

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ  
НАРОДОВ**

**Факультет физико-математических и естественных  
наук**

**Кафедра теории вероятностей и кибербезопасности**

**Отчет лабораторной работы 5**

**Дисциплина: Администрирование сетевых подсистем**

Студент: Астахова Марина

Группа: НПИбд-02-23

# **Тема: Расширенная настройка HTTP-сервера Apache**

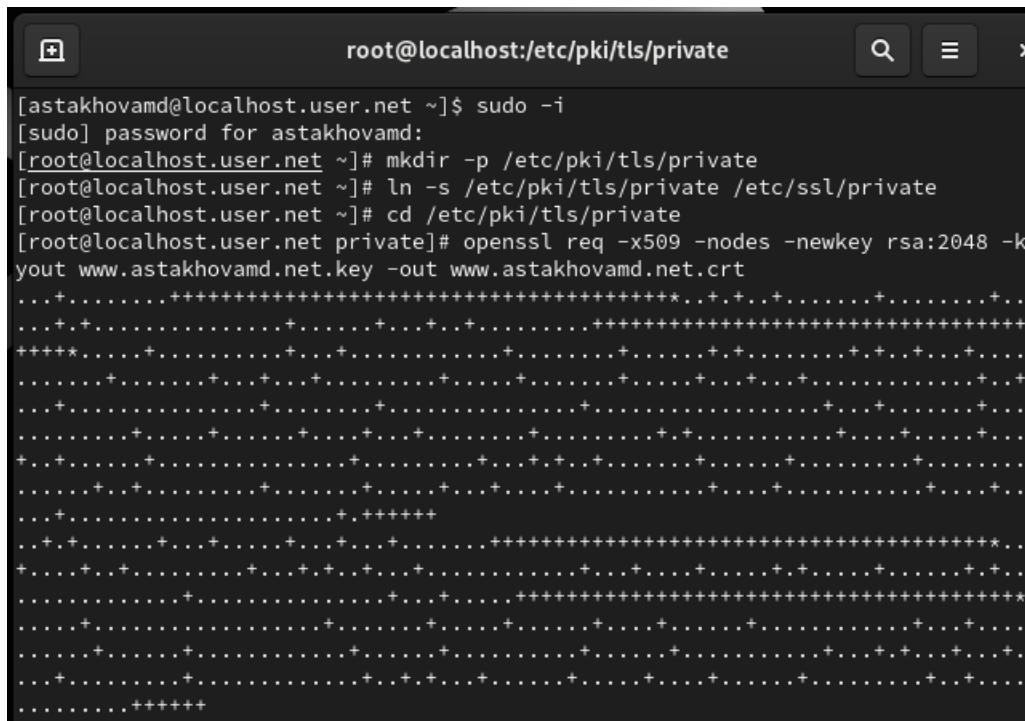
## **5.1. Цель работы.**

Приобретение практических навыков по расширенному конфигурированию HTTP сервера Apache в части безопасности и возможности использования PHP.

## **5.2. Выполнение работы**

**1. Сгенерируйте криптографический ключ самоподписанный сертификат безопасности для возможности перехода веб-сервера от работы через протокол HTTP к работе через протокол HTTPS. Конфигурирование HTTP-сервера для работы через протокол HTTPS.**

В каталоге /etc/ssl создали каталог private и сгенерировали ключ:



The screenshot shows a terminal window titled "root@localhost:/etc/pki/tls/private". The terminal session is as follows:

```
[astakhovamd@localhost.user.net ~]$ sudo -i  
[sudo] password for astakhovamd:  
[root@localhost.user.net ~]# mkdir -p /etc/pki/tls/private  
[root@localhost.user.net ~]# ln -s /etc/pki/tls/private /etc/ssl/private  
[root@localhost.user.net ~]# cd /etc/pki/tls/private  
[root@localhost.user.net private]# openssl req -x509 -nodes -newkey rsa:2048 -keyout www.astakhovamd.net.key -out www.astakhovamd.net.crt
```

