

ДЗ 22

Цель: Использование серверных и клиентских сертификатов на примере Web-приложения на базе Apache

1. Установить и настроить сервер LAMP
2. Настройка сайта с самоподписаным сертификатом

Для выполнения данной работы, мной было принято решение о ручной установке и настройке сервера LAMP (это хоть и более меленый способ, зато позволит запомнить шаги поэтапно для последующего их воспроизведения в случае необходимости).

И так приступим:

Для изучения данной работы мной был собран тестовый стенд на базе Linux Mint 19.2 Cinnamon x86-64.

Установим из штатных репозиториев последнюю доступную в ветке stable версию Apache2:

sudo apt install apache2

```
usr@vb:~$ sudo apt install apache2
[sudo] пароль для usr:
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
Предлагаемые пакеты:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Следующие НОВЫЕ пакеты будут установлены:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
Обновлено 0 пакетов, установлено 8 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
Необходимо скачать 1 604 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 6 493 kB.
Хотите продолжить? [Д/Н] у
Пол:1 http://archive.ubuntu.com/ubuntu bionic amd64 libapr1 amd64 1.6.3-2 [90,9 kB]
Пол:2 http://archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1 amd64 1.6.1-2 [84,4 kB]
Пол:3 http://archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-2 [10,6 kB]
Пол:4 http://archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1-ldap amd64 1.6.1-2 [8 764 B]
Пол:5 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2-bin amd64 2.4.29-lubuntu4.11 [1 071 kB]
Пол:6 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2-utils amd64 2.4.29-lubuntu4.11 [83,9 kB]
Пол:7 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2-data all 2.4.29-lubuntu4.11 [160 kB]
Пол:8 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2 amd64 2.4.29-lubuntu4.11 [95,1 kB]
Получено 1 604 kB за 5c (343 kB/s)
Выбор ранее не выбранного пакета libapr1:amd64.
(Чтение базы данных ... на данный момент установлен 294081 файл и каталог.)
Подготовка к распаковке .../0-libapr1_1.6.3-2_amd64.deb ...
Распаковывается libapr1:amd64 (1.6.3-2) ...
Выбор ранее не выбранного пакета libaprutil1:amd64.
Подготовка к распаковке .../1-libaprutil1_1.6.1-2_amd64.deb ...
Распаковывается libaprutil1:amd64 (1.6.1-2) ...
Выбор ранее не выбранного пакета libaprutil1-dbd-sqlite3:amd64.
Подготовка к распаковке .../2-libaprutil1-dbd-sqlite3_1.6.1-2_amd64.deb ...
Распаковывается libaprutil1-dbd-sqlite3:amd64 (1.6.1-2) ...
Выбор ранее не выбранного пакета libaprutil1-ldap:amd64.
Подготовка к распаковке .../3-libaprutil1-ldap_1.6.1-2_amd64.deb ...
Распаковывается libaprutil1-ldap:amd64 (1.6.1-2) ...
Выбор ранее не выбранного пакета apache2-bin.
Подготовка к распаковке .../4-apache2-bin_2.4.29-lubuntu4.11_amd64.deb ...
Распаковывается apache2-bin (2.4.29-lubuntu4.11) ...
Выбор ранее не выбранного пакета apache2-utils.
Подготовка к распаковке .../5-apache2-utils_2.4.29-lubuntu4.11_amd64.deb ...
Распаковывается apache2-utils (2.4.29-lubuntu4.11) ...

/usr@vb:~
```

Далее аналогично установим сервер баз данных MariaDB

sudo apt install mariadb-server

```
usr@vb:~$ sudo apt install mariadb-server
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состояниях... Готово
Будут установлены следующие дополнительные пакеты:
  galera-3 libaiol libconfig-inifiles-perl libdbi-perl libjemalloc1 mariadb-client-10.1 mariadb-client-core-10.1 mariadb-common
  mariadb-server-10.1 mariadb-server-core-10.1 mysql-common socat
Предлагаемые пакеты:
  libmldb-perl libnet-daemon-perl libsql-statement-perl mailx mariadb-test tinyca
Рекомендуемые пакеты:
  libdbd-mysql-perl libterm-readkey-perl libhtml-template-perl
Следующие НОВЫЕ пакеты будут установлены:
  galera-3 libaiol libconfig-inifiles-perl libdbi-perl libjemalloc1 mariadb-client-10.1 mariadb-client-core-10.1 mariadb-common
  mariadb-server mariadb-server-10.1 mariadb-server-core-10.1 mysql-common socat
Обновлено 0 пакетов, установлено 13 новых пакетов, для удаления отмечено 0 пакетов, и 5 пакетов не обновлено.
Необходимо скачать 22,7 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 178 MB.
Хотите продолжить? [Д/н] у
Пол:1 http://archive.ubuntu.com/ubuntu bionic/main amd64 mysql-common all 5.8+1.0.4 [7 308 B]
Пол:2 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-common all 1:10.1.43-0ubuntu0.18.04.1 [29,6 kB]
Пол:3 http://archive.ubuntu.com/ubuntu bionic/universe amd64 galera-3 amd64 25.3.20-1 [947 kB]
Пол:4 http://archive.ubuntu.com/ubuntu bionic/main amd64 libdbi-perl amd64 1.640-1 [724 kB]
Пол:5 http://archive.ubuntu.com/ubuntu bionic/main amd64 libconfig-inifiles-perl all 2.94-1 [40,4 kB]
Пол:6 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libaiol amd64 0.3.110-Subuntu0.1 [6 476 B]
Пол:7 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-client-core-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1 [4 778 kB]
Пол:8 http://archive.ubuntu.com/ubuntu bionic/universe amd64 libjemalloc1 amd64 3.6.0-11 [82,4 kB]
Пол:9 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-client-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1 [5 658 kB]
Пол:10 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-server mariadb-server-core-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1 [4 960 kB]
Пол:11 http://archive.ubuntu.com/ubuntu bionic/main amd64 socat amd64 1.7.3.2-2ubuntu2 [342 kB]
Пол:12 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-server-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1 [5 108 kB]
Пол:13 http://archive.ubuntu.com/ubuntu bionic mariadb-updates/universe amd64 mariadb-server all 1:10.1.43-0ubuntu0.18.04.1 [28,5 kB]
Получено 22,7 MB за 30c (764 kB/s)
Предварительная настройка пакетов ...
Выбор ранее не выбранного пакета mysql-common.
(Чтение базы данных ... на данный момент установлено 294780 файлов и каталогов.)
Подготовка к распаковке .../00-mysql-common_5.8+1.0.4_all.deb ...
Распаковывается mysql-common (5.8+1.0.4) ...
Выбор ранее не выбранного пакета mariadb-common.
Подготовка к распаковке .../01-mariadb-common_1%3a10.1.43-0ubuntu0.18.04.1_all.deb ...
Распаковывается mariadb-common (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета galera-3.
Подготовка к распаковке .../02-galera-3_25.3.20-1_amd64.deb ...
Распаковывается galera-3 (25.3.20-1) ...
Выбор ранее не выбранного пакета libdbi-perl.
Подготовка к распаковке .../03_libdbi-perl_1.640-1_amd64.deb ...
/usr@vb:~$
```

Установим интерпретатор языка программирования *PHP 7.2* и расширений, необходимых для его работы с *Apache* и *MySQL*:

