

Рекомендации Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по эффективному распознаванию фишинговых писем

Фишинг (англ. phishing) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.

Такой вид интернет-мошенничества, как правило, основан на психологической манипуляции и его цель — вывести человека на такие эмоции, как интерес, страх, жадность, злость, желание помочь. Это позволяет ослабить концентрацию человека, усыпить его бдительность.

Так, применение различных психологических приемов делает такой вид интернет-мошенничества чрезвычайно эффективным, в том числе в органах государственной власти.

***Пример.** Для злоумышленника не составляет труда найти в открытых источниках информацию о структуре Вашего органа власти, определить ключевых должностных лиц и домен корпоративной почты Вашего органа власти. Это позволяет злоумышленнику сделать фишинговую рассылку примерно следующего содержания: «Уважаемый! В период с 1 марта по 3 апреля Управлением информационных технологий производится ревизия почтовых ящиков сотрудников Все неиспользуемые почты будут отключены. Если вы получили данное письмо и планируете использовать данный почтовый ящик в будущем, просьба оперативно войти в личный кабинет по следующей ссылке:»*

При этом ссылка, конечно же, ведет на поддельную форму авторизации в корпоративную почту. Если тот или иной сотрудник органа власти вовремя не поймет, что данная рассылка является фишинговой, и перейдет по ссылке, он окажется на странице, которая внешне неотличима от настоящей формы ввода учетных данных. Конечно же, введя логин и пароль, такой сотрудник «добровольно» передаст их злоумышленникам.

Первоначальные действия при получении электронного письма:

Если Вы получили письмо, в котором от Вас требуют какого-либо взаимодействия, в том числе незамедлительного, или же такое письмо вызывает у Вас любопытство, чувство страха или побуждает к действиям, например, «открой», «прочитай», «ознакомься», то задумайтесь и задайте себе следующие вопросы:

ожидая ли я это письмо?

есть ли смысл в том, что от меня требуют?

знаю ли я автора этого письма?

уверен ли я в безопасности полученного электронного письма?

Если ответ хотя бы на один из озвученных выше вопросов «нет» - внимательно проанализируйте содержимое письма и, при необходимости, свяжитесь для консультации с представителем технической поддержки Вашего органа власти.

Имейте в виду, что особого внимания требуют письма, которые:

содержат ссылку для перехода на сторонний ресурс (возможно, ссылка ведет на фишинговый поддельный ресурс). При этом еще большего внимания заслуживают письма, содержащие «короткие ссылки», так как невозможно определить, куда ведет такая ссылка;

содержат вложение (возможно, файл содержит вредоносный код для заражения вашего компьютера);

составлены на иностранном языке;

имеют большое количество получателей;

содержат орфографические ошибки;

связаны с финансовой, банковской сферой или геополитической обстановкой.

Как анализировать электронные письма?

1. Проверьте адрес отправителя (домен адреса электронной почты, с которой пришло письмо, должен совпадать с доменом, указанным на официальном сайте организации, от имени которой якобы направлено письмо, а логин такой почты, в свою очередь, должен совпадать с принятой логикой их построения в той или иной организации). Проверяйте адрес отправителя, даже в случае совпадения имени с уже известным контактом;

2. Проверьте полное имя отправителя (для проверки полного имени отправителя, наведите курсор мышки на указанное в письме имя отправителя) и затем проанализируйте высветившийся адрес электронной почты в соответствии с информацией из официальных источников (см. пункт выше);

3. Проверьте, при наличии, ссылки, даже если письмо получено от другого пользователя Вашей информационной системы, и помните о том, что сам факт направления Вам по электронной почте ссылок, ведущих на сторонний ресурс, является подозрительным:

- обратите внимание на название сайта, на который Вам предлагают перейти. В нем может быть изменен порядок букв или, например, некоторые буквы могут быть заменены на цифры (например, www.s0branie.ru). Кроме того, для введения в заблуждение злоумышленником могут быть использованы специализированные сервисы сокращения ссылок (например, bit.ly, tinyurl.com);

- наведите курсор мышки на ссылку (не нажимая на нее, ссылка появится или рядом с курсором или в левой нижней части окна)

и проверьте, чтобы URL, указанный в электронном сообщении, и URL, отображаемый при наведении курсора на ссылку, совпадали;

- также Вы можете вручную (не копируя ее) вбить полученную ссылку в строке поисковой системы (Яндекс, mail.ru и др.). Такой метод позволит Вам заметить возможные «ошибки» в полученной ссылке;

4. Проверьте наличие вложений. Если отправитель, электронное письмо и причина, по которой Вас просят открыть вложение, вызывает даже самое незначительное подозрение – ни при каких обстоятельствах не открывайте его.

5. Обращайте внимание на возможные опечатки, орфографические ошибки, большое количество прописных букв, совпадение названий организации, имени отправителя и содержимого в тексте электронного письма;

6. Если полученное письмо вызывает сомнения, по возможности, свяжитесь с отправителем или со справочной организации, от которой пришло такое электронное письмо, по другому каналу связи. При этом контактные данные нужно брать из авторитетных источников, например, на официальном сайте организации, а не из направленного Вам письма.

