

# **Отчёт по лабораторной работе 5**

**Расширенная настройка HTTP-сервера Apache**

Суннатилло Махмудов

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Теоретические сведения</b>	<b>6</b>
2.1	Основные свойства HTTPS . . . . .	6
2.2	Этапы установления HTTPS-соединения . . . . .	7
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
3.1	Конфигурирование HTTP-сервера для работы через протокол HTTPS	8
3.2	Конфигурирование HTTP-сервера для работы с PHP . . . . .	11
3.3	Внесение изменений в настройки внутреннего окружения . . . . .	13
<b>4</b>	<b>Вывод</b>	<b>15</b>
<b>5</b>	<b>Контрольные вопросы</b>	<b>16</b>
<b>6</b>	<b>Список литературы</b>	<b>17</b>

## Список иллюстраций

3.1	Генерация ключа и сертификата . . . . .	8
3.2	Редактирование конфигурационного файла . . . . .	9
3.3	Предупреждение браузера о небезопасном соединении . . . . .	10
3.4	Подключение к сайту по HTTPS . . . . .	10
3.5	Просмотр сертификата в браузере . . . . .	11
3.6	Установка пакетов PHP . . . . .	12
3.7	Создание index.php с вызовом phpinfo() . . . . .	12
3.8	Вывод phpinfo() в браузере . . . . .	13
3.9	Копирование конфигурационных файлов и сертификатов в окружение Vagrant . . . . .	13

## **Список таблиц**

# 1 Цель работы

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

## 2 Теоретические сведения

**HTTPS (HyperText Transfer Protocol Secure)** — расширение протокола HTTP, обеспечивающее безопасную передачу данных между клиентом (браузером) и сервером за счет использования шифрования. Работает поверх TLS/SSL, защищая соединение от перехвата и подмены информации.

- **Клиент** — программа (обычно веб-браузер), отправляющая запросы к серверу.
- **Сервер** — веб-сервер, обрабатывающий запросы и отправляющий ответы.
- **SSL/TLS-сертификат** — цифровой сертификат, подтверждающий подлинность сайта и содержащий ключи для шифрования.
- **Шифрование** — обеспечивает конфиденциальность данных, передаваемых по сети.

### 2.1 Основные свойства HTTPS

- **Аутентификация** — подтверждает, что клиент общается именно с тем сервером, к которому обращался.
- **Конфиденциальность** — данные передаются в зашифрованном виде и недоступны для перехвата.

- **Целостность** — защищает информацию от подмены или изменения при передаче.

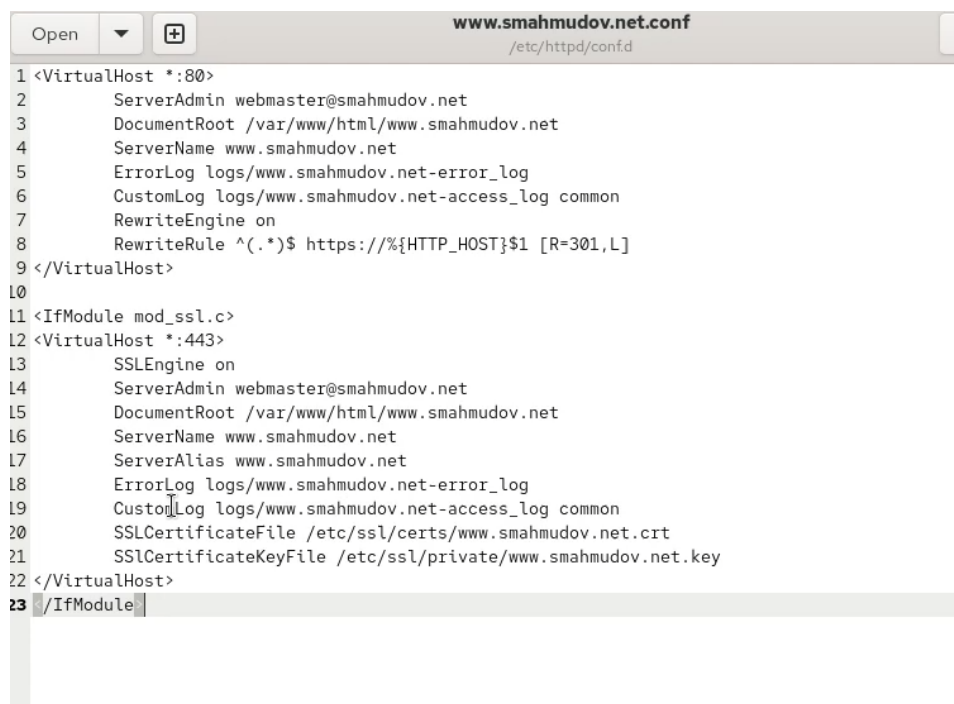
## 2.2 Этапы установления HTTPS-соединения

1. **Client Hello** — клиент отправляет список поддерживаемых шифров и параметров.
2. **Server Hello** — сервер выбирает параметры и передает свой SSL/TLS-сертификат.
3. **Обмен ключами** — клиент и сервер договариваются о сессионных ключах для шифрования.
4. **Secure Connection** — все дальнейшие данные передаются по зашифрованному каналу.





