ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по настройке механизмов безопасности почтового сервера, созданного с использованием программного обеспечения с открытым исходным кодом Exim, от атак, связанных с подменой отправителя (спуфинг-атак)

2025

1. Настройка механизма SPF

1.1 Exim поддерживает проверку SPF-записи с помощью модуля spf или внешней библиотеки exim-spf.

1.2 В случае использования встроенной поддержки SPF в Exim необходимо, чтобы Exim был скомпилирован с поддержкой SPF (WITH_SPFCHECK=YES).

1.3 Для того, чтобы проверить, что Exim поддерживает SPF необходимо выполнить следующие команды в терминале (командной строке) операционной системы на базе Linux (далее по тексту все команды аналогично выполняются в терминале (командной строке) операционной системы):

exim -bV | grep SPF

Если после выполнения указанной команды выводится сообщение «Support for: SPF», значит SPF поддерживается. В случае, если в выводе нет указанной строки, то необходимо перейти к пункту 6.5.

1.4 Также рекомендуется осуществить следующую настройку конфигурации почтового сервера:

открыть файл /etc/exim/exim.conf в любом текстовом редакторе, например:

nano /etc/exim/exim.conf;

найти раздел *acl_check_rcpt*, отвечающий за обработку входящей почты и добавить в него следующие строки для проверки SPF:

deny

spf = fail

message = Ваш почтовый сервер не прошел SPF-проверку ($sender_host_address не разрешен для $sender_address_domain);

также рекомендуется дополнительно настроить проверку SoftFail добавлением строк:

warn

spf = softfail

message = Предупреждение: Домен $sender_address_domain настроен с SPF SoftFail;

далее необходимо сохранить файл путем нажатия сочетания клавиш сохранить изменения путем нажатия сочетания клавиш Ctrl+O и закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

перезапустить Exim командой *systemctl restart exim*.

1.5 Для установки и настройки модуля exim-spf (внешняя библиотека) необходимо:

произвести установку библиотеки exim-spf командой:

для Debian (Ubuntu, Astra Linux):

apt install exim4-daemon-heavy libspf2-2;

CentOS (RHEL):

yum install exim exim-spf.

1.6 После установки необходимо проверить поддержку SPF командой:

exim -bV | grep SPF;

в случае, если в выводе есть запись «Support for SPF», то все установлено правильно.

Также рекомендуется следующую настройку конфигурации почтового сервера:

открыть конфигурационный файл Exim в любом текстовом редакторе, например командой: *nano /etc/exim/exim.conf*;

в разделе acl_check_rcpt добавить следующие строки:

deny

spf = fail

message = Отправитель $sender_address_domain не прошел SPF проверку.

далее необходимо сохранить файл путем нажатия сочетания клавиш сохранить изменения путем нажатия сочетания клавиш Ctrl+O и закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

перезапустить Exim командой *systemctl restart exim*.

Для проверка корректности проверки SPF необходимо:

отправить тестовое письмо с почтового сервера, не имеющего корректной SPF-записи;

открыть заголовки письма в почтовом клиенте и найти строку, например, X-SPF-Check: SPF Fail (192.168.1.100).

В случае, если письмо отклонено, в логах Exim будет строка:

Rejected: SPF check failed for sender@example.ru.

В случае, если SPF настроен правильно, должен быть ответ вида:

v=spf1 ip4:192.168.1.1 -all.

2. Настройка механизма DKIM

2.1 Необходимо установить нужные пакеты и убедиться, что Exim поддерживает DKIM. Осуществить установку (обновление) необходимо следующими командами:

для Debian (Ubuntu, Astra Linux):

apt update && apt install exim4;

для CentOS (RHEL):

yum install exim.

6.8 Проверить поддержку DKIM необходимо командой:

exim -bV | grep -i dkim

В случае, если в выводе терминала (командной строки) есть «Support for DKIM», значит Exim поддерживает DKIM.

