МВД России

**МИНИСТЕРСТВО
ВНУТРЕННИХ ДЕЛ
ПО РЕСПУБЛИКЕ ТАТАРСТАН
(МВД по Республике Татарстан)**

ул. Дзержинского, д. 19, г. Казань, 420111

19.06.2025 № 1/6618

на № _____ от _____

Заместителю Премьер-министра
Республики Татарстан

Фазлеевой Л.Р.

О направлении рекомендации

Уважаемая Лейла Ринатовна!

В рамках работы по линии выявления угроз информационной безопасности граждан, общества и государства регулярно фиксируются противоправные деяния, совершаемые в отношении несовершеннолетних посредством информационно-коммуникационных технологий. Особое беспокойство вызывают угрозы совершения кибератак на информационные ресурсы учебных заведений и связанных с ними утечек персональных данных несовершеннолетних, а также рассылок заведомо ложных сообщений об актах терроризма. Похищенная личная информация в дальнейшем используется криминальными элементами в преступных целях, связанных со склонением несовершеннолетних к совершению самоубийства, понуждения их к действиям сексуального характера, использованием в целях изготовления порнографических материалов, вовлечения в совершение действий, представляющих опасность для их жизни и здоровья.

В целях противодействия угрозам совершения кибератак на информационные ресурсы учебных заведений, а также рассылкам на адреса электронных почтовых ящиков образовательных учреждений заведомо ложных сообщений об актах терроризма разработаны рекомендации о мерах по повышению защищенности информационной инфраструктуры образовательных учреждений.

Учитывая изложенное, направляю данные рекомендации для их реализации.

Приложение:

рекомендации о мерах по повышению защищенности информационной инфраструктуры образовательных учреждений Российской Федерации на 2 листах;

рекомендации по настройке механизмов безопасности почтовых сервисов от атак, связанных с подменой отправителя (спуфинг-атак) на 20 листах.

Врио Министра
генерал-майор полиции А.В. Соколов

003914

РЕКОМЕНДАЦИИ
о мерах по повышению защищенности информационной инфраструктуры образовательных учреждений Российской Федерации

Анализ сведений об угрозах безопасности информации, проводимый в условиях складывающейся обстановки, указывает на увеличение числа компьютерных атак и связанных с ними утечек персональных данных.

Продолжают фиксироваться факты большого количества фишинговых писем, попыток внедрения вирусов-шифровальщиков через почтовые вложения, а также рассылок заведомо ложных сообщений об актах терроризма.

В целях предотвращения реализации угроз безопасности информационной инфраструктуры образовательных учреждений Российской Федерации необходимо принять дополнительные меры защиты информации

1. Обеспечить применение средств антивирусной защиты и антиспама, а также своевременное обновление их баз данных.

2. Настроить в средствах антивирусной защиты, антиспама (при наличии) проверку всех поступающих на электронную почту вложений.

3. Проинформировать пользователей информационной системы о необходимости безопасной работы с электронной почтой, а именно:

- внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- не открывать письма от неизвестных адресатов;
- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т. д.);
- не нажимать на ссылки из письма, если они заменены на слова;
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы;
- не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
- не переходить по ссылкам и не скачивать файлы, содержащиеся во входящих почтовых сообщениях, если средствами антивирусной защиты в указанных вложениях обнаружено вредоносное программное обеспечение;
- внимательно относиться к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;
- в случае появления сомнений, направлять полученное письмо как вложение администратору информационной системы.

4. Активировать (по возможности) механизмы проверки электронной почты, проверки подлинности домена-отправителя (например, использовать технологии DKIM, DMARC, SPF), а также настроить проверку входящих писем с использованием этих технологий.

5. Заблокировать (при возможности) получение пользователя информационной системы в электронных письмах вложений с расширениями ADE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH.

6. Заблокировать доставку писем от зарубежных доменов-отправителей.

7. Обеспечить регулярное обновление используемого программного обеспечения, в том числе на сетевых устройствах (маршрутизаторах, коммутаторах).

8. Обеспечить использование устойчивых длинных паролей административных учетных записей.

При поступлении на адрес электронной почты заведомо ложного сообщения об акте терроризма необходимо принять следующие меры:

1. Поступившее сообщение об акте терроризма не удалять.

