## Лабораторная работа 8. Сетевая безопасность

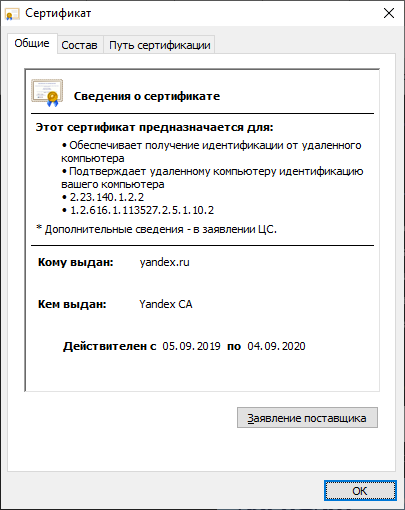
1. Продемонстрировать и объяснить поля цифрового сертификата на SSL-соединении

SSL (англ. Secure Sockets Layer — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

Проще говоря, это цифровая подпись сайта, которая нужна для работы протокола защищенной передачи данных в сети. Она обеспечивает шифрованное соединение между пользователем и сайтом. То есть информация, которой они обмениваются, защищена от посторонних — провайдера, оператора, администратора вайфай-сети и прочих. Еще с помощью этого сертификата подтверждается подлинность сайта — пользователь может проверить, какой компании на самом деле принадлежит ресурс.

Чтобы посмотреть данные о SSL-сертификате перейдём на сайт, адрес которого начинается с https://.

Рассмотрим SSL-сертификат сайта <https://www.yandex.ru>

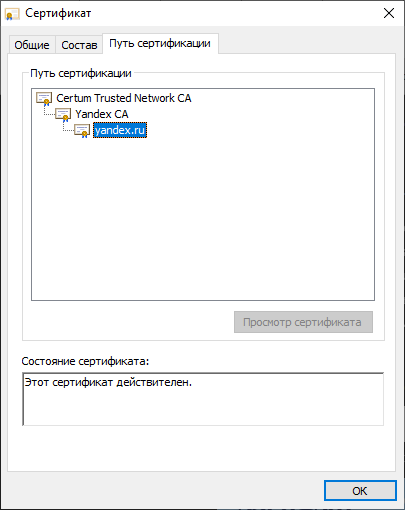


В данном случае он выдан:

* для идентификации удалённого компьютера (веб-сайта);
* для домена yandex.ru;
* центром сертификации Yandex CA;
* на срок с 05.09.2019 по 04.09.2020.

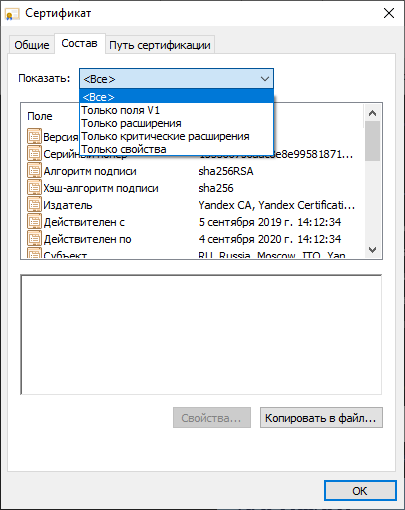
На вкладке «Путь сертификации» показано, кто и чей сертификат заверил.

Центров сертификации верхнего уровня существует много. Для взаимного подтверждения полномочий и удостоверения выданных сертификатов используются цепочки, одна из которых показана далее.



В данном случае SSL-сертификат для домена yandex.ru выдал центр сертификации Yandex CA и, соответственно, подписал его своей цифровой подписью. А сертификат Yandex CA подписал другой центр сертификации — Certrum Trusted Network CA.

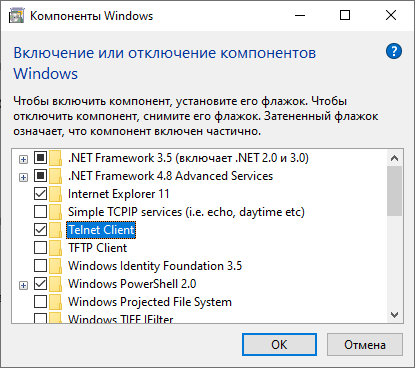
В вкладке “Состав” представлено много характеристик сертификата.

