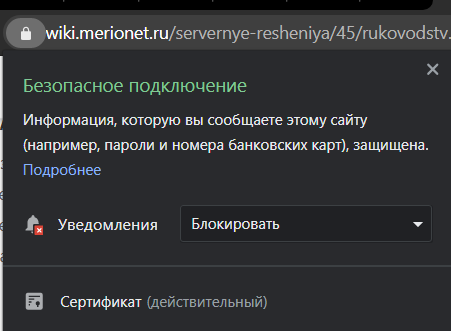
**Лабораторная работа 8. Сетевая безопасность**

***Сертификат Secure Socket Layer (SSL)*** - это протокол безопасности, который защищает данные между двумя компьютерами с использованием шифрования, т.е то файл данных, который в цифровом виде связывает криптографический ключ с сервером или доменом, а также с названием и местонахождением организации.

Если в браузере в адресной строке загорелся зеленый значок замка, а протокол соединения - это https, то это значит, что веб-сайт защищен с использованием шифрования SSL. Если щелкнуть информационную панель сайта, появится дополнительная информация о подключении, а также информация о самом сертификате SSL.



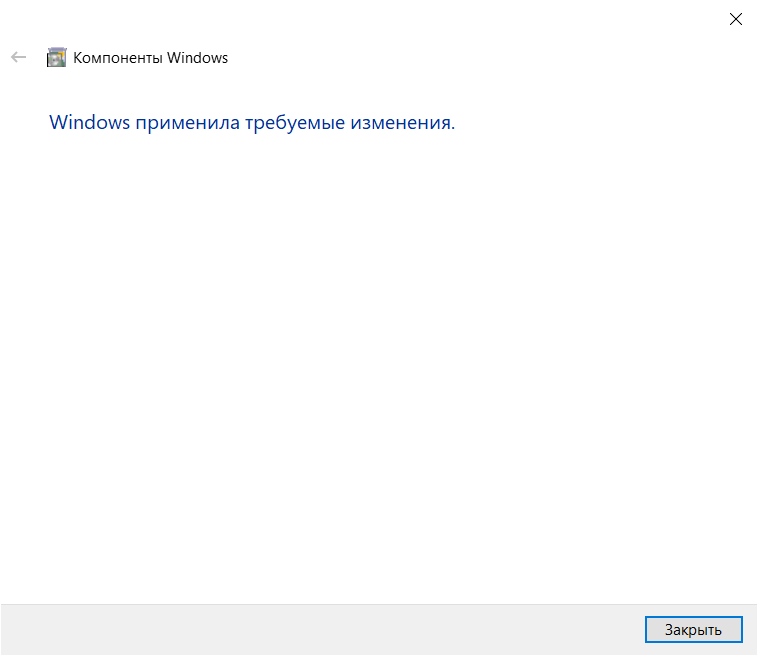
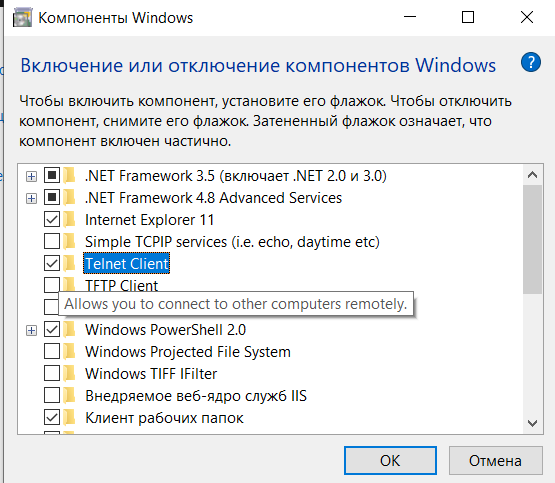
HTTPS представляет собой защищенный вариант HTTP протокола (hypertext transfer protocol – протокола передачи гипертекста), который первоначально использовался для передачи гипертекстовых документов. Со временем его стали применять и для передачи любых данных через Интернет. HTTP построен на принципе отношений «клиент- сервер»:

* клиент инициирует соединение, для чего посылает запрос серверу;
* сервер получает запрос, обрабатывает его и отправляет клиенту полученные результаты.

