# Лабораторная работа Диалоговые протоколы

Практически все протоколы верхних уровней строятся на основе диалога: первая сторона отправляет запрос, вторая сторона отвечает на него. В ряде протоколов диалог может состоять из одного запроса и одного ответа (например, в протоколе HTTP), в других диалог может включать десятки запросов и ответов (например, FTP, POP3, SMTP).

## Протокол SMTP

Протокол SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты) отвечает за отправку почты другому адресату.

Сеанс работы протокола SMTP состоит из нескольких этапов: аутентификация, передача параметров письма (адреса, тема), отправка текста сообщения и завершение соединения.

Поскольку работа с почтой производится от имени конкретного пользователя, то первым этапом диалога идёт авторизация – клиент передаёт серверу имя пользователя и пароль. Протокол поддерживает безопасные методы аутентификации с применением SSL, рекомендуется по возможности использовать именно такую безопасную аутентификацию, поскольку в противном случае данные могут быть перехвачены третьими лицами. Если всё же используется нешифрованная аутентификация, то в протоколе SMTP предусмотрено кодирование имени пользователя и пароля кодировкой base64: это обеспечивает минимальную защиту, которая, впрочем, легко вскрывается.

К письму могут прилагаться двоичные файлы, но из-за того, что протокол предусматривает передачу только ASCII-информации, файлы должны быть закодированы в текстовый формат по стандарту MIME.

Основные команды протокола SMTP приведены в следующей таблице:

Табл. . Команды протокола SMTP

| Команда | Параметры | Описание |
| --- | --- | --- |
| HELO / EHLO | домен | Начало сессии. В качестве домена можно использовать localhost. |
| AUTH LOGIN |  | Аутентификация: сервер запросит логин и пароль, закодированные с помощью base64 |
| MAIL FROM: | e-mail отправителя | Адрес отправителя письма[[1]](#footnote-1) |
| RCPT TO: | e-mail получателя | Адрес получателя письма |
| DATA |  | После этой команды сервер все данные воспринимает как тело письма. Признаком окончания тела является строка с единственной точкой. |
| HELP | [команда] | Вывод справочной информации по указанной команде (если она указана) |
| QUIT |  | Завершение сеанса |

### Пример сеанса работы по протоколу SMTP

При подключении к серверу SMTP появляется приветствие:

220 smtp5.gmail.com ESMTP ready

Трёхзначный код, идущий в начале строки, содержит информацию от сервера об успешности операции или ошибки, и используется программами, работающими с почтой. Текст, идущий после кода, содержит ту же информацию в форме, понятной человеку.

Первой командой сеанса должна быть команда приветствия:

EHLO localhost

Команда EHLO (Extended Hello) в качестве параметра должна содержать доменное имя компьютера, с которого отправляется письмо. Если компьютер не имеет доменного имени, то допускается указывать в качестве параметра адрес отправителя. В ответ на команду EHLO сервер присылает список своих возможностей:

250-SIZE 73400320

250-8BITMIME

250-PIPELINING

250 AUTH PLAIN LOGIN XOAUTH2

Следующим шагом должна быть авторизация:

AUTH LOGIN

В ответ сервер присылает приглашение ввести логин:

334 VXNlcm5hbWU6

Поскольку логин ожидается в кодировке base64, то и приглашение тоже закодировано в этой же кодировке (если раскодировать строку после кода 334, то получится слово «Username:»). Нужно отправить логин и пароль:

334 VXNlcm5hbWU6

bG9naW4=

334 UGFzc3dvcmQ6

cGFzc3dvcmQ=

Если авторизация прошла успешно, сервер отвечает соответствующей строкой:

235 Authentication succeeded

На следующем шаге нужно ввести информацию об отправителе и получателе письма (в лабораторной работе письмо можно отправить на тот же адрес):

MAIL FROM: <user@gmail.com>

250 OK

RCPT TO: <user@gmail.com>[[2]](#footnote-2)

250 OK

Если указанные отправитель и получатель устраивают сервер, он отвечает кодом 250:

250 Accepted

После этого нужно отправить текст письма с помощью команды DATA. Признаком завершения письма является одиночная точка на новой строке:

DATA

354 Enter message, ending with "." on a line by itself

Это тестовое сообщение.

Оно состоит из двух строк.

.

250 OK id=1f6TMJ-0007v0-1V

В конце сеанса нужно ввести команду QUIT, которая закроет соединение:

QUIT

221 smtp3.gmail.com closing connection closed

Если сеанс прошёл успешно, то через несколько секунд письмо появится в почтовом ящике.

