Протоколы работы с почтой: SMTP, POP3, IMAP4.

1. Обзор почтовых протоколов.
2. Схема работы почтовых протоколов стека TCP/IP
   - SMTP
   - POP
   - IMAP
3. Наиболее известные WEB-клиенты работы с почтой.
4. Настройки безопасности в почтовых системах:
   - TLS
   - SSL
   - цифровая подпись
   - сертификат
   - Понятие СПАМ.

1. Обзор почтовых протоколов.

Электронная почта существуют уже более трёх десятилетий: до 1990 года она использовалась преимущественно в научных организациях, в 90-е - получила широкую известность и стала использоваться повсеместно.

По оценкам 2015 г. в мире более 2,5 миллиардов человек пользуются услугами электронной почты. Отправляется 85 миллиардов сообщений в день. В целом же трафик электронной почты занимает только 4% всего сетевого. Как и любой форме коммуникаций, электронной почте присущ определенный стиль и набор соглашений. В частности, общение по электронной почте носит неформальный и демократичный характер.

См. http://www.worldometers.info/ru/

Электронная почта даёт возможность посылать и получать сообщения, отвечать на письма корреспондентов автоматически, используя их адреса, рассылать копии письма сразу нескольким получателям, переправлять полученное письмо по другому адресу, использовать вместо адресов (числовых или доменных имен) логические имена, создавать несколько подразделов почтового ящика для разного рода корреспонденции, включать в письма текстовые файлы, пользоваться системой "отражателей почты" для ведения дискуссий с группой ваших корреспондентов и т.д.

Развитие технологии Internet привело к появлению современных протоколов для обмена сообщениями, которые предоставляют большие возможности для обработки писем,

разнообразные сервисы и удобство в работе. Так, например, протокол SMTP, работающий по принципу клиент-сервер, предназначен для отправки сообщений с компьютера к адресату. Обычно доступ к серверу SMTP не защищается паролем, так что можно использовать для отправки писем любой известный сервер в сети. В отличие от серверов для отправки писем, доступ к серверам для хранения сообщений защищается паролем. Поэтому необходимо использовать сервер или службу, в которой существует учётная запись. Эти серверы работают по протоколам POP и IMAP, которые различаются способом хранения писем.

В соответствии с протоколом POP3 поступающие на определенный адрес сообщения хранятся на сервере до того момента, пока они не будут в течение очередного сеанса загружены на компьютер. После загрузки сообщений, можно отключиться от сети и приступить к чтению почты. Таким образом, использование почты по протоколу POP3 является наиболее быстрым и удобным в использовании.

Протокол IMAP удобен тем людям, которые пользуются постоянным подключением к сети. Сообщения, поступившие на адрес, также хранятся на сервере, но, в отличие от POP3, при проверке почты сначала будут загружены только заголовки сообщений. Само письмо можно будет прочитать после выбора заголовка сообщения (оно загрузиться с сервера). Ясно, что при коммутируемом соединении работа с почтой по этому протоколу приводит к неоправданным потерям времени.

Существует несколько протоколов приема передачи почты между многопользовательскими системами.

Краткое описание некоторых из них:

SMTP (Simple Mail Transfer Protocol) - это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP, причем передача должна быть обязательно инициирована самой передающей системой.

POP, POP2, POP3 (Post Office Protocol) - три достаточно простых невзаимозаменяемых протокола, разработанные для доставки почты пользователю с центрального mail-сервера, ее удаления с него и для идентификации пользователя по имени/паролю. POP включает в себя SMTP, который используется для передачи почты, исходящей от пользователя. Почтовые сообщения могут быть получены в виде заголовков, без получения письма целиком.

IMAP2, IMAP2bis, IMAP3, IMAP4, IMAP4rev1 (Internet Message Access Protocol).

IMAP осуществляет хранение почты на сервере в файловых директориях, а также предоставляет клиенту возможность производить поиск строк в почтовых сообщениях на самом сервере.

IMAP2 - используется в редких случаях.

IMAP3 - несовместимое ни с чем решение, не используется.

IMAP2bis - расширение IMAP2, позволяет серверам разбираться в MIME-структуре (Multipurpose Internet Mail Extensions) сообщения, используется до сих пор.