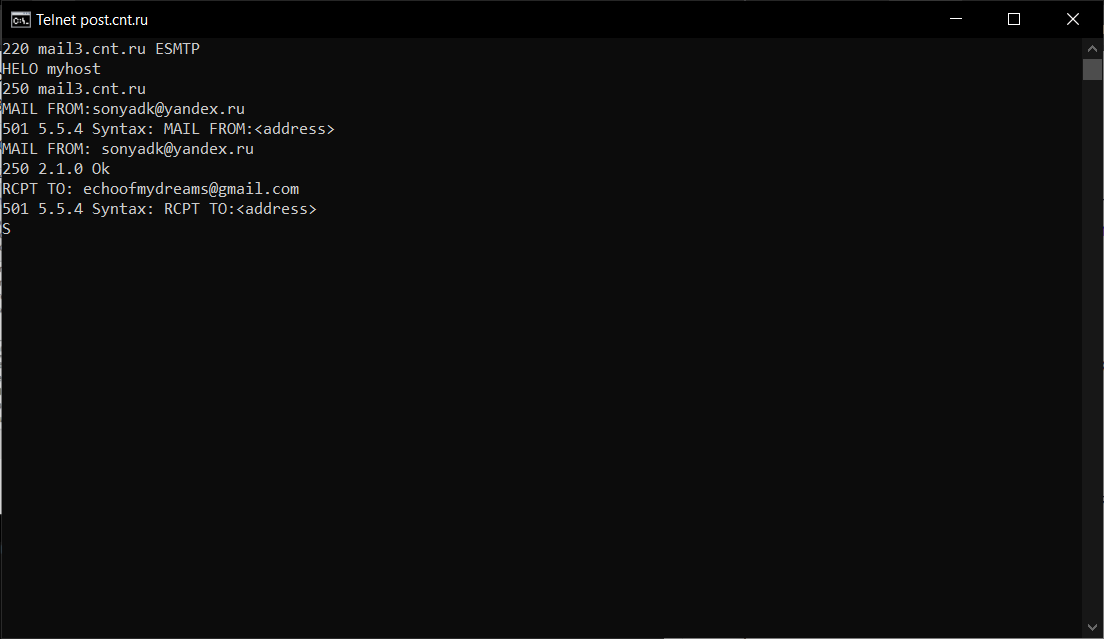
В HTTP данные передаются без шифрования, в открытом виде. На пути от клиента к серверу информация проходит через десятки и сотни узлов, и доступ к ней может получить кто угодно на любом этапе передачи. То же самое может случиться при подключении к Интернету через незащищенную сеть Wi-Fi в общественном месте – баре, клубе, на улице или в метро.

От постороннего доступа необходимо защищать банковские, коммерческие, юридические и любые персональные данные – паспортные, медицинские, налоговые, судебные и пр. В этих случаях для передачи конфиденциальной информации используется соединение HTTPS (HTTP Secure) – безопасная версия стандартного HTTP соединения. Оно подходит для любых устройств с выходом в Интернет – планшетов, мобильных телефонов, смартфонов, настольных ПК и ноутбуков. HTTPS не требует настроек со стороны пользователя – он автоматически начинает работать в нужный момент.

Включим для начала telnet клиент.



К сожалению дальше не удалось сделать задание из-за ошибков в доступе.



Дальше необходимо было использовать команду DATA

Сервер предложит ввести текст письма, выдав в ответ на DATA сообщение с номером 354:

*354 Please start mail input.*

Теперь можно вводить любой текст на английском языке:

*Hello,Me!*

*...*

*Good Bye!*

*.*

После ввода точки письмо будет принято к доставке получателю, о чем сервер сообщит кодом 250:

*250 Mail queued for delivery.*

Для завершения SMTP - сессии используется команда QUIT Письмо будет доставлено получателю, и в качестве адреса отправителя, в почтовом клиенте, будет отображаться введенная почта.

В связи с проблемой спама и несовершенством протокола SMTP, подавляющее большинство почтовых серверов настраивается таким образом, что обойтись 3-мя вышеупомянутыми командами наверняка не получится, что и не получилось сделать((