РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 5  
*дисциплина:* *Администрирование сетевых подсистем*

Студент:

Группа:

**МОСКВА**

2023 г.

# Цель работы:

Приобретение практических навыков по расширенному конфигурированию

HTTP-сервера Apache в части безопасности и возможности использования PHP.

# Задание:

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

2. Настройте веб-сервер для работы с PHP .

3. Напишите (или скорректируйте) скрипт для Vagrant, фиксирующий действия по расширенной настройке HTTP-сервера во внутреннем окружении виртуальной машины server.

# Выполнение работы:

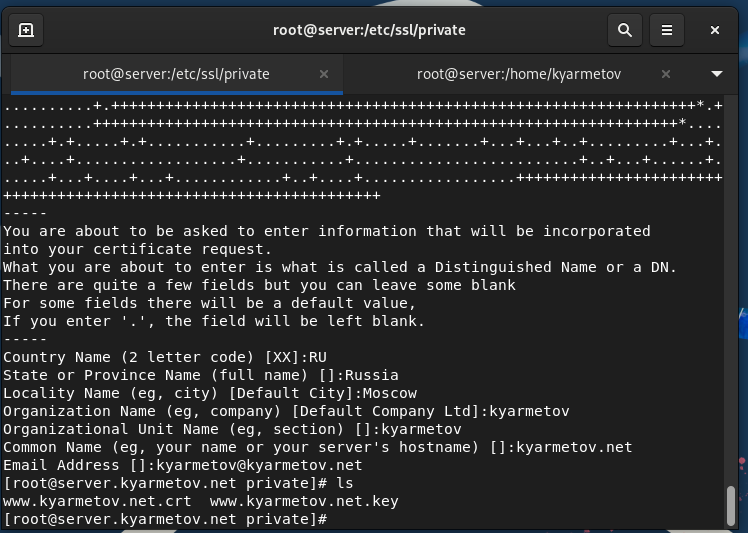
## 1.Конфигурирование HTTP-сервера для работы через протокол HTTPS

Загружаю свою операционную систему и перехожу в рабочий каталог с проектом:

Запускаю виртуальную машину server: make server

На виртуальной машине server вхожу под своим пользователем и открываю терминал. Перехожу в режим суперпользователя: sudo -i

Генерирую ключ для веб-сервера [www.kyarmetov.net](http://www.saburceva.net):



Сгенерированные ключи и сертификат появились в соответствующих подкаталогах в каталоге

Для перехода веб-сервера [www.kyarmetov.net](http://www.saburceva.net/) на функционирование через протокол HTTPS требуется изменить его конфирурационный файл. Перехожу в каталог с конфигурационными файлами: cd /etc/httpd/conf.d

Открываю на редактирование файл /etc/httpd/conf.d/www.kyarmetov.net.conf и заменяю его содержимое на следующее:

<VirtualHost \*:80> Создать виртуальный хост на порту 80. Здесь мы используем звездочку вместо ip адреса, это значит, что веб-сервер будет слушать соединения на всех адресах, как на внешнем, так и на localhost

ServerAdmin [webmaster@kyarmetov.net](mailto:webmaster@saburceva.net)

Указывается электронный адрес администратора веб-сервера

DocumentRoot /var/www/html/www.kyarmetov.net

Указывается папка, в которой будут находиться данные сайта

ServerName [www.kyarmetov.net](http://www.saburceva.net/) Указывается домен

ServerAlias [www.kyarmetov.net](http://www.saburceva.net/) Указывается псевдоним домена

ErrorLog logs/www.kyarmetov.net-error\_log

Путь к каталогу для сохранения лог-файлов ошибок

CustomLog logs/www.kyarmetov.net-access\_log common

Путь к каталогу для сохранения лог-файлов доступа

RewriteEngine on Подключён модуль mod\_rewrite

RewriteRule ^(.\*)$ https://%{HTTP\_HOST}$1 [R=301,L]

Перенаправляем запросы к любой странице на сайт https://%{HTTP\_HOST}, используя перенаправление 301.

