Лабораторная работа №4
Настройка почтового сервера.

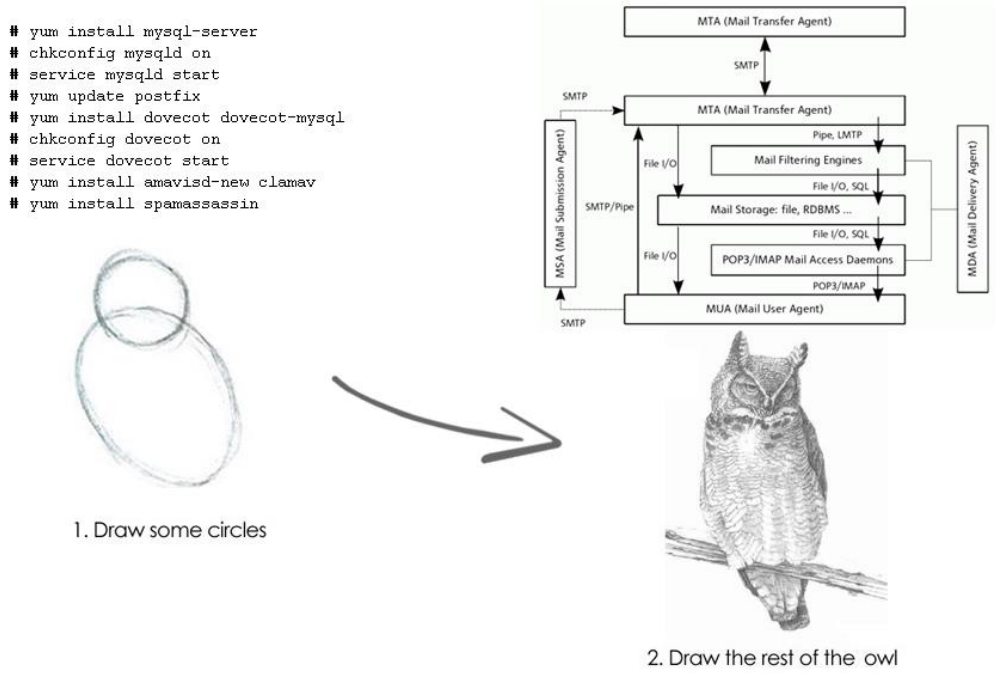


Рисунок 1 Как настроить почтовый сервер

Дисклеймер!

Все материалы, указанные в работе, рассказывают общие принципы работы почтовых серверов. Однако, в связи с особенностями ОС Астра Линукс на некоторых версиях настройки могут отличаться. Настройка выполнялась автором на ОС Астра Линукс версии 1.7 x86-64.

Версия postfix: 3.4.14

Версия dovecot: 2.3.4.1

Автор не гарантирует корректную работу почты на других версиях дистрибутива или утилит!

Введение

Каждый в повседневной жизни сталкивался с отправкой писем по электронной почте. Для этого необходимо зарегистрироваться на любом существующем почтовом сервисе от различных компаний и начать работу с ним. Однако, часто существует необходимость разворачивания собственных почтовых серверов в локальной сети. Это может быть сервер для работы с почтой внутри предприятия, веб-сайт, которому вы хотите дать возможность принимать письма от пользователей или сервер для защиты конфиденциальных писем.

Настройка почтового сервера является нетривиальной задачей. В лабораторной работе будет рассмотрен пример установки системы, состоящей из трех утилит – Postfix, Dovecot и Thunderbird.

Считается, что создателем электронной почты является Рей Томлинсон, разработавший программу для обмена сообщениями в сети ARPANET в 1971 году.

Именно он ввел символ @ как знак для отделения имени почтового домена от имени почтового ящика. Персональных компьютеров на тот момент было мало, поэтому задачей для первых почтовых серверов была пересылка писем между двумя конкретными компьютерами. Однако, с ростом числа устройств стало необходимо модернизировать работу почтовых серверов для решения более сложных задач.

Архитектура почтовой системы.