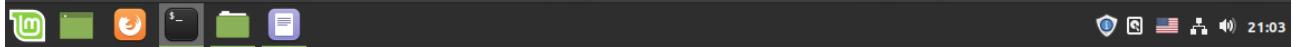
sudo apt install php7.2 libapache2-mod-php7.2 php-mysql

```
usr@vb:~$ sudo apt install php7.2 libapache2-mod-php7.2 php-mysql
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состояниях... Готово
Будут установлены следующие дополнительные пакеты:
  php-common php7.2-cli php7.2-common php7.2-json php7.2-mysql php7.2-opcache php7.2-readline
Предлагаемые пакеты:
  php-pear
Следующие НОВЫЕ пакеты будут установлены:
  libapache2-mod-php7.2 php-common php-mysql php7.2 php7.2-cli php7.2-common php7.2-json php7.2-mysql php7.2-opcache php7.2-readline
Обновлено 0 пакетов, установлено 10 новых пакетов, для удаления отмечено 0 пакетов, и 5 пакетов не обновлено.
Необходимо скачать 3 983 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 17,6 MB.
Хотите продолжить? [Д/н] 1
/usr@vb:~$
```

Сразу установим дополнительные расширения для *PHP*, которые, скорее всего, пригодятся в будущем:

sudo apt install php-curl php-json php-cgi php-gd php-zip php-mbstring php-xml php-xmlrpc

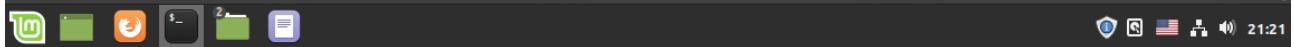
```
usr@vb:~$ sudo apt install php-curl php-json php-cgi php-gd php-zip php-mbstring php-xml php-xmlrpc
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
 libxmlrpc-epi0 php7.2-cgi php7.2-curl php7.2-gd php7.2-mbstring php7.2-xml php7.2-xmlrpc php7.2-zip
Предлагаемые пакеты:
 php-pear
Следующие НОВЫЕ пакеты будут установлены:
 libxmlrpc-epi0 php7.2-cgi php7.2-curl php7.2-gd php7.2-mbstring php7.2-xml php7.2-xmlrpc php7.2-zip
Обновлено 0 пакетов, установлено 16 новых пакетов, для удаления отмечено 0 пакетов, и 5 пакетов не обновлено.
Необходимо скачать 2 097 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 12,4 MB.
Хотите продолжить? [Д/Н] 
```



Добавим правила файервола, разрешающие входящие подключения по 80 порту:

sudo ufw allow in 80/tcp

```
usr@vb:~$ sudo ufw allow in 80/tcp
[sudo] пароль для usr:
Правила обновлены
Правила обновлены (v6)
usr@vb:~$ 
```



Как показала проверка, страница открывается → LAMP работает.

The screenshot shows a Mozilla Firefox window displaying the Apache2 Ubuntu Default Page. The title bar reads "Apache2 Ubuntu Default Page: It works - Mozilla Firefox". The main content features the Ubuntu logo and the text "ubuntu" below it, followed by a red banner with "It works!". Below the banner, there is descriptive text about the default welcome page and configuration details. A "Configuration Overview" section is present, detailing the file structure under "/etc/apache2/". A note at the bottom states that "apache2.conf" is the main configuration file. The bottom of the screen shows the standard Ubuntu desktop taskbar with icons for Dash, Home, Dash to Dock, and other applications.

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
--- apache2.conf
   `-- ports.conf
--- mods-enabled
   |-- *.load
   |-- *.conf
--- conf-enabled
   '-- *.conf
--- sites-enabled
   '-- *.conf
```

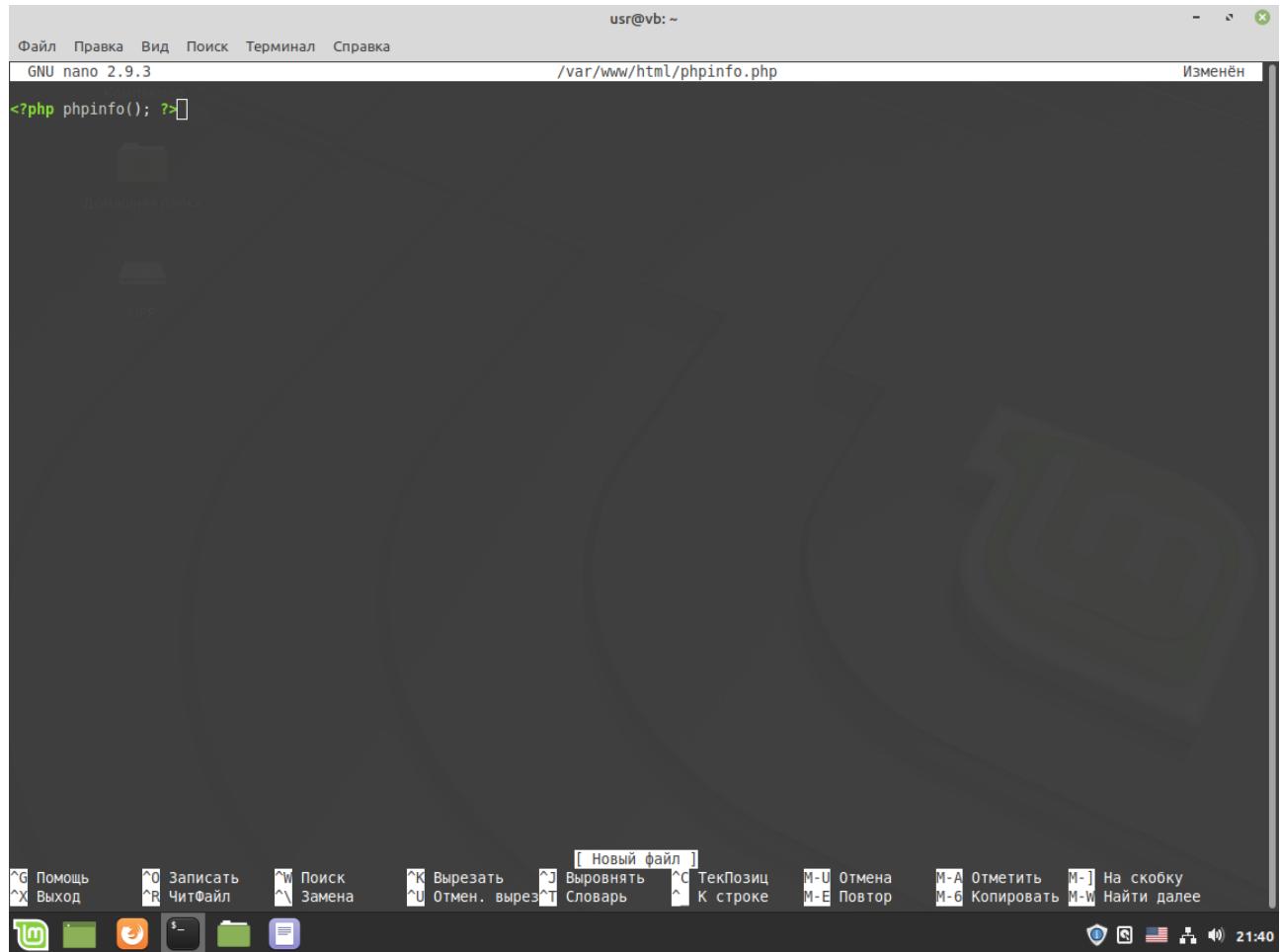
- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.



Создадим пустой файл `phpinfo.php` в директории `/var/www/html`

`sudo nano /var/www/html/phpinfo.php`