</VirtualHost> Описание виртуального хоста начинается с <VirtualHost> и заканчивается </VirtualHost>

<IfModule mod\_ssl.c> Весь код в этой секции будет выполнен только в том случае, если активирован модуль mod\_ssl. Это нужно для безопасности, чтобы если модуль не активирован, то код не вызывал ошибок

<VirtualHost \*:443> Создать виртуальный хост на порту 443

SSLEngine on Подключена поддержка SSL

ServerAdmin [webmaster@kyarmetov.net](mailto:webmaster@saburceva.net)

Указывается электронный адрес

администратора веб-сервера

DocumentRoot /var/www/html/www.kyarmetov.net

Указывается папка, в которой будут

находиться данные сайта

ServerName [www.kyarmetov.net](http://www.saburceva.net/) Указывается домен

ServerAlias [www.kyarmetov.net](http://www.saburceva.net/) Указывается псевдоним домена

ErrorLog logs/www.kyarmetov.net-error\_log

Указывается путь к каталогу для

сохранения лог-файлов ошибок

CustomLog logs/www.kyarmetov.net-access\_log common

Указывается путь к каталогу для

сохранения лог-файлов доступа

SSLCertificateFile /etc/pki/tls/certs/www.kyarmetov.net.crt

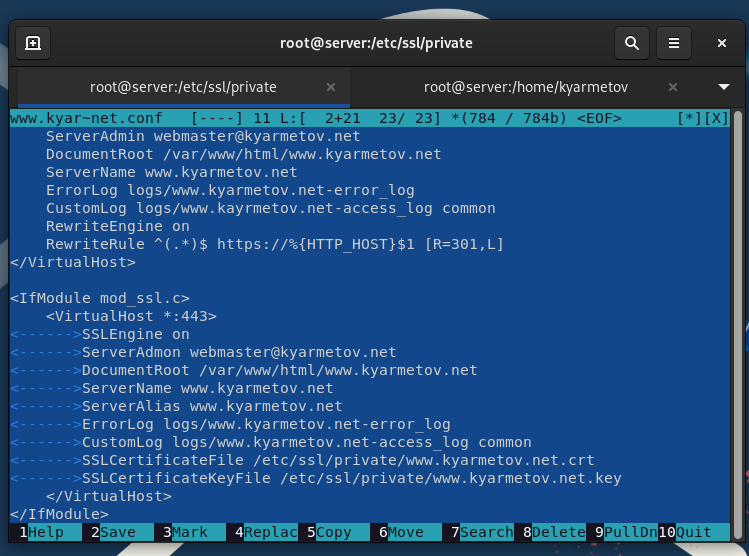
Указывается путь к файлам сертификата

SSLCertificateKeyFile /etc/pki/tls/private/www.kyarmetov.net.key

Указывается путь к файлам приватного ключа

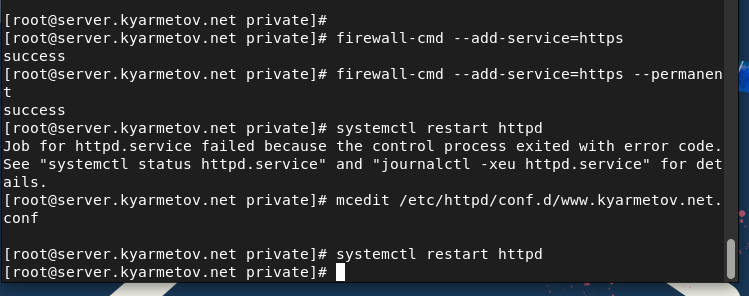
</VirtualHost> Конец описания виртуального хоста

</IfModule>



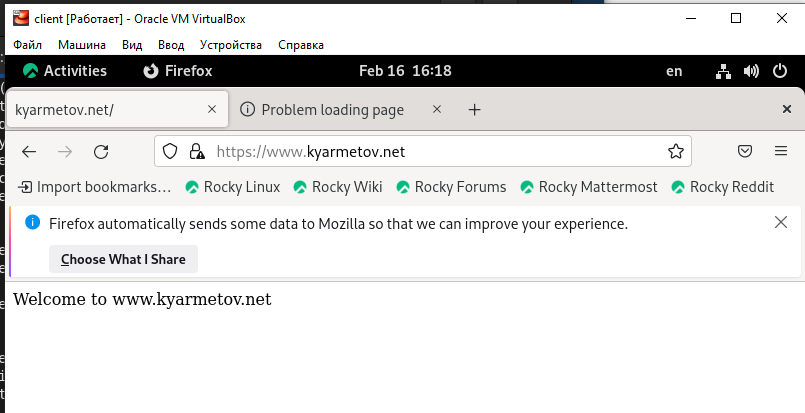
Вношу изменения в настройки межсетевого экрана на сервере, разрешив работу с https