Почтовая система состоит из следующих компонентов:

- Пользовательский агент (MUA – Mail User Agent)
- Агент передачи электронной почты (MSA – Mail Submission Agent)
- Транспортный агент (MTA – Mail Transport Agent)
- Агент доставки (MDA – Mail Delivery Agent)
- Агент доступа (MAA – Mail Access Agent)

Рассмотрим каждый из компонентов подробнее:

Пользовательский агент (*MUA*)

Пользовательский агент используют для составления и чтения электронных писем. Письма составляются в соответствии с требованиями стандарта MIME (***M**ultipurpose **I**nternet **M**ail **E**xtensions*), описанном в документе RFC 5322. Примерами таких программ являются Microsoft Outlook, Mozilla Thunderbird, Evolution, а также веб-интерфейсы у сайтов 2andex, gmail и т.п. Самым первым и одним из самых простых MUA является утилита /bin/mail, с помощью которой возможно отправить письмо из командной строки. Основной задачей агента кроме составления письма является его передача следующему агенту – MTA или MSA.

Агент передачи электронной почты (*MSA*)

Является посредником между пользовательским агентом и транспортным. Необходим для проверки корректности введенных данных, например адреса получателя. Если адрес указан неверно, то письмо будет отфильтровано – это позволяет уменьшить нагрузку на сеть, очистив её от писем с неправильными данными. Кроме этого, MSA применяется для организации шифрованного и безопасного обмена сообщениями с пользовательскими агентами, что позволит избежать несанкционированного доступа к почтовому серверу и пересылке вредоносных сообщений.

Транспортные агенты (*MTA*)

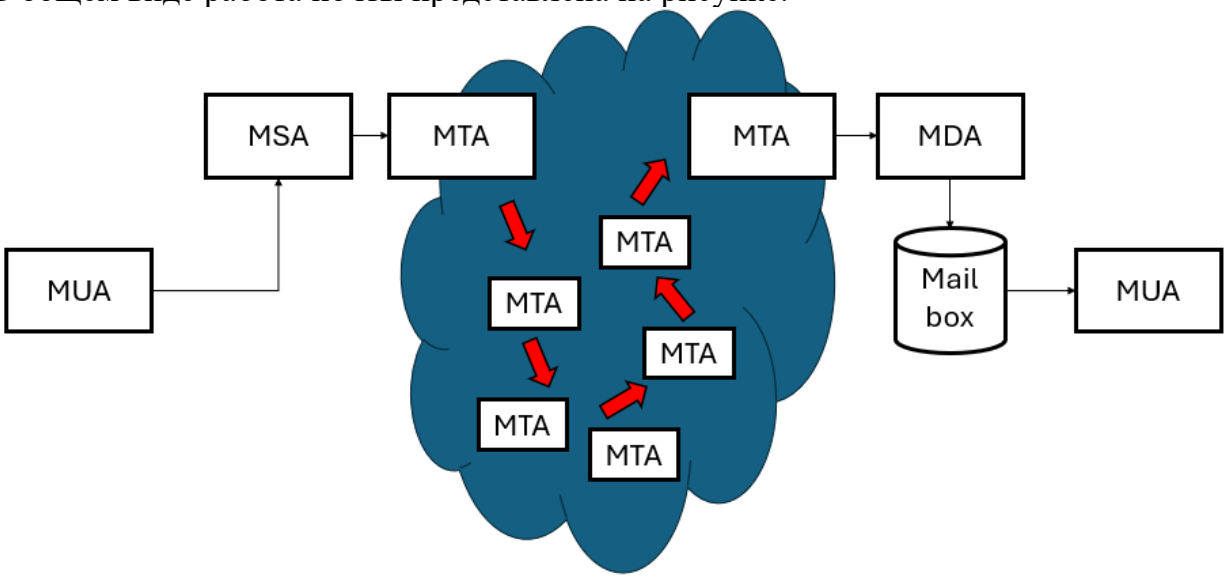
Одним из самых важных компонентов электронной почты являются транспортные агенты, позволяющие пересылать сообщение от клиента на другие транспортные агенты в других подсетях для дальнейшей доставки. Примером программ, выступающих в роли транспортных агентов являются sendmail, postfix, exim. Для передачи писем транспортные агенты узнают адрес целевого почтового сервера используя MX запись DNS сервера. Серверы, предназначенные только для

пересылки данных и не поддерживающие обработку локальной почты называются relay-server.