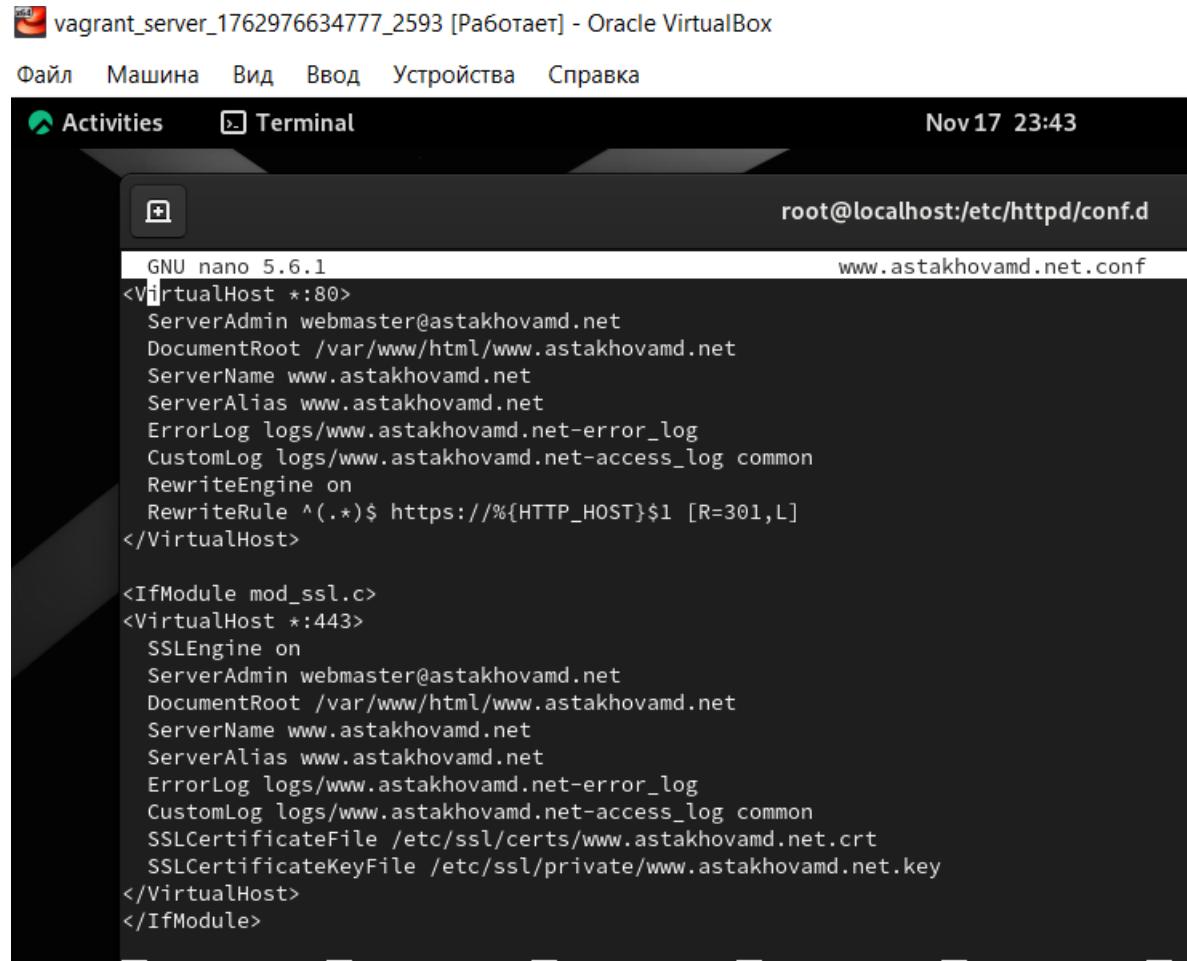
The terminal then displays a large block of generated RSA key data, consisting of a grid of '+' and '.' characters.