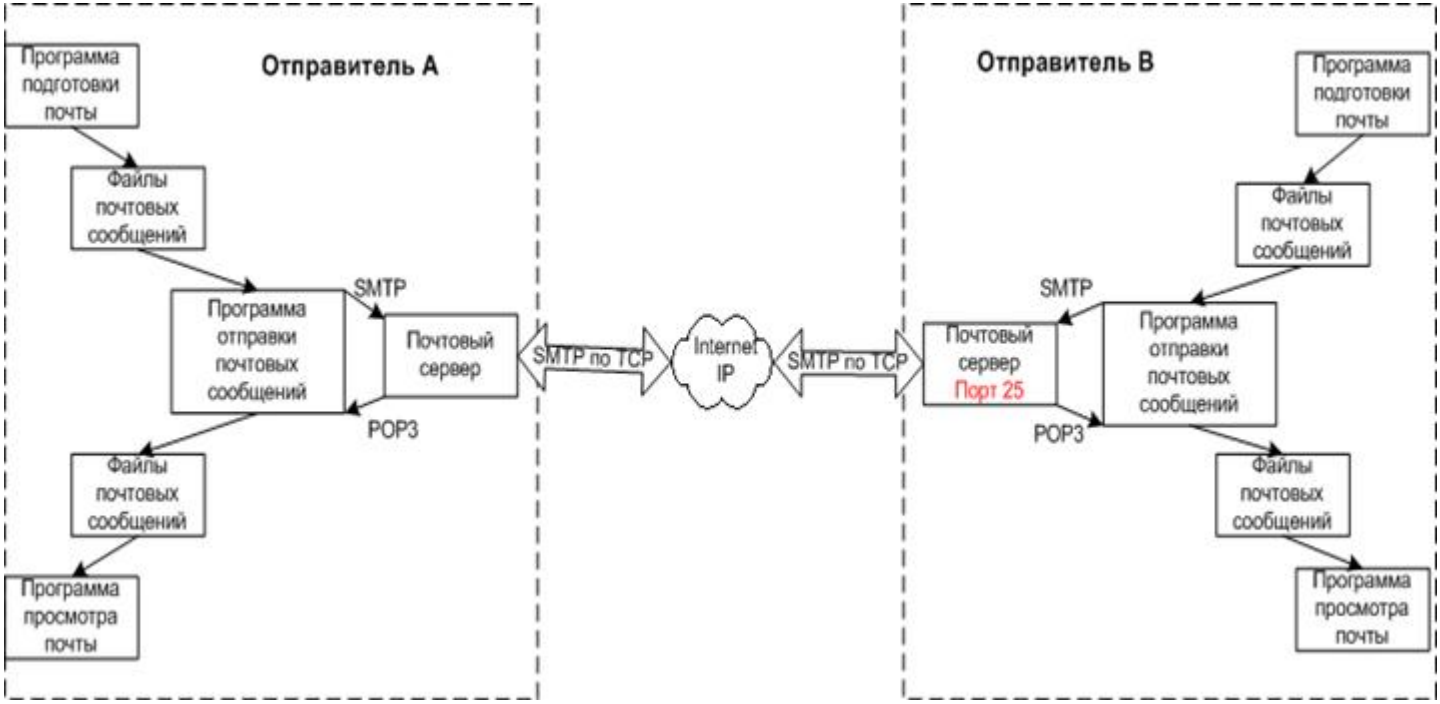
IMAP4 - переработанный и расширенный IMAP2bis, который можно использовать где угодно.

IMAP4rev1 - расширяет IMAP большим набором функций, включая те, которые используются в DMSP (Distributed Mail System for Personal Computers).

ACAP (Application Configuration Access Protocol) - протокол, разработанный для работы с IMAP4; добавляет возможность поисковой подписки и подписки на доски объявлений, почтовые ящики и используется для поиска адресных книг.

DMSP (или PCMAIL) - протокол для приема/отправки почты, особенность которого заключается в том, что пользователь может иметь более одной рабочей станции в своем пользовании. Рабочая станция содержит статусную информацию о почте, директорию, через которую происходит обмен, которая при подключении к серверу обновляется до текущего состояния на mail-сервере.

MIME - стандарт, определяющий механизмы для отправки разного рода информации с помощью электронной почты, включая текст на языках, отличных от английского, для которых используются символьные кодировки, отличные от ASCII, а также 8-битный бинарный контент, такой как картинки, музыка, фильмы и программы.


Отправитель А
Программа подготовки почты
Файлы почтовых сообщений
Программа отправки почтовых сообщений
SMTP
POP3
Почтовый сервер
Файлы почтовых сообщений
Программа просмотра почты
SMTP по TCP
Internet IP
SMTP по TCP
Отправитель В
Программа подготовки почты
Файлы почтовых сообщений
SMTP
Почтовый сервер
Порт 25
Программа отправки почтовых сообщений
POP3
Файлы почтовых сообщений
Программа просмотра почты