Агенты доставки (*MDA*) и агенты доступа (MAA)

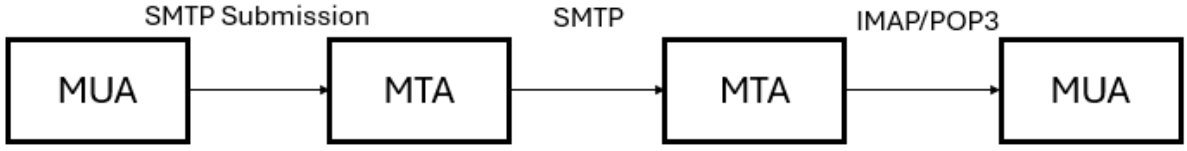
В простейшем случае передача почты возможна только с использованием транспортных агентов – письмо формируется вручную администратором на одном ПК, передается MTA, который пересылает письмо на другой ПК, где он помещается в файл с письмами. Однако, такой способ не сработает, когда компьютер-получатель будет выключен. Также для удобства в современном мире клиент может получать доступ к письмам с разных устройств – компьютера, ноутбука, мобильного телефона. В рамках рассмотренной выше модели такой подход невозможен. Поэтому удобнее было бы иметь постоянно работающий сервер, на который будет приходить входящая почта, а клиенты будут получать к ней доступ из приложений в любое время и с любого устройства. В роли такого сервера выступает агент доставки, который принимает входящие сообщения, обрабатывает их и сохраняет в базе данных, из которой в дальнейшем их возможно изымать и передавать клиентам с помощью агентов доступа.

В общем виде работа почты представлена на рисунке.



Письмо формируется на MUA, передается агенту MSA, где происходит проверка на правильность введенной информации и наличие спама. Далее письмо передается транспортному агенту, который пересылает его другим MTA. Конечной целью является транспортный агент домена получателя. От него письмо передается агенту доставки, который сохраняет письмо в почтовом ящике и ждет, когда пользователь сможет его оттуда достать, используя агента доступа и прочитать.

Почтовые протоколы



SMTP (*Simple Mail Transfer Protocol*) — это протокол, работающий поверх TCP/IP. Предназначен для передачи исходящей почты другим агентам. С помощью протокола SMTP возможно осуществить передачу между ***MUA – MSA, MUA – MTA, MSA-MTA, MTA-MTA, MTA-MDA.***

Существует модификации протокола SMTP – SMTP Submission (SMTP с авторизацией) и ESMTP.

Для передачи сообщений из почтового ящика, сконфигурированного агентом доставки, служат два протокола – POP3 и IMAP.

POP3 (*Post Office Protocol Version 3)* – один из первых протоколов доставки сообщений. Его преимуществом является то, что он не нагружает SMTP сервер, однако его функционал очень ограничен. С помощью POP3 возможно достать и удалить письмо по требованию пользователя. Для более сложной работы служит протокол **IMAP** (*Internet Message Access Protocol*) – с его помощью клиент может отслеживать состояние сообщения, организовывать систему папок для сортировки сообщений и допускает одновременный доступ нескольких клиентов к почтовому ящику. IMAP позволяет отдельно выдать пользователю заголовки писем, что уменьшает нагрузку на сеть – клиенту не требуется скачивать целиком письмо, чтобы в дальнейшем с ним работать.

Почтовый сервер Postfix.

Postfix – современным агентом передачи сообщений (MTA) или сервером SMTP. Он был разработан Витсе Венемой, экспертом в области Unix и безопасности. Postfix отличается простотой использования, разработан с учетом безопасности и модульности, причем каждый модуль работает с минимально необходимым уровнем привилегий. Postfix тесно интегрирован с системами Unix/Linux и не предоставляет функциональности, которые уже есть в Unix/Linux. Это надежное решение как для простых, так и для сложных условий.

Изначально Postfix был разработан как замена Sendmail — старого традиционного SMTP-сервера в системах Unix. По сравнению с Sendmail, Postfix безопаснее и проще в настройке. Он совместим с Sendmail, так что при замене Sendmail на Postfix, существующие скрипты и программы будут продолжать работать без изменений.

Postfix включает в себя несколько программ, взаимодействующих с пользователем или работающих в фоновом режиме.

