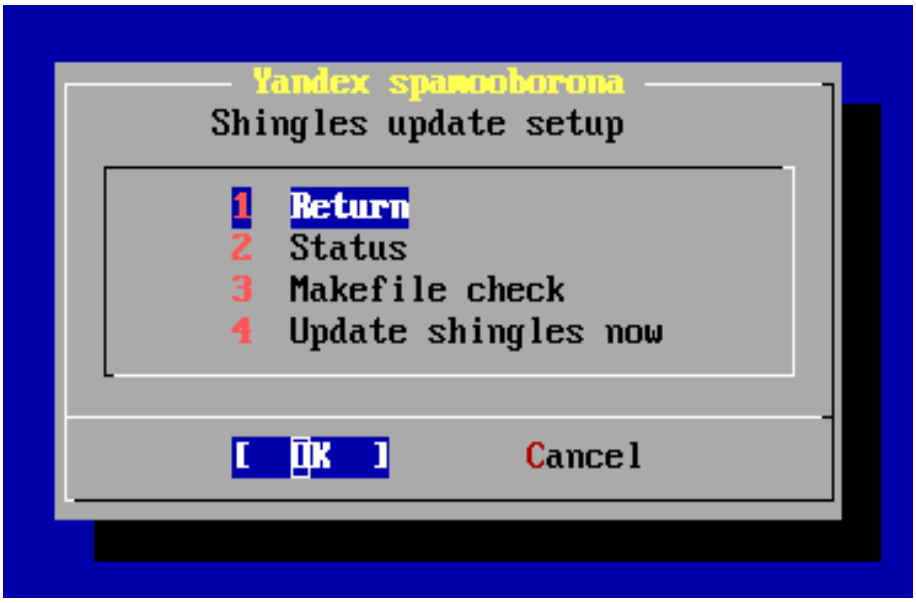
- «Status» позволяет определить корректность получения обновлений коллекции. При правильных настройках и работающем обновлении вы увидите STATUS: LIVE. При любом другом статусе кроме «BAD», вы можете попытаться получить обновления, выбрав «Update rules now». Также доступна информация о дате последнего обновления коллекции.



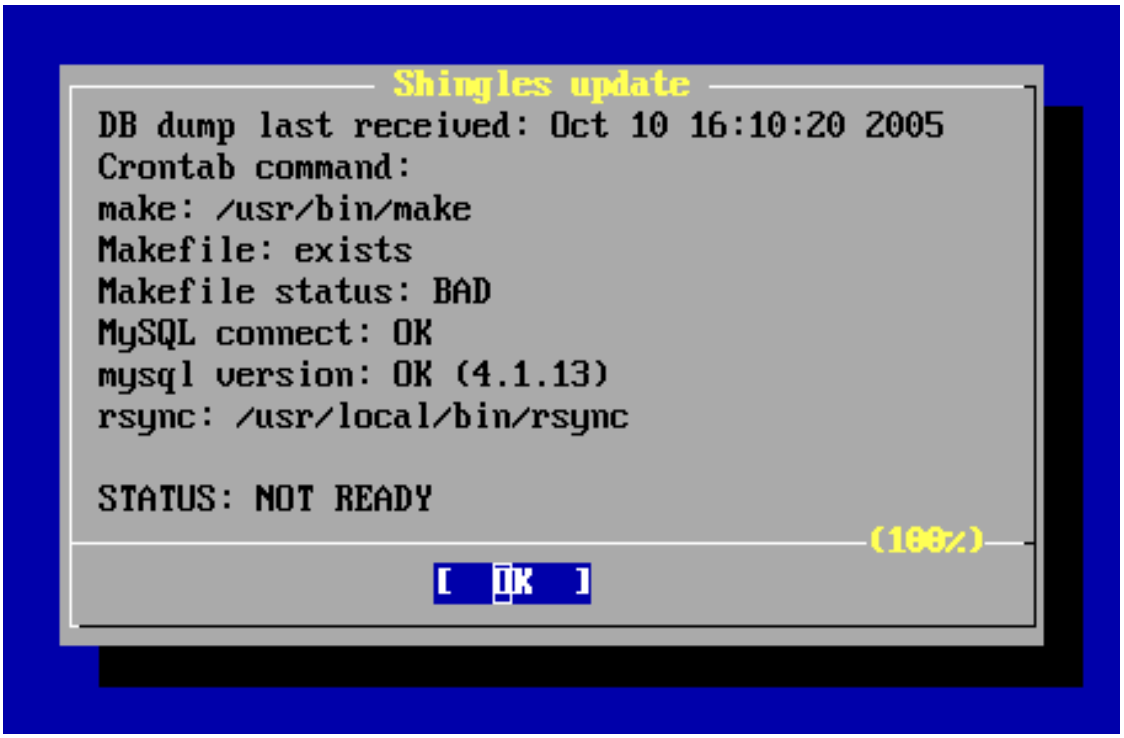
- «Update rules now» запускает сценарий получения обновления коллекции.