- для порта **80** настроено перенаправление всех HTTP-запросов на HTTPS;
- определены директории для корня сайта и логов ошибок/доступа;
- для порта **443** включён SSL и указаны пути к сертификату и приватному ключу;
- заданы доменное имя сервера и алиас.



```

1 <VirtualHost *:80>
2     ServerAdmin webmaster@smahmudov.net
3     DocumentRoot /var/www/html/www.smahmudov.net
4     ServerName www.smahmudov.net
5     ErrorLog logs/www.smahmudov.net-error_log
6     CustomLog logs/www.smahmudov.net-access_log common
7     RewriteEngine on
8     RewriteRule ^(.*)$ https://%{HTTP_HOST}%1 [R=301,L]
9 </VirtualHost>
10
11 <IfModule mod_ssl.c>
12 <VirtualHost *:443>
13     SSLEngine on
14     ServerAdmin webmaster@smahmudov.net
15     DocumentRoot /var/www/html/www.smahmudov.net
16     ServerName www.smahmudov.net
17     ServerAlias www.smahmudov.net
18     ErrorLog logs/www.smahmudov.net-error_log
19     CustomLog logs/www.smahmudov.net-access_log common
20     SSLCertificateFile /etc/ssl/certs/www.smahmudov.net.crt
21     SSLCertificateKeyFile /etc/ssl/private/www.smahmudov.net.key
22 </VirtualHost>
23 </IfModule>

```

Рис. 3.2: Редактирование конфигурационного файла

3. После перезапуска веб-сервера при обращении к сайту по HTTPS браузер выдал предупреждение о небезопасном соединении, так как использован самоподписанный сертификат.

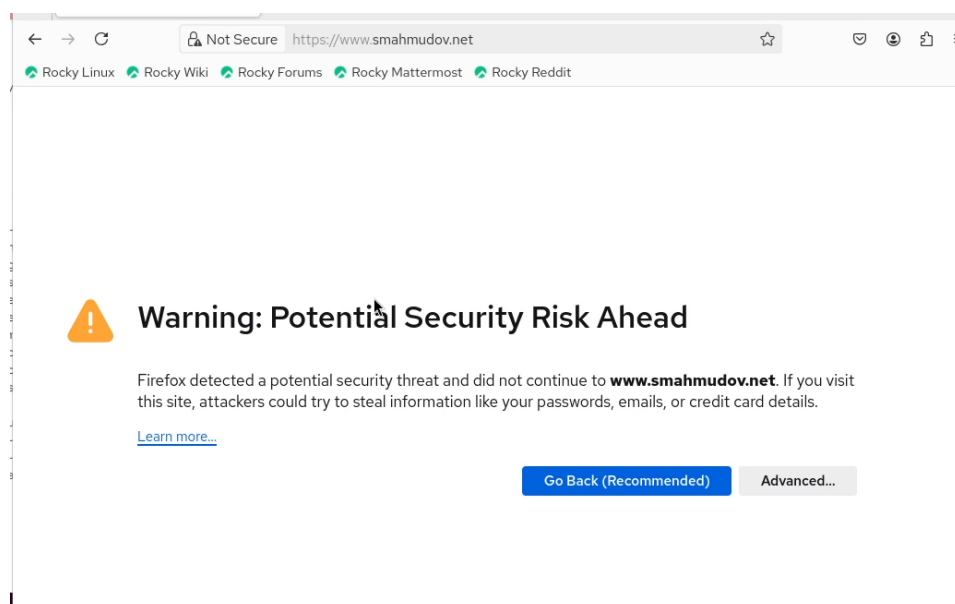


Рис. 3.3: Предупреждение браузера о небезопасном соединении

После добавления исключения сайт открылся корректно по защищённому протоколу:

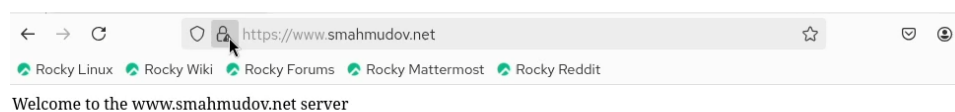


Рис. 3.4: Подключение к сайту по HTTPS

4. В настройках браузера был просмотрен сертификат. Он содержит следующие данные:

- Страна: **RU**
- Город: **Moscow**

- Организация: **smahmudov**
- Домен: **smahmudov.net**
- E-mail: **smahmudov@smahmudov.net**

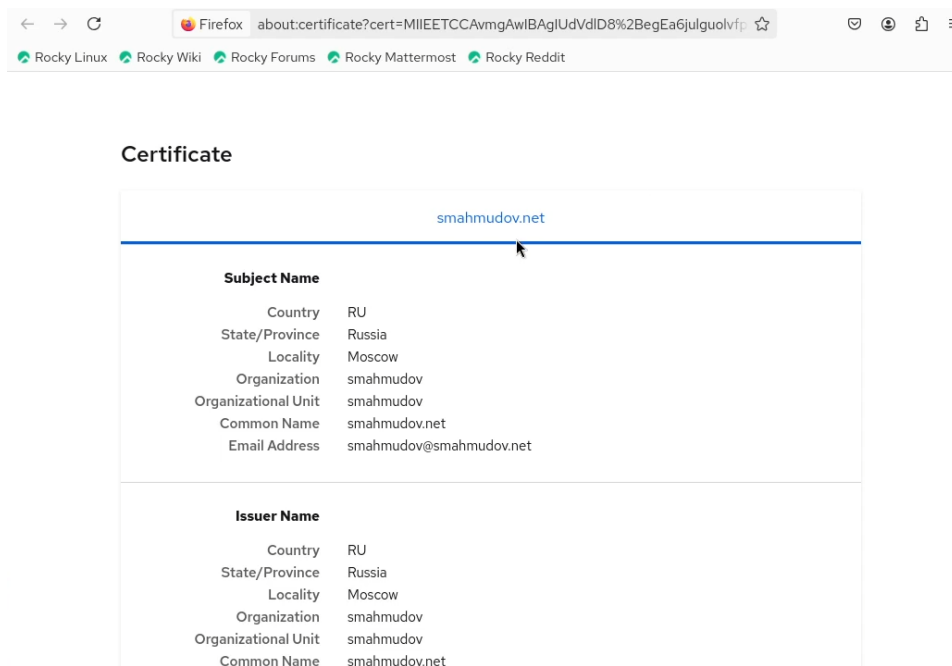


Рис. 3.5: Просмотр сертификата в браузере

## 3.2 Конфигурирование HTTP-сервера для работы с РНР

1. На сервер были установлены необходимые пакеты для поддержки РНР.



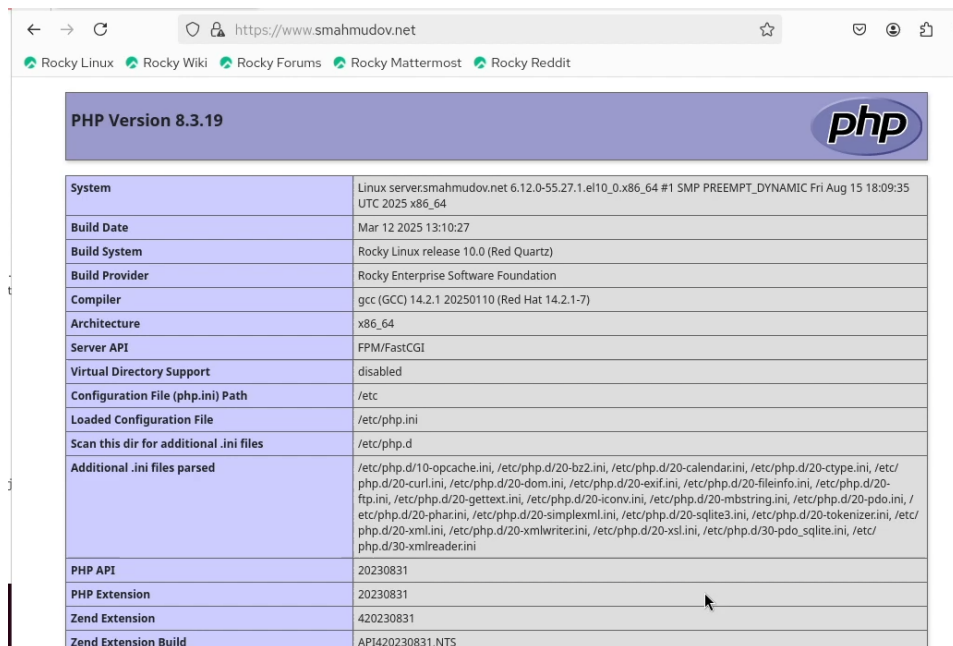
Рис. 3.6: Установка пакетов PHP

- В каталоге **/var/www/html/www.smahmudov.net** файл *index.html* был заменён на *index.php* с минимальным содержимым для вывода информации о конфигурации PHP.