2. Осуществить копирование текста сообщения об акте терроризма в виде снимков экрана устройства (скриншотов либо фотоизображений, полученных посредством цифровой фотофиксации).

2.1. На скриншотах (фотоизображениях) должна отображаться следующая информация об объекте:

- название темы письма (в том числе если письмо не имеет названия: «<Без темы>»);
- адрес электронной почты отправителя письма, зафиксированный в графе, обозначенной реквизитом «От:»;
- дата и время отправления письма;
- текст письма (включая подпись к нему, например: «С уважением, Иван Иванов»), который может содержаться непосредственно в письме и/или во вложении к нему в виде прикрепленного файла.

2.2. Зафиксировать на скриншоте/фотоизображении наличие в письме вложения, а также при открытии его зафиксировать аналогичным способом текст, который оно содержит.

3. Исключить копирование текста сообщения об акте терроризма (скриншоты/фотоизображения) ненадлежащего качества, обусловленного небрежным копированием, фотографированием текстов.

4. При невозможности фиксации сообщений об акте терроризма в виде скриншотов/фотоизображений осуществить их фиксацию посредством функций копирования и вставки в документ Word (с сохранением указанной информации об объекте).

5. О поступившем сообщении об акте терроризма незамедлительно сообщить по единому номеру вызова экстренных оперативных служб «112» либо в ближайший орган внутренних дел.

