ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по настройке механизмов безопасности почтового сервера Microsoft Exchange Server от атак, связанных с подменой отправителя (спуфинг-атак)

2025

1. Настройка механизма SPF

1.1 Настройка проверки SPF-записи в Microsoft Exchange Server требует дополнительной настройки, так как локальный Exchange Server не поддерживает проверку SPF-записи. Для реализации проверки SPF рекомендуется использовать один из подходов: настройку «Transport Rules» (Exchange Mail Flow Rules) или использование сторонних агентов (например, Exchange Antispam Agents, SpamAssassin, PFSense).

1.2 Настройка проверки SPF с помощью «Transport Rules» в Exchange Server

Для настройки проверки SPF-записи необходимо:

открыть Exchange Admin Center (EAC) в браузере (для Exchange 2016/2019: https://your-exchange-server/ecp, для Exchange 2013: https://your-exchange-server/ecp);

авторизоваться под учетной записью администратора Exchange;

перейти в раздел «Mail Flow», далее в «Rules»;

осуществить создание нового правила путем нажатия на «+» (Создать правило / Create a new rule);

в поле «Name» (Имя) указать SPF Check;

в разделе «Apply this rule if...» (Применять правило, если...) выбрать «A message header...» (Заголовок сообщения) далее выбрать «includes any of these words» (содержит слова);

в поле «Enter text» (Введите текст) указать:

Header name: Received-SPF

Header includes: Fail;

определить действия для указанного правила в разделе «Do the following...» (Действие) для этого необходимо выбрать одно из следующих действий:

отклонить сообщение - «Reject the message with the explanation» (Отклонить сообщение с объяснением) и ввести текст, например: «SPF check failed. Unauthorized sender.»;

пометить сообщение в теме - «Prepend the subject with…» (Добавить в начало темы) и ввести текст: «[SPF FAIL]»;

переместить в папку спама - «Set the message header to this value» (Установить заголовок сообщения) и указать «X-Spam-Flag» далее - «YES»;

сохранить изменения нажатием «Save» (Сохранить).

1.3 Для проверки корректности настройки проверки SPF необходимо:

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

открыть письмо в Outlook и посмотреть заголовки;

в случае, если правило сработало, то в заголовках будет строка *Received-SPF: Fail (domain.com: unauthorized sender)*;

в случае, если выбрана опция Reject, письмо не дойдет;

в случае, если выбрана опция Prepend subject, письмо будет с пометкой [SPF FAIL].

1.4 Настройка проверки SPF через Antispam Agent (Exchange Edge Transport).

1.5 В случае, если ваш Exchange Server выполняет роль Edge Transport, то рекомендуется включить встроенные Antispam Agents. Для этого необходимо:

открыть командную оболочку языка сценариев PowerShell и выполнить команду:

& $env:ExchangeInstallPath\Scripts\Install-AntispamAgents.ps1;

перезапустить Exchange Transport Service командой *Restart-Service MSExchangeTransport*.

1.6 Для настройка параметров проверки SPF-записи необходимо:

включить проверку SPF командой *Set-SenderIDConfig -Enabled $true*;

указать одно из действий при ошибке проверки SPF:

Для Reject (отклонить) *Set-SenderIDConfig -SpoofedDomainAction Reject*;

Для пометки заголовка *Set-SenderIDConfig -SpoofedDomainAction StampStatus*.

1.7 Для проверки корректности настройки проверки SPF необходимо:

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

проверить заголовки Received-SPF в Outlook (аналогично пункту 5.3).

2. Настройка механизма DKIM

2.1 Exchange Server (локальный, 2016/2019) требует установки стороннего DKIM-агента.

2.2 Рекомендуется использовать «Exchange DKIM Signer» - бесплатный open-source модуль для подписывания писем.

Установка DKIM-агента осуществляется следующим образом:

2.3 Необходимо загрузить «Exchange DKIM Signer» (https://github.com/Pro/dkim-exchange), распаковать скачанный архив и запустить ExchangeDkimSigner.Setup.exe, следовать инструкциям мастера установки.

2.4 Для генерации DKIM-ключей необходимо:

открыть «Exchange DKIM Signer Config Tool»;

перейти в C:\Program Files\Exchange DkimSigner;

запустить «Configuration.DkimSigner.exe»;

добавить домен путем нажатия «Add domain» и ввести имя вашего домена (example.ru);

сгенерировать приватный ключ путем нажатия «Generate new key» (рекомендуется выбирать 2048-bit);

сохранить приватный ключ в C:\Program Files\Exchange DkimSigner\Keys\example.com.pem;

скопировать публичный ключ в разделе «Public Key DNS Record» для добавления его значения в DNS -запись (смотреть пункт 2.3).

2.5 Для включения DKIM в Exchange Server необходимо в разделе «DKIM Signer Config Tool» выбрать «Enable DKIM». После этого необходимо перезапустить службу Exchange Transport командой:

Restart-Service MSExchangeTransport

2.6 Для проверки корректности настройки 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

3. Настройка механизма DMARC

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

3.2 Для настройки проверки DMARC необходимо авторизоваться в консоли администратора Exchange и открыть раздел «Mail Flow» (Поток почты).

3.3 Перейти в раздел «Rules» (Правила) и создать новое правило.

3.4 Ввести имя правила, например, «DMARC Verification» (Проверка DMARC).

3.5 В разделе «Apply this rule if...» (Применить это правило, если...) необходимо выбрать условие «The sender is located...» (Отправитель находится…) и выбрать ваш домен.

3.6 В разделе «Do the following...» (Выполнить следующее...) необходимо выбрать действие «Prepend the subject of the message with text...» (Добавить в начало темы сообщения текст...) и ввести «DMARC Failed» (DMARC не пройден:).

3.7 После необходимо выбрать «More options» (Дополнительные параметры) и установить флажок «Stop processing more rules» (Остановить обработку других правил).

5.21 Для применения правил необходимо нажать на кнопку сохранения «Save» (Сохранить).