Работа Postfixa схожа с работой маршрутизатора – он принимает сообщения из нескольких источников и передает их определенным адресатам. Для определения пути маршрутизатор использует таблицы маршрутизации, postfix в свою очередь использует карты (map). Карты представляют из себя файлы или базы данных, содержащие пары «ключ: значение». Для ускорения доступа некоторые карты возможно индексировать. Файлы карт имеют суффикс, обозначающий тип использованного индекса – например «.db». Вместо карт возможно использовать и классические базы данных – mysql, postgres mariadb и другие. Postfix по-разному реагирует на изменения в картах. Если карта не индексирована и является обычным файлом, до для его обработки системой необходимо её целиком перегрузить. При работе с индексированными картами основной демон postfix – master сам перегружает процесс, ответственный за работу с ними. Для работы с базами данных

перегружать систему в целом не нужно, однако время запросов к ней ниже, чем к картам.

Одной из основных частей postfix является очередь, содержащая почту, которая ожидает доставки. Менеджер очереди использует обычно стратегию FIFO для доступа к её элементам, однако возможно применение алгоритма для выдачи в первую очередь приоритетных сообщений.

Утилиты для работы с postfix

Вместе с postfix устанавливаются утилиты командной строки, позволяющие решать задачи администрирования почтового сервера.

Команда	Описание	
postfix [start | stop | reload]	Запуск, остановка и перегрузка конфигурации	
postconf	Вывод конфигурации системы	
postalias	Создание индексированной карты из файла псевдонимов alias	
postmap имя файла	Создание индексированной карты из файла	
postqueue [ключ]	Команда работы с очередью	
	-f	Очистка очереди и доставка ее получателям
	-p	Вывести содержимое очереди
	-s	Доставить всю почту только для домена. Используется с параметром: -s имя домена.
postsuper [ключ]	Работа с очередью от имени суперпользователя.	
	-d	Удаление сообщения с указанным ID. Для удаления всех сообщений возможно использовать ключевое слово ALL.
	-h	Удержание сообщения
	-H	Освобождение сообщений

Основные файлы конфигураций postfix.

Все конфигурационные файлы postfix расположены по адресу /etc/postfix.

main.cf

Основным конфигурационным файлом системы является main.cf. Он содержит в себе набор параметров, которым можно установить определенные значения. После определения параметра к нему возможно обратиться из другой строчки, используя знак $. Например:

```
mydoman = mpsu.stu
myorign = $mydomain
```

Строки, начинающиеся с пробела, интерпретируются как продолжение предыдущей строки, поэтому важно следить, чтобы при объявлении нового параметра он находился сразу с начала строки.
Файл main.cf может содержать более 500 параметров, однако наибольший интерес представляют только некоторые из них. Рассмотрим основные из них:

- mydomain – определение имени домена сети
- myorign – определение имени почтового домена, подставляемого в адреса
- mydestination – локальный почтовый домен. Если он совпадает с доменом в адресе получателя в доставленном письме, то с помощью программы local происходит их доставка в почтовые ящики.
- relayhost – пересылка всех нелокальных сообщений на указанный хост
- mynetworks - список всех хостов и сетей, для которых Postfix может пересылать сообщения
- home_mailbox – адрес директории, которая будет использована как почтовый ящик

master.cf

Конфигурационный файл настройки транспортных служб. В него необходимо внести информацию о той службе, которая будет непосредственно передавать сообщение от одного компьютера к другому. По умолчанию в файле указана служба smtp.

Настройка защищенного соединения.

По умолчанию вся почта передается в незашифрованном виде, что является небезопасным. Используя приложения для перехвата пакетов возможно прочитать передаваемые сообщения. Для защиты используются различные протоколы, один из них – TLS (Transport Layer Security). Протокол использует метод шифрования, основанный на передаче сертификатов безопасности.