Что делать, если Вы обнаружили фишинговое письмо?

1. Не переходите по ссылке, особенно, если они длинные или, наоборот, созданы при помощи сервисов сокращения ссылок;

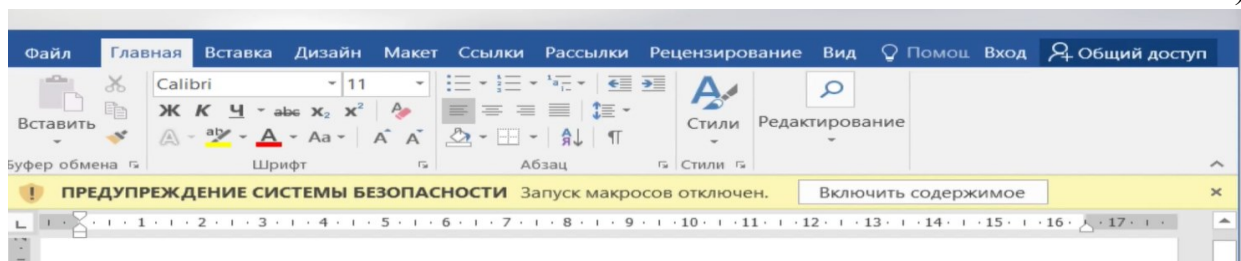
2. Не нажимайте на ссылки, если они заменены на слова;

3. Не копируйте адрес ссылки;

4. Не открывайте и не скачивайте вложения, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;

5. Не загружайте картинки от незнакомых людей;

6. Не запускайте макросы в офисных приложениях (*макрос – это набор команд и инструкций, группируемых вместе в виде единой команды для автоматического выполнения задачи.*);



7. Не пересылайте письма коллегам;

8. Проинформируйте службу технической поддержки своего органа власти/администратора информационной системы, направив ему полученное письмо **как вложение**;

9. Удалите фишинговое письмо.

**Рекомендации Министерства цифрового развития, связи и массовых
коммуникаций Российской Федерации по настройке SPF, DKIM, DMARC**

Оглавление

Введение	2
1. SPF (Sender Policy Framework)	3
1.1. Настройка на стороне отправителя	3
1.2. Настройка на стороне получателя	4
1.2.1. Почтовый сервер Postfix	4
1.2.2. Почтовый сервер Exim	5
1.2.3. Почтовый сервер MS Exchange	6
2. DKIM (DomainKeys Identified Mail)	7
2.1. Настройка доменной зоны	7
2.2. Почтовый сервер Postfix	7
2.3. Почтовый сервер Exim	9
2.4. Почтовый сервер MS Exchange	10
2.4.1. Общий подход	10
2.4.2. Настройка SASL	10
2.4.3. Настройка почтового сервера Postfix	11
2.4.4. Настройка MS Exchange	13
3. DMARC (Domain-based Message Authentication, Reporting and Conformance)	15
2.1. Настройка доменной зоны	15
2.2. Почтовый сервер Postfix	16
2.3. Настройка Exim	17

ВВЕДЕНИЕ

Документ описывает технологии, настройки серверов электронной почты и принципы противодействия фишингу и спуфингу. Тема противодействия спаму не затрагивается, ввиду ее обширности и особой специфики, требующей отдельного рассмотрения. В этой связи такие меры, направленные на борьбу со спамом, как проверка по DNSBL (DNS black list), проверка PTR записи хоста при входящем подключении по SMTP; проверка корректности представления сервера в SMTP HELO заголовке, graylisting и других мер в рамках указанных рекомендаций не рассматриваются.

Следует отметить, что технологии для борьбы с фишингом и спуфингом электронной почты, как правило, используются в работе систем выявления спам сообщений.

Настройка механизмов борьбы с фишингом и спуфингом электронной почты условно разделяется на настройку механизмов на стороне отправителя электронной почты и на стороне получателя.

Настройка механизмов на стороне отправителя предполагает предоставление дополнительной информации получателю, которая может быть использована для подтверждения факта отправки почты с данного сервера. Настройки механизмов на стороне получателя предполагают возможное использование нижеуказанной информации для принятия соответствующих мер по противодействию возможному фишингу и спуфингу.

1. SPF (SENDER POLICY FRAMEWORK)

1.1. Настройка на стороне отправителя

SPF (Sender Policy Framework) – это расширение для протокола отправки электронной почты с использованием протокола SMTP, позволяющее проверить, не подделан ли домен отправителя. Для размещения политики SPF владелец домена указывает список почтовых серверов или ip-адресов, которые могут отправлять письма (авторизованы использовать этот домен в командах SMTP HELO и MAIL FROM).

Для настройки политики необходимо обладать возможностью редактирования записей доменной зоны, от имени которой почтовый сервер отправляет электронные сообщения. Настройка механизма предполагает добавление новой записи типа TXT, которая будет описывать перечень dns и ip-адресов, которые, в свою очередь, могут быть источником отправки электронного сообщения.