## Протокол POP3

Протокол POP3 (Post Office Protocol) предназначен для получения почты с почтового сервера на локальную машину.

Основные команды протокола POP3 приведены в следующей таблице:

Табл. . Команды протокола POP3

| Команда | Параметры | Описание |
| --- | --- | --- |
| USER | имя пользователя | Аутентификация пользователя |
| PASS | пароль | Пароль открытым текстом |
| STAT |  | Получение количества сообщений в ящике и их размер |
| LIST | [сообщение] | Получение информации обо всех сообщениях в ящике (или о конкретном сообщении, если оно указано) |
| DELE | сообщение | Удаление указанного сообщения |
| RETR | сообщение | Загрузка указанного сообщения |
| QUIT |  | Завершение сеанса |

### Пример сеанса работы по протоколу POP3

Сеанс работы по протоколу POP3 также строится по принципу диалога: пользователь отправляет команду серверу, а тот отвечает. Перед началом сеанса сервер присылает строку, обозначающую успешное начало работы:

+OK

Начинается сеанс с авторизации пользователя, логин и пароль не нужно кодировать:

USER mylogin

+OK

PASS mypassword

+OK Welcome!

С помощью команды STAT можно посмотреть общую статистику ящика:

STAT

+OK 2 3769

Этот ответ означает, что в ящике два письма, суммарный размер 3769 байт. Можно вывести список всех писем (он может быть очень большой):

LIST

+OK 2 messages (3769 octets)

1 1871

2 1898

Для каждого письма выводится его размер. Чтобы посмотреть письмо, используется команда RETR, в качестве параметра указывается номер нужного письма:

RETR 1

+OK 1871 octets

Delivered-To: mylogin@gmail.com

Return-path: <mylogin@gmail.com>

Received: by smtp3.gmail.com with esmtpa

Message-Id: <0007v0-1V.mylogin-gmail-com@smtp3.gmail.com>

From: mylogin@gmail.com

Date: Thu, 12 Apr 2018 06:57:17 +0300

Это тестовое сообщение.

Оно состоит из двух строк.

Как видно из этого листинга, команда RETR выводит также служебные заголовки письма.

Чтобы удалить сообщение, используется команда DELE:

DELE 1

+OK message 1 deleted

Для завершения сеанса нужно использовать команду QUIT:

QUIT

+OK POP3 server at gmail.com signing off

closed

## Используемые утилиты

Поскольку протоколы POP3 и SMTP основаны на текстовом диалоге между клиентом и сервером, допустимо использовать вместо специальной почтовой программы обычный клиент telnet или одну из совместимых с этим протоколом альтернативных программ. Для подключения к почтовому серверу нужно знать имя сервера и порт.

Имя почтового сервера может не совпадать с именем почтового адреса, например, для адреса user@gmail.com почтовый сервер для получения почты будет pop.gmail.com, а для отправки почты - smtp.gmail.com. Имена почтовых серверов для каждого домена обычно хранятся в записи типа MX на DNS-сервере (а при её отсутствии – используется адрес сервера из записи типа A), кроме того, их обычно можно получить в документации почтовой службы.

Стандартные номера портов для почтовых протоколов определены стандартами, однако, конкретные почтовые сервера могут их изменять, поэтому надежнее будет проверить номера портов в документации почтового сервера.

Табл. Стандартные номера портов

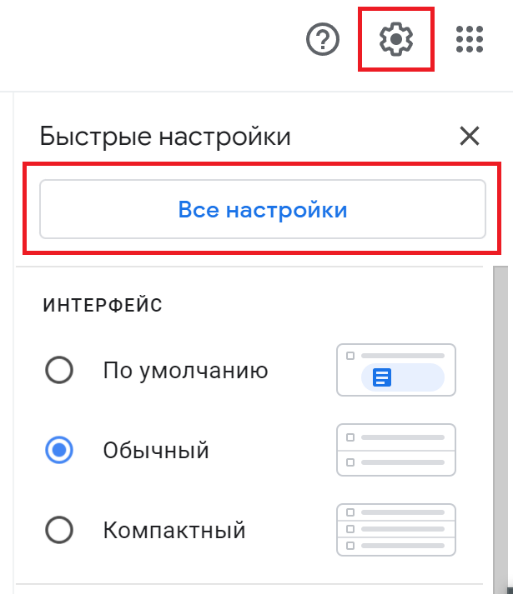
|  | Номер порта | |
| --- | --- | --- |
| Протокол | Без шифрования | С шифрованием |
| POP3 | 110 | 995 |
| IMAP | 143 | 993 |
| SMTP | 25 | 465 |

Для кодирования и раскодирования пароля в base64 для протокола SMTP можно использовать одну из подходящих утилит, или же один из онлайновых перекодировщиков.

