

В рамках данной дисциплины предполагается рассмотрение следующих классических прикладных протоколов семейства TCP/IP:

1. FTP;
2. Telnet;
3. SMTP, POP, IMAP;
4. HTTP.

Для подробного рассмотрения безопасности прикладных протоколов предусмотрена отдельная дисциплина, поэтому соответствующий материал во многом опущен.

(В таблицах ниже серым цветом выделена информация для поверхностного изучения. Аргументы команд так же приводятся для ознакомления – без подробного описания.)

Протоколы электронной почты

Сообщениями протоколов электронной почты являются *электронные письма* (emails). Электронные письма имеют текстовую природу.

По аналогии с бумажным письмом, электронное письмо так же состоит из конверта (envelope) и содержимого (content). Содержимое, в свою очередь, состоит из заголовка (header) и основного текста (body). Структура (прежде всего, синтаксис) электронных писем неоднократно регламентировалась стандартами (начиная с RFC 822 и более старых, заканчивая RFC 5322). Для обеспечения прав и обязанностей, связанных с электронными письмами, предусмотрены два механизма: DKIM (DomainKeys Identified Mail) Signatures (RFC 6376) и SPF (Sender Policy Framework) (RFC 7208).

Изначально, в отношении всех компонентов электронного письма допускалась только 7-мибитная кодировка US-ASCII.

Очень значимым расширением электронной почты является MIME (Multipurpose Internet Mail Extensions) (RFC 2045 – 2049 и много обновлений), позволяющее включать в основной текст электронного письма (и «прикреплять» к электронному письму) различные мультимедийные данные.

В настоящее время определены следующие MIME-типы:

1. text – текст (основное содержимое письма, указывается кодировка, возможна 8-мибитная кодировка).
 2. image – изображение.
 3. audio – звук.
 4. video – видео.
 5. application – электронные данные, не подпадающие ни под один из других типов.
- +6 multipart – комбинация нескольких типов.
- +7 message – письмо в письме либо внешнее приложение к письму (attachment).
- Каждый из типов имеет некоторое количество подтипов.

Одно из последних расширений (RFC 6532) позволяет полностью интернационализировать электронную почту – разрешает использовать кодировку UTF-8 вместо US-ASCII уже в адресах и напрямую в заголовках (второй шаг после MIME).

Стандарты четко не ограничивают размеры электронного письма и его составных частей. Однако, в реализациях, размер содержимого обычно не должен превышать 64 килобайта, а общий объем (включая приложения) – несколько мегабайтов.

Одним из ключевых понятий системы электронной почты является понятие *почтового ящика* (mailbox, иногда maildrop). Электронный почтовый ящик по своей сути ничем не отличается от почтового ящика для бумажных писем, но не всегда представляет собой файловое хранилище.

Почтовые ящики могут быть расположены как на выделенных для этого почтовых серверах – лучше переводить как MxEs (Mail eXchanges), так и на пользовательских станциях. Могут быть как локальными, так и удаленными от пользователя.

Фактически, в системе электронной почты адресуются именно почтовые ящики. Современный формат адреса:

```
<address> = <mailbox> / <group>

<mailbox> = <name-addr> / <addr-spec>
<name-addr> = {<display-name>[<CFWS>] "<"<addr-spec>">} [<CFWS>] / <obs-angle-addr>
<addr-spec> = <local-part> @ <domain>

<group> = {<display-name> "<"[<mailbox-list> / <CFWS> / <obs-group-list>] ">"} [<CFWS>]
<mailbox-list> = {<mailbox> *("<"<mailbox>") / <obs-mbox-list>}
```

Где: <display-name> – имя человека либо название программы (отправителя либо получателя, просто отображается, при пересылке не используется); <local-part> – название почтового ящика (отправителя либо получателя, может содержать все печатные US-ASCII-символы кроме метасимволов: (), <, >, [], :, ;, @, \, , , ., ", метасимвол-точка является исключением, но точка не может быть крайней и не может встречаться более одного раза подряд, регистр букв учитывается, экранирование заключением в двойные кавычки позволяет включить в название все символы, при этом \ и " заменяются на \\ и \" соответственно; <domain> – доменное название, относящееся к домену либо к станции (источника либо назначения), где расположен данный почтовый ящик, <cfws> – комментарий (в круглых скобках) или стандартный разделитель (один либо несколько пробелов или табуляций).