В случае, когда доменное имя сервера электронной почты совпадает с именем основного домена, запись TXT будет иметь следующий вид:

```
"v=spf1 a -all"
```

В случае, когда доменное имя сервера электронной почты задано в записи MX доменной зоны, то запись TXT будет иметь следующий вид:

```
"v=spf1 mx -all"
```

В случаях, когда серверы электронной почты не имеют доменного имени, в запись добавляются их ip-адреса (например, 1.1.1.1 и 2.2.2.2). В этом случае запись TXT будет иметь следующий вид:

```
"v=spf1 ip4:1.1.1.1 ip4:2.2.2.2 -all"
```

Формат SPF допускает совместное использование нескольких видов описания. Однако, ключи «v=spf1» и «all» должны присутствовать в записи в единственном экземпляре, в начале и в конце записи соответственно.

Ниже приведен пример настройки механизма SPF для домена digital.gov.ru:

```
digital.gov.ru. 300 IN TXT "v=spf1 mx a ip4:212.164.137.119  
ip4:84.42.67.50 ip4:185.194.32.26 ip4:185.194.32.204 ip4:185.194.32.205  
ip4:109.120.189.156 ip4:91.206.127.97 ip4:185.194.34.50  
ip4:185.194.34.51 include:_spf.armgs.team ~all"
```

В данной записи помимо ключей «mx», «a» и «ip4» присутствует ключ «include». Данный ключ указывает на то, что к записи необходимо добавить параметры, указанные для соответствующей TXT записи домена, заданного в качестве параметра – в данном случае домена _spf.armgs.team. Кроме того, для ключа «all» указан модификатор «~». Данный модификатор предполагает, что письма, не прошедшие проверку SPF должны особым образом пометаться на стороне клиента и передаваться далее по цепочке

пересылки электронных сообщений. В случае с модификатором «-» владелец домена рекомендует отклонять сообщения, не прошедшие проверку SPF.

Важно знать, что записи SPF не распространяются на поддомены. То есть запись SPF для домена gov.ru не имеет силы для домена digital.gov.ru.

Кроме того, следует отметить, что адрес сервера отправителя почты при получении указывается в нескольких местах и видимый пользователю адрес может не совпадать с реальным адресом сервера отправителя. Например, видимый пользователю адрес имеет вид «user@digital.gov.ru», а сервер, с которого доставлено сообщение, имеет доменное имя mxs.armsg.team. В связи с этим, надо учитывать, что SPF никак не защищает видимый пользователю адрес отправителя, а сам SPF вообще не работает с содержимым письма, которое видит пользователь, в частности с адресом отправителя. Таким образом, письмо с поддельным отправителем в поле «From» без труда может пройти SPF-авторизацию.

1.2. Настройка на стороне получателя

1.2.1. Почтовый сервер Postfix

1. Установите модуль postfix-policyd-spf-python. Для этого в операционных системах, основанных на Linux Debian, требуется выполнить с правами администратора следующую команду:

```
apt-get install postfix-policyd-spf-perl
```

2. В конфигурационный файл /etc/postfix/master.cf необходимо добавить следующие строки:

```
policy-spf unix - n n - 0 spawn
user=nobody argv=/usr/bin/policyd-spf /etc/postfix-policyd-spf-
python/policyd-spf.conf
```

3. В конфигурационный файл /etc/postfix/main.cf необходимо добавить следующую строку:

```
policy-spf_time_limit = 3600s
```

4. В конфигурационном файле /etc/postfix/main.cf дополните набор smtpd_recipient_restrictions следующим правилом:

```
check_policy_service unix:private/policyd-spf
```

Рекомендуем указывать это правило после правила reject_unauth_destination:

5. В конфигурационном файле /etc/postfix-policyd-spf-python/policyd-spf.conf проверьте наличие следующей записи:

```
TestOnly=0
```

6. Перезапустите почтовый сервер. Для этого в операционных системах, использующих `systemd`, требуется выполнить с правами администратора следующую команду:

```
systemctl restart postfix
```

7. Проверьте журналы postfix, чтобы удостовериться, что SPF проверяется правильно. По умолчанию они размещаются в следующих файлах:

```
/var/log/mail.log
/var/log/mail.error
/var/log/mail.info
/var/log/mail.warn
```

1.2.2. Почтовый сервер Exim

1. Установите пакет программного обеспечения `spf-tools-perl`. Для этого в операционных системах, основанных на Linux Debian, требуется выполнить с правами администратора следующую команду.

```
apt-get install spf-tools-perl
```

2. В конфигурационном файле `/etc/exim4/update-exim4.conf.conf` проверьте значение следующего параметра:

```
dc_use_split_config='false'
```

В конфигурационном файле Exim `/etc/exim4/update-exim4.conf.conf` настройка `dc_use_split_config` определяет, будет ли Exim использовать разделенный конфигурационный файл или однофайловую конфигурацию.

Если `dc_use_split_config='true'`, то Exim будет ожидать, что его конфигурация будет разделена на несколько файлов в каталоге `/etc/exim4/conf.d/`. Это может быть полезно для больших или сложных конфигураций, где разделение на отдельные файлы может упростить управление и обслуживание.