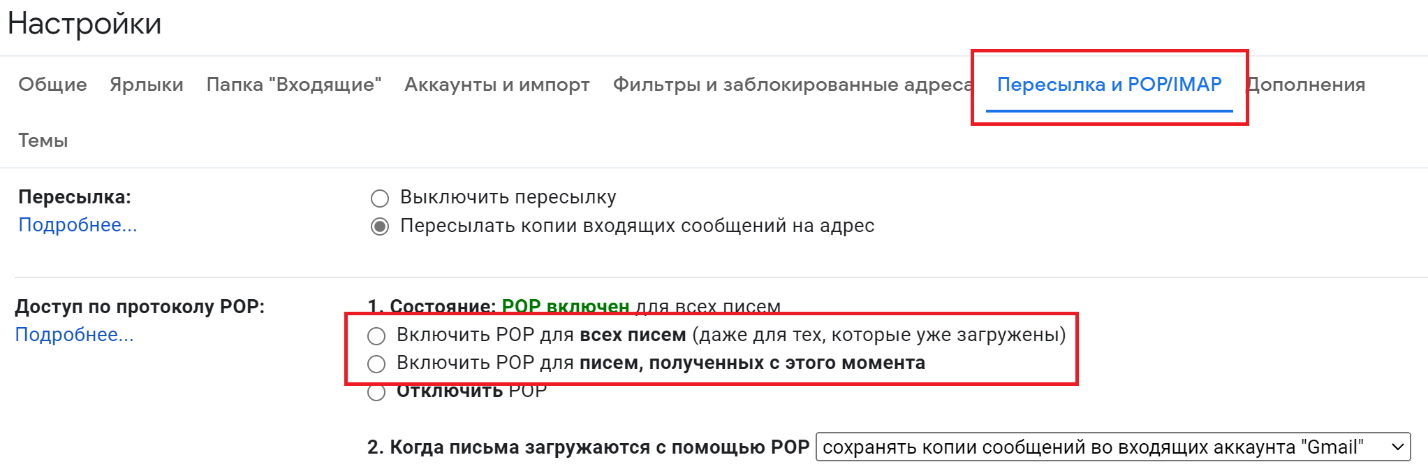
## Безопасность

Поскольку злоумышленники пытаются получить доступ к аккаунтам пользователя и использовать их для выполнения злонамеренных действий (например, рассылки спама), компании защищают доступ к аккаунтам. Поэтому для выполнения работы может потребоваться временно внести изменения в настройки почтового сервера.

При использовании почтового сервера Gmail нужно зайти в настройки (значок шестеренки в правом верхнем углу сайта, в появившемся меню нажать кнопку «Все настройки»):

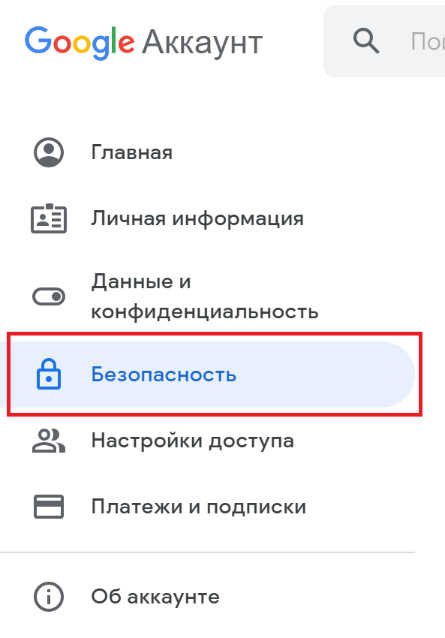


В настройках нужно перейти на вкладку «Пересылка и POP/IMAP», и включить протокол POP, выбрав одну из опций (для лабораторной работы подойдёт любая из них) и нажать кнопку «Сохранить» в нижней части страницы:

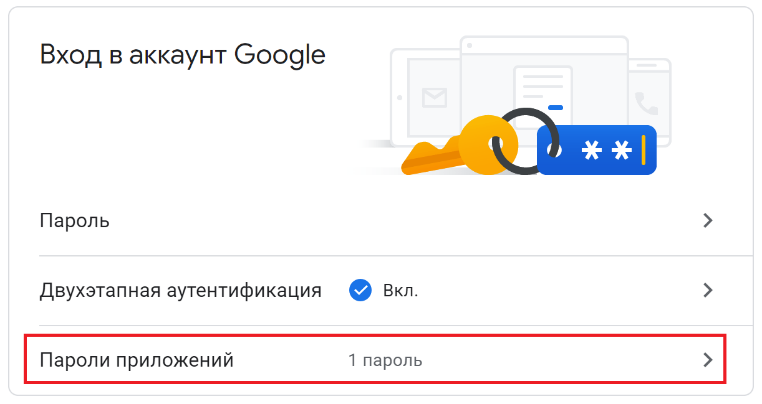


После выполнения лабораторной работы эту опцию можно снова отключить.

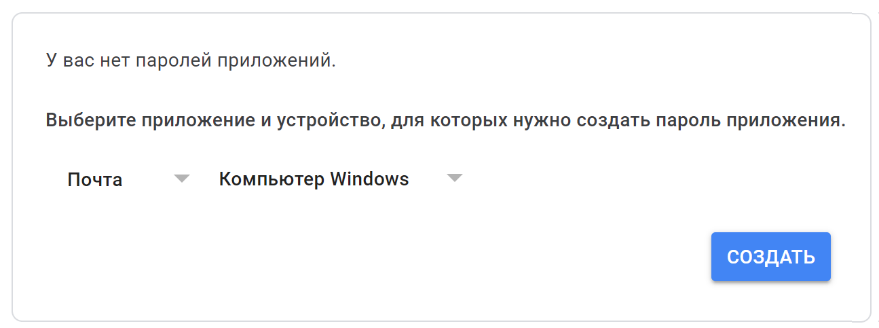
Вторая опция безопасности, которую требуется настроить – это двухфакторная авторизация. При включенной двухфакторной авторизации обычный пароль не подходит, потому что почтовые клиенты не могут запрашивать одноразовые коды. В этом случае нужно создать специальный пароль приложения. Для этого нужно зайти в аккаунт пользователя Google на сайте <https://myaccount.google.com> и выбрать там раздел «Безопасность»:



Далее в разделе «Вход в аккаунт Google» нужно открыть раздел «Пароли приложений»:



Здесь нужно создать пароль приложения для почты:



Система сгенерирует 16-символьный пароль приложения, который нужно сразу скопировать, поскольку повторно отобразить его нельзя:

Изображение выглядит как текст

Автоматически созданное описание

Этот пароль можно использовать для авторизации в протоколах SMTP (закодировав его с помощью base64) и POP3. Пробелы в пароле не нужны, они отображаются для удобства!

После выполнения лабораторной работы можно удалить созданный аккаунт приложения.

В других сервисах (Microsoft, Mail.ru и т.д.) также есть пароли приложений, которые можно создать при включенной двухфакторной авторизации.

## Задание

При выполнении лабораторной работы потребуется подключение к почтовому серверу. Допустимо использовать любой сервер, на котором имеется учетная запись и который поддерживает требуемые протоколы.

В связи с тем, что большинство бесплатных почтовых серверов в настоящее время требуют шифрованного соединения, рекомендуется использовать программу OpenSSL[[3]](#footnote-3), находящуюся в папке первой лабораторной работы. Запускать программу можно с помощью командного файла go.bat, содержащего параметры запуска программы OpenSSL. Перед использованием необходимо отредактировать файл go.bat, указав в нём сервер и порт используемой почтовой службы.

В отчёт следует вставить полные логи сеансов связи с каждым из серверов. Если использовалось подключение к реальной, а не специально созданной тестовой учетной записи, то в целях безопасности пароли из отчета нужно удалить, даже если он закодирован base64!

### Отправка письма

Используя SMTP-сервер, отправить письмо на свой адрес.

### Получение письма

Используя POP3-сервер получить количество писем в ящике, список писем с информацией о них, загрузить своё письмо, отправленное ранее через SMTP-сервер, удалить это письмо.

1. Некоторые почтовые сервера требуют заключать адрес в угловые скобки: <user@gmail.com>. Это же относится и к адресу получателя в команде RCPT TO. [↑](#footnote-ref-1)
2. Из-за ошибки в некоторых версиях программы OpenSSL заглавная буква R в начале строки воспринимается как команда повторной установки соединения. В этом случае рекомендуется набирать команду строчными буквами: rcpt to. [↑](#footnote-ref-2)
3. https://www.openssl.org/ [↑](#footnote-ref-3)