```
usr@vb:~$ sudo nano /var/www/html/phpinfo.php
usr@vb:~$
```



На основе данного файла проверим корректность работы нашего PHP откроем адрес `localhost/phpinfo.php` и, если всё сработало корректно, увидим следующую страницу браузера:

PHP Version 7.2.24-Ubuntu0.18.04.1

System

Build Date	Oct 28 2019 12:07:07
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-finfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini

PHP API

PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTorso Support	available - disabled

PCRE (Perl Compatible Regular Expressions) Support

PCRE Library Version	8.39 2016-06-14
PCRE JIT Support	enabled

PDO

PDO support	enabled
PDO drivers	mysql

pdo_mysql

PDO Driver for MySQL	enabled	
Client API version	mysqlnd 5.0.12-dev - 20150407 - \$Id: 3591daad22de08524295e1bd073aceff11e6579 \$	
Directive	Local Value	Master Value
pdo_mysql.default_socket	/var/run/mysql/mysqld.sock	/var/run/mysql/mysqld.sock

Phar

Phar: PHP Archive support	enabled
Phar EXT version	2.0.2
Phar API version	1.1.1
SVN revision	\$Id: f1155e62742ca367e521a3e412667d8ee34eed9 \$
Phar-based phar archives	enabled
Tar-based phar archives	enabled
ZIP-based phar archives	enabled
gzip compression	enabled

как видно на скриншоте ниже, MySQL тоже работает:

PCRE (Perl Compatible Regular Expressions) Support

PCRE Library Version	8.39 2016-06-14
PCRE JIT Support	enabled

PDO

PDO support	enabled
PDO drivers	mysql

pdo_mysql

PDO Driver for MySQL	enabled	
Client API version	mysqlnd 5.0.12-dev - 20150407 - \$Id: 3591daad22de08524295e1bd073aceff11e6579 \$	
Directive	Local Value	Master Value
pdo_mysql.default_socket	/var/run/mysql/mysqld.sock	/var/run/mysql/mysqld.sock

Phar

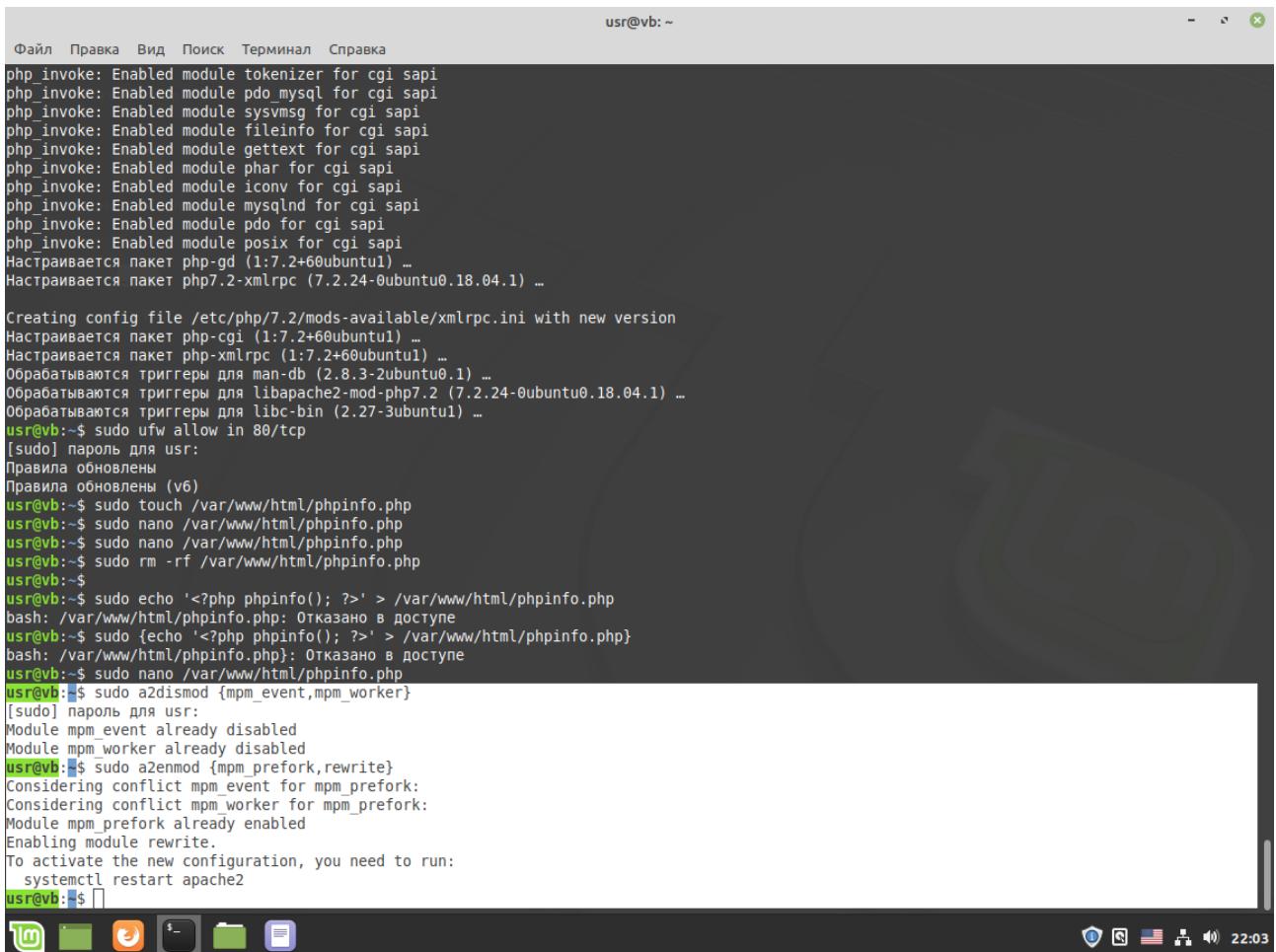
Phar: PHP Archive support	enabled
Phar EXT version	2.0.2
Phar API version	1.1.1
SVN revision	\$Id: f1155e62742ca367e521a3e412667d8ee34eed9 \$
Phar-based phar archives	enabled
Tar-based phar archives	enabled
ZIP-based phar archives	enabled
gzip compression	enabled

далее переходим к настройке LAMP и следующим шагом настроим Apache2

Для обработки запросов будет использоваться модуль **mpm_prefork**, так как он совместим с большинством систем. Поэтому его нужно активировать, а **mpm_event** и **mpm_worker** отключить:

```
sudo a2dismod {mpm_event,mpm_worker}
```

```
sudo a2enmod {mpm_prefork,rewrite}
```

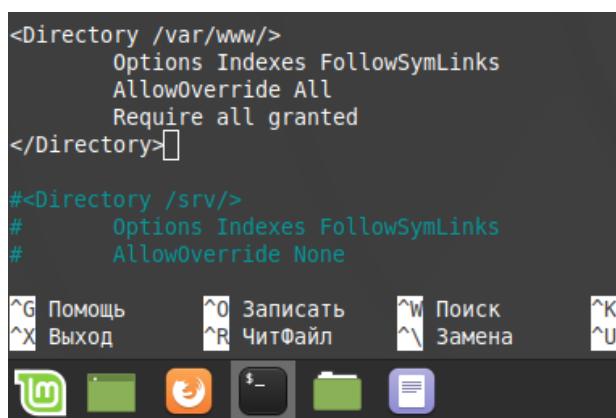


```
usr@vb: ~
Файл Правка Вид Поиск Терминал Справка
php_invoke: Enabled module tokenizer for cgi sapi
php_invoke: Enabled module pdo_mysql for cgi sapi
php_invoke: Enabled module sysvmsg for cgi sapi
php_invoke: Enabled module fileinfo for cgi sapi
php_invoke: Enabled module gettext for cgi sapi
php_invoke: Enabled module phar for cgi sapi
php_invoke: Enabled module iconv for cgi sapi
php_invoke: Enabled module mysqlnd for cgi sapi
php_invoke: Enabled module pdo for cgi sapi
php_invoke: Enabled module posix for cgi sapi
Настраивается пакет php-gd (1:7.2+6@ubuntu1) ...
Настраивается пакет php7.2-xmlrpc (7.2.24-0ubuntu0.18.04.1) ...