МВД по Республике Татарстан

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

2025

Содержание

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

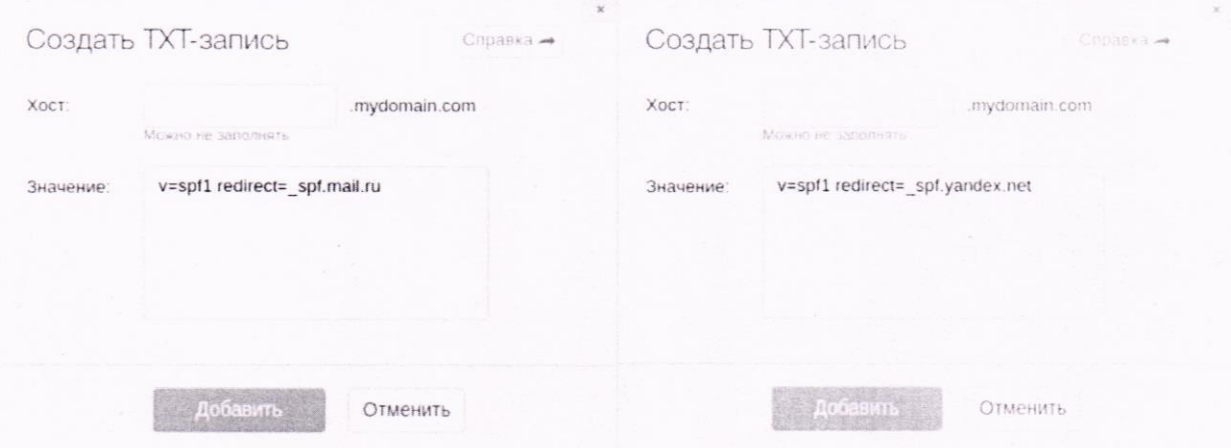


Рисунок 1 — Поле добавления SPF-записи в DNS

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

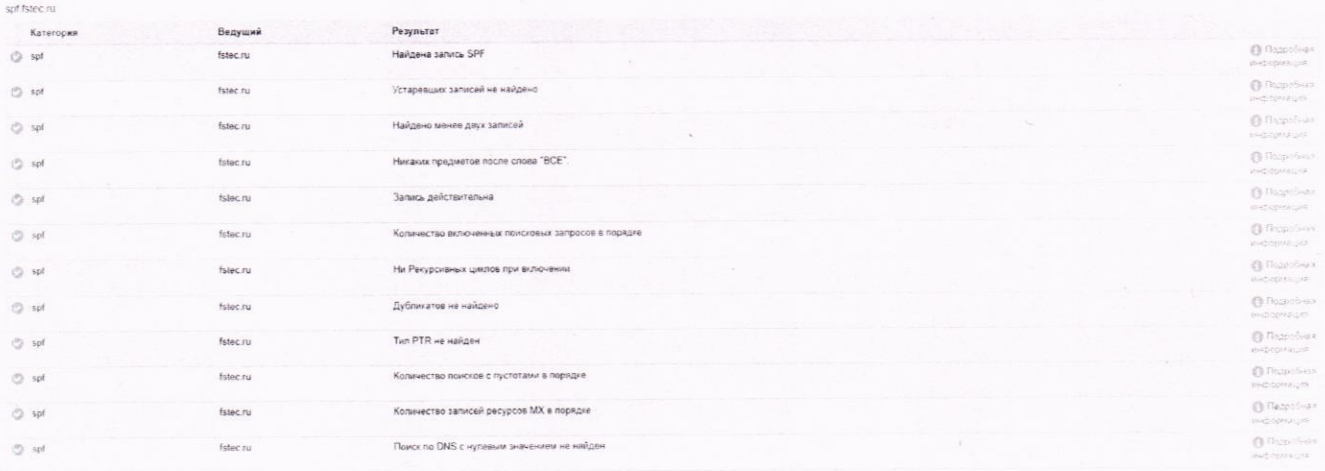
Итогом проверки для домена fstec.ru будет:

```
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

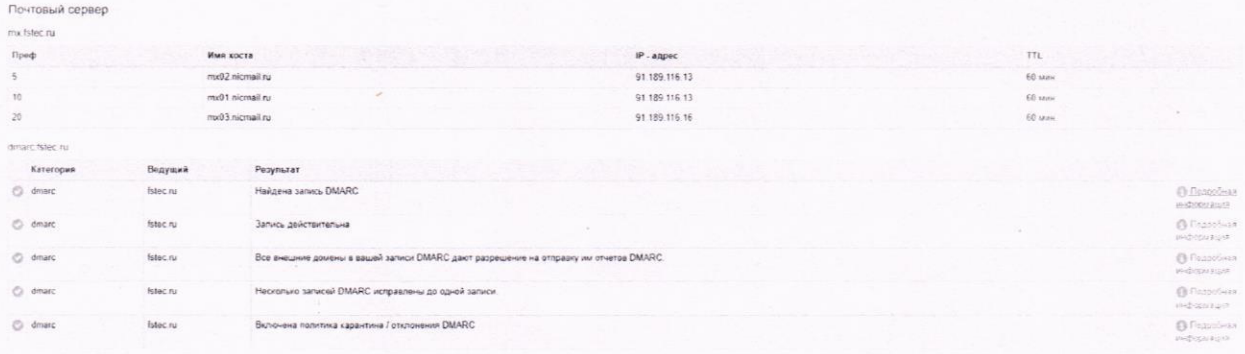
для операционных систем на базе Linux

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.

4. Настройка механизмов безопасности SPF, DKIM, DMARK для почтового сервера, созданного с использованием программного обеспечения с открытым исходным кодом Postfix

Настройка механизма SPF

4.1 Для проверки SPF-записи для входящей почты в Postfix рекомендуется использовать Postfix Policyd-SPF.

Для установки Postfix Policyd-SPF необходимо выполнить следующие команды в терминале (командной строке) операционной системы (далее по тексту все команды аналогично выполняются в терминале (командной строке) операционной системы):

Для Debian (Ubuntu, Astra Linux):

sudo apt update

sudo apt install postfix-policyd-spf-python

Для CentOS (RHEL):

sudo yum install epel-release

sudo yum install postfix-policyd-spf-python

4.2 После установки необходимо осуществить следующую настройку конфигурации Postfix:

открыть конфигурационный файл Postfix командой *sudo nano /etc/postfix/main.cf;*

добавить в конец файла строку:

policy-spf_time_limit = 3600;

сохранить изменения путем нажатия сочетания клавиш Ctrl+O;

закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

открыть файл /etc/postfix/master.cf командой *sudo nano /etc/postfix/master.cf;*

добавить в конец следующую команду:

policyd-spf unix - n n - 0 spawn

user=policyd-spf argv=/usr/bin/policyd-spf

4.3 Для того, чтобы включить проверку SPF-записи необходимо осуществить следующую настройку конфигурации Postfix:

открыть файл /etc/postfix/main.cf командой *sudo nano /etc/postfix/main.cf;*

найти строку smtpd_recipient_restrictions и добавить check_policy_service unix:private/policyd-spf перед permit следующим образом:

smtpd_recipient_restrictions =

reject_unauth_destination,

check_policy_service unix:private/policyd-spf,

permit

сохранить изменения путем нажатия сочетания клавиш Ctrl+O;

закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

перезапустить сервис Postfix после внесения изменений и применить их командой *sudo systemctl restart postfix* или *sudo service postfix restart.*

4.4 Для проверки настройки SPF-записи необходимо:

отправить тестовое письмо с любого почтового адреса на ваш сервер Postfix;

проверить заголовки командой *sudo tail -f /var/log/mail.log.*

В случае, если SPF настроен правильно, то в логах появится запись *SPF check: pass.* В случае, если письмо не проходит проверку SPF, то в логах появится запись *SPF check: fail.*

Настройка механизма DKIM

4.5 Для настройки DKIM в Postfix необходимо установить пакет OpenDKIM путем выполнения команд:

для Debian (Ubuntu, Astra Linux):

sudo apt update

sudo apt install opendkim opendkim-tools -y

для CentOS (RHEL):

sudo yum install epel-release -y;

sudo yum install opendkim opendkim-tools -y.

4.6 После установки необходимо осуществить следующую настройку OpenDKIM:

создать директории для хранения ключей DKIM командами:

sudo mkdir -p /etc/opendkim/keys

sudo chown -R opendkim:opendkim /etc/opendkim

sudo chmod -R 700 /etc/opendkim/keys

создать подпапку для вашего домена (в примере заменить example.ru на ваш реальный домен):

sudo mkdir -p /etc/opendkim/keys/example.ru

сгенерировать DKIM-ключи командой:

sudo opendkim-genkey -b 2048 -d example.com -D /etc/opendkim/keys/example.com -s selector1 -v

Расшифровка параметров:

-b 2048 — длина ключа (рекомендуется 2048 бит);

-d example.ru — ваш домен;

-D /etc/opendkim/keys/example.ru — папка для ключей;

-s selector1 — селектор (можно задать другое имя);

-v — включение режима отладки.

После выполнения команды появятся два файла:

selector1.private — закрытый ключ (используется на сервере);

selector1.txt — публичный ключ (для DNS).

4.7 Необходимо открыть основной конфигурационный файл /etc/opendkim.conf командой:

sudo nano /etc/opendkim.conf;

Добавить или заменить в файле строки следующим образом (в примере директории и порты заменить на реальные данные почтового сервера):

AutoRestart Yes
AutoRestartRate 10/1h
Syslog Yes
LogWhy Yes
Canonicalization relaxed/simple
Mode sv
SignatureAlgorithm rsa-sha256
KeyTable /etc/opendkim/keytable
SigningTable /etc/opendkim/signingtable
TrustedHosts /etc/opendkim/trustedhosts
Socket inet:8891@localhost

4.8 Необходимо настроить таблицы ключей DKIM путем выполнения следующих действий.

Создать файл KeyTable командой:

sudo nano /etc/opendkim/keytable;

добавить в открытый файл строку и сохранить:

selector1._domainkey.example.ru
example.ru:selector1:/etc/opendkim/keys/example.com/selector1.private

Где:

selector1._domainkey.example.ru — DKIM-селектор.
example.ru — ваш домен.
selector1.private — путь к закрытому ключу.

4.9 Осуществить настройку таблицы подписываемых доменов путем создания файла SigningTable командой:

sudo nano /etc/opendkim/signingtable;

и добавлением в созданный файл строки:

**@example.ru selector1._domainkey.example.ru;*

В таком случае все письма с домена example.ru будут подписаны селектором selector1.

4.10 Осуществить настройку доверенных хостов путем создания файла TrustedHosts командой:

sudo nano /etc/opendkim/trustedhosts;

И добавлением строк, содержащих адреса доверенных хостов, например:

127.0.0.1
localhost
example.ru

В случае, если сервер использует внутреннюю сеть, необходимо добавить диапазон IP-адресов следующим образом:

192.168.1.0/24.

4.11 Реализовать настройку Postfix для работы с OpenDKIM следующим образом:

открыть файл /etc/postfix/main.cf командой:

sudo nano /etc/postfix/main.cf;

добавить в конец строки (в примере порты заменить на реальные данные почтового сервера):

 # Подключение OpenDKIM

milter_protocol = 6

milter_default_action = accept

smtpd_milters = inet:localhost:8891

non_smtpd_milters = inet:localhost:8891.

После необходимо перезапустить Postfix командой:

sudo systemctl restart postfix;

4.12 Необходимо добавить DKIM-записи в DNS для этого открыть созданный ранее файл selector1.txt командой:

cat /etc/opendkim/keys/example.com/selector1.txt

В файле будет строка вида:

selector1._domainkey IN TXT ("v=DKIM1; k=rsa; p=MIIBIjANBgkqh...");

скопировать значение публичного ключа *p=MIIBIjANBgkqh…* для добавления его значения в DNS -запись (смотреть пункт 2.3).

4.13 После добавления DNS-записи необходимо перезапустить OpenDKIM следующими командами:

sudo systemctl restart opendkim или *sudo systemctl enable opendkim;*

4.14 Проверка работы OpenDKIM осуществляется командой:

sudo systemctl status opendkim

В случае, если в выводе терминала (командной строки) появилась строка *"Active: active (running)"*, значит сервис работает.

Для проверка слушающего порта необходимо выполнить команду:

netstat -an | grep 8891

Ожидаемый вывод терминала (командной строки):

tcp 0 0 127.0.0.1:8891 0.0.0.0: LISTEN*

Настройка механизма DMARC

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

4.16 Для осуществления настройки DMARC в Postfix необходимо установить OpenDMARC командами:

для Debian (Ubuntu, Astra Linux):

apt update && apt install opendmarc

для CentOS (RHEL):

yum install epel-release

yum install opendmarc

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 mail.example.ru

PidFile /var/run/opendmarc.pid

UMask 0002