Если `dc_use_split_config='false'`, то Exim будет ожидать единую конфигурацию в одном файле. Это может быть проще для меньших или менее сложных конфигураций. В данном примере используется вариант, когда `dc_use_split_config` установлен в значение `'false'`.

3. В начало конфигурационного файла `/etc/exim4/exim4.conf.localmacros` добавьте следующую строку. Если файл не существует – создайте его:

```
CHECK_RCPT_SPF=yes
```

4. Обновите текущую конфигурацию почтового сервера. Для этого требуется выполнить с правами администратора следующую команду:

```
update-exim4.conf
```

5. Проверьте корректность полученной конфигурации, выполнив следующую команду:

```
exim4 -bV
```


6. Если проверка завершилась успешно, перезапустите почтовый сервер. Для этого в операционных системах, использующих systemd, требуется выполнить с правами администратора следующую команду:

```
systemctl restart exim4
```

1.2.3. Почтовый сервер MS Exchange

1. Откройте Exchange Management Console.
2. Перейдите в «Organization Configuration» → «Hub Transport».
3. Выберите политику «Default Policy» и нажмите «Edit».
4. Выберите вкладку «Message Filtering».
5. Поставьте галочку «Sender ID» и выберите «Enforce».
6. Сохраните изменения.
7. Перезапустите службу «Microsoft Exchange Transport».

2. DKIM (DOMAINKEYS IDENTIFIED MAIL)

2.1. Настройка доменной зоны

DomainKeys Identified Mail (DKIM) — метод e-mail-аутентификации, разработанный для обнаружения подделки электронных писем. DKIM дает возможность получателю убедиться, что письмо действительно было отправлено с заявленного домена, упрощает борьбу с поддельными адресами отправителей, которые часто используются в фишинговых письмах и в почтовом спаме.

Для настройки политики необходимо обладать возможностью редактирования записей доменной зоны, от имени которой почтовый сервер отправляет электронные сообщения, а также публичным ключом подписи (процесс генерации ключей подписи сообщений рассматривается ниже). Настройка механизма предполагает добавление новой записи типа TXT с именем «селектор._domainkey.доменное_имя». Где «селектор» - уникальный идентификатор записи, «доменное_имя» - доменное имя сервера отправки почты. Формат записи имеет следующий вид:

```
селектор._domainkey.доменное_имя TXT "v=DKIM1;k=rsa; p=<публичный_ключ>"
```

2.2. Почтовый сервер Postfix.

1. Для подписи всех исходящих сообщения, при использовании почтового сервера postfix, следует использовать программное обеспечение OpenDKIM. Для установки OpenDKIM в операционных системах, основанных на Linux Debian, требуется выполнить с правами администратора следующую команду:

```
apt-get install opendkim opendkim-tools
```

2. Создайте директорию, в которой будет сохраняться конфигурационная информация для приложения opendkim. Для этого с правами администратора выполните следующую команду:

```
mkdir -p /etc/postfix/dkim/keys
```

3. В конфигурационном файле /etc/opendkim.conf проверьте значения следующих параметров:

AutoRestart	Yes
AutoRestartRate	10/1h
Umask	002
Syslog	yes
SyslogSuccess	Yes
LogWhy	Yes
Canonicalization	relaxed/simple
ExternalIgnoreList	refile:/etc/postfix/dkim/TrustedHosts
InternalHosts	refile:/etc/postfix/dkim/TrustedHosts

KeyTable	refile:/etc/postfix/dkim/KeyTable
SigningTable	refile:/etc/postfix/dkim/SigningTable
Mode	sv
PidFile	/run/opendkim/opendkim.pid
SignatureAlgorithm	rsa-sha256
UserID	opendkim:opendkim
Socket	inet:8891@localhost

4. Создайте конфигурационный файл `/etc/postfix/dkim/TrustedHosts` и добавьте туда перечень доверенных источников получения почтовых сообщений. Возможный вариант содержимого файла приведен ниже:

```
127.0.0.1
localhost
*.my-domain
```

5. В директории `/etc/postfix/dkim/keys/` создайте каталог, в котором будут находиться сгенерированные ключи. Для этого с правами администратора выполните следующую команду (**не забывайте подставить доменное имя своего домена вместо my-domain**):

```
mkdir /etc/postfix/dkim/my-domain/
```

6. Создайте ключи подписи электронных писем. Для этого выполните с правами администратора следующую команду (**не забывайте подставить доменное имя своего домена вместо my-domain**):

```
opendkim-genkey --directory=/etc/postfix/dkim/keys/my-domain/
--domain=my-domain --selector=selector
```

После создания ключа в директории будут располагаться файлы `my-domain.private` и `my-domain.txt`, в которых сохранены секретный ключ подписи и параметры конфигурации для задания доменной записи, обозначенной в разделе 2.1.

