ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по базовой настройке механизмов безопасности почтовых сервисов от атак, связанных с подменой отправителя (спуфинг-атак)

2025

1. Инструкция по базовой настройке механизма безопасности Sender Policy Framework (SPF)

1.1 Прежде чем осуществлять настройку проверки SPF-записи для используемых почтовых серверов, необходимо опубликовать SPF-запись в DNS (в случае аренды домена на стороннем хостинге).

В случае использования внешних почтовых сервисов например Почта Mail, Яндекс.Почта без аренды домена настройка механизма безопасности SPF предусмотрена указанными сервисами по умолчанию и не является настраиваемой.

1.2 Необходимо определить список разрешенных серверов, которые должны отправлять почту от имени вашего домена (например, серверы Postfix, Exim, почтовые шлюзы (при наличии), внешние сервисы рассылки Почта Mail, Яндекс.Почта).

1.3 Необходимо создать SPF-запись путем добавления TXT-записи в DNS домена.

Например, SPF-запись для почтового сервера, работающего на IP-адресе 192.168.1.100 выглядит следующим образом:

v=spf1 ip4:192.168.1.100 -all

В случае использования внешнего почтового сервиса, например, Яндекс.Почты, SPF-запись выглядит следующим образом:

v=spf1 redirect:_spf.yandex.net -all

В случае комбинации локального сервера и внешних сервисов SPF-запись выглядит следующим образом:

v=spf1 ip4:192.168.1.100 include:_spf.yandex.net -all

1.4 Расшифровка параметров:

v=spf1 является версией, всегда принимает значение spf1;

a – разрешает прием писем с адреса, который указан в A и\или AAAA записи домена отправителя;

mx – разрешает принимать письма с адреса, который указан в mx записи домена;

all – определяет, что будет происходить с письмами, которые не соответствуют установленной политике: "-" – отклонять, "+" – пропускать, "~" – дополнительные проверки, "?" – нейтрально;

include – разрешает принимать письма с серверов, разрешенных SPF-записями домена;

ip4 и ip6 – уточняющие параметры для указания конкретных адресов.

1.5 Для добавления созданной SPF-записи в DNS домена необходимо:

открыть DNS-менеджер (например, панель управления хостингом, на котором осуществляется аренда домена);

перейти в зону вашего домена;

добавить новую TXT-запись со следующими параметрами:

Имя: @ (или ваш домен, например, example.ru)

Тип: TXT

Значение: *v=spf1 ip4:192.168.1.100 -all*

сохранить изменения.

Отмечаем, что после добавления записи необходимо подождать до 24 часов для обновления DNS.

1.6 В случае использования в качестве основного почтового сервиса Почта Mail или Яндекс.Почта для настройки SPF-записи необходимо:

перейти в раздел «Домены» — «Мои домены»;

найти нужный домен, нажать на значок шестеренки и выбрать «Настройки DNS»;

удалить имеющиеся TXT-записи, начинающиеся с v=spf1 (предварительно скопировав значения spf-записи, если есть необходимость отправлять почту также и с указанных в ней серверов);

выбрать «Добавить DNS-запись», далее выбрать «TXT» и в открывшемся окне разместить следующее значение:

v=spf1 redirect=_spf.mail.ru или *v=spf1 redirect=_spf.yandex.net* соответственно

