*Настройка SPF, DKIM и DMARC*

**Шаг 1: Настройка SPF (Sender Policy Framework)**

1.1. SPF - мера безопасности, разработанная для того, чтобы не дать другим отправлять электронные письма от Вашего имени. Она определяет, каким IP-адресам разрешена отправка, а каким нет.

1.2. Чтобы настроить SPF, необходимо добавить запись TXT в настройки DNS домена. Эта запись должна выглядеть следующим образом:

//

Имя: [Your\_Domain].

Значение: v=spf1 ip4:[Your\_Mail\_Server\_IP] a mx ~all

//

Замените [Your\_Domain] на доменное имя и [Your\_Mail\_Server\_IP] на IP-адрес Вашего почтового сервера.

**Шаг 2: Настройка DKIM (DomainKeys Identified Mail)**

2.1. DKIM - метод проверки подлинности почтовых сообщений. Когда каждое письмо отправляется, оно подписывается с помощью закрытого ключа, а затем проверяется на принимающем почтовом сервере (или у провайдера) с помощью открытого ключа в DNS.

2.2. Сначала устанавливаем opendkim и opendkim-tools. Процесс установки зависит от операционной системы:

Для CentOS:

//

*yum install opendkim -y*

//

Для Debian/Ubuntu:

//

*apt install opendkim opendkim-tools -y*

//

2.3. Далее запустите службу opendkim и включите ее запуск при загрузке:

//

*systemctl start opendkim*

*systemctl enable opendkim*

//

2.4. Создайте каталог для хранения ключей:

//

*mkdir -p /etc/opendkim/keys/yourdomain.com*

//

2.5. Сгенерируйте ключи с помощью инструмента opendkim-genkey:

//

*opendkim-genkey --directory /etc/opendkim/keys/yourdomain.com/ --domain yourdomain.com --selector dkim*

//

Не забудьте заменить "yourdomain.com" на реальное доменное имя.

2.6. Установите соответствующие разрешения для ключей:

//

*chown -R opendkim:opendkim /etc/opendkim/keys/yourdomain.com*

//

2.7. Теперь необходимо настроить opendkim. Откройте файл /etc/opendkim.conf и добавьте следующие настройки:

//

*AutoRestart             Yes*

*AutoRestartRate      10/1h*

*Umask                    002*

*Syslog                  Yes*

*SyslogSuccess          Yes*

*LogWhy                  Yes*

*Canonicalization        relaxed/simple*

*ExternalIgnoreList     refile:/etc/opendkim/TrustedHosts*

*InternalHosts            refile:/etc/opendkim/TrustedHosts*

*KeyTable                refile:/etc/opendkim/KeyTable*

*SigningTable            refile:/etc/opendkim/SigningTable*

*Mode                    sv*

*PidFile                  /var/run/opendkim/opendkim.pid*

*SignatureAlgorithm      rsa-sha256*

*UserID                  opendkim:opendkim*

*Socket                  inet:8891@localhost*

//

2.8. Добавьте свой домен в файл /etc/opendkim/TrustedHosts:

//

*127.0.0.1*

*localhost*

*\*.yourdomain.com*

//

2.9. Измените файл /etc/opendkim/KeyTable, чтобы он выглядел следующим образом:

//

*dkim.\_domainkey.yourdomain.com yourdomain.com:dkim:/etc/opendkim/keys/yourdomain.com/dkim.private*

//

2.10. Измените файл /etc/opendkim/SigningTable так, чтобы он выглядел следующим образом:

//

*\*@yourdomain.com dkim.\_domainkey.yourdomain.com*

//

2.11. Если используете Debian/Ubuntu, укажите порт для opendkim:

//

*echo 'SOCKET="inet:8891@localhost"' >> /etc/default/opendkim*

//

2.12. Добавьте DKIM в конфигурацию postfix:

//

*postconf -e 'milter\_default\_action=accept'*

*postconf -e 'milter\_protocol=2'*

*postconf -e 'smtpd\_milters=inet:127.0.0.1:8891'*

*postconf -e 'non\_smtpd\_milters=inet:127.0.0.1:8891'*

//

2.13. Перезапустите службы opendkim и postfix, чтобы применить изменения:

//

*systemctl restart opendkim*

*systemctl restart postfix*

//

2.14. Наконец, добавьте открытый ключ в настройки DNS домена. Ключи находятся в файле /etc/opendkim/keys/yourdomain.com/dkim.txt.

**Шаг 3: Настройка DMARC (Domain-based Message Authentication, Reporting & Conformance)**

3.1. DMARC - система проверки электронной почты, разработанная для обнаружения и предотвращения подделки электронной почты.

3.2. Чтобы настроить DMARC, добавьте запись TXT в настройки домена:

//

*Name: \_dmarc.[Your\_Domain].*

*Значение: v=DMARC1; p=none; aspf=r; sp=none*

//

Замените [Your\_Domain] на имя Вашего домена.

После выполнения этих шагов у электронных писем сервера будет гораздо меньше шансов быть помеченными как спам, что гарантирует, что они дойдут до адресатов.