Подготовка ключа

```
----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
----  
Country Name (2 letter code) [XX]:RU  
State or Province Name (full name) []:Russia  
Locality Name (eg, city) [Default City]:Moscow  
Organization Name (eg, company) [Default Company Ltd]:astakhovamd  
Organizational Unit Name (eg, section) []:astakhovamd  
Common Name (eg, your name or your server's hostname) []:astakhovamd.net  
Email Address []:astakhovamd@astakhovamd.net  
[root@localhost.user.net private]# mv www.astakhovamd.net.crt /etc/pki/tls/certs  
[root@localhost.user.net private]# cp /etc/ssl/private/www.astakhovamd.net.crt /etc/ssl/cert/  
cp: cannot stat '/etc/ssl/private/www.astakhovamd.net.crt': No such file or directory  
[root@localhost.user.net private]#
```

Открыли на редактирование файл

/etc/httpd/conf.d/www.astakhovamd.net.conf и заменили его содержимое на следующее



vagrant\_server\_1762976634777\_2593 [Работает] - Oracle VirtualBox

Файл Машина Вид Ввод Устройства Справка

Activities Terminal Nov 17 23:43

```
root@localhost:/etc/httpd/conf.d  
www.astakhovamd.net.conf  
GNU nano 5.6.1  
<VirtualHost *:80>  
    ServerAdmin webmaster@astakhovamd.net  
    DocumentRoot /var/www/html/www.astakhovamd.net  
    ServerName www.astakhovamd.net  
    ServerAlias www.astakhovamd.net  
    ErrorLog logs/www.astakhovamd.net-error_log  
    CustomLog logs/www.astakhovamd.net-access_log common  
    RewriteEngine on  
    RewriteRule ^(.*)$ https:// %{HTTP_HOST} $1 [R=301,L]  
</VirtualHost>  
  
<IfModule mod_ssl.c>  
<VirtualHost *:443>  
    SSLEngine on  
    ServerAdmin webmaster@astakhovamd.net  
    DocumentRoot /var/www/html/www.astakhovamd.net  
    ServerName www.astakhovamd.net  
    ServerAlias www.astakhovamd.net  
    ErrorLog logs/www.astakhovamd.net-error_log  
    CustomLog logs/www.astakhovamd.net-access_log common  
    SSLCertificateFile /etc/ssl/certs/www.astakhovamd.net.crt  
    SSLCertificateKeyFile /etc/ssl/private/www.astakhovamd.net.key  
</VirtualHost>  
</IfModule>
```

Внесли изменения в настройки межсетевого экрана на сервере, разрешив работу с https:

```
[root@localhost.user.net conf.d]# sudo nano www.astakhovam.net.conf
[root@localhost.user.net conf.d]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http ssh
[root@localhost.user.net conf.d]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-client
bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ce
ph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcpc
dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server f
inger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-replication freeipa-trust ftp galera ganglia-client gangl
ia-master git gpgsql grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target
isns jenkins kadmin kdeconnect kerberos kibana klogind kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-contro
l-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure
kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios
-nx netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole ple
x pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv p
tp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rooht rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-
client samba-dc sane sip sipsl slp smtp smtp-submission smtptsm snmp snmpfsls snmptrap spotify-sync squid ssdp ssh steam-streaming
svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile3
8 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-clie
r zerotier
[root@localhost.user.net conf.d]# firewall-cmd --add-service=https
success
[root@localhost.user.net conf.d]# firewall-cmd --add-service=https --permanent
success
[root@localhost.user.net conf.d]# firewall-cmd --reload
success
```

```
rver zerotier
[root@localhost.user.net conf.d]# firewall-cmd --add-service=https
success
[root@localhost.user.net conf.d]# firewall-cmd --add-service=https --permanent
success
[root@localhost.user.net conf.d]# firewall-cmd --reload
success
[root@localhost.user.net conf.d]# systemctl restart httpd
```