1.9.2 Shingles

Пункт меню «Shingles» предназначен для выполнения типовых операций с обновляемой БД шинглов (для режима работы с локальной копией БД шинглов).

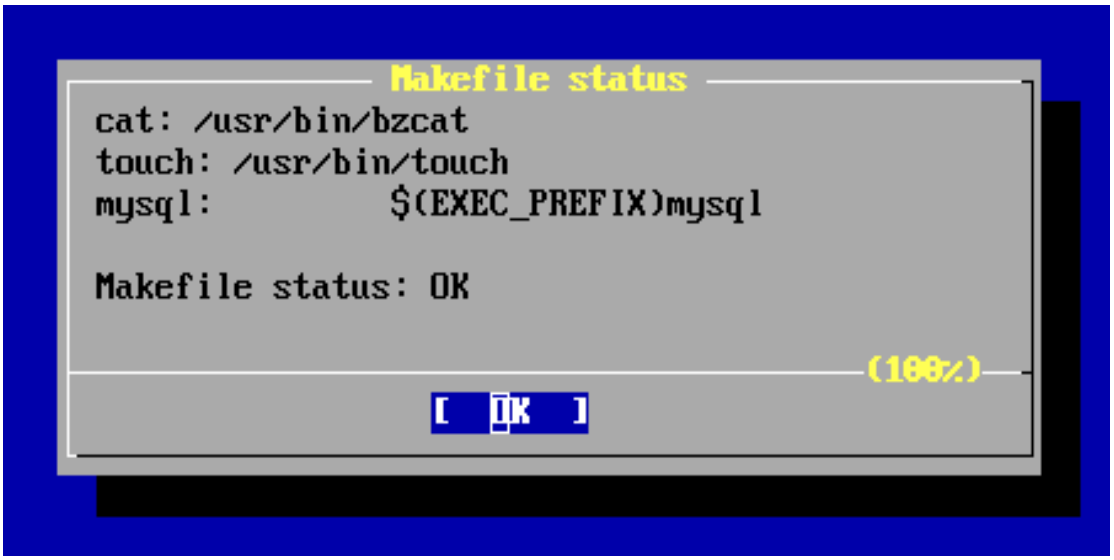


- «Status» выполняет проверку настройки обновления и выводит статусную информацию. При правильной настройке и работающем обновлении вы увидите STATUS: LIVE. Если Makefile status не равен «OK», то выполните проверку «Makefile check».



- «Makefile check» отображает состояние файла `Makefile`. Если status не равен «OK», то выводится описание причины. Обратите внимание, что EXEC_PREFIX задаётся в самом файле Makefile и может быть изменен как в нем, так и в парамет-

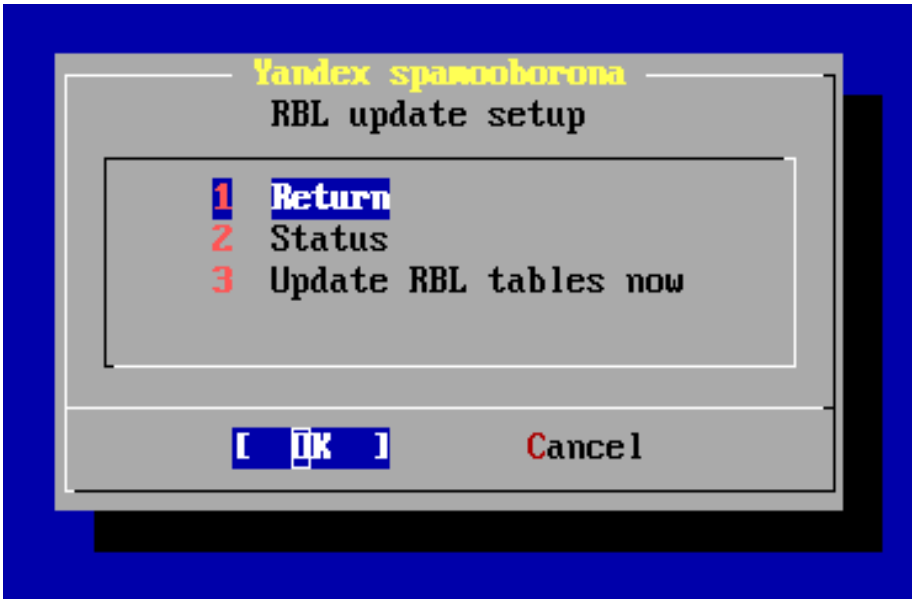
рах командной строки, например `make -D EXEC_PREFIX=/opt/mysql/bin`.