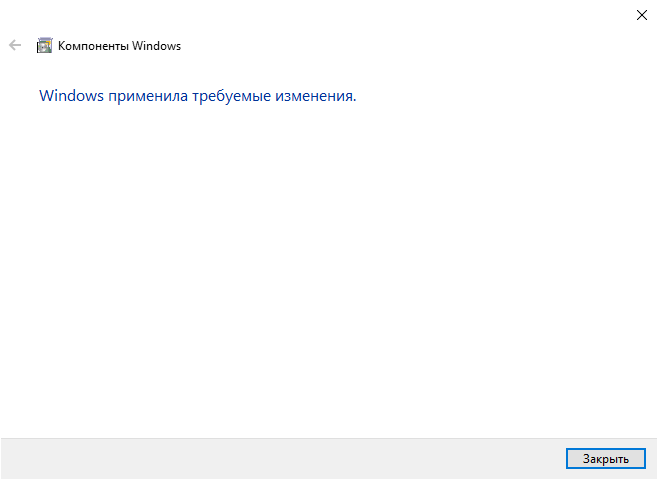


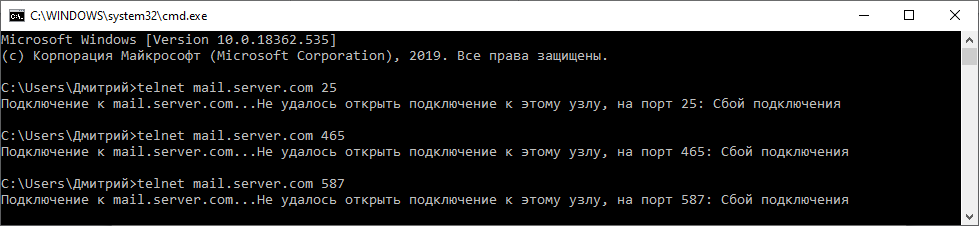
Для удобства просмотра их можно сгруппировать:

* поля V1 — это поля с базовой информацией о сертификате, соответствующей первой версии стандарта (X.509, version 1); эта группа полей поддерживается для обратной совместимости сертификатов с разными браузерами;
* расширения — поля, не входящие в группу полей V1;
* критические расширения — поля, ошибка в которых приведён к признанию SSL-сертификата недействительным;
* свойства — цифровая подпись сертификата и её алгоритм.

1. Продемонстрировать отправку сообщения по электронной почте через telnet
   1. Для начала убедимся, что telnet активирован в системе (в данном случае Windows 10)





* 1. 

Администраторы сервера выбирают, какой порт будут использовать клиенты для ретрансляции исходящей почты — 25 или 587. Спецификации и многие серверы поддерживают и тот, и другой порты. Хотя некоторые серверы поддерживают порт 465 для безопасного SMTP, но предпочтительнее использовать стандартные порты и ESMTP-команды, если необходима защищённая сессия между клиентом и сервером.

Некоторые серверы настроены на отклонение всех ретрансляций по порту 25, но пользователям, прошедшим аутентификацию по порту 587, позволено перенаправлять сообщения на любой действительный адрес.

Некоторые провайдеры перехватывают порт 25, перенаправляя трафик на свой собственный SMTP-сервер вне зависимости от адреса назначения. Таким образом, их пользователи не могут получить доступ к серверу за пределами провайдерской сети по порту 25.

* 1. Пример простейшей SMTP-сессии

C: — клиент, S: — серверa

S: (ожидает соединения)

C: (Подключается к порту 25 сервера)

S:220 mail.company.tld ESMTP is glad to see you!

C:HELO

S:250 domain name should be qualified

C:MAIL FROM: <someusername@somecompany.ru>

S:250 someusername@somecompany.ru sender accepted

C:RCPT TO: <user1@company.tld>

S:250 user1@company.tld ok

C:RCPT TO: <user2@company.tld>

S:550 user2@company.tld unknown user account

C:DATA

S:354 Enter mail, end with "." on a line by itself

C:From: Some User <someusername@somecompany.ru>

C:To: User1 <user1@company.tld>

C:Subject: tema

C:Content-Type: text/plain

C:

C:Hi!

C:.

S:250 769947 message accepted for delivery

C:QUIT

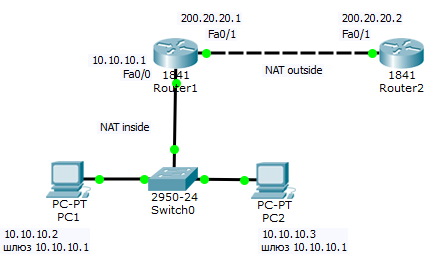
S:221 mail.company.tld CommuniGate Pro SMTP closing connection

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.

1. Настроить сетевую трансляцию адресов (SNAT) для общего доступа в интернет

[Статический NAT](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3) - сопоставляет один NAT inside (внутренний=частный локальный ip-адрес) с одним NAT outside (глобальным=публичным внешним ip-адресом). Здесь ISP (Internet Service Provider) - поставщик Интернет-услуг (Интернет-провайдер).



Алгоритм настройки R1

Ниже приведена последовательность команд конфигурирования маршрутизатора R1 по шагам.

Шаг 1. Настройка дефолта на R1

R1(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.2

Шаг 2. Настройка внутреннего интерфейса в отношение NAT

R1(config)# interface fastethernet 0/0

R1(config-if)# ip nat inside

Шаг 3. Настройка внешнего интерфейса в отношение NAT

R1(config)# interface fastethernet 0/1

R1(config-if)# ip nat outside

Шаг 4. Настройка сопоставления ip-адресов.

R1(config)# ip nat inside source static 10.10.10.2 200.10.21.5

В результате этой команды ip-адресу 200.10.21.5 всегда будет соответствовать внутренний ip-адрес 10.10.10.2, т.е. если мы будем обращаться к адресу 200.10.21.5 то отвечать будет PC1.