Имеется совместимость с устаревшим форматом (не отображено). Поддерживаются псевдонимы и групповая рассылка.

При рассмотрении любой почтовой системы прежде всего выделяются взаимодействующие процессы, которые принято называть почтовыми агентами. Традиционно в список почтовых агентов включают:

1. MTAs (Mail Transport Agents) – доставляют письма между почтовыми серверами.
2. MDAs (Mail Delivery Agents) – помещают доставленные сообщения в почтовые ящики пользователей.
3. MUAs (Mail User Agents) – реализуют интерфейс пользователей с их почтовыми ящиками.
- +4. MSAs (Mail Submission Agents) – позволяют вводить письма разными способами.

Следует отметить, что количественное и качественное наполнение списка почтовых агентов разнится (выше показан «усредненный» список). Например, в стандартах RFC термин MDA почти не упоминается. Изначально выделялись только MUA и MTA. Недавно на стороне отправителя между MUA и MTA был «вставлен» MSA.

Наличие удаленных почтовых ящиков (расположенных на удаленных от пользователя почтовых серверах) привело к такой отличительной особенности системы электронной почты как выделение в рамках одной прикладной задачи двух групп базовых прикладных протоколов – протоколов для передачи почты и протоколов для приема почты.

В свою очередь, в рамках каждого из почтовых протоколов берется за основу клиент-серверная модель и используется транспорт TCP.

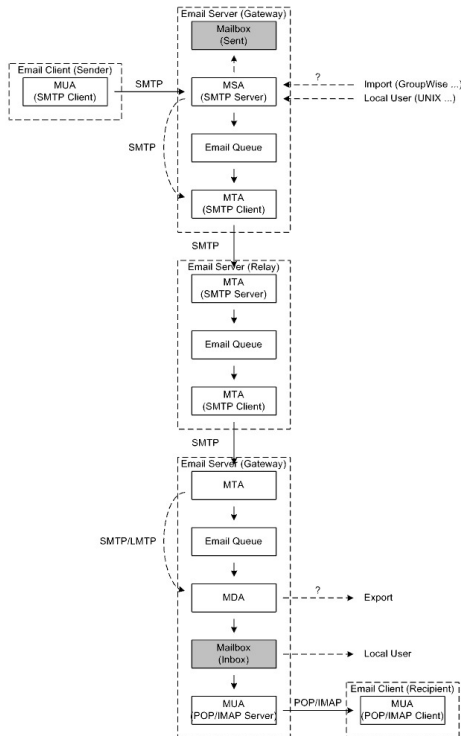


Рисунок – Обобщенная структура системы электронной почты

Протокол SMTP (Simple Mail Transfer Protocol) (основное RFC – RFC 5321) применяется для передачи электронной почты в почтовый ящик – от пользовательской станции (отправителя) к почтовому серверу и от одного почтового сервера к другому. (В очень редких случаях, при «необычных» почтовых ящиках, письмо может передаваться и от почтового сервера к пользовательской станции, например, «прямо на экран монитора»).

Таким образом, SMTP-клиентом (передатчиком письма) может быть как пользовательская станция, так и почтовый сервер, а SMTP-сервером (приемником письма) как правило является почтовый сервер. Правила взаимодействия между SMTP-клиентом и SMTP-сервером аналогичны правилам взаимодействия между FTP-клиентом и FTP-сервером. Задействуется одно соединение. Стандартный номер программного порта SMTP-сервера – 25. Для MSA предусмотрен альтернативный номер порта – 587, но многие почтовые системы для MSA по-прежнему используют порт 25.

Физическим почтовым клиентом является оконечная пользовательская станция, за которой работает пользователь-отправитель или пользователь-получатель письма. Физическим почтовым сервером обычно является оконечная серверная станция. Логическим почтовым клиентом и логическим почтовым сервером являются определенные программы. Логический почтовый клиент не всегда находится на физическом почтовом клиенте, он может находиться на физическом почтовом сервере (что свойственно ОС UNIX, локальный пользователь может быть подключен и через удаленный терминал посредством SSH). И почтовые агенты могут соотноситься со станциями по-разному. На почтовом клиенте может располагаться только MUA, на почтовом сервере могут располагаться все почтовые агенты. MSA + MTA, равно как MTA + MDA, обычно совмещены на одном почтовом сервере, но в общем случае могут быть «разнесены» (при этом взаимодействуют так же по протоколу SMTP).