RejectFailures false

Syslog true

TrustedAuthservIDs mail.example.com

IgnoreAuthenticatedClients true

SPFIgnoreResults false

Socket inet:8893@127.0.0.1;

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

4.17 Для настройки OpenDMARC в Postfix необходимо осуществить следующую настройку конфигурации:

открыть конфигурацию Postfix командой:

nano /etc/postfix/main.cf;

добавить поддержку DMARC строками (в примере IP-адреса и порты заменить на реальные данные почтового сервера):

smtpd_milters = inet:127.0.0.1:8893

non_smtpd_milters = inet:127.0.0.1:8893

milter_default_action = accept;

перезапустить Postfix и OpenDMARC командами:

systemctl restart opendmarc

systemctl restart postfix.

Осуществить проверку работоспособности DMARC путем отправки тестового письма с использованием почтового сервера и просмотра заголовков письма (View Message Headers). В случае, если строка *Authentication-Results: dmarc=pass header.from=example.ru* содержит «pass», значит DMARC работает.

5. Настройка механизмов безопасности SPF, DKIM, DMARK для почтового сервера Microsoft Exchange Server

Настройка механизма SPF

5.1 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).

5.2 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).

5.3 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].

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

5.5. 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*.

5.6 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*.

5.7 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).

Настройка механизма DKIM

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

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

Установка DKIM-агента осуществляется следующим образом:

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

5.11 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).

5.12 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

5.13 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

Настройка механизма DMARC

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

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

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

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

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

5.19 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:).

5.20 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).

6. Настройка механизмов безопасности SPF, DKIM, DMARK для почтового сервера, созданного с использованием программного обеспечения с открытым исходным кодом Exim

Настройка механизма SPF

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

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

6.3 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.

6.4 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*.

6.5 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.

6.6 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.

Настройка механизма DKIM

6.7 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.

6.9 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).

6.10 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.

6.11 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*.

Настройка механизма DMARC

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

6.13 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

6.14 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

6.15 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;

6.16 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

6.17 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

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

warn control = dmarc_enable_forensic

6.19 Для применения настроек необходимо перезапустить Exim командами:

update-exim4.conf

systemctl restart exim4.