2.2 Для создания DKIM-ключей необходимо:

создать каталог для хранения ключей и установить ему права доступа командами:

mkdir -p /etc/exim4/dkim

chown -R Debian-exim:Debian-exim /etc/exim4/dkim

chmod 700 /etc/exim4/dkim;

сгенерировать ключевую пару командами:

openssl genpkey -algorithm RSA -out /etc/exim4/dkim/private.key -pkeyopt rsa_keygen_bits:2048

openssl rsa -in /etc/exim4/dkim/private.key -pubout -out /etc/exim4/dkim/public.key

и выставить необходимые правила путем ввода следующих команд:

*chown Debian-exim:Debian-exim /etc/exim4/dkim/**

chmod 600 /etc/exim4/dkim/;*

скопировать значение публичного ключа из */etc/exim4/dkim/public.key* для добавления его значения в DNS -запись (смотреть пункт 2.3).

2.3 Для настройки подписывания электронных писем сервером Exim необходимо:

открыть конфигурационный файл Exim командой:

nano /etc/exim4/exim4.conf.template;

добавить в секцию MAIN CONFIGURATION следующие строки (в примере заменить example.ru на ваш реальный домен):

DKIM_DOMAIN = example.ru

DKIM_SELECTOR = default

DKIM_PRIVATE_KEY = /etc/exim4/dkim/private.key

DKIM_CANON = relaxed

DKIM_STRICT = false

сохранить изменения путем нажатия сочетания клавиш Ctrl+O;

закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

перезапустить Exim командами:

update-exim4.conf

systemctl restart exim4.

2.4 Для проверки DKIM необходимо отправить тестовое письмо с использованием почтового сервера и проверить заголовки сообщения (Message Headers). Работоспособность DKIM подтверждается в случае нахождения в них строки:

DKIM-Signature: v=1; a=rsa-sha256; d=example.ru

Кроме того, возможно использовать для проверки DKIM следующую команду: *exim -bP dkim*.

3. Настройка механизма DMARC

3.1 Перед настройкой DMARC в Exim необходимо убедиться, что SPF, DKIM и DMARC записи размещены в DNS (разделы 1-3).

3.2 Для осуществления настройки DMARC в Exim необходимо установить OpenDMARC командами:

для Debian (Ubuntu, Astra Linux):

apt update && apt install opendmarc

для CentOS (RHEL):

yum install epel-release

yum install opendmarc

3.3 Для настройки OpenDMARC необходимо осуществить следующую настройку конфигурации:

открыть конфигурационный файл OpenDMARC командой:

nano /etc/opendmarc.conf;

настроить следующие параметры (в примере директории, IP-адрес и порт заменить на реальные данные почтового сервера):

AuthservID example.ru

ForensicReports true

ForensicReportsSentBy noreply@example.ru

HistoryFile /usr/local/etc/exim/dmarc.dat

3.4 Необходимо создать с необходимыми правами файл для сбора статистики в директории */usr/local/etc/exim* командами:

touch dmarc.dat

chmod 666 dmarc.dat

сохранить изменения путем нажатия сочетания клавиш Ctrl+O и закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

3.5 Для настройки DMARC в Exim необходимо осуществить следующую настройку конфигурации:

открыть конфигурацию Exim командой:

cat configure | grep dmarc

dmarc_tld_file = /usr/local/etc/exim/public_suffix_list.dat

dmarc_history_file = /usr/local/etc/exim/dmarc.dat

dmarc_forensic_sender = noreply@example.ru

3.6 Кроме того, рекомендуется отключить проверки DMARC для доверенных хостов (если они специально не требуют такого обслуживания) из списка *+relayfromhosts* в соответствующем правиле ACL командой:

control = dmarc_disable_verify

3.7 Для остальных хостов рекомендуется включить проверку DMARC и оперативное информирование по запросам правилом:

warn control = dmarc_enable_forensic

3.8 Для применения настроек необходимо перезапустить Exim командами:

update-exim4.conf

systemctl restart exim4.