7. Создайте конфигурационный файл `/etc/postfix/dkim/KeyTable` и добавьте туда перечень ключей, которые могут быть использованы для подписи исходящих сообщений. Возможный вариант содержимого файла приведен ниже:

```
selector._domainkey.my-domain
my-domain:selector:/etc/postfix/dkim/keys/my-domain/selector.private
```

8. Создайте конфигурационный файл `/etc/postfix/dkim/SigningTable` и добавьте туда перечень идентификаторов ключей (указывается в качестве первого параметра в файле `KeyTable`), которые будут использоваться для подписи сообщений с разных доменных имен. Возможный вариант содержимого файла приведен ниже:

```
*@my-domain selector._domainkey.my-domain
```

9. Укажите порт, на котором работает OpenDKIM. Для этого в конфигурационном файле `/etc/default/opendkim` проверьте значение следующего параметра:

```
SOCKET="inet:8891@localhost"
```

10. На следующем этапе в настройки postfix внесите «взаимодействие» с DKIM, выполнив следующие команды:

```
postconf -e 'milter_default_action=accept'
postconf -e 'milter_protocol=6'
postconf -e 'smtpd_milters=inet:127.0.0.1:8891'
postconf -e 'non_smtpd_milters=inet:127.0.0.1:8891'
```

11. Измените владельца конфигурационных файлов opendkim. Для этого от имени администратора выполните следующую команду:

```
chown -R opendkim:opendkim /etc/postfix/dkim
```

12. Для применения настроек перезапустите соответствующие сервисы. Для этого от имени администратора выполните следующие команды:

```
systemctl restart opendkim
systemctl restart postfix
```

2.3. Почтовый сервер Exim.

Настроить DKIM на сервере Exim можно, выполнив следующие действия:

1. Создайте закрытый ключ RSA, сгенерировав ключ OpenSSL. Это создаст 2048-битный закрытый ключ RSA и сохранит его в файле с именем **my_key.pem**:

```
openssl genrsa -out my_key.pem 2048
```

2. Сгенерируйте строку открытого ключа, используя закрытый ключ:

```
openssl rsa -in my_key.pem -pubout -out my_pubkey.pem
```

Это создаст открытый ключ RSA и сохранит его в файле с именем **my_pubkey.pem**, который должен быть использован для задания доменной записи, обозначенной в разделе 2.1.

3. В начало конфигурационного файла **/etc/exim4/exim4.conf.localmacros** добавьте следующие строки. Если файл не существует – создайте его:

```
DKIM_SELECTOR=selector
DKIM_PRIVATE_KEY = <YOUR PRIVATE KEY STRING>
```

4. Обновите текущую конфигурацию почтового сервера. Для этого требуется выполнить с правами администратора следующую команду:

```
update-exim4.conf
```

5. Проверьте корректность полученной конфигурации, выполнив следующую команду:

```
exim4 -bV
```

6. Если проверка завершилась успешно, перезапустите почтовый сервер. Для этого в операционных системах, использующих systemd, требуется выполнить с правами администратора следующую команду:

```
systemctl restart exim4
```

2.4. Почтовый сервер MS Exchange.

2.4.1. Общий подход

Если вы используете MS Exchange, то вам необходимо воспользоваться сторонними приложениями, так как встроенная функциональность MS Exchange не поддерживает подпись исходящих сообщений.

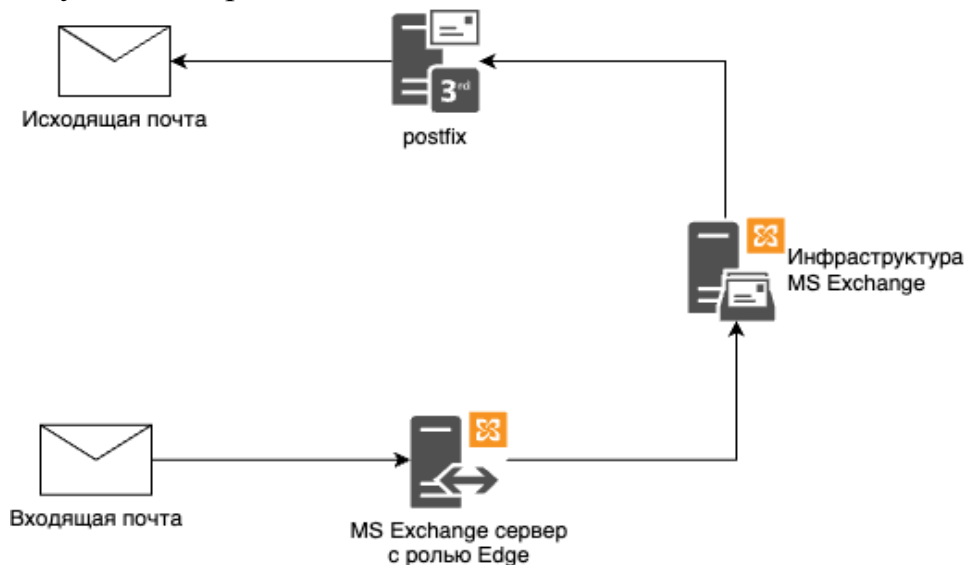
Существуют **два варианта** таких инструментов:

- установка приложения Exchange DKIM Signer;
- установка Postfix (совместно с OpenDKIM).

В указанных рекомендациях рассмотрен второй вариант, который:

- позволяет удалять из электронных писем RFC (технические) заголовки, которые, в свою очередь, раскрывают информацию о внутренних серверах и внутренних ip-адресах;
- не зависит от конкретной почтовой системы, используемой в компании.