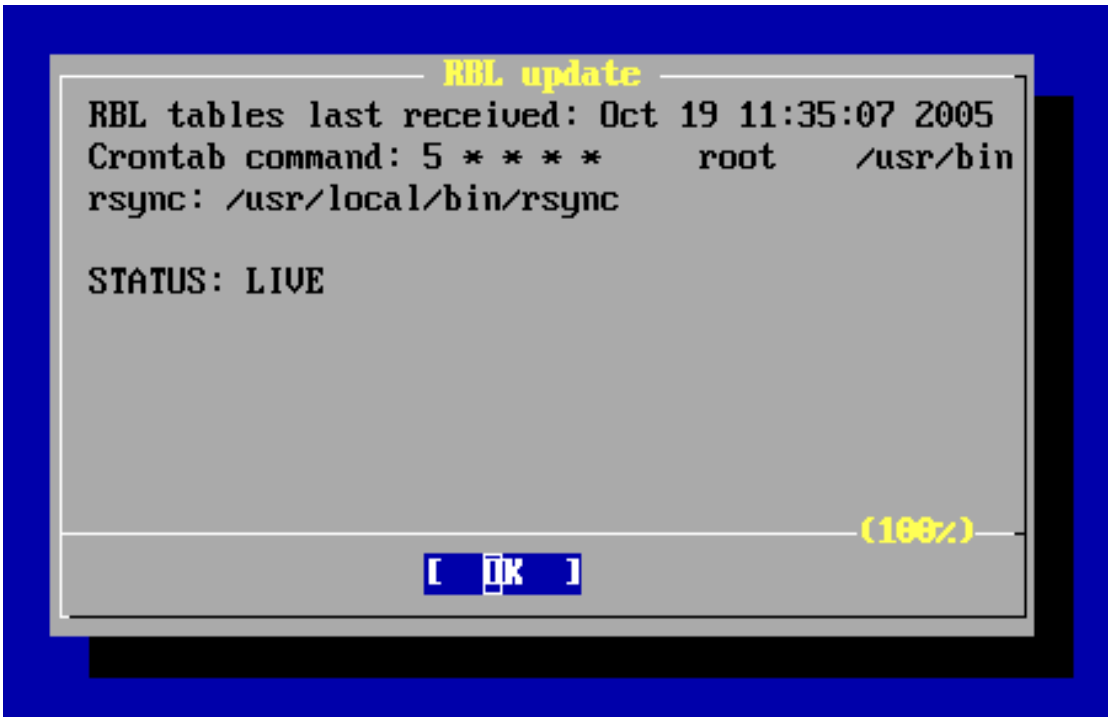
- «Update shingles now» запускает сценарий получения обновления локальной копии БД шинглов. Имейте в виду, что время загрузки локальной копии БД шинглов может быть значительным. Если `Makefile` еще не был создан, после получения архива локальной копии и шаблона `Makefile.dist` сценарий автоматически создаст `Makefile` копией из шаблона.

1.9.3 RBL tables

По аналогии с подразделом «Shingles» пункт «RBL tables» содержит средства администрирования обновлений RBL DNS зон (для режима работы с локальной копией RBL).



- «Status» проверяет настройку обновления и выводит информацию о состоянии. При правильной настройке и работающем обновлении вы увидите STATUS: LIVE.