Для организации защищенного соединения в main.cf необходимо указать следующие параметры:

```
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_generic_maps = hash:/etc/postfix/generic
smtp_tls_CAfile = /etc/ssl/certs/Entrust_Root_Certification_Authority.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_session_cache
smtp_tls_session_cache_timeout = 600s
smtp_tls_wrappermode = yes
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = encrypt
smtp_tls_loglevel = 1
```

Обратим внимание на два из них: smtp_sasl_password_maps и smtp_generic_maps. В этих параметрах указывается адрес карт с указанием информации, необходимой для соединения.

smtp_sasl_password_maps указывает на файл sasl_passwd. Он создается пользователем и содержит сервер, с которым будет проходить соединение, адрес удаленного почтового ящика и его пароль. Параметр smtp_generic_maps, указывающий на файл generic, содержащий имя почты на клиенте и имя почты на удаленном сервере. Например, если мы хотим отправить сообщение с почтового сервера mpsu.stu на сервер yandex.ru, то файлы будут иметь следующий вид:

/etc/postfix/generic

```
server@mpsu.stu studentmpsu@yandex.ru
```

/etc/postfix/sasl_passwd

```
smtp.yandex.ru studentmpsu@yandex.ru:qwerty22
```

Агент доставки Dovecot.

Для того, чтобы получать письма, используя приложение почтового клиента, необходимо установить открытый IMAP-сервер Dovecot. Для базовой настройки сервера необходимо указать в конфигурационном файле 10-auth.conf тип подключения и в файле 10-mail.conf – файл, в который будет использован, как почтовый ящик. Например:

/etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
auth_mechanisms = plain login
```

/etc/dovecot/conf.d/10-mail.conf

```
mail_location = maildir:~/Maildir
```

2. Практическая часть

2.1. Задание 1

Произведите предварительные настройки.

2.1.1. Установите необходимые программы для работы почтового сервера.

```
sudo apt-get install postfix dovecot-imapd astrase-fix-maildir
```

2.1.2 На сервере создайте двух пользователей, от имени которых будет происходить пересылка почтовых сообщений.

Имя: вашиинициалыmailserver (например sabmailserver) Минимальный мандатный уровень: 1	Имя: вашиинициалыmailclient (например sabmailclient) Минимальный мандатный уровень: 1

Максимальный мандатный уровень: 2 Максимальный мандатный уровень: 2

2.1.3. От имени созданных пользователей создайте в их домашних директориях файл, в котором будет храниться их почта. Выдайте на созданную директорию права таким образом, чтобы работать с ней (чтение и запись) могли производить только сами пользователи.

2.2. Задание 2.

Настройте почтовый сервер и обменяйтесь сообщениями между сервером и клиентом.

2.2.1. Настройте сервер postfix. В параметрах укажите значения mynetworks для вашей сети, mydestination*;* в параметре home_mailbox укажите адрес созданных почтовых ящиков. После указанных параметров укажите значение smtpd_relay_restrictions (см. ниже). Без него письма будут блокированы. Пример настройки фала:

```
mynetworks = X.X.X.X/YY
mydestination = $myhostname, localhost, ваш домен
home_mailbox = Maildir/
smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination
```

После настройки перезапустите службу.

2.2.2. Настройте сервер dovecot в соответствии с указаниями выше. После настройки перезапустите службу.

2.2.3. На сервере откройте приложение Thunderbird, укажите в нем установленные параметры и создайте почтовый аккаунт.

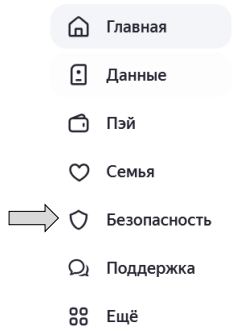
2.2.5. Отправьте любое письмо с сервера на сервер.

2.2.6. Запустите Thunderbird на машине клиента и зарегистрируйте клиента. Отправьте письмо с клиента на сервер и с сервера на клиент.

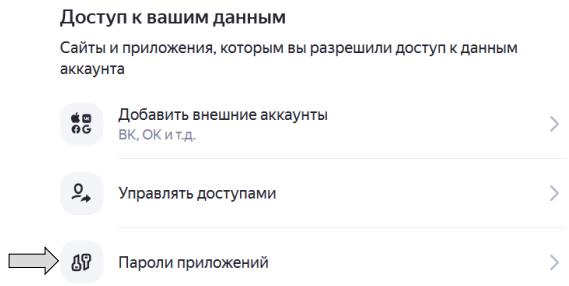
2.3. Задание 3.

Создайте почту yandex.ru и отправьте любое сообщение на неё от сервера и клиента.

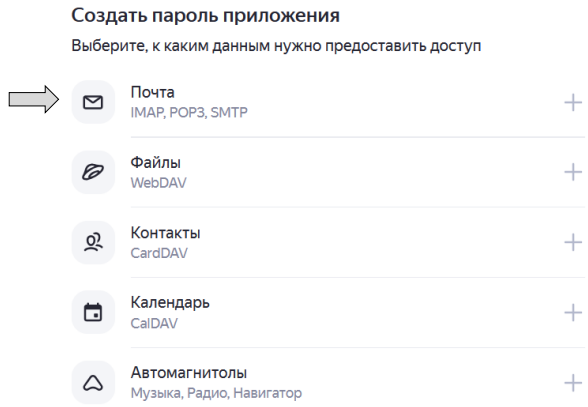
2.3.1. Создайте пароль для доступа с локального сервера на созданную почту яндекс. Для этого переходим на сайт https://id.yandex.ru/, в раздел «Безопасность»:



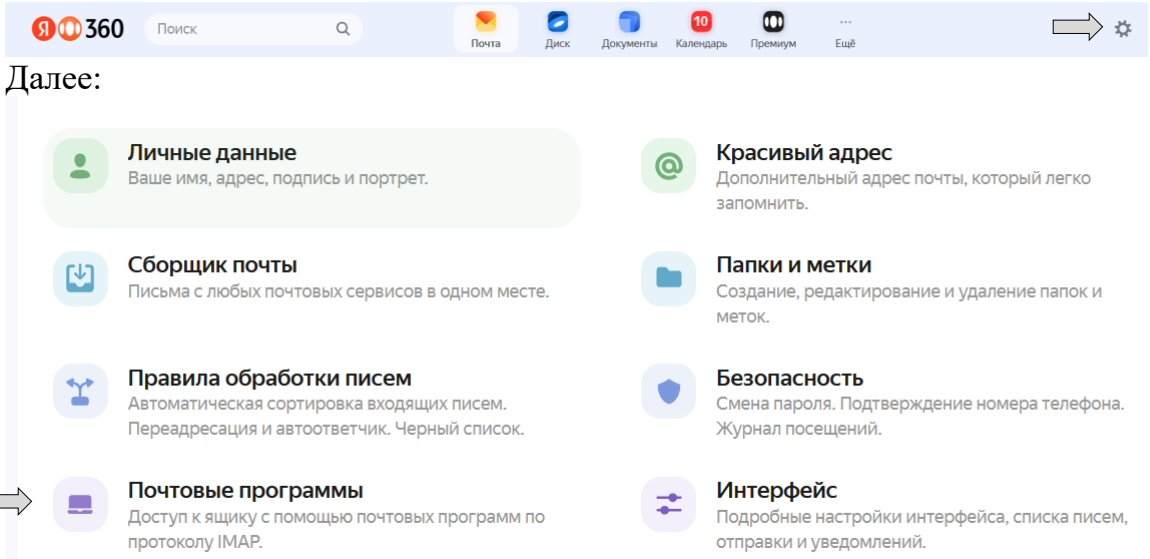
В разделе «Доступ к вашим данным» найдите пункт «Пароли приложений»



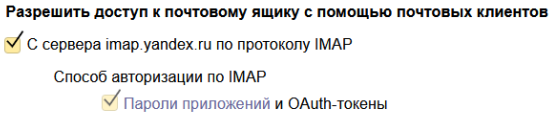
Создайте пароль для почтового сервера. Пароль сгенерируется автоматически, вам необходимо придумать ему название.



2.3.2. Выдайте разрешение на подключение к почте по протоколу IMAP. Для этого в Яндекс почте выбираем пункт «Все настройки» -> «Почтовые программы» -> «Разрешить доступ к почтовому ящику» - ставим галочки «С сервера imap.yandex.ru по протоколу IMAP», Способ авторизации – «Пароли приложений и OAuth-токены»



Выбираем пункты:



2.3.3. Организуйте передачу писем на почту yandex.ru по защищенному протоколу TLS. В качестве параметра relayhost укажите «smtp.yandex.ru:465».

Контрольные вопросы:

1. Для чего необходимы почтовые сервера?
2. Как происходит процесс передачи почты?
3. Для чего необходим компонент MDA?
4. Как работает протокол SMTP?
5. В чем отличие протоколов IMAP и POP3?