2. Схема работы почтовых протоколов стека TCP/IP

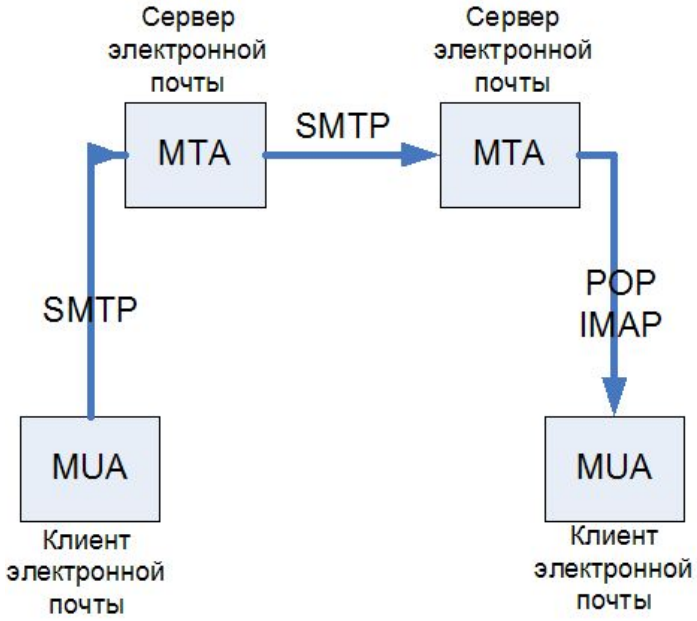
2.1. SMTP.

В Интернете для доставки электронной почты машина-источник устанавливает TCP-соединение с портом 25 машины приемника. Этот порт прослушивается почтовым демоном, и их общение происходит с помощью протокола SMTP (Simple Mail Transfer Protocol простой протокол электронной почты). Этот демон принимает входящие соединения и копирует сообщения из них в соответствующие почтовые ящики. Если письмо невозможно доставить, отправителю, то отправляется сообщение об ошибки, содержащее первую часть этого письма.

MTA (Mail Transfer Agent) - агент передачи почты - является основным компонентом системы передачи почты Internet, который представляет данный сетевой компьютер для сетевой системы электронной почты.

Обычно пользователи работают не с MTA, а с программой **MUA (Mail User Agent)** - клиентом электронной почты. Схематично принцип взаимодействия показан на рисунке.

Протокол SMTP представляет собой простой ASCII протокол. Установив TCP-соединение с портом 25. передающая машина выступающая в роли клиента, ждет запроса принимающей машины, работающей в режиме сервера. Сервер начинает диалог с того что посылает текстовую строку, содержащую его идентификатор и сообщающую о его готовности (или неготовности) к приему почты. Если сервер не готов, клиент разрывает соединение и продолжает попытку позднее.



Если сервер готов принимать почту, клиент объявляет, от кого поступила почта и кому она предназначается. Если получатель почты существует, сервер дает клиенту добро на пересылку сообщения. Затем клиент посылает сообщение. А сервер подтверждает его получение. Контрольные суммы не проверяются, так как протокол TCP обеспечивает надежный байтовый поток. Если у отправителя есть еще почта. Она также отправляется. После передачи всей почты в обоих направлениях соединение разрывается.

2.1.1. Простейший пример SMTP-сессии C: - клиент, S: - сервер

```
S: (ожидает соединения)
C: (Подключается к порту 25 сервера)
S:220 mail.company.tld ESMTP CommuniGate Pro 5.1.4i is glad to see you!
C:HELO
S:250 domain name should be qualified
C:MAIL FROM:
S:250 someusername@somecompany.ru sender accepted
C:RCPT TO:
S:250 user1@company.tld ok
C:RCPT TO:
S:550 user2@company.tld  unknown user account
C:DATA
S:354 Enter mail, end with "." on a line by itself
C:Hi!
C:.
S:250 769947 message accepted for delivery
C:QUIT
S:221 mail.company.tld CommuniGate Pro SMTP closing connection
S: (закрывает соединение)
```

В результате такой сессии письмо будет доставлено адресату user1@company.tld, но не будет доставлено адресату user2@company.tld, потому что такого адреса не существует.

2.1.2. Некоторые команды SMTP

HELO {SP} {string}{CRLF}	Идентифицирует SMTP-сервер отправителя, открывает сеанс {SP} пробел
QUIT{CRLF}	Завершает SMTP-сеанс.
MAIL {SP} FROM:{reverse-path} {CRLF}	Задает адрес отправителя.
RCPT {SP} TO:{forward-path} {CRLF}	Задает адрес получателя.
DATA {CRLF}	Указывает на начало сообщения. Для окончания сообщения указывается {CRLF}.
VRFY {SP} {string}{CRLF}	проверяет существование получателя.
EXPN {SP} {string}{CRLF}	показывает список адресов для списка рассылки.
NOOP{CRLF}	пустая операция
TURN{CRLF}	сервер и клиент меняются ролями после ответа сервера 200 OK
RSET{CRLF}	сброс сессии в исходное состояние
HELP{CRLF}	информация о поддерживаемых командах

Из-за проблем со спамом, почти все современные сервера игнорируют команды VRFY и EXPN, как раскрывающие информацию о пользователе.

Для решения некоторых проблем был разработан расширенный протокол SMTP, ESMTP. Клиенты, желающие использовать его, должны начинать сессию связи с посылки приветствия EHLO вместо HELO. Если команда не принимается сервером, значить, сервер поддерживает только обычный протокол SMTP и клиенту следует работать в обычном режиме. Если же EHLO принято, значить, установлена сессия ESMTP и возможна работа с новыми параметрами и командами.