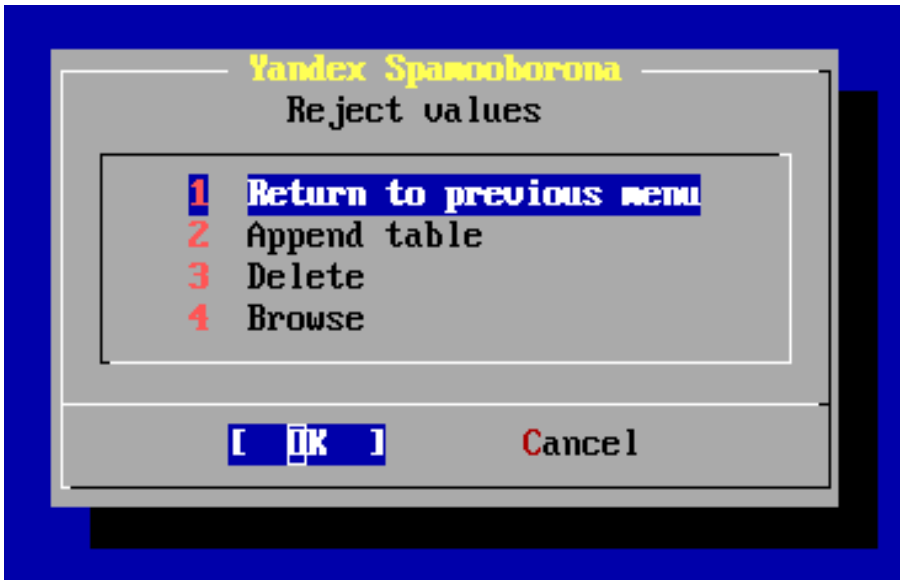


- «Update RBL tables now» запускает сценарий получения обновления локальной копии таблиц RBL DNS.

1.10 Reject values table

Раздел «Reject values table» предназначен для работы с таблицей персональных порогов отказа.

В случае, когда включен режим, допускающий отказ от приема почты по превышению порога набранных баллов, с помощью этой таблицы можно указать, на какие адреса почта должна доставляться в любом случае. Для этого надо установить порог reject = 0.



- «Append table» позволяет выполнить добавление записи в формате локальный адрес – пороговое значение reject.
- «Delete» удаляет указанный почтовый адрес из таблицы.
- «Browse» выводит содержимое таблицы персональных порогов.

Приложение 2. Возможные проблемы и их решение

Проблема	Причина и решение
Проблема с MySQL: sp-milter: db localhost problem: Client does not support authentication protocol requested by server; consider upgrading MySQL client	Способ авторизации MySQL не совпадает. Требуется использовать опцию old-passwords (см. гл.1.4 Необходимые пакеты сторонних производителей)
Проблема с MySQL при попытке обновления локальной базы шинглов в /var/db/so-dump	На сервере установлена более ранняя версия MySQL чем 4.1. Согласно требованиям (п.1.4 Необходимые пакеты сторонних производителей) в случае локальной базы шинглов версия MySQL должна быть строго 4.1. Требуется модернизация MySQL до 4.1.

«Спамооборона» не запускается	Для определения причин этой проблемы необходимо:
	1. Направить протокол работы продукта в стандартный почтовый лог. Для этого проверить и при необходимости исправить в spam.ini строки
	`spam.Syslog: 1`
	`#spam.fnLog:  /var/yamail/log/spam.log`
	`#spam.fnStatistics: /var/yamail/log/spamstat.log`
	2. Перезапустить «Спамооборону», для этого:
	- запустить скрипт администрирования adm_so;
	- выполнить Spamooborona stop;
	- выполнить Spamooborona start.
	3. Проверить /var/log/maillog на наличие строк вида
	`MESS_F *** All success rules: 2688`
	
	Отсутствие данных строк означает, что «Спамооборона» не запускается.
	
	Для решения проблемы требуется:
	- проверить системный журнал /var/log/messages на предмет наличия строк вида
	`Security key invalid`
	
	Наличия такой строки означает использование неверного ключевого файла, например, по причине редактирования пользователем файла Spam.ini, либо порчи последнего при его передаче на регистрацию.
	Требуется заново зарегистрировать продукт (гл. 2.4).
	- проверить и при необходимости исправить настройки почтового сервера, прописав там запуск продукта согласно документации.
	
	Если это сделать невозможно, или проблема не устраняется — обратиться в Службу технической поддержки, приложив к письму архив, в который упаковать файл spam.ini и текстовый файл со скопированными туда выдержками из файлов maillog и

	messages.
Почта не доставляется	Убедиться, что «Спамооборона» запускается, для чего выполнить описанные выше действия. Если «Спамооборона», но почта не доставляется адресатам, это означает, что передача почты почтовым сервером не настроена должным образом. Для исправления проблемы требуется проверить и при необходимости исправить настройки почтового сервера, направив почту через фильтр. Если настройки почтового сервера корректны, но проблема не устраняется, обратитесь в Службу технической поддержки.

Почта доставляется, но маркировка спама не происходит	Убедиться, что почта действительно не размечается, для этого:
	1. Открыть в почтовом клиенте свойства письма
	2. Проверить наличие в нем служебных заголовков
	`X-Spam-Yversion`
	`X-Spam-Flag`
	Отсутствие данных строк означает, что почтовый сервер не настроен должным образом и не направляет почту через фильтр.
	Для исправления проблемы требуется проверить и при необходимости исправить настройки почтового сервера, направив почту через «Спамооборону» согласно документации.
	
	Если настройки сервера корректны, но проблема не устранена, обратитесь в Службу технической поддержки.