Рис. 3.7: Создание index.php с вызовом phpinfo()

- Для корректной работы были скорректированы права доступа к каталогу с веб-контентом и восстановлен контекст SELinux. После этого веб-сервер был перезапущен.
- При обращении к сайту **https://www.smahmudov.net** в браузере отобразилась служебная страница PHP с подробной информацией о версии и параметрах окружения.




<div> <div>PHP Version 8.3.19</div>  </div>	
System	Linux serversmahmudov.net 6.12.0-55.27.1.el10_0.x86_64 #1 SMP PREEMPT_DYNAMIC Fri Aug 15 18:09:35 UTC 2025 x86_64
Build Date	Mar 12 2025 13:10:27
Build System	Rocky Linux release 10.0 (Red Quartz)
Build Provider	Rocky Enterprise Software Foundation
Compiler	gcc (GCC) 14.2.1 20250110 (Red Hat 14.2.1-7)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini
PHP API	20230831
PHP Extension	20230831
Zend Extension	420230831
Zend Extension Build	API420230831,NTS

Рис. 3.8: Вывод `phpinfo()` в браузере

### 3.3 Внесение изменений в настройки внутреннего окружения

1. Конфигурационные файлы веб-сервера и каталоги сайта были скопированы в структуру **`/vagrant/provision/server/http`** для сохранения и последующего использования. Также были добавлены сертификат и приватный ключ.

```
[root@server.smahmudov.net www.smahmudov.net]#
[root@server.smahmudov.net www.smahmudov.net]# 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.smahmudov.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.smahmudov.net.conf'? y
[root@server.smahmudov.net www.smahmudov.net]# cp -R /var/www/html/* /vagrant/provision/server/http/var/www/html/
cp: overwrite '/vagrant/provision/server/http/var/www/html/server.smahmudov.net/index.html'? y
[root@server.smahmudov.net www.smahmudov.net]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/private
[root@server.smahmudov.net www.smahmudov.net]# cp -R /etc/pki/tls/private/www.smahmudov.net.key /vagrant/provision/server/http/etc/pki/tls/private/
[root@server.smahmudov.net www.smahmudov.net]# cp -R /etc/pki/tls/certs/www.smahmudov.net.crt /vagrant/provision/server/http/etc/pki/tls/certs/
[root@server.smahmudov.net www.smahmudov.net]#
```

Рис. 3.9: Копирование конфигурационных файлов и сертификатов в окружение Vagrant

2. В скрипт **/vagrant/provision/server/http.sh** были внесены изменения:

- добавлена установка PHP;
- настроен межсетевой экран для разрешения работы с HTTPS.

## 4 Вывод

В ходе лабораторной работы был настроен веб-сервер **Apache** для работы через протокол **HTTPS** с использованием самоподписанного SSL-сертификата. Реализовано автоматическое перенаправление с HTTP на HTTPS, проверена корректность сертификата и установлено защищённое соединение. Дополнительно была выполнена установка и настройка **PHP**, что позволило протестировать работоспособность динамических страниц с помощью встроенной функции **phpinfo()**. Результаты подтвердили правильную конфигурацию веб-сервера и поддержку защищённого доступа.

## 5 Контрольные вопросы

### 1. В чём отличие HTTP от HTTPS?

HTTP передаёт данные в открытом виде и не обеспечивает защиты от перехвата или подмены.

HTTPS работает поверх протокола **TLS/SSL**, что позволяет шифровать весь трафик и гарантировать безопасное соединение между клиентом и сервером.

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

Безопасность достигается за счёт использования **шифрования, аутентификации и контроля целостности данных**. Для этого применяется SSL/TLS-сертификат, который подтверждает подлинность сервера и позволяет установить защищённый канал связи.

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

Сертификационный центр (Certificate Authority, CA) — это организация, которая выпускает и подписывает цифровые сертификаты, подтверждающие подлинность владельца ресурса.

Примеры: **DigiCert, GlobalSign, Let's Encrypt**.



## 6 Список литературы

1. Apache HTTP Server Version 2.4 Documentation. — URL: <http://httpd.apache.org/docs/current/> (дата обр. 13.09.2021).
2. Httpd — Apache Hypertext Transfer Protocol Server. — URL: <https://httpd.apache.org/docs/2.4/pr> (дата обр. 13.09.2021).