2.1.3. Принципы формирования кода отклика в системе SMTP.

Любой код отклика содержит три цифры. 1-я цифра говорит о том, является ли отклик положительным, отрицательным или промежуточным. Отправитель, проанализировав первую цифру, может решить, продолжать выполнение задачи, повторить последнюю операцию или отказаться от своей затеи. Для уточнения типа ошибки отправитель может проанализировать вторую цифру, последняя цифра уточняет диагноз.

Код	Назначение
1yz	Промежуточный позитивный отклик. Команда воспринята. Отправитель должен послать следующую команду.
2yz	Позитивное подтверждение завершения операции. Можно посылать следующий запрос.
3yz	Позитивный промежуточный отклик, сходный с 1yz, используется в случае групповых команд.
4yz	Временный негативный отклик. Команда не исполнена, но характер ошибки временный и выполнение процедуры может быть позже повторено.
5yz	Окончательный негативный отклик. Команда не воспринята, запрошенная операция не выполнена и не будет выполнена.

x0z	Синтаксис - эти отклики относятся к синтаксическим ошибкам или к командам синтаксически корректным но примененным неправильно.
x1z	Информация - относится к командам, которые запрашивают информацию, например, статусную или справочную.
x2z	Соединения - относится к телекоммуникационному каналу.
x3z	Пока не определен.
x4z	Пока не определен.
x5z	Почтовая система - эти отклики индицируют статус получателя или отправителя почты.

2.1.4. Список кодов и откликов на почтовые команды и сообщения.

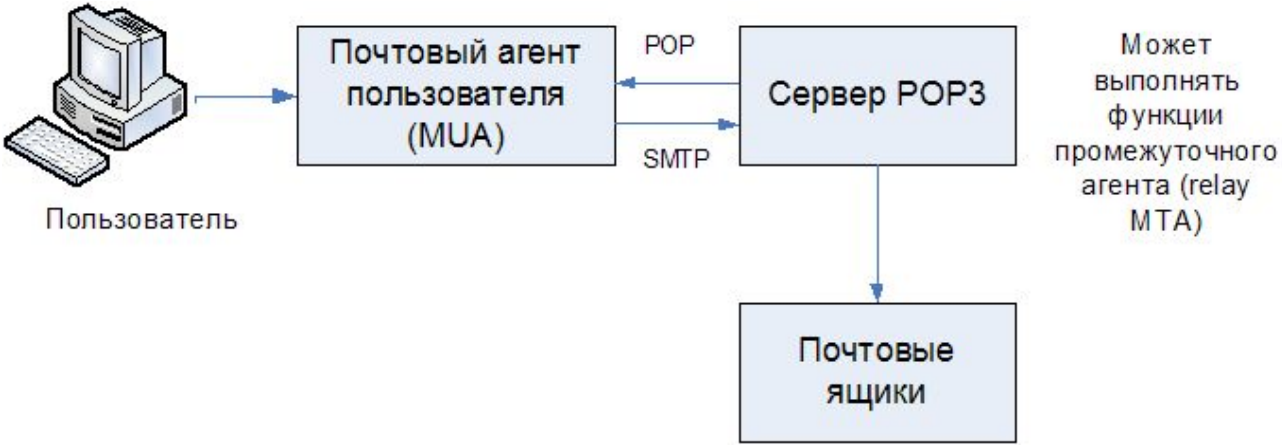
211	Сообщение о состоянии системы или справочный отклик (help).
214	Help message - сообщение для сведения. [Информация о том, как использовать приемник или значение конкретной нестандартной команды; этот отклик полезен только для пользователей-людей].
220	<domain> Service ready - сервер готов к обслуживанию.
221	<domain> Service closing transmission channel - сервер закрывает канал;
250	Requested mail action okay, completed - процедура успешно завершена;
251	User not local; will forward to <forward-path> - адресат не местный, сообщение ему будет переадресовано.
354	Start mail input; end with <CRLF>.<CRLF> - начало ввода сообщения, завершение символьной последовательностью
421	<domain> Service not available, closing transmission channel - сервер не доступен, процедура прерывается. [Это может быть ответом на любую команду, если сервер знает, что он должен прервать обслуживание]
450	Requested mail action not taken: mailbox unavailable - запрошенная процедура не выполнена [Напр., из-за отсутствия доступа к почтовому ящику].
451	Requested action aborted: error in processing - выполнение процедуры прервано из-за ошибки.
452	Requested action not taken: insufficient system storage - операция не выполнена из-за недостатка системной памяти.
500	Syntax error, команда не узнана. [Среди прочего, это может указывать на то, что командная строка имеет слишком большую длину].
501	Syntax error in parameters or arguments - синтаксическая ошибка в параметрах или аргументах.
502	Command not implemented - нелегальная команда.
503	Bad sequence of commands - неудачная последовательность команд.
504	Command parameter not implemented - ошибка в параметрах команды.
550	Requested action not taken: mailbox unavailable - Запрошенная операция не выполнена [Напр., почтовый ящик не найден или доступ к нему невозможен].
551	User not local; please try <forward-path> - адресат не местный, рекомендуется переадресовать сообщение по адресу <forward-path>.
552	Requested mail action aborted: exceeded storage allocation - операция прервана из-за превышения лимитов памяти (слишком много адресатов или слишком длинное сообщение).
553	Requested action not taken: mailbox name not allowed - операция не выполнена [Например, ошибка в записи адреса почтового ящика].
554	Transaction failed - процедура не выполнена.