Creating config file /etc/php/7.2/mods-available/xmlrpc.ini with new version
Настраивается пакет php-cgi (1:7.2+6@ubuntu1) ...
Настраивается пакет php-xmlrpc (1:7.2+6@ubuntu1) ...
Обрабатываются триггеры для man-db (2.8.3-2ubuntu0.1) ...
Обрабатываются триггеры для libapache2-mod-php7.2 (7.2.24-0ubuntu0.18.04.1) ...
Обрабатываются триггеры для libc-bin (2.27-3ubuntu1) ...
usr@vb:~$ sudo ufw allow in 80/tcp
[sudo] пароль для usr:
Правила обновлены
Правила обновлены (v6)
usr@vb:~$ sudo touch /var/www/html/phpinfo.php
usr@vb:~$ sudo nano /var/www/html/phpinfo.php
usr@vb:~$ sudo nano /var/www/html/phpinfo.php
usr@vb:~$ sudo rm -rf /var/www/html/phpinfo.php
usr@vb:~$ 
usr@vb:~$ sudo echo '<?php phpinfo(); ?>' > /var/www/html/phpinfo.php
bash: /var/www/html/phpinfo.php: Отказано в доступе
usr@vb:~$ sudo {echo '<?php phpinfo(); ?>' > /var/www/html/phpinfo.php}
bash: /var/www/html/phpinfo.php: Отказано в доступе
usr@vb:~$ sudo nano /var/www/html/phpinfo.php
usr@vb:~$ sudo a2dismod {mpm_event,mpm_worker}
[sudo] пароль для usr:
Module mpm_event already disabled
Module mpm_worker already disabled
usr@vb:~$ sudo a2enmod {mpm_prefork,rewrite}
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
usr@vb:~$ 
```

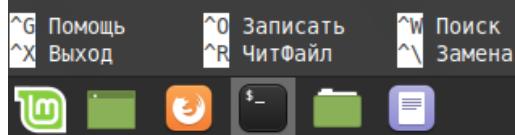
чтобы использовать файлы **htaccess** для настроек, нам необходимо в файле **/etc/apache2/apache2.conf** изменить значение **AllowOverride** с **None** на **All** для нужных директорий, к примеру, для **/var/www**:

```
sudo nano /etc/apache2/apache2.conf
```



```
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>

#<Directory /srv/>
#    Options Indexes FollowSymLinks
#    AllowOverride None
```



теперь необходимо перезапустить Apache2:

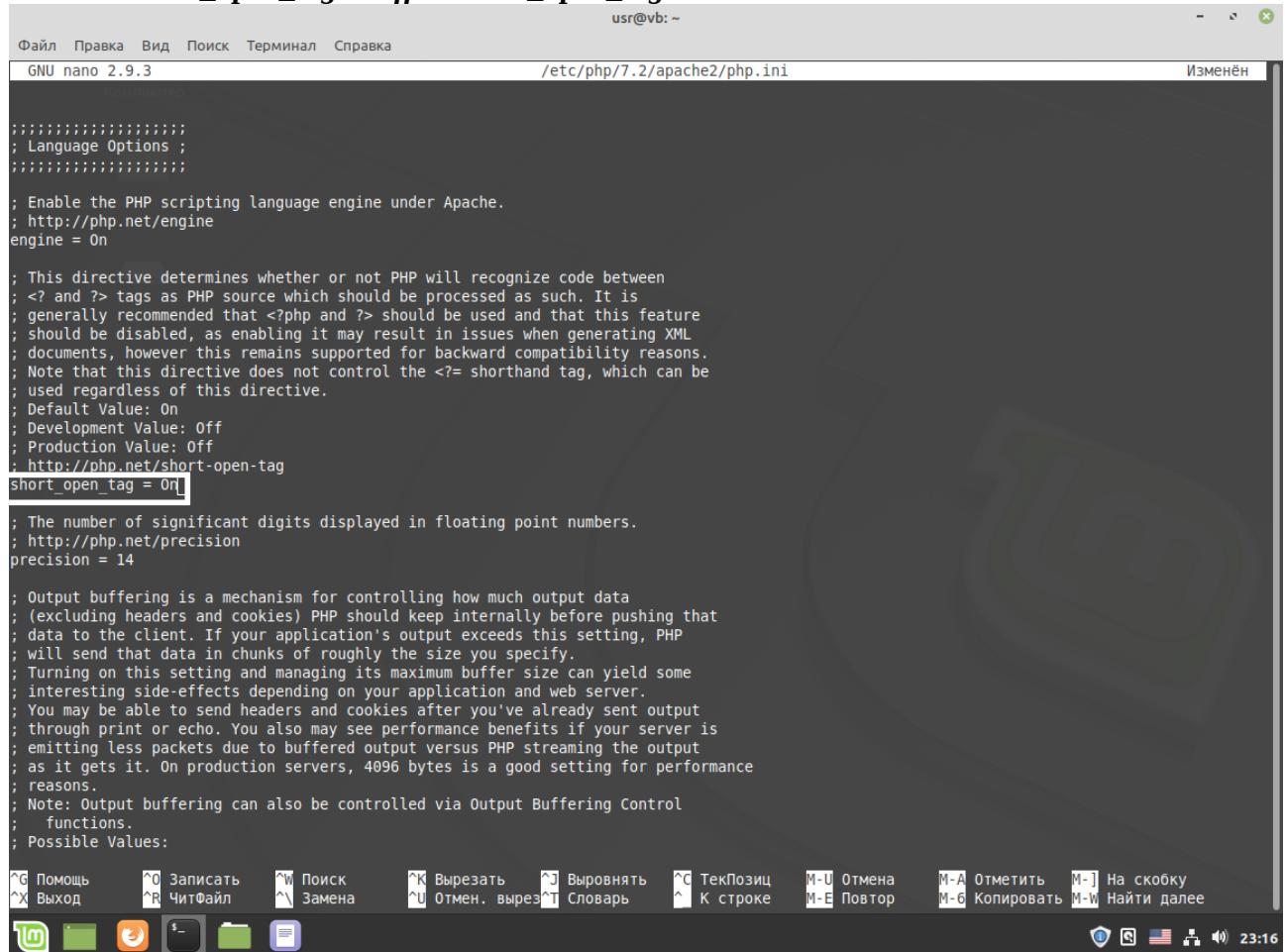
```
sudo systemctl restart apache2
```

Переходим к настройке PHP.

По-умолчанию, короткие теги, обрамляющие скрипты PHP, отключены; это может привести к тому, что некоторые скрипты, использующие эти теги, могут не выполняться. Выполним включение тегов в файле `php.ini`:

```
sudo nano /etc/php/7.2/apache2/php.ini
```

Заменим `short_open_tag = Off` на `short_open_tag = On`



```
usr@vb: ~
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.9.3           /etc/php/7.2/apache2/php.ini           Изменён
;;;;
;; Language Options ;;
;;;;
; Enable the PHP scripting language engine under Apache.
; http://php.net/engine
engine = On

; This directive determines whether or not PHP will recognize code between
; <? and ?> tags as PHP source which should be processed as such. It is
; generally recommended that <?php and ?> should be used and that this feature
; should be disabled, as enabling it may result in issues when generating XML
; documents, however this remains supported for backward compatibility reasons.
; Note that this directive does not control the <?= shorthand tag, which can be
; used regardless of this directive.
; Default Value: On
; Development Value: Off
; Production Value: Off
; http://php.net/short-open-tag
short_open_tag = On

; The number of significant digits displayed in floating point numbers.
; http://php.net/precision
precision = 14

; Output buffering is a mechanism for controlling how much output data
; (excluding headers and cookies) PHP should keep internally before pushing that
; data to the client. If your application's output exceeds this setting, PHP
; will send that data in chunks of roughly the size you specify.
; Turning on this setting and managing its maximum buffer size can yield some
; interesting side-effects depending on your application and web server.
; You may be able to send headers and cookies after you've already sent output
; through print or echo. You also may see performance benefits if your server is
; emitting less packets due to buffered output versus PHP streaming the output
; as it gets it. On production servers, 4096 bytes is a good setting for performance
; reasons.
; Note: Output buffering can also be controlled via Output Buffering Control
;       functions.
; Possible Values:
^G Помощь      ^O Записать      ^W Поиск      ^K Вырезать      ^J Выровнять      ^C ТекПозиц      M-U Отмена      M-A Отметить      M-] На скобку
^X Выход      ^R ЧитФайл      ^M Замена      ^U Отмен. вырез      ^T Словарь      ^L К строке      M-E Повтор      M-B Копировать      M-W Найти далее
[Icons] 23:16
```

Необходимо включить ошибки, вывод которых в PHP по-умолчанию тоже отключён.