## **2. Настроим веб-сервер для работы с PHP. Конфигурирование HTTP-сервера для работы с PHP.**

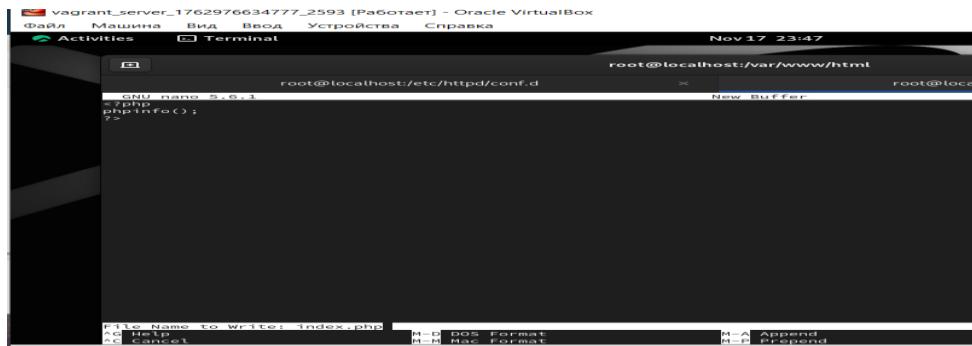
Установили пакеты для работы с PHP:

```
[astakhovam@localhost user.net ~]$ sudo -i
[sudo] password for astakhovam:
[root@localhost user.net ~]# dnf -y install php
Last metadata expiration check: 2:01:27 ago on Mon 17 Nov 2025 09:44:16 PM UTC.
Dependencies resolved.
=====


| Package                                              | Architecture | Version             | Repository        | Size  |
|------------------------------------------------------|--------------|---------------------|-------------------|-------|
| <hr/>                                                |              |                     |                   |       |
| Installing:                                          |              |                     |                   |       |
| php                                                  | x86_64       | 8.0.30-3.el9_6      | appstream         | 8.2 k |
| Installing dependencies:                             |              |                     |                   |       |
| nginx-filesystem                                     | noarch       | 2:1.20.1-22.el9_6.3 | appstream         | 9.6 k |
| php-common                                           | x86_64       | 8.0.30-3.el9_6      | appstream         | 666 k |
| Installing weak dependencies:                        |              |                     |                   |       |
| php-cli                                              | x86_64       | 8.0.30-3.el9_6      | appstream         | 3.1 M |
| php-fpm                                              | x86_64       | 8.0.30-3.el9_6      | appstream         | 1.6 M |
| php-mbstring                                         | x86_64       | 8.0.30-3.el9_6      | appstream         | 466 k |
| php-opcache                                          | x86_64       | 8.0.30-3.el9_6      | appstream         | 510 k |
| php-pdo                                              | x86_64       | 8.0.30-3.el9_6      | appstream         | 81 k  |
| php-xml                                              | x86_64       | 8.0.30-3.el9_6      | appstream         | 132 k |
| <hr/>                                                |              |                     |                   |       |
| Transaction Summary                                  |              |                     |                   |       |
| <hr/>                                                |              |                     |                   |       |
| Install 9 Packages                                   |              |                     |                   |       |
| <hr/>                                                |              |                     |                   |       |
| Total download size: 6.5 M                           |              |                     |                   |       |
| Installed size: 35 M                                 |              |                     |                   |       |
| Downloading Packages:                                |              |                     |                   |       |
| (1/9): php-xml-8.0.30-3.el9_6.x86_64.rpm             |              |                     | 25 kB/s   132 kB  | 00:05 |
| (2/9): php-opcache-8.0.30-3.el9_6.x86_64.rpm         |              |                     | 91 kB/s   510 kB  | 00:05 |
| (3/9): nginx-filesystem-1.20.1-22.el9_6.3.noarch.rpm |              |                     | 249 kB/s   9.6 kB | 00:00 |
| (4/9): php-common-8.0.30-3.el9_6.x86_64.rpm          |              |                     | 1.1 MB/s   666 kB | 00:00 |
| (5/9): php-8.0.30-3.el9_6.x86_64.rpm                 |              |                     | 167 kB/s   8.2 kB | 00:00 |
| (6/9): php-pdo-8.0.30-3.el9_6.x86_64.rpm             |              |                     | 628 kB/s   81 kB  | 00:00 |
| (7/9): php-fpm-8.0.30-3.el9_6.x86_64.rpm             |              |                     | 244 kB/s   1.6 MB | 00:06 |