2.2. POP.

Post Office Protocol Version 3 - протокол почтового отделения, версия 3 - это сетевой протокол, используемый почтовым клиентом для получения сообщений электронной почты с сервера. Обычно используется в паре с протоколом SMTP.

Предыдущие версии протокола (POP, POP2) устарели. Альтернативным протоколом для сбора сообщений с почтового сервера является IMAP.

По умолчанию использует TCP-порт 110. Существуют реализации POP3-серверов, поддерживающие TLS и SSL.



После установки соединения протокол POP3 проходит три последовательных состояния

Авторизация - клиент проходит процедуру аутентификации

Транзакция - клиент получает информацию о состоянии почтового ящика, принимает и удаляет почту.

Обновление - сервер удаляет выбранные письма и закрывает соединение.

Не смотря на то, что протокол POP3 действительно поддерживает возможность получения одного или нескольких писем и оставления их на сервере, большинство программ обработки электронной почты просто скачивают все письма и опустошают почтовый ящик на сервере.

Пример сессии

```
S: <Сервер ожидает входящих соединений на порту 110>
C: <подключается к серверу>
S:   +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:   APOP mrose c4c9334bac560ecc979e58001b3e22fb
S:   +OK mrose's maildrop has 2 messages (320 octets)
C:   STAT
S:   +OK 2 320
C:   LIST
S:   +OK 2 messages (320 octets)
S:   1 120
```

```
S:   2 200
S:   .
C:   RETR 1
S:   +OK 120 octets
S:   <сервер передает сообщение 1>
S:   .
C:   DELE 1
S:   +OK message 1 deleted
C:   RETR 2
S:   +OK 200 octets
S:   <сервер передает сообщение 2>
S:   .
C:   DELE 2
S:   +OK message 2 deleted
C:   QUIT
S:   +OK dewey POP3 server signing off (maildrop empty)
C:  <закрывает соединение>
S:  <продолждает ждать входящие соединения>
```

2.3. IMAP.

Пользователю, имеющему одну учетную запись у одного провайдера и всегда соединяющегося с провайдером с одной и той же машины, вполне достаточно протокола POP3. Этот протокол используется повсеместно благодаря его простоте и надежности. Но у многих пользователей есть одна учетная запись в учебном заведении или на работе, но они хотят иметь к ней доступ и из дома, и с места работы (учебы), и во время командировки те из разных мест. Хотя протокол POP3 и позволяет разрешить такую ситуацию. Но проблема в том что при таком использовании электронной почты вся корреспонденция пользователя очень быстро распространится по случайным машинам, с которых он получал доступ в Интернет, и некоторые из этих компьютеров могут вообще не принадлежать пользователь.

Это неудобство привело к созданию альтернативного протокола для получения почты, IMAP.

IMAP (англ. Internet Message Access Protocol) - интернет-протокол прикладного уровня для доступа к электронной почте.

IMAP предоставляет пользователю богатые возможности для работы с почтовыми ящиками, находящимися на центральном сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без необходимости постоянной пересылки с сервера и обратно файлов с полным содержанием писем.

IMAP был разработан для замены более простого протокола POP3 и имеет следующие

преимущества по сравнению с последним:

- Письма хранятся на сервере, а не на клиенте. Возможен доступ к одному и тому же почтовому ящику с разных клиентов. Поддерживается также одновременный доступ нескольких клиентов. В протоколе есть механизмы с помощью которых клиент может быть проинформирован об изменениях, сделанных другими клиентами.
- Поддержка нескольких почтовых ящиков (или папок). Клиент может создавать, удалять и переименовывать почтовые ящики на сервере, а также перемещать письма из одного почтового ящика в другой.
- Возможно создание общих папок, к которым могут иметь доступ несколько пользователей.
- Информация о состоянии писем хранится на сервере и доступна всем клиентам. Письма могут быть помечены как прочитанные, важные и т. п.
- Поддержка поиска на сервере. Нет необходимости скачивать с сервера множество сообщений для того чтобы найти одно нужное.
- Поддержка онлайн-работы. Клиент может поддерживать с сервером постоянное соединение, при этом сервер в реальном времени информирует клиента об изменениях в почтовых ящиках, в том числе о новых письмах.
- Предусмотрен механизм расширения возможностей протокола.