В случае с MS Exchange схема получения и отправки почты должна выглядеть следующим образом:



При реализации взаимодействия MS Exchange и почтового сервера Postfix аутентификация пользователей производится с помощью SASL.

2.4.2. Настройка SASL.

1. Установите пакет программного обеспечения sasl2. Для этого в операционных системах, основанных на Linux Debian, требуется выполнить с правами администратора следующую команду.

```
apt-get install sasl2-bin libsasl2-modules
```

2. Создайте файл `/etc/postfix/sasl/smtpd.conf` с содержимым:

```
pwcheck_method: auxprop
auxprop_plugin: sasldb
mech_list: ntlm digest-md5 login plain
```

3. Добавьте пользователя Postfix в группу SASL. Для этого требуется выполнить с правами администратора следующую команду.

```
adduser postfix sasl
```

4. Отредактируйте файл /etc/default/saslauthd (*корректно для Debian 11, в других дистрибутивах расположение файла может меняться*). Установите значения переменных:

```
START=yes
MECHANISMS="sasldb"
```

5. Перезапустите службу. Для этого требуется выполнить с правами администратора следующую команду.

```
systemctl enable saslauthd
systemctl start saslauthd
```

6. Добавьте пользователя в базу sasldb2:

```
saslpasswd2 -c -u my-domain username
```

Для получения списка пользователей в sasldb2 используйте команду:

```
sasldblistusers2
```

2.4.3. Настройка почтового сервера Postfix.

Приведенная ниже конфигурация предназначена исключительно для взаимодействия с сервером MS Exchange.

1. Сконфигурируйте поддержку dkim в Postfix в соответствии с указаниями подраздела 2.1.

2. В конфигурационном файле /etc/postfix/main.conf проверьте значения следующих параметров:

```
smtpd_tls_cert_file=/etc/ssl/certs/<ваш сертификат>.cert
smtpd_tls_key_file=/etc/ssl/private/<ваш приватный ключ>.key
tls_high_cipherlist =
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES
:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS
smtpd_sasl_local_domain = <ваш домен>
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sender_login_maps = hash:/etc/postfix/login
smtp_helo_name = <имя сервера>
```

3. В файле /etc/postfix/master.cf оставьте незакомментированными только следующие строчки:

smtp	inet	n	-	y	-	-	smtpd
pickup	unix	n	-	y	60	1	pickup
cleanup	unix	n	-	y	-	0	cleanup
qmgr	unix	n	-	n	300	1	qmgr
tlsmgr	unix	-	-	y	1000?	1	tlsmgr

rewrite	unix	-	-	y	-	-	trivial-rewrite
bounce	unix	-	-	y	-	0	bounce
defer	unix	-	-	y	-	0	bounce
trace	unix	-	-	y	-	0	bounce
verify	unix	-	-	y	-	1	verify
flush	unix	n	-	y	1000?	0	flush
proxymap	unix	-	-	n	-	-	proxymap
proxywrite	unix	-	-	n	-	1	proxymap
smtp	unix	-	-	y	-	-	smtp
relay	unix	-	-	y	-	-	smtp
showq	unix	n	-	y	-	-	showq
error	unix	-	-	y	-	-	error
retry	unix	-	-	y	-	-	error
discard	unix	-	-	y	-	-	discard
local	unix	-	n	n	-	-	local
virtual	unix	-	n	n	-	-	virtual
lmtp	unix	-	-	y	-	-	lmtp
anvil	unix	-	-	y	-	1	anvil
scache	unix	-	-	y	-	1	scache

4. В конфигурационный файл `/etc/postfix/headers` необходимо добавить следующие строки:

```
/^Received:/      IGNORE
/^X-Originating-IP:/  IGNORE
/^X-ClientProxiedBy:/  IGNORE
```

Указанные настройки предназначены для удаления служебных почтовых заголовков, которые раскрывают информацию о внутренней инфраструктуре.

5. Установите содержимое файла `/etc/postfix/login`:

```
@<ваш домен>      <имя пользователя в формате имя@домен>
```

Пример:

```
@example.com      user@example.com
```

Такой файл определяет список пользователей, которые могут отправлять письма с вашего домена. Такие же имена пользователя должны использоваться в настройках основной почтовой системы.

Это же имя пользователя нужно использовать в подразделе 2.3.2.

6. В конфигурационный файл `/etc/postfix/transport` необходимо добавить следующие строки:

```
<ваш домен>      smtp:<внутренний почтовый сервер>
```

Пример:

```
example.com      smtp:mail.example.com
```

7. Для применения настроек перезапустите соответствующие сервисы. Для этого от имени администратора выполните следующую команду:

```
systemctl restart postfix
```

2.4.4. Настройка MS Exchange

Вместо того, чтобы направлять все исходящие сообщения непосредственно в Интернет, направьте исходящую почту организации через Postfix.