Перезапускаю веб-сервер: systemctl restart httpd

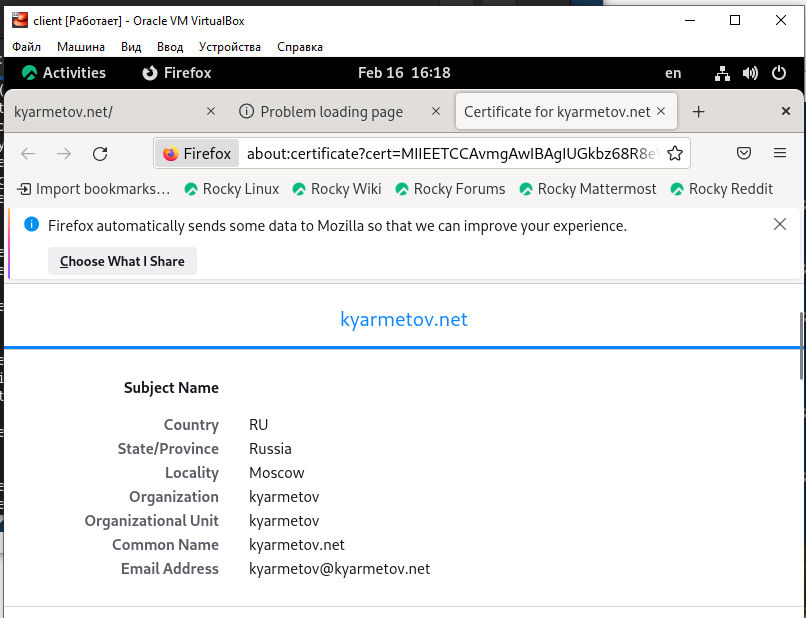


На виртуальной машине client в строке браузера ввожу название веб-сервера [www.kyarmetov.net](http://www.saburceva.net/). Происходит автоматическое переключение на работу по протоколу HTTPS.

На открывшейся странице с сообщением о незащищённости соединения нажимаю кнопку «Дополнительно», затем добавляю адрес сервера в постоянные исключения.

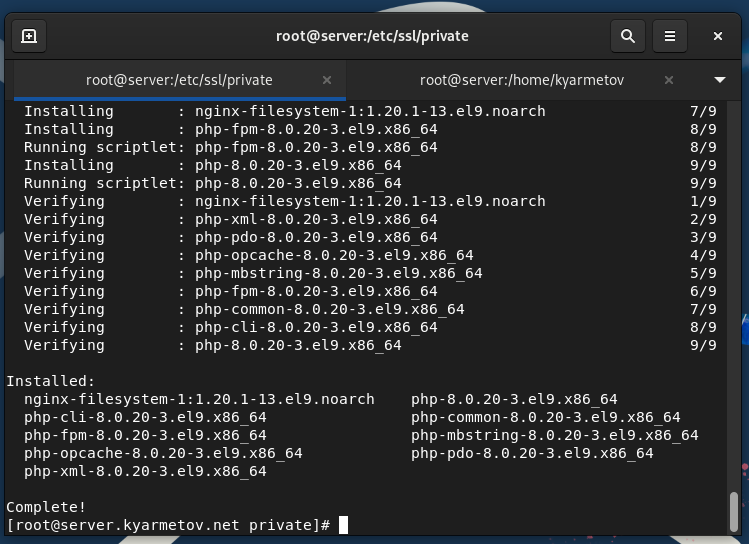


Затем просматриваю содержание сертификата (нажмите на значок с замком в адресной строке и кнопку «Подробнее»).