Текущая версия протокола имеет обозначение IMAP4rev1 (IMAP, версия 4, ревизия 1). Протокол поддерживает передачу пароля пользователя в зашифрованном виде. Кроме того, IMAP-трафик можно зашифровать с помощью SSL.

3. Наиболее известные WEB-клиенты работы с почтой.

Eudora Mail - клиент электронной почты, который появился еще на заре Интернета, когда электронная почта была чуть ли не единственным средством общения.

Evolution - графическая клиентская программа управления электронной почтой, контактами и временем для платформы Linux. Разработана и поддерживается фирмой Novell. Содержит календарь, систему планирования временем, адресную книги, поддерживает все распространенные почтовые протоколы IMAP, POP, SMTP.

Fidolook - клиент электронной почты, который является встраиваемым дополнением к Outlook Express из состава пакета Internet Explorer. Существенно расширяет такие возможности Outlook Express, как цитирование сообщений, шаблоны сообщений, настройка заголовков сообщения, возможности работы с папками новостей, импорт и экспорт сообщений.

Foxmail! - бесплатная программа для работы с электронной почтой для ОС Windows. Разрабатывается китайской корпорацией TenCent. Поддерживает протоколы SMTP, POP3 и RSS. Основные возможности:

- отправка писем без участия SMTP-сервера (компьютер пользователя выступает в роли SMTP-сервера);
- возможность установки пароля на аккаунт;
- настройка приёма почты с нескольких E-mail адресов в один аккаунт;
- сортировщик писем на основе фильтров;

- создание и редактирование шаблонов новых писем;
- работа с диспетчером писем (управление сообщениями на сервере);
- возможность шифрования сообщений;
- удобная адресная книга, интегрированная в интерфейс;
- RSS-агрегатор .

KMail - клиент электронной почты, распространённый в операционных системах семейства *nix. Поддерживает SMTP, POP3, IMAP, локальные почтовые ящики, а также существует поддержка, антивирусов, антиспама, пользовательских фильтров.

M2 - внутреннее название почтового и новостного клиента, встроенного в браузер Opera и официально называемого Opera Mail. Его интерфейс отличается от остальных почтовых клиентов с целью обеспечения лучшей интеграции с Opera, а также имеется фильтр спама, поддержка POP3 и IMAP, новостных групп, RSS и Atom новостных лент.

MailMan - почтовый клиент для мобильных устройств и телефонов, является java приложением. Основные возможности:

- работа с файловой системой (сохранение, добавление вложений файлов любых форматов, работа с адресной книгой, сохранение истории загрузок на диск в .txt, проигрывание заданной мелодии);
- возможность работы с кодировками и транслитом;
- просмотр html, wml, pda и xml-подобных страниц в виде текста без ссылок и изображений с возможностью настройки шрифта;

- огромное количество параметров и гибкая настройка;
- программа распространяется бесплатно.

Microsoft Outlook - компьютерная программа-органайзер с функциями почтового клиента, входящая в пакет офисных программ Microsoft Office. Основные возможности:

- является полноценным Органайзером, предоставляющим функции календаря, планировщика задач, записной книжки и менеджера контактов;
- позволяет отслеживать работу с документами пакета Microsoft Office для автоматического составления дневника работы;
- может использоваться как отдельное приложение, так и выступать в роли клиента для почтового сервера Microsoft Exchange Server, что предоставляет дополнительные функции для совместной работы пользователей одной организации: общие почтовые ящики, папки задач, календари, конференции, планирование и резервирование времени общих встреч, согласование документов.

Mozilla Thunderbird - бесплатная, свободно распространяемая программа для работы с электронной почтой и группами новостей. Является составной частью проекта Mozilla. Поддерживает протоколы SMTP, POP3, IMAP, NNTP, RSS, работает в Windows, Mac OS X и Linux, причём набор возможностей и расположение элементов управления на всех платформах одинаковые.

Outlook Express - программа для работы с электронной почтой и группами новостей, которая поставляется в составе ОС Windows, начиная с Windows 95 OSR 2.5, а также вместе с браузером Internet Explorer, начиная с версии 4.0. Новая версия Outlook Express, включенная в

состав Windows Vista вместе с Internet Explorer 7.0, носит название Windows Mail. Название Outlook Express предполагает, что эта программа является "облегчённой" версией Microsoft Outlook и, в отличие от Outlook Express, не имеет функций для работы с группами новостей.

The Bat! - условно-бесплатная программа для работы с электронной почтой для ОС Windows. Разрабатывается молдавской компаниией RitLabs. Поддерживает протоколы SMTP, POP3, IMAP, имеет довольно развитую систему фильтрации сообщений и поддерживает большое количество кириллических кодировок. Существуют две версии программы: Home и Professional. В версии Professional имеется возможность проверки орфографии, шифрации сообщений и биометрической аутентификации.

4. Настройки безопасности в почтовых системах: TLS, SSL, цифровая подпись, сертификат. Понятие СПАМ.

4.1. TLS.

TLS (англ. Transport Layer Security) — криптографический протокол, обеспечивающий безопасную передачу данных между пользователями в сети Интернет.