```

В каталоге /var/www/html/www.astakhovAMD.net замените файл index.html на index.php следующего содержания:



Скорректировали права доступа и восстановили контекст:

```
Complete!
[root@localhost user.net ~]# cd /var/www/html/
[root@localhost user.net html]# sudo nano www.astakhovam.net
[root@localhost user.net html]# chown -R apache:apache /var/www
[root@localhost user.net html]# restorecon -vR /etc
[root@localhost user.net html]# restorecon -vR /var/www
[root@localhost user.net html]# systemctl restart httpd
```

**3. Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке HTTP-сервера во внутреннем окружении виртуальной машины server. Внесение изменений в настройки внутреннего окружения виртуальной машины**

В имеющийся скрипт /vagrant/provision/server/http.sh внесли изменения, добавив установку PHP и настройку межсетевого экрана, разрешающую работать с https.

```
[root@localhost user.net conf.d]# 
[root@localhost user.net conf.d]# 
[root@localhost user.net conf.d]# 
[root@localhost user.net conf.d]# 
[root@localhost user.net conf.d]# cp -R /etc/httpd/conf.d/* /vagrant/provision/server/http/etc/httpd/conf.d
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/autoindex.conf'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/fcgid.conf'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/manual.conf'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/README'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/server.astakhovamd.net.conf'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/ssl.conf'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/userdir.conf'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/welcome.conf'? Y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/www.astakhovamd.net.conf'? Y
[root@localhost user.net conf.d]# cp -R /var/www/html/* /vagrant/provision/server/http/var/www/html
cp: overwrite '/vagrant/provision/server/http/var/www/html/www.astakhovamd.net/index.html'? Y
cp: overwrite '/vagrant/provision/server/http/var/www/html/www.astakhovamd.net/index.html'? Y
[root@localhost user.net conf.d]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/private
[root@localhost user.net conf.d]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/certs
[root@localhost user.net conf.d]# cp -R /etc/pki/tls/private/www.astakhovamd.net.key/vagrant/provision/server/http/etc/pki/tls/private
cp: missing destination file operand after '/etc/pki/tls/private/www.astakhovamd.net.key/vagrant/provision/server/http/etc/pki/tls/private'
try 'cp --help' for more information.
[root@localhost user.net conf.d]# cp -R /etc/pki/tls/private/www.astakhovamd.net.key /vagrant/provision/server/http/etc/pki/tls/private
[root@localhost user.net conf.d]# cp -R /etc/pki/tls/certs/www.astakhovamd.net.crt /vagrant/provision/server/http/etc/pki/tls/certs
[root@localhost user.net conf.d]#
```

```
root@localhost:/vagrant/provision/server
root@localhost:/vagrant/provision/server | http.sh
GNU nano 5.6.1
#!/bin/bash

set -e

dnf update -y
dnf install -y httpd
dnf install -y php php-cli php-fpm php-common php-mysqlnd
systemctl enable httpd
systemctl start httpd
dnf install -y firewalld
systemctl enable firewalld
systemctl start firewalld
firewall-cmd --zone=public --add-service=http --permanent
firewall-cmd --zone=public --add-service=https --permanent
firewall-cmd --reload

echo "<?php phpinfo(); ?>" > /var/www/html/info.php
chmod 644 /var/www/html/info.php
```

## 5.3. Итог работы

Были приобретены практические навыки по расширенному конфигурированию HTTP сервера Apache в части безопасности и возможности использования PHP.

## 5.4. Контрольные вопросы

## **1. В чём отличие HTTP от HTTPS?**

**HTTP (Hypertext Transfer Protocol)** можно сравнить с передачей информации в открытом виде, аналогично отправке незапечатанной почтовой открытки. В такой ситуации данные не защищены от несанкционированного доступа, перехвата или прочтения третьими лицами в процессе их передачи по сети.