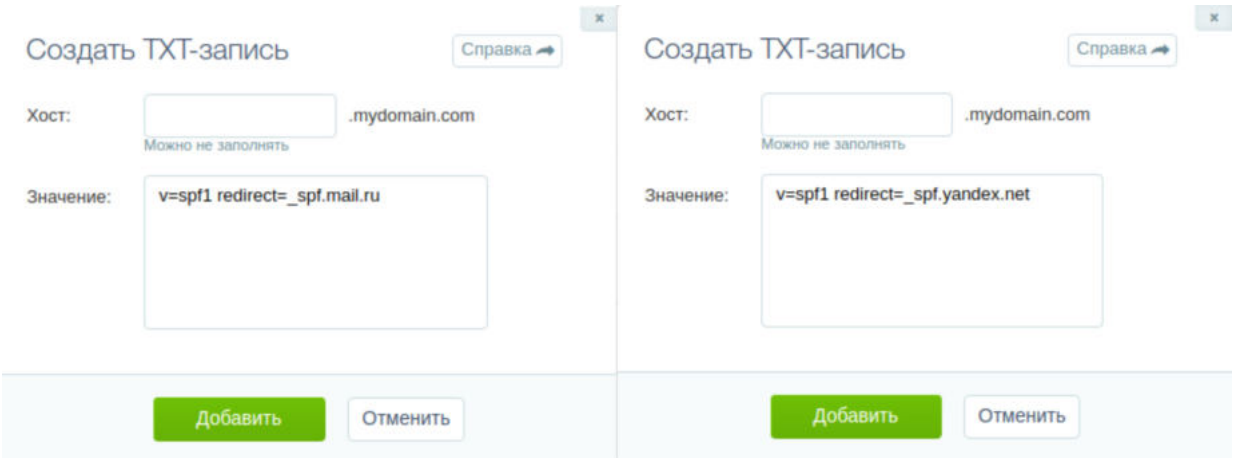


Рисунок 1 — Поле добавления SPF-записи в DNS

1.7 В случае, если имеется необходимость отправлять письма не только с серверов Mail.ru, то дополнительные серверы указываются в SPF-записи в следующем формате:

v=spf1 ip4:IP1 ip4:IP2 ip4:IP3 include:_spf.mail.ru -all

где IP-1, IP-2, IP-3 — IP-адреса дополнительных серверов;

сохранить изменения с помощью кнопки «Добавить»;

подождать, пока изменения в DNS вступят в силу (этот процесс может занимать до 72 часов).

1.8 Для осуществления проверки правильности добавления SPF-записи необходимо:

запустить терминал (командную строку) операционной системы и проверить, что DNS правильно отдает SPF-запись путем ввода команды, например:

для операционной системы Windows

nslookup -type=txt fstec.ru

для операционных систем на базе Linux

dig fstec.ru TXT

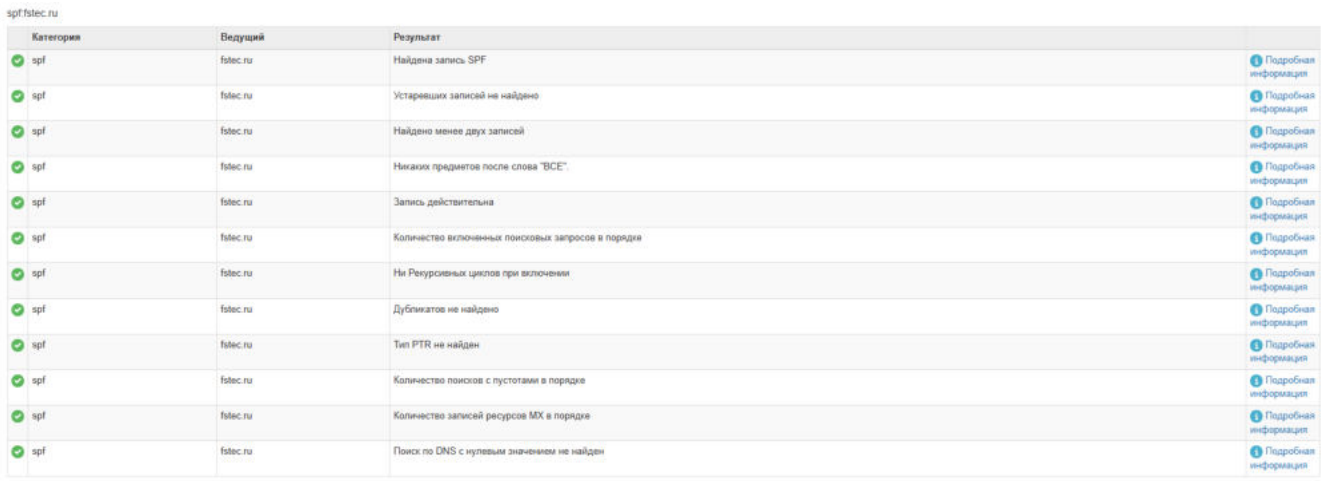
Итогом проверки для домена fstec.ru будет:

```
fstec.ru        text =

        "v=spf1 include:dc1.nicmail.ru include:dc2.nicmail.ru -all"
```

Рисунок 2 — Итог проверки SPF-записи

Для онлайн-проверки SPF-записи возможно использовать сервис https://mxtoolbox.com/SPF.aspx.