Почта помечается флагом SKIP	Адресат не входит в число защищаемых, либо работа продукта блокирована системой защиты. *Обращаем Ваше внимание на то, что адресатом считается истинный получатель, который был указан в команде RCPT TO протокола SMTP.* Убедиться, что:. 1. Адресат есть в списке пользователей В случае его отсутствия, требуется его добавить, для этого необходимо: - запустить скрипт администрирования adm_so - внести данного адресата в список пользователей 2. Домен адресата зарегистрирован, то есть присутствует среди перечисленных в файле конфигурации spam.ini доменов. В случае отсутствия домена в этом списке, требуется его зарегистрировать, Для этого: - скопировать во временную директорию файл spam.ini - добавить в этот файл новый домен - сохранить текущие so.key и spam.ini - заново зарегистрировать продукт, используя обновленный spam.ini и выполнив опи-

	санные выше действия. 3. Срок лицензионного использования продукта не истек. В случае истечения срока лицензии, требуется получить новую, для чего достаточно получить новый ключевой файл в компании «ДиалогНаука». В случае, если предлагаемые действия не решат проблему, обратитесь в Службу технической поддержки.
Большое время обработки письма	Запросы к серверам DNS или MySQL обрабатываются с задержками или не обрабатываются вообще, система ожидает ответа. Проверить время отклика сервера шинглов и сервера RBL DNS вручную или через административный интерфейс adm_so. Если ответы RBL DNS сервера отсутствуют, проверить содержимое файлов /etc/resolv.conf и /etc/namedb/named.conf (/etc/named.conf). Если настройки в порядке, но соединения нет, проверить настройки межсетевых экранов, не блокируют ли они запросы.
Нет доступа к серверу обновлений	Удостовериться, что нет доступа к серверу обновлений, для чего: 1. Запустить скрипт администрирования системы adm_so и выполнить: Update Shingles Update RBL 2. Проверить ответ на наличие строк вида: `rsync: failed to connect to cso.yandex.ru: Operation timed out` 3. Выполнить: Update Rules 4. Проверить ответ на наличие строк вида: … `Operation timed out` Наличие данных строк означает невозможность установить связь с сервером обновлений. Для исправления проблемы требуется проверить настройки межсетевых экранов и обеспечить доступ к серверу обновлений, открыв соединения на сервер «Спамообороны» для требуемых портов (873 для rsync, 80 для fetch, 443 для https, 53 для dns, 25) и прочее согласно документации.
Базы шинглов или RBL не обновляются	Убедиться, что есть доступ к серверу обновлений, для этого необходимо выполнить описанные в предыдущем пункте («Нет доступа к серверу обновлений») действия. Если настройки корректны, но проблема не устранена, обратитесь в службу технической поддержки, приложив к письму архив, в который поместить файл spam.ini и текстовый файл со скопированным туда протоколом произведенных действий.
Обновления правил фильтрации (файл so.dat) невозможно загрузить с сервера, либо устанавли-	Доступ к серверу обновлений закрыт, неверный формат запроса либо ключ заблокирован.

ваемые обновления испорчены (нулевой длины)	1. Убедиться, что есть доступ к серверу обновлений, для чего выполнить описанные в пункте «Нет доступа к серверу обновлений» действия. 2. В случае если доступ к серверу обновлений открыт, требуется проверить формат запроса: логин и пароль должны совпадать с серийным номером и ключом, прописанным в файле so.key. Например, если в файле so.key прописано: serial: 111111111 key: 22222222222222222222 формат запроса при получении файла so.dat должен быть fetch https://111111111:22222222222222222222@cso.yandex.ru/111111111/so.dat Если формат запроса отличается от указанного, это означает, что используется неверный ключ либо устаревший протокол. Требуется зайти на страницу «Загрузить» сайта компании «ДиалогНаука» (http://www.dialognauka.ru/so), и ознакомиться с инструкциями по обновлению. 3. Если доступ к серверу обновлений открыт, и формат запроса совпадает с предписанным, но получение данных невозможно, это означает, что ключ заблокирован. В случае, когда проблема не устраняется, либо ключ заблокирован, требуется обратиться в Службу технической поддержки, приложив к письму архив, в который поместить файлы so.dat, spam.ini и текстовый файл со скопированным туда протоколом произведенных действий.
Почта помечается только флагами NO и SKIP, флаг YES нигде не встречается.	Неправильный so.dat, вероятно неверное значение ключа. Обратитесь в службу технической поддержки.
Не стартует автодобавление в «белый список» (maillog parser)	Отсутствуют модули DBI или DBD::MySQL, необходимые для работы автодобавления, необходимо их установить.