**HTTPS (Hypertext Transfer Protocol Secure)**, напротив, обеспечивает безопасную передачу данных. Его функционирование эквивалентно отправке запечатанного и криптографически зашифрованного письма. Это гарантирует, что:

1. *Конфиденциальность*: Содержимое сообщения недоступно для прочтения посторонними лицами, поскольку оно зашифровано.
2. *Аутентификация*: Получатель может удостовериться в подлинности отправителя (веб-сервера) благодаря использованию цифровых сертификатов, что исключает возможность подмены отправителя.
3. *Целостность*: Получатель уверен, что данные не были изменены или повреждены в процессе передачи.

## **2. Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?**

Безопасность контента при работе через HTTPS обеспечивается благодаря использованию протоколов SSL (Secure Sockets Layer) и его преемника TLS (Transport Layer Security). Эти протоколы работают на транспортном уровне и обеспечивают три ключевых аспекта безопасности:

### **A. Шифрование (Confidentiality):**

Все данные, передаваемые между браузером и сервером (HTTP-запросы и ответы), шифруются. Это означает, что если злоумышленник перехватит трафик, он получит лишь бессмысленный набор символов, который не сможет прочитать.

Для шифрования используется комбинация асимметричного (для обмена ключами) и симметричного (для основной передачи данных) шифрования.

### **B. Аутентификация (Authentication):**

HTTPS позволяет клиенту (браузеру) удостовериться в подлинности веб-сервера. Это предотвращает атаки типа "человек посередине" (Man-in-the-Middle), когда злоумышленник выдает себя за легитимный сервер.

Аутентификация осуществляется с помощью цифровых сертификатов. Сервер предоставляет свой сертификат браузеру. Браузер проверяет этот сертификат:

1. Действителен ли он (не истёк ли срок).
2. Выдан ли он доверенным Сертификационным Центром (СА).
3. Соответствует ли доменное имя в сертификате тому домену, к которому обращается пользователь.

### **C. Целостность данных (Integrity):**

HTTPS гарантирует, что данные не были изменены или повреждены во время передачи. Для этого используются криптографические хеш-функции и цифровые подписи. Сервер и клиент могут проверить, что полученные данные точно соответствуют отправленным.

### **3. Что такое сертификационный центр? Приведите пример.**

Сертификационный Центр (СА - Certificate Authority) — это доверенная сторонняя организация, которая выдает и управляет цифровыми сертификатами, используемыми для обеспечения безопасности в интернете (например, для HTTPS).

#### **Роль Сертификационного Центра:**

##### **1. Проверка личности:**

СА проверяет личность владельца веб-сайта или организации, которая запрашивает сертификат. Уровень проверки может варьироваться от простой проверки владения доменом (Domain Validation - DV) до более строгой проверки организации (Organization Validation - OV) или расширенной проверки (Extended Validation - EV).

##### **2. Выдача сертификатов:**

После успешной проверки СА выдает цифровой сертификат, который содержит:

- A. Публичный ключ владельца.
- B. Имя домена (или доменов), для которого выдан сертификат.
- C. Срок действия сертификата.
- D. Название СА, который выдал сертификат.

- E. Цифровую подпись самого СА, которая подтверждает подлинность сертификата.

### **3. Поддержание доверия:**

Браузеры и операционные системы имеют встроенный список "корневых" (root) сертификатов доверенных СА. Когда браузер получает сертификат от веб-сайта, он проверяет, подписан ли этот сертификат одним из доверенных корневых СА (или промежуточным СА, который, в свою очередь, подписан корневым СА). Если цепочка доверия действительна, браузер считает сертификат подлинным и устанавливает безопасное соединение.

### **Пример Сертификационного Центра:**

Один из самых известных и широко используемых сертификационных центров, особенно для бесплатных сертификатов, это Let's Encrypt.

Let's Encrypt — это некоммерческий СА, который предоставляет бесплатные цифровые сертификаты X.509 для TLS-шифрования. Его цель — сделать использование HTTPS стандартным для всех веб-сайтов, упрощая процесс получения и установки сертификатов. Благодаря Let's Encrypt, многие мелкие и средние сайты могут использовать HTTPS без дополнительных затрат.

Другие известные коммерческие СА включают:

- a. DigiCert
- b. Sectigo (ранее Comodo)
- c. GlobalSign
- d. GoDaddy