```
error_reporting = E_ALL
display_errors = On
```

после внесения изменений перезапустим Apache2 командой:

```
sudo systemctl restart apache2
```

```
usr@vb: ~
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.9.3                               /etc/php/7.2/apache2/php.ini                                         Изменён
; E_CORE_WARNING    - warnings (non-fatal errors) that occur during PHP's
;                     initial startup
; E_COMPILE_ERROR   - fatal compile-time errors
; E_COMPILE_WARNING - compile-time warnings (non-fatal errors)
; E_USER_ERROR      - user-generated error message
; E_USER_WARNING    - user-generated warning message
; E_USER_NOTICE     - user-generated notice message
; E_DEPRECATED      - warn about code that will not work in future versions
;                     of PHP
; E_USER_DEPRECATED - user-generated deprecation warnings

; Common Values:
; E_ALL (Show all errors, warnings and notices including coding standards.)
; E_ALL & ~E_NOTICE (Show all errors, except for notices)
; E_ALL & ~E_NOTICE & ~E_STRICT (Show all errors, except for notices and coding standards warnings.)
; E_COMPILE_ERROR|E_RECOVERABLE_ERROR|E_CORE_ERROR (Show only errors)
; Default Value: E_ALL & ~E_NOTICE & ~E_STRICT & ~E_DEPRECATED
; Development Value: E_ALL
; Production Value: E_ALL & ~E_DEPRECATED & ~E_STRICT
; http://php.net/error-reporting
error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT
display_errors = On

; This directive controls whether or not and where PHP will output errors,
; notices and warnings too. Error output is very useful during development, but
; it could be very dangerous in production environments. Depending on the code
; which is triggering the error, sensitive information could potentially leak
; out of your application such as database usernames and passwords or worse.
; For production environments, we recommend logging errors rather than
; sending them to STDOUT.
; Possible Values:
; Off = Do not display any errors
; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)
; On or stdout = Display errors to STDOUT
; Default Value: On
; Development Value: On
; Production Value: Off
; http://php.net/display-errors
display_errors = Off

^C Помощь      ^O Записать      ^W Поиск      ^K Вырезать      ^J Выровнять      ^C ТекПозиц
^X Выход      ^R ЧитФайл      ^M Замена      ^U Отмен. вырез      ^T Словарь      M-U Отмена
^S К строке      M-E Повтор      M-A Отметить      M-[ На скобку
M-B Копировать      M-W Найти далее

```

Далее необходимо выполнить настройку **MariaDB**, для этого выполним команду

sudo mysql_secure_installation

И будем следовать инструкциям.

```
usr@vb: ~
Файл Правка Вид Поиск Терминал Справка
/usr@vb:~$ sudo mysql_secure_installation
[sudo] пароль для usr:

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
... skipping.

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
- Dropping test database...
... Success!
- Removing privileges on test database...
```

На этом процесс установки и настройки сервера LAMP считаю оконченным, можно перейти к рассмотрению **пункта 2**:

Настройка сайта с самоподписанным сертификатом

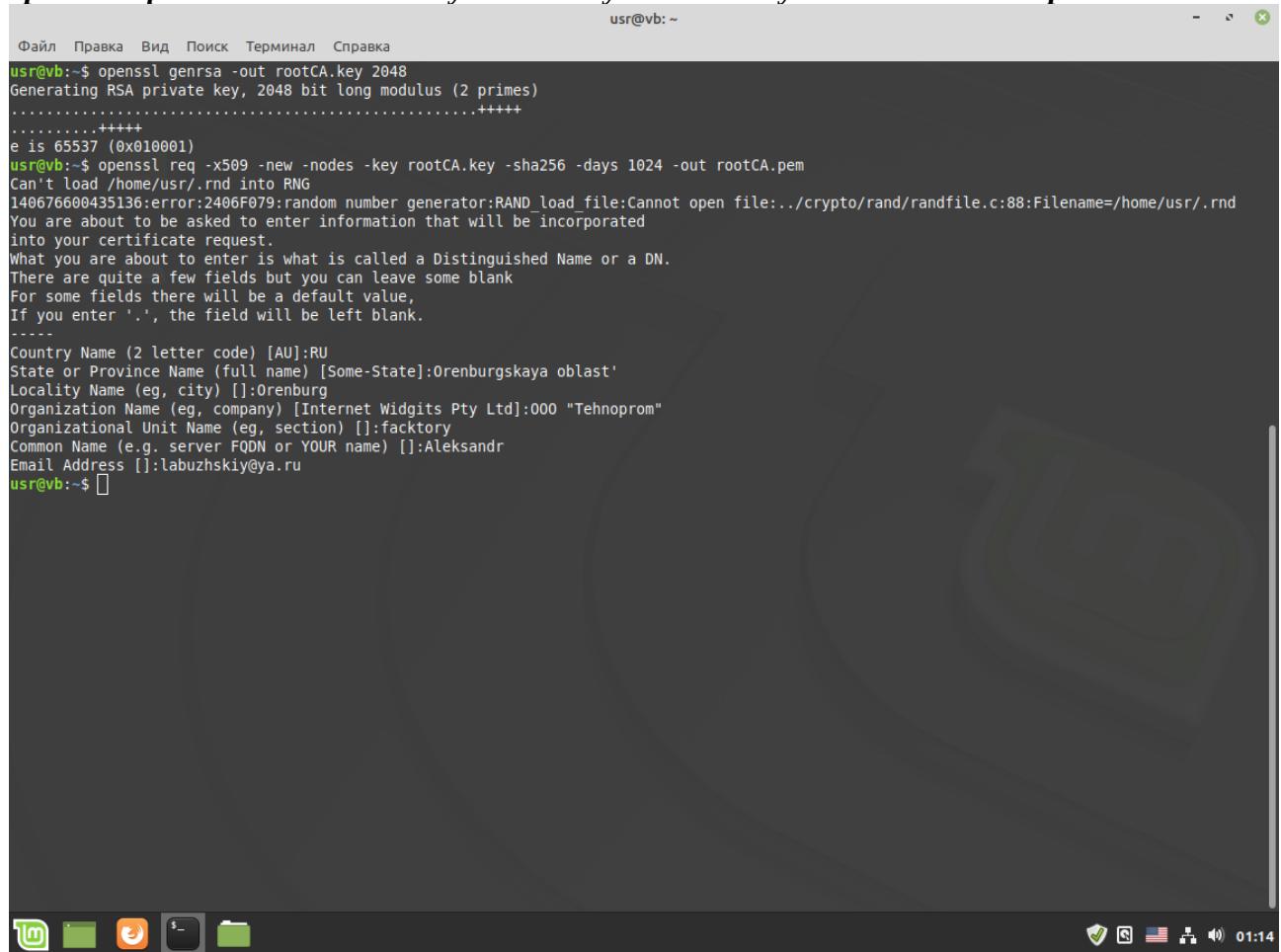
Чтобы выпустить сертификат для локального домена, нужен корневой сертификат. На его основе будут выпускаться все остальные сертификаты. Да, для каждого нового top level домена нужно выпускать свой сертификат. Получить корневой сертификат достаточно просто.

Сначала сформируем закрытый ключ:

```
openssl genrsa -out rootCA.key 2048
```

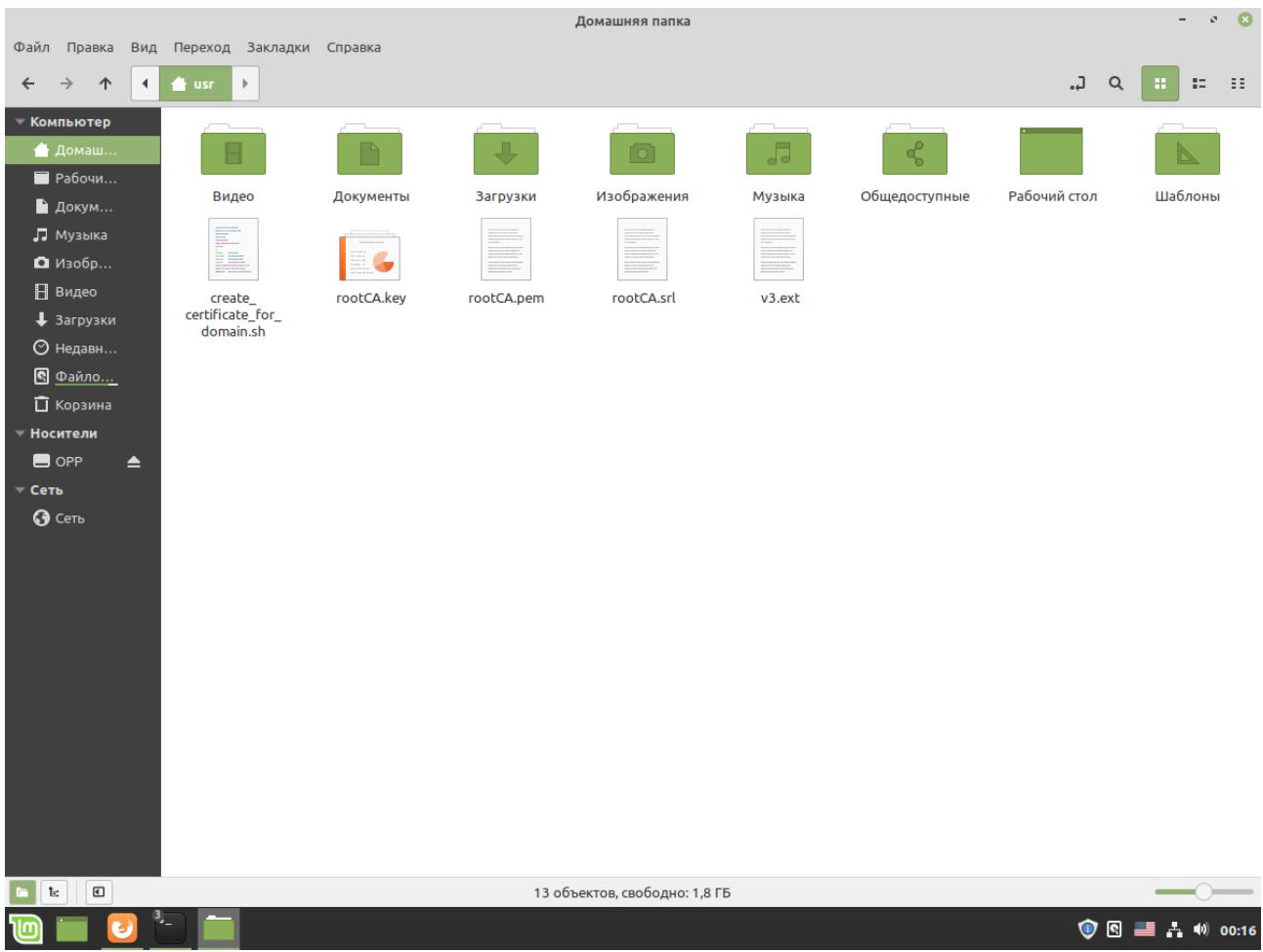
Затем сам сертификат:

```
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
```



```
usr@vb:~$ openssl genrsa -out rootCA.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
usr@vb:~$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
Can't load /home/usr/.rnd into RNG
140676600435136:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/home/usr/.rnd
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) [AU]:RU
State or Province Name (full name) [Some-State]:Orenburgskaya oblast'
Locality Name (eg, city) []:Orenburg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:000 "Tehnoprom"
Organizational Unit Name (eg, section) []:factory
Common Name (e.g. server FQDN or YOUR name) []:Aleksandr
Email Address []:labuzhskiy@ya.ru
usr@vb:~$
```

Нужно будет ввести страну, город, компанию и т.д. В результате получаем два файла: **rootCA.key** и **rootCA.pem** в домашней директории текущего пользователя. Здесь же и станем создавать основной **bash-скрипт**, автоматизирующий процедуру создания сертификатов пользователей, и вспомогательный файл **v3.ext**



Переходим к главному, выпуск самоподписанного сертификата. Нам понадобится вспомогательный конфигурационный файл. Оформим все это в виде bash скрипта, но перед этим составим вспомогательный файл v3.ext

```
root@vb: ~
GNU nano 2.9.3          ./v3.ext

authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = %DOMAIN%
DNS.2 = *.%DOMAIN%
```

И оформим необходимые нам шаги для получения сертификата пользователя в виде bash-скрипта с именем create_certificate_for_domain.sh

sudo nano ~/create_certificate_for_domain.sh

The screenshot shows a terminal window titled "create_certificate_for_domain.sh" with the following content:

```
usr@vb: ~
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.9.3                                         create_certificate_for_domain.sh
Изменён
if [ -z "$1" ]
then
    echo "Please supply a subdomain to create a certificate for";
    echo "e.g. mysite.localhost"
    exit;
fi
#device = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
#subjectAltName = @alt_names
#Создадим новый приватный ключ, если он не существует или будем использовать существующий:
if [ -f device.key ]; then
    KEY_OPT "-key"
else
    KEY_OPT "-keyout"
fi
#Запросим у пользователя название домена. Добавим возможность задания "общего имени" (оно используется при формировании сертификата):
DOMAIN $1
COMMON_NAME=${2:-$1}
#Чтобы не отвечать на вопросы в интерактивном режиме, сформируем строку с ответами. И зададим время действия сертификата:
SUBJECT="/C=CA/ST=None/L=NB/O=None/CN=$COMMON_NAME"
NUM_OF_DAYS 999
#Формируем csr файл (Certificate Signing Request) на основе ключа
openssl req -new -newkey rsa 2048 -sha256 -nodes $KEY_OPT device.key -subj "$SUBJECT" -out device.csr
#На основе вспомогательного файла v3.ext создаем временный файл с указанием нашего домена
cat v3.ext | sed s/%DOMAIN%/$COMMON_NAME/g > /tmp/_v3.ext
#Выпускаем сертификат
openssl x509 -req -in device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out device.crt -days $NUM_OF_DAYS -sha256 -extfile /tmp/_v3.ext
#Переименовываем сертификат и удаляем временный файл:
mv device.csr $DOMAIN.csr
cp device.crt $DOMAIN.crt
# remove temp file
rm -f device.csr;
```

The terminal window has a menu bar at the top with Russian labels: Файл, Правка, Вид, Поиск, Терминал, Справка. The title bar says "create_certificate_for_domain.sh". The status bar at the bottom shows keyboard shortcuts for various functions like Cut, Paste, Find, etc., and the current time "02:12".

Мы расположили скрипт в одной директории со сгенерированными выше корневыми сертификатами. После завершения оформления скрипта, запускаем его на выполнение с параметром имени, для примера tehnoprom.info:

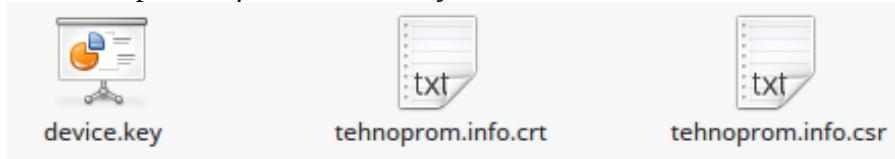
The screenshot shows a terminal window with the following session:

```
usr@vb:~$ ./create_certificate_for_domain.sh
Please supply a subdomain to create a certificate for
e.g. mysite.localhost
usr@vb:~$ ./create_certificate_for_domain.sh tehnoprom.info
Can't load /home/usr/.rnd into RNG
139789829296576:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/home/usr/.rnd
Generating an RSA private key
.....+++++
.....+++++
writing new private key to 'device.key'
-----
Signature ok
subject=C = CA, ST = None, L = NB, O = None, CN = tehnoprom.info
Getting CA Private Key
usr@vb:~$
```

The terminal window has a menu bar at the top with Russian labels: Файл, Правка, Вид, Поиск, Терминал, Справка. The title bar says "create_certificate_for_domain.sh". The status bar at the bottom shows keyboard shortcuts for various functions like Cut, Paste, Find, etc., and the current time "02:12".

После того, как скрипт отработал, в каталоге /home пользователя, рядом с корневым сертификатом появились дополнительные файлы сертификатов и ключей:

tehnoprom.info.crt, tehnoprom.info.csr, device.key



собирай эти файлы в отдельной директории (я назвал её *cert* и скопировал в */etc/apache2*).

Теперь нужно перейти к настройке apache2:

Для начала скопируем содержимое *000-default.conf* в *tehnoprom1.conf* и будем редактировать конечный получившийся файл, добавив в него пути до сертификата пользователя и файла ключа.

***cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/tehnoprom1.conf
sudo nano /etc/apache2/sites-available/tehnoprom1.conf***

```
Файл Правка Вид Поиск Терминал Справка
/etc/apache2/sites-enabled/tehnoprom1.info.conf 1482/1482 100%
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    #Index index.php index.html index.htm

    SSLCertificateFile /etc/apache2/cert/tehnoprom.info.crt
    SSLCertificateKeyFile /etc/apache2/cert/device.key

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

теперь отредактируем файл defaults-ssl.conf, добавив в него пути к сгенерированному нами корневому сертификату и путь размещения нашего веб-сайта:

root@vb: /etc/apache2/sites-available

GNU nano 2.9.3 /etc/apache2/sites-enabled/default-ssl.conf

```
<IfModule mod_ssl.c>
<VirtualHost default :443>
    ServerAdmin webmaster@localhost
        DocumentRoot /var/www/tehnoprom1.info
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        # SSL Engine Switch:
        # Enable/Disable SSL for this virtual host.
        SSLEngine on

        # A self-signed (snakeoil) certificate can be created by installing
        # the ssl-cert package. See
        # /usr/share/doc/apache2/README.Debian.gz for more info.
        # If both key and certificate are stored in the same file, only the
        # SSLCertificateFile directive is needed.
        SSLCertificateFile /home/usr/rootCA.pem
        SSLCertificateKeyFile /home/usr/rootCA.key

        # Server Certificate Chain:
        # Point SSLCertificateChainFile at a file containing the
        # concatenation of PEM encoded CA certificates which form the
        # certificate chain for the server certificate. Alternatively
        # the referenced file can be the same as SSLCertificateFile
        # when the CA certificates are directly appended to the server
        # certificate for convinience.
        #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

```

[Read 135 lines]

Файл Правка Вид Поиск Терминал Справка /etc/apache2/sites-available/tehnoprom1.conf 1910/1910 100%

Помощь Записать Поиск Вырезать Вывороть ТекПозиц Отмена Отметить На скобку Выход ЧитФайл Замена Отмен. вырез Словарь К строке Повтор Копировать Найти далее

mc [root@LM]:/etc/apache2/sites-available

Далее вернёмся в конфигурационный файл `/etc/apache2/sites-available/tehnoprom1.conf` и допишем в него следующий код, чтобы защитить наш веб-сайт:

mc [root@LM]:/etc/apache2/sites-available

File Edit View Search Terminal Help /etc/apache2/sites-available/tehnoprom1.conf 1910/1910 100%

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    #index index.php index.html index.htm

    SSLCertificateFile /etc/apache2/cert/tehnoprom.info.crt
    SSLCertificateKeyFile /etc/apache2/cert/device.key

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    ProxyPassMatch ^/(.*\.php)(/.*)$ unix:/run/php/php7.2-fpm.sock|fcgi://localhost/var/www/tehnoprom1.info
    <IfModule mod_header.c>
        Header always append X-Frame-Options SAMEORIGIN
        Header set X-Content-Type-Options nosniff
        Header set X-XSS-Protection "1; mode=block"
    </IfModule>
    <Directory /var/www/tehnoprom1.info>
        AllowOverride None
        Options +indexes +ExecCGI
        Order deny,allow
        Allow from all
    </Directory>
</VirtualHost>
```

vim: syntax=apache ts=4 sw=4 sts=4 sr noet 1 Помощь 2 Развёрн 3 Выход 4 Hex 5 Перейти 6 7 Поиск 8 Исходный 9 Формат 10 Выход

И чтобы он заработал, выполним следующие манипуляции:

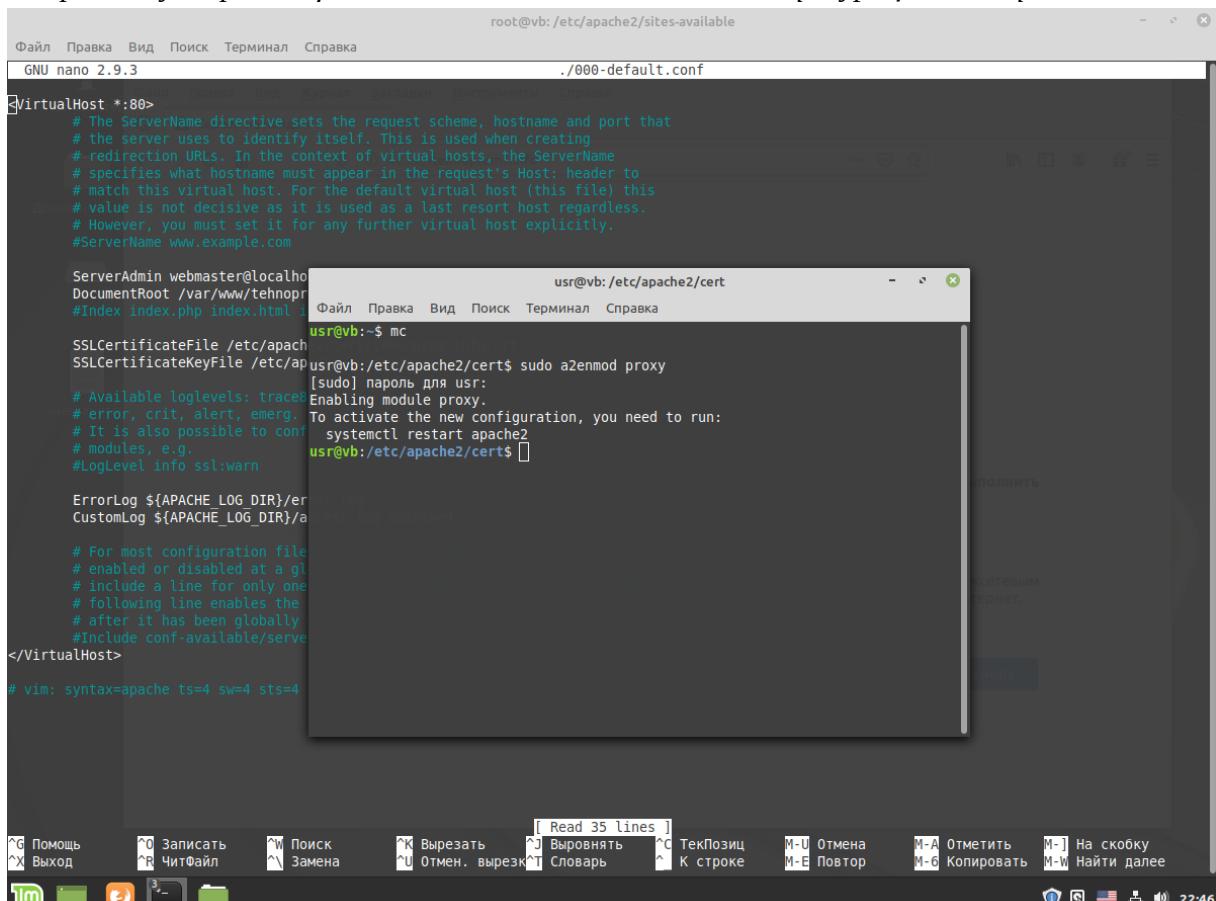
history:

.....