spf:fstec.ru

	Категория	Ведущий	Результат	
✓	spf	fstec.ru	Найдена запись SPF	Подробная информация
✓	spf	fstec.ru	Устаревших записей не найдено	Подробная информация
✓	spf	fstec.ru	Найдено менее двух записей	Подробная информация
✓	spf	fstec.ru	Никаких предметов после слова "ВСЕ"	Подробная информация
✓	spf	fstec.ru	Запись действительна	Подробная информация
✓	spf	fstec.ru	Количество включенных поисковых запросов в порядке	Подробная информация
✓	spf	fstec.ru	Ни Рекурсивных циклов при включении	Подробная информация
✓	spf	fstec.ru	Дубликатов не найдено	Подробная информация
✓	spf	fstec.ru	Тип PTR не найден	Подробная информация
✓	spf	fstec.ru	Количество поисков с пустотами в порядке	Подробная информация
✓	spf	fstec.ru	Количество записей ресурсов MX в порядке	Подробная информация
✓	spf	fstec.ru	Поиск по DNS с нулевым значением не найден	Подробная информация

Рисунок 3 — Проверка правильности настройки SPF для домена с использованием сервиса

2. Инструкция по базовой настройке функции безопасности Domain Keys Indentfied Mail (DKIM)

2.1 Прежде чем осуществлять настройку проверки DKIM-записи для используемых почтовых серверов, необходимо опубликовать DKIM-запись в DNS (в случае аренды домена на стороннем хостинге).

В случае использования внешних почтовых сервисов например Почта Mail, Яндекс.Почта без аренды домена настройка механизма безопасности DKIM предусмотрена указанными сервисами по умолчанию и не является настраиваемой.

2.2 Для создания DKIM-записи необходимо сгенерировать ключевую пару DKIM: приватный и публичный ключи для осуществления подписи исходящих электронных писем. Инструменты для генерации ключевой пары могут отличаться в зависимости от используемого почтового сервера. Процесс генерации ключевой пары описан в настоящем документе далее по тексту.

2.3 Для добавления в DNS новой записи необходимо:

войти в панель управления DNS;

добавить новую TXT-запись (по аналогии с настройкой SPF-записи, приведенной в пункте 1) со следующими параметрами:

Имя: *selector1._domainkey.example.ru*

Тип: *TXT*

Значение: *"v=DKIM1; k=rsa; p=MIIBIjANBgkqh…"* (вставить после «*p=*» сгенерированный открытый ключ);

сохранить изменения.

Отмечаем, что после добавления записи необходимо подождать до 24 часов для обновления DNS.

После выполненной настройки необходимо перезапустить почтовые сервисы и осуществить проверку DKIM.

2.4 Проверить корректность DKIM-записи в DNS возможно с использованием терминала (командной строки) операционной системы путем ввода команды, например:

для операционной системы Windows

nslookup -type=txt selector1._domainkey.example.ru;

для операционных систем на базе Linux

dig TXT selector1._domainkey.example.ru.

В результате в терминале (командной строке) операционной системы должно быть выведено значение ранее размещенной DKIM-записи.

2.5 Проверить DKIM в отправленных письмах возможно путем отправки письма на любой другой почтовый адрес, а также наличием следующих записей в заголовках письма:

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.ru; s=selector1;

Кроме того, в случае, если в заголовках присутствует запись *dkim=pass*, значит DKIM работает.

Для онлайн-проверки DKIM-записи возможно использовать сервис https://mxtoolbox.com/dkim.aspx.

3. Инструкция по базовой настройке механизма безопасности Domain-based Message Authentication, Reporting, and Conformance (DMARC)

3.1 Прежде чем осуществлять настройку проверки DMARC-записи для используемых почтовых серверов, необходимо опубликовать DMARC-запись в DNS (в случае аренды домена на стороннем хостинге).

В случае использования внешних почтовых сервисов например Почта Mail, Яндекс.Почта без аренды домена настройка механизма безопасности DMARC предусмотрена указанными сервисами по умолчанию и не является настраиваемой.

3.2 Необходимо убедиться, что SPF и DKIM уже настроены, так как DMARC полагается на эти механизмы.

3.3 Необходимо создать DMARC-запись для последующего добавления в DNS, например:

v=DMARC1; p=reject; rua=mailto:dmarc@example.ru; sp=reject; aspf=s; adkim=s; ri=604800; ruf=mailto:dmarc-failures@example.ru; fo=1

Расшифровка параметров:

v - версия протокола DMARC, принимает значение v=DMARC1 (обязательный параметр);

p – правило для домена. (обязательный параметр), принимает значения none, quarantine и reject, где:

none – не делает ничего, кроме подготовки отчетов;

quarantine – добавляет письмо в СПАМ;

reject – отклоняет письмо;

rua=mailto:dmarc@example.ru - адрес электронной почты на который присылать уведомления о результатах проверки;

adkim=s — строгая проверка DKIM (s = strict, r = relaxed).

aspf=s — строгая проверка SPF.

ri - интервал в секундах, определяющий как часто получать и агрегировать XML-отчеты;

ruf=mailto:dmarc-failures@example.ru — куда отправлять отчеты о сбоях (опционально).

fo=1 — отправлять отчеты о всех сбоях (по SPF и DKIM).