## 2.Конфигурирование HTTP-сервера для работы с PHP

Устанавливаю пакеты для работы с PHP: dnf -y install php



В каталоге /var/www/html/www.kyarmetov.net заменяю файл index.html на index.php следующего содержания:

<?php

phpinfo();

?>

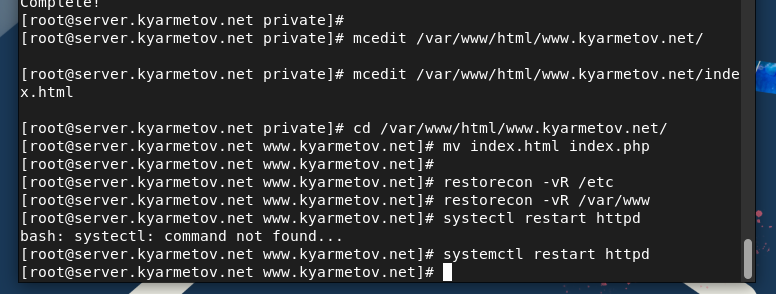
Корректирую права доступа в каталог с веб-контентом: chown -R apache:apache /var/www

Восстанавливаю контекст безопасности в SELinux:

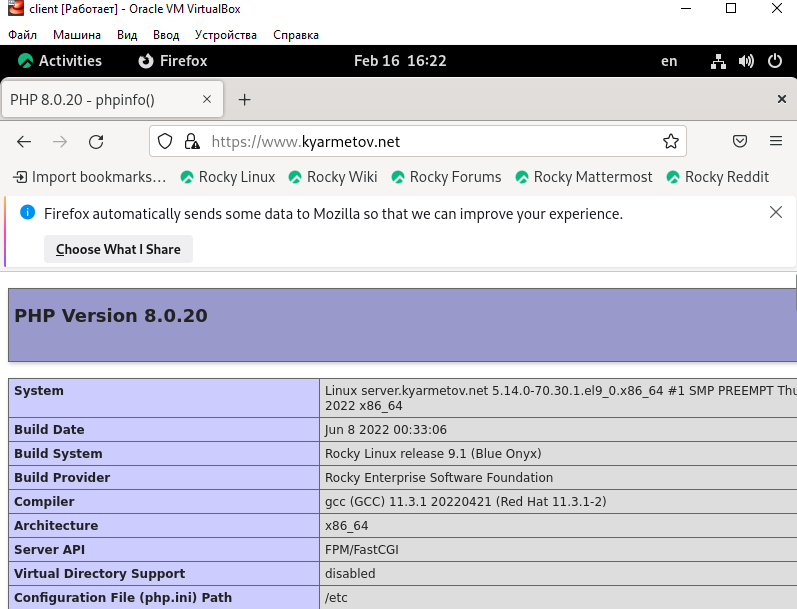
restorecon -vR /etc

restorecon -vR /var/www

Перезапускаю HTTP-сервер: systemctl restart httpd



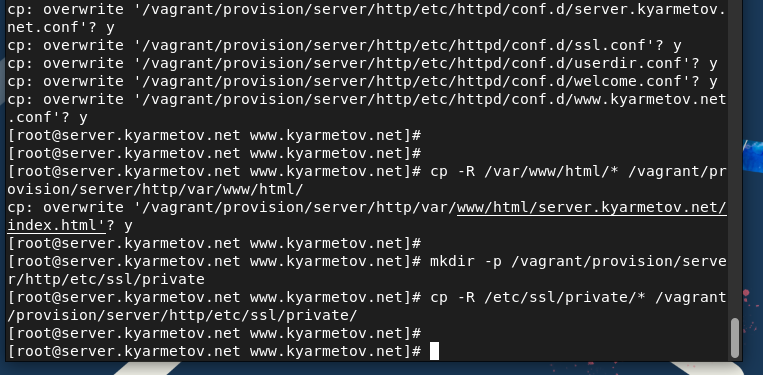
На виртуальной машине client в строке браузера ввожу название веб-сервера www.kyarmetov.net . Выведена страница с информацией об используемой на веб-сервере версии PHP.



## 3.Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перехожу в каталог для внесение изменений в настройки внутреннего окружения /vagrant/provision/server/http и в соответствующие каталоги копирую конфигурационные файлы:

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



# Вывод:

Я приобрел практические навыки по расширенному конфигурированию

HTTP-сервера Apache в части безопасности и возможности использования PHP.