1. Создайте соединитель отправки, использующий маршрутизацию через промежуточный узел, с помощью Центра администрирования MS Exchange:

1.1. В ЕАС (Exchange admin center) перейдите к разделу **Mail flow > Send connectors** и нажмите кнопку «Добавить». Запустится мастер создания коннектора.

1.2. На первой странице укажите следующие сведения:

– имя: введите описательное имя коннектора, например, «Сервис подписи исходящей почты»;

– тип: выберите описательное значение (например, Internet или Custom)¹.

1.3. На следующей странице выберите **Route mail through smart hosts** и нажмите кнопку «Добавить». В открывшемся диалоговом окне **Add smart host** определите промежуточный узел, используя одно из следующих значений:

– IP-адрес (например, 192.168.3.2);

– полное доменное имя (FQDN) (например, securitydevice01.contoso.com. При этом, обратите внимание, что исходные серверы MS Exchange должны иметь возможность разрешать интеллектуальный узел в DNS с помощью этого полного доменного имени).

1.4. Вы можете указать несколько промежуточных узлов, повторив действия, указанные в подразделе 1.3. По завершении, нажмите кнопку «Далее».

1.5. На следующей странице, в разделе **Route mail through smart hosts**, выберите способ проверки подлинности, необходимый промежуточному узлу.

В данном случае используется парольная проверка подлинности в Postfix. Поэтому необходимо активировать **Basic authentication**, ввести актуальные данные аутентификации. Затем необходимо указать **Offer basic authentication only after starting TLS** для обеспечения безопасного соединения.

¹ Дополнительные сведения о типах использования соединителей отправки: <https://learn.microsoft.com/ru-ru/exchange/mail-flow/connectors/send-connectors?view=exchserver-2019#send-connector-usage-types>

1.6. На следующей странице в разделе **Address space** нажмите кнопку «Добавить». В открывшемся диалоговом окне **Add domain** введите следующие сведения:

- тип: убедитесь, что smtp введен;
- полное доменное имя (FQDN). Введите звездочку (*), чтобы указать, что соединитель отправки применяется к сообщениям, адресованным всем внешним доменам. Вы также можете указать определенный внешний домен (например, postfix.ru), либо домен и все его поддомены (например, *.postfix.ru);
- затраты: убедитесь, что введено значение «1. Чем ниже значение, тем предпочтительнее будет этот маршрут для указанных доменов».

1.7. На предыдущей странице имеется параметр **Scoped send connector**, который важен, если серверы Exchange установлены на нескольких сайтах Active Directory в организации:

- если не выбрать Scoped send connector, действия, соединитель можно использовать на всех транспортных серверах (серверах почтовых ящиков Exchange 2013 или более поздних версий и транспортных серверах концентратора Exchange 2010) во всем Active Directory. Это значение используется по умолчанию;
- если включить параметр Scoped send connector, соединитель смогут использовать только другие транспортные серверы на том же сайте Active Directory.

1.8. На следующей странице в разделе Source server нажмите кнопку «Добавить». В открывшемся диалоговом окне Select a Server выберите один или несколько серверов почтовых ящиков, которые вы хотите использовать для отправки исходящей почты на промежуточный узел. Если в вашей среде несколько серверов почтовых ящиков, выберите те из них, которые могут направлять почту на промежуточный узел. Если у вас только один сервер почтовых ящиков, выберите его. Выбрав по крайней мере один сервер почтовых ящиков, нажмите кнопку добавить, кнопку «ОК», а затем кнопку «Готово».

Созданный соединитель появится в списке соединителей отправки.

2. Создайте соединитель отправки, использующий маршрутизацию через промежуточный узел, с помощью командной консоли MS Exchange:

2.1. Запустите командную консоль Exchange.²

2.2. Используйте следующий синтаксис:

²<https://learn.microsoft.com/ru-ru/powershell/exchange/open-the-exchange-management-shell?view=exchange-ps>

```
New-SendConnector -Name <Name> -AddressSpaces * -Custom -
DnsRoutingEnabled $false -SmartHosts <SmartHost1>[,<SmartHost2>...] [-
SourceTransportServer <fqdn1>,<fqdn2>...]
```

Не забудьте указать параметры аутентификации **Basic authentication** с использованием **Offer basic authentication only after starting TLS**.

3. DMARC (DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE)

2.1. Настройка доменной зоны

DMARC – это техническая спецификация, призванная усилить защиту от спамеров, подделывающих адреса отправителей.

DMARC представляет собой набор правил обработки электронных сообщений, которые не прошли авторизацию. Настройка позволяет выбрать порядок работы с такими письмами: не делать с ними ничего, либо помещать их в спам, либо просто отклонять.

Для обеспечения работоспособности DMARC необходимо настроить SPF и DKIM. Почтовый провайдер при получении электронного письма проверяет его при помощи SPF и DKIM. Если сообщение не прошло проверку ни по SPF, ни по DKIM, то применяется DMARC-политика.