3.4 Для добавления в DNS новой записи необходимо:

войти в панель управления DNS;

добавить новую TXT-запись (по аналогии с настройкой SPF-записи, приведенной в пункте 1) со следующими параметрами:

Имя: *_dmarc.example.ru*

Тип: *TXT*

Значение: *"v=DMARC1; p=reject; rua=mailto:dmarc@example.ru; sp=reject; aspf=s; adkim=s; ri=604800; ruf=mailto:dmarc-failures@example.ru; fo=1"*.

сохранить изменения.

Отмечаем, что после добавления записи необходимо подождать до 24 часов для обновления DNS.

3.5 После выполненной настройки необходимо перезапустить почтовые сервисы и осуществить проверку DMARC.

Проверить корректность DMARC-записи в DNS возможно с использованием терминала (командной строки) операционной системы путем ввода команды, например:

для операционной системы Windows

nslookup -type=txt _dmarc.example.ru

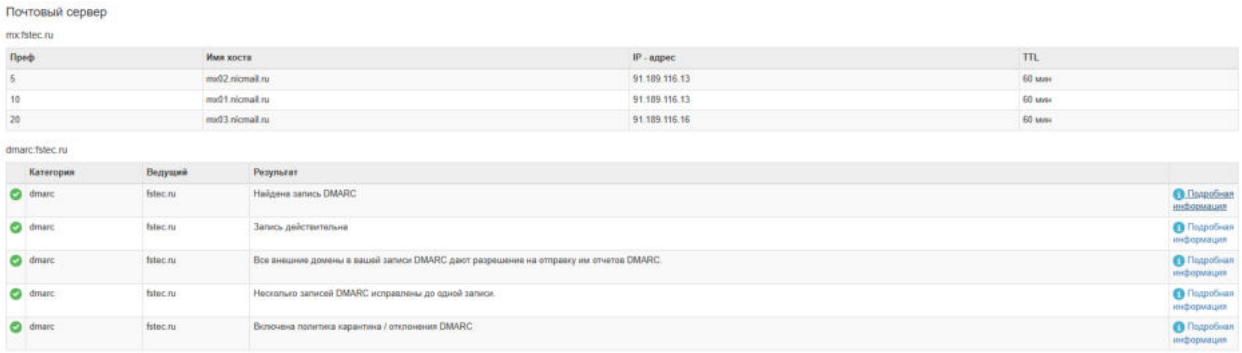
для операционных систем на базе Linux

dig TXT _dmarc.example.ru

Ожидаемый результат вывода терминала (командной строки):

_dmarc.example.ru "v=DMARC1; p=reject; rua=mailto:dmarc@example.ru; sp=reject; aspf=s; adkim=s; ri=604800; ruf=mailto:dmarc-failures@example.ru; fo=1"

Для онлайн-проверки DMARC-записи возможно использовать сервис https://mxtoolbox.com/DMARC.aspx.



Почтовый сервер

mx.fstec.ru

Преф	Имя хоста	IP - адрес	TTL
5	mx02.nicmail.ru	91.189.116.13	60 мин
10	mx01.nicmail.ru	91.189.116.13	60 мин
20	mx03.nicmail.ru	91.189.116.16	60 мин

dmarc.fstec.ru

	Категория	Ведущий	Результат	
✓	dmarc	fstec.ru	Найдена запись DMARC	Подробная информация
✓	dmarc	fstec.ru	Запись действительна	Подробная информация
✓	dmarc	fstec.ru	Все внешние домены в вашей записи DMARC дают разрешение на отправку им отчетов DMARC.	Подробная информация
✓	dmarc	fstec.ru	Несколько записей DMARC исправлены до одной записи.	Подробная информация
✓	dmarc	fstec.ru	Включена политика карантина / отклонения DMARC	Подробная информация

Рисунок 4 — Проверка правильности настройки DMARC для домена с использованием сервиса

3.6 Также необходимо реализовать мониторинг DMARC-отчетов, которые начнут приходить на указанные email-адреса (rua= и ruf=).

Отчеты бывают двух типов:

Агрегированные (rua=) — статистика прохождения SPF/DKIM.

Отчеты о сбоях (ruf=) — письма, которые не прошли проверку.

Обычно отчеты приходят в XML-формате, их можно анализировать вручную или с помощью сервисов DMARC Analyzer, Postmark DMARC.