```
32 sudo a2enmod proxy
33 a2dissite 000-default.conf
34 a2ensite tehnoprom1.conf
35 systemctl reload apache2
36 a2ensite tehnoprom1.conf
```

.....

исправив путь размещения сайта во всех остальных конфигурационных файлах, и



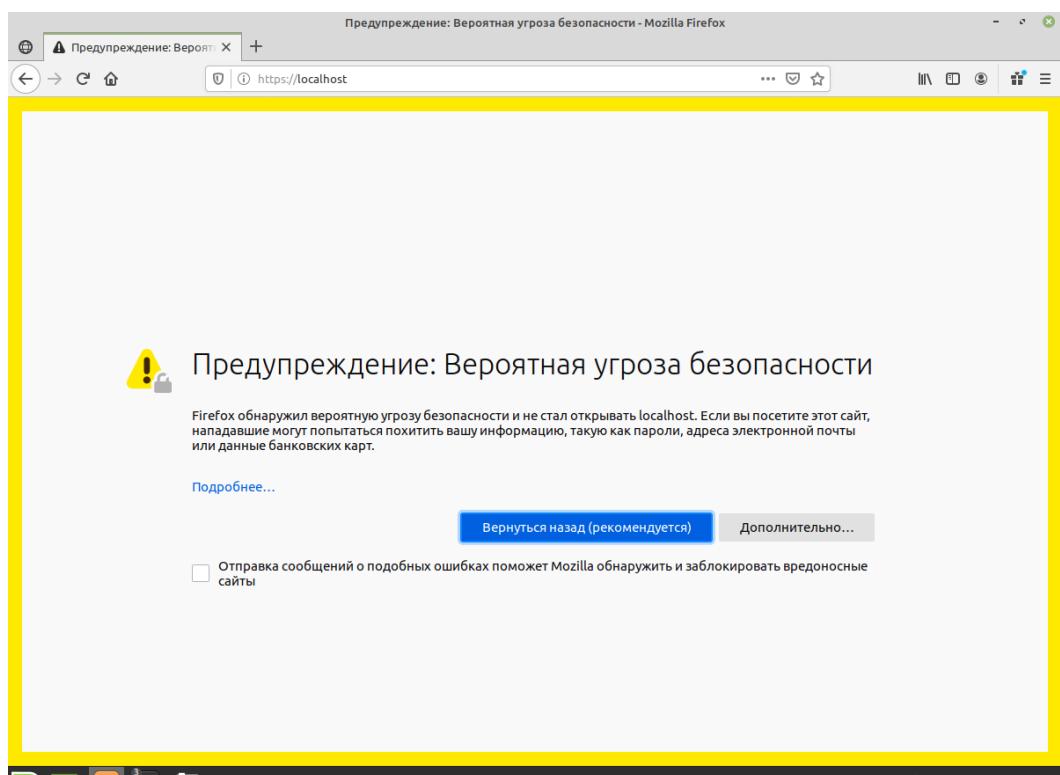
```
root@vb:/etc/apache2/sites-available
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.9.3 ./.000-default.conf
VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

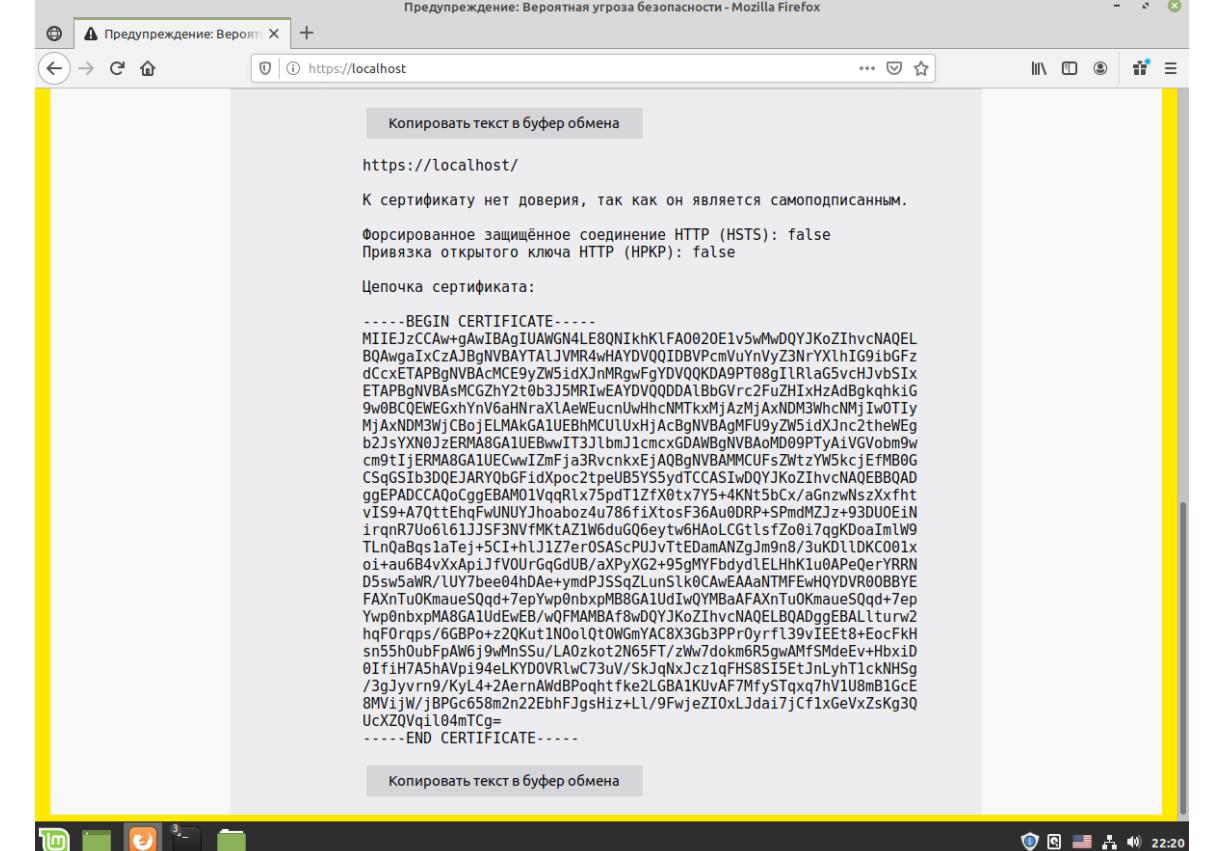