TLS-протокол основан на Netscape SSL-протоколе версии 3.0 и состоит из двух частей — TLS Record Protocol и TLS Handshake Protocol. Различие между SSL 3.0 и TLS 1.0 незначительные, поэтому далее в тексте термин «SSL» будет относиться к ним обоим.Большинство современных браузеров поддерживает данный протокол.TLS Working Group, основанная в 1996 году, продолжает работать над протоколом.

4.2. SSL.

SSL, используя криптографию, предоставляет возможности аутентификации и безопасной передачи данных через Интернет. Часто происходит лишь аутентификация сервера, в то время как клиент остается неаутентифицированным. Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытого ключа (PKI), которая позволяет защитить клиент-серверные приложения от перехвата сообщений, редактирования существующих сообщений и создания поддельных.

SSL включает в себя три основных фазы:

Диалог между сторонами, целью которого является выбор алгоритма шифрования

Обмен ключами на основе криптосистем с открытым ключом или аутентификация на основе сертификатов.

Передача данных, шифруемых при помощи симметричных алгоритмов шифрования

В первой фазе клиент и сервер обсуждают выбор криптографического алгоритма для дальнейшего использования. В данной версии протокола доступны следующие алгоритмы:

Для обмена ключами и проверки их подлинности применяются комбинации алгоритмов: RSA (асимметричный шифр), Diffie-Hellman (безопасный обмен ключами), DSA (алгоритм цифровой подписи) и алгоритмы технологии Fortezza.

Для симметричного шифрования: RC2, RC4, IDEA, DES, Triple DES или AES;

Для хэш-функций: MD5 или SHA.

SSL (англ. Secure Sockets Layer — протокол защищённых сокетов) — криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создаётся защищённое соединение между клиентом и сервером. SSL изначально разработан компанией Netscape Communications, в настоящее время принят IETF как стандарт. Поддерживается всеми популярными браузерами.

Использует шифрование с открытым ключом для подтверждения подлинности передатчика и

получателя. Поддерживает надёжность передачи данных за счёт использования корректирующих кодов и безопасных хэш-функций.

SSL состоит из двух уровней. На нижнем уровне многоуровневого транспортного протокола (например, TCP) он является протоколом записи и используется для инкапсуляции (то есть формирования пакета) различных протоколов. Для каждого инкапсулированного протокола он обеспечивает условия, при которых сервер и клиент могут подтверждать друг другу свою подлинность, выполнять алгоритмы шифрования и производить обмен криптографическими ключами, прежде чем протокол прикладной программы начнёт передавать и получать данные.

Для доступа к страницам, защищённым протоколом SSL, в URL вместо обычного префикса (schema) http, как правило, применяется префикс https (порт 443), указывающий на то, что будет использоваться SSL соединение. Так как операции шифрования / расшифрования требуют много вычислительных ресурсов, чтобы снизить нагрузку на веб-серверы, используют аппаратные SSL-ускорители.

Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат.

4.3. Цифровая подпись.

Электронная цифровая подпись (ЭЦП)— реквизит электронного документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от подделки.

Цифровая подпись обеспечивает:

Удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно, подпись станет недействительной.

Невозможность отказа от авторства. Так как создать корректную подпись можно лишь, зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Возможны следующие угрозы цифровой подписи:

Злоумышленник может попытаться подделать подпись для выбранного им документа.

Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила.

Злоумышленник может попытаться подделать подпись для хоть какого-нибудь документа.

При использовании надёжной хэш-функции, вычислительно сложно создать поддельный документ с таким же хэшем, как у подлинного. Однако, эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях.

Тем не менее, возможны ещё такие угрозы системам цифровой подписи:

Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа.

Злоумышленник может обманом заставить владельца подписать какой-либо документ, например используя протокол слепой подписи.

Злоумышленник может подменить открытый ключ владельца (см. управление ключами) на свой собственный, выдавая себя за него.

4.4. Сертификат.

Сертификат (сертификат открытого ключа, сертификат ЭЦП) — цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Содержит информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д.

Открытый ключ может быть использован для организации защищённого канала связи с владельцем двумя способами:

- для проверки подписи владельца (аутентификация)
- для шифрования посылаемых ему данных (конфиденциальность)

Существует две модели организации инфраструктуры сертификатов: централизованная (PKI) и децентрализованная (PGP). В централизованной модели существуют корневые центры сертификации, подписи которых обязан доверять каждый пользователь. В децентрализованной модели каждый пользователь самостоятельно выбирает, каким сертификатам он доверяет и в какой степени.

4.5. Спам.

Спам (англ. spam) — сообщения, массово рассылаемые людям, не выразившим желание их получать. В первую очередь термин «спам» относится к электронным письмам.

Способы борьбы со спамом

Превентивные методы Самый надёжный способ борьбы со спамом — не позволить спамерам узнать электронный адрес. Это трудная задача, но некоторые меры предосторожности можно предпринять.

