

SPF (Sender Policy Framework)

SPF позволяет владельцу домена, с помощью специальной записи в [DNS](#), указать список серверов, имеющих право отправлять электронную почту с обратными адресами в этом домене.

Принимающая сторона запрашивает SPF-информацию с помощью простого DNS-запроса, проверяя таким образом сервер отправителя.

<http://www.openspf.org/>

⚠ Можно использовать совместно с [DKIM \(Domain Keys Identified Mail\)](#)

Настройка

Нужно создать новую запись [DNS](#):

Имя записи	@
Тип записи	TXT
Значение	v=spf1 +a +mx -all

Пример готовой записи:

```
domain.ru. IN TXT "v=spf1 +a +mx -all"
```

Пояснения:

v=	версия SPF
+a	разрешить прием писем от узла, IP-адрес которого совпадает с IP-адресом в А-записи для домена
+mx	разрешить прием писем, если отправляющий узел указан в одной из MX-записей домена
-all	сообщения, не прошедшие проверку будут отвергнуты, можно указать ~all, в этом случае письмо, не прошедшее верификацию, не должно быть отклонено, и может быть изучено более тщательно (SoftFail)

Google (Gmail)

Нужно создать новую запись [DNS](#):

Имя записи	@
Тип записи	TXT
Значение	v=spf1 include:_spf.google.com ~all

Пример готовой записи:

```
domain.ru. IN TXT "v=spf1 include:_spf.google.com ~all"
```

[Настройка SPF-записи - Домены - Справочный центр Timeweb](#)

Тестирование

[SPF Record Testing Tools](#)

[Проверьте Ваши SPF и DKIM записи](#)

Ссылки

 [Sender Policy Framework](#)

<http://sysadminmosaic.ru/spf/spf>

2022-06-17 19:15