Добавьте в вашу DNS-зону запись вида:

```
_dmarc.<ваш_домен>.ru.      IN      TXT      "v=DMARC1; p=reject;
rua=mailto:dmarc@<ваш_домен>.ru; sp=reject; aspf=s; adkim=s; ri=604800"
```

где:

Поле	Значение	Комментарий
v	DMARC1	Версия протокола DMARC
P	reject	Отклонять письма не прошедшие проверку DMARC
rua	mailto:dmarc@<ваш_домен>.ru	Адрес электронной почты на который присылать уведомления о результатах проверки
sp	reject	Отклонять письма с поддоменов, не прошедшие проверку DMARC
aspf	s	Определяет тип проверки 'strict' для SPF-записей
adkim	s	Определяет тип проверки 'strict' для DKIM-подписей

Ri	604800	Интервал в секундах, определяющий как часто получать агрегированные XML-отчеты
----	--------	--------------------------------------------------------------------------------

В случае, если у вас есть поддомены, с которых вы отправляете почту, то:

– в политике установите `sp=none`;

– настройте для каждого поддомена соответствующие политики SPF, DKIM, DMARC.

В результате этих настроек все поддомены должны соответствовать политике DMARC.

2.2. Почтовый сервер Postfix

1. Установите пакет программного обеспечения `opendmarc`. Для этого в операционных системах, основанных на Linux Debian, требуется выполнить с правами администратора следующую команду:

```
apt install opendmarc
```

2. В конфигурационном файле `/etc/opendmarc.conf` проверьте значения следующих параметров.

```
AuthservID          OpenDMARC
TrustedAuthservIDs  <ваш_домен>
RejectFailures      true
IgnoreAuthenticatedClients true
RequiredHeaders      true
SPFSelfValidate      true
ForensicReports      true
ForensicReportsSentBy noreply@<ваш_домен>
Socket               inet:8892@localhost
HistoryFile          /var/log/dmarc.dat
```

3. На следующем этапе в настройки postfix внесите одновременное «взаимодействие» с DKIM и DMARC. Для этого требуется выполнить с правами администратора следующие команды:

```
postconf -e 'smtpd_milters=inet:127.0.0.1:8891, inet:127.0.0.1:8892'
postconf -e 'non_smtpd_milters=inet:127.0.0.1:8891, inet:127.0.0.1:8892'
```

Следует отметить, что параметры команд предполагают, что `opendkim` настроен в соответствии с инструкцией, приведенной в подразделе 2.2.

4. Для применения настроек, перезапустите соответствующие сервисы. Для этого от имени администратора выполните следующие команды:

```
systemctl restart opendmarc
systemctl restart postfix
```

2.3. Настройка Exim

. Определите расположение актуального конфигурационного файла сервера Exim. Для этого выполните следующую команду.

```
exim4 -bV
```

2. Проверьте, что в актуальном конфигурационном файле приведенные ниже параметры имеют соответствующие значения и, в случае необходимости, отредактируйте их.

```
dmarc_history_file      = /var/log/dmarc.dat
dmarc_forensic_sender   = noreply@<ваш домен>
accept_authenticated = *
accept_hosts = +relay_from_hosts
begin acl
  acl_check_rcpt:
    warn domains          = +local_domains
    warn hosts            = +local_hosts
    warn control          = dmarc_disable_verify
    warn !domains         = +screwed_up_dmarc_records
    warn control          = dmarc_enable_forensic
  acl_check_data:
    warn dmarc_status     = accept : none : off
    warn !authenticated   = *
    warn log_message      = DMARC DEBUG: $dmarc_status $dmarc_used_domain
    warn dmarc_status     = !accept
    warn !authenticated   = *
    warn log_message      = DMARC DEBUG: '$dmarc_status' for
$dmarc_used_domain
    warn dmarc_status     = quarantine
    warn !authenticated   = *
    set $acl_m_quarantine = 1
    deny condition        = ${if eq{$dmarc_domain_policy}{reject}}
    deny message          = Messages from $dmarc_used_domain break
mailing lists
    deny dmarc_status     = reject
    deny !authenticated   = *
    deny message          = Message from $dmarc_used_domain failed
sender's DMARC policy, REJECT
    warn add_header       = :at_start:${authresults {$primary_hostname}}

begin routers
  localuser:
    transport = ${if =={$acl_m_quarantine}{1}
{local_delivery_quarantine}{local_delivery}}

begin transport:
  local_delivery_quarantine:
    driver = appendfile
    directory = /home/mail-quarantine/Maildir
    user = mail-quarantine
    home_directory = /home/mail-quarantine
    current_directory = /home/mail-quarantine
    maildir_format
    delivery_date_add
    envelope_to_add
    return_path_add
    group = mail
    mode = 0660
```

Обратите внимание, что указанные параметры располагаются в разных частях конфигурационного файла.

3. Создайте пользователя mail-quarantine. Для этого от имени администратора выполните следующую команду:

```
useradd -m -G main mail-quarantine
```

4. Обновите текущую конфигурацию почтового сервера. Для этого требуется выполнить с правами администратора следующую команду:

```
update-exim4.conf
```

5. Проверьте корректность полученной конфигурации, выполнив следующую команду:

```
exim4 -bV
```

6. Если проверка завершилась успешно, перезапустите почтовый сервер. Для этого в операционных системах, использующих systemd, требуется выполнить с правами администратора следующую команду:

```
systemctl restart exim4
```