К сожалению, даже такие суровые меры не дают полной гарантии того, что спамер не узнает электронный адрес. Методы сбора адресов включают использование вирусов с целью охоты за контакт-листами пользователей. Вирусы эксплуатируют изъяны в известных почтовых программах и отправляют адреса из контакт-листа злоумышленнику или самостоятельно отправляют по этим адресам копии нежелательных писем.

Автоматическая фильтрация Существует программное обеспечение (ПО) для автоматического определения спама (т. н. фильтры). Оно может быть предназначено для

конечных пользователей или для использования на серверах. Это ПО использует два основных подхода.

Первый заключается в том, что анализируется содержание письма и делается вывод, спам это или нет. Если письмо классифицировано как спам, оно может быть помечено, перемещено в другую папку или даже удалено. Такое ПО может работать как на сервере, так и на компьютере клиента. При таком подходе вы не видите отфильтрованного спама, но продолжаете полностью или частично нести издержки, связанные с его приемом, так как антиспамное ПО в любом случае получает каждое спамерское письмо (затрачивая ваши деньги), а только потом решает, показывать его или нет. С другой стороны, если ПО работает на сервере, вы не несёте издержек по копированию его на свой компьютер.

Второй подход заключается в том, чтобы, применяя различные методы, опознать отправителя как спамера, не заглядывая в текст письма. Это ПО может работать только на сервере, который непосредственно принимает письма. При таком подходе можно уменьшить издержки — деньги затрачиваются только на общение со спамерскими почтовыми программами (т. е. на отказы принимать письма) и обращения к другим серверам (если таковые нужны) при проверке. Выигрыш, однако, не такой большой, как можно было бы ожидать. Если получатель отказывается принять письмо, спамерская программа пытается обойти защиту и отправить его другим способом. Каждую такую попытку приходиться отражать отдельно, что увеличивает нагрузку на сервер.

Методы автоматической фильтрации

Программы автоматической фильтрации используют статистический анализ содержания

письма для принятия решения, является ли оно спамом. Наибольшего успеха удалось достичь с помощью алгоритмов, основанных на теореме Байеса. Для работы этих методов требуется «обучение» фильтров, т. е. нужно использовать рассортированные вручную письма для выявления статистических особенностей нормальных писем и спама.

Неавтоматическая фильтрация Многие программы и почтовые сервисы в Паутине позволяют пользователю задавать собственные фильтры. Такие фильтры могут состоять из слов или, реже, регулярных выражений, в зависимости от наличия или отсутствия которых сообщение попадает или не попадает в мусорный ящик. Однако такая фильтрация трудоёмкая и негибкая, кроме того, требует от пользователя известной степени знакомства с компьютерами. С другой стороны, она позволяет эффективно отсеять часть спама, и пользователь точно знает, какие сообщения будут отсеяны и почему.

Черные списки В черные списки заносятся IP-адреса компьютеров, о которых известно, что с них ведется рассылка спама. Также широко используются списки компьютеров, которые можно использовать для рассылки — «открытые релеи» и «открытые прокси», а также — списки «диалапов» — клиентских адресов, на которых не может быть почтовых серверов. Можно использовать локальный список или список, поддерживаемый кем-то еще. Благодаря простоте реализации, широкое распространение получили черные списки, запрос к которым осуществляется через службу DNS. Они получили название DNSBL (DNS Black List). В настоящее время этот метод не очень эффективен. Спамеры находят новые компьютеры для своих целей быстрее, чем их успевают заносить в черные списки. Кроме того, несколько компьютеров, отправляющих спам, могут скомпрометировать весь почтовый домен или подсеть, и тысячи законопослушных пользователей на неопределённое время будут лишены возможности отправлять почту серверам, использующим такой чёрный список.

Авторизация почтовых серверов Были предложены различные способы для подтверждения того, что компьютер, отправляющий письмо, действительно имеет на это право (Sender ID, SPF, Caller ID, Yahoo DomainKeys, MessageLevel[1]), но они пока не получили широкого распространения. Кроме того, эти технологии ограничивают некоторые распространённые виды функциональности почтовых серверов: становится невозможно автоматически перенаправлять корреспонденцию с одного почтового сервера на другой (SMTP Forwarding).

Среди провайдеров распространена политика, согласно которой клиентам разрешается устанавливать SMTP-соединения только с серверами провайдера. В этом случае становится невозможно использовать некоторые из механизмов авторизации.

Серые списки Метод серых списков основан на том, что «поведение» программного обеспечения, предназначенного для рассылки спама отличается от поведения обычных почтовых серверов, а именно, спамерские программы не пытаются повторно отправить письмо при возникновении вре́менной ошибки, как того требует протокол SMTP. Точнее, пытаясь обойти защиту, при последующих попытках они используют другой релей, другой обратный адрес и т. п., поэтому это выглядят для принимающей стороны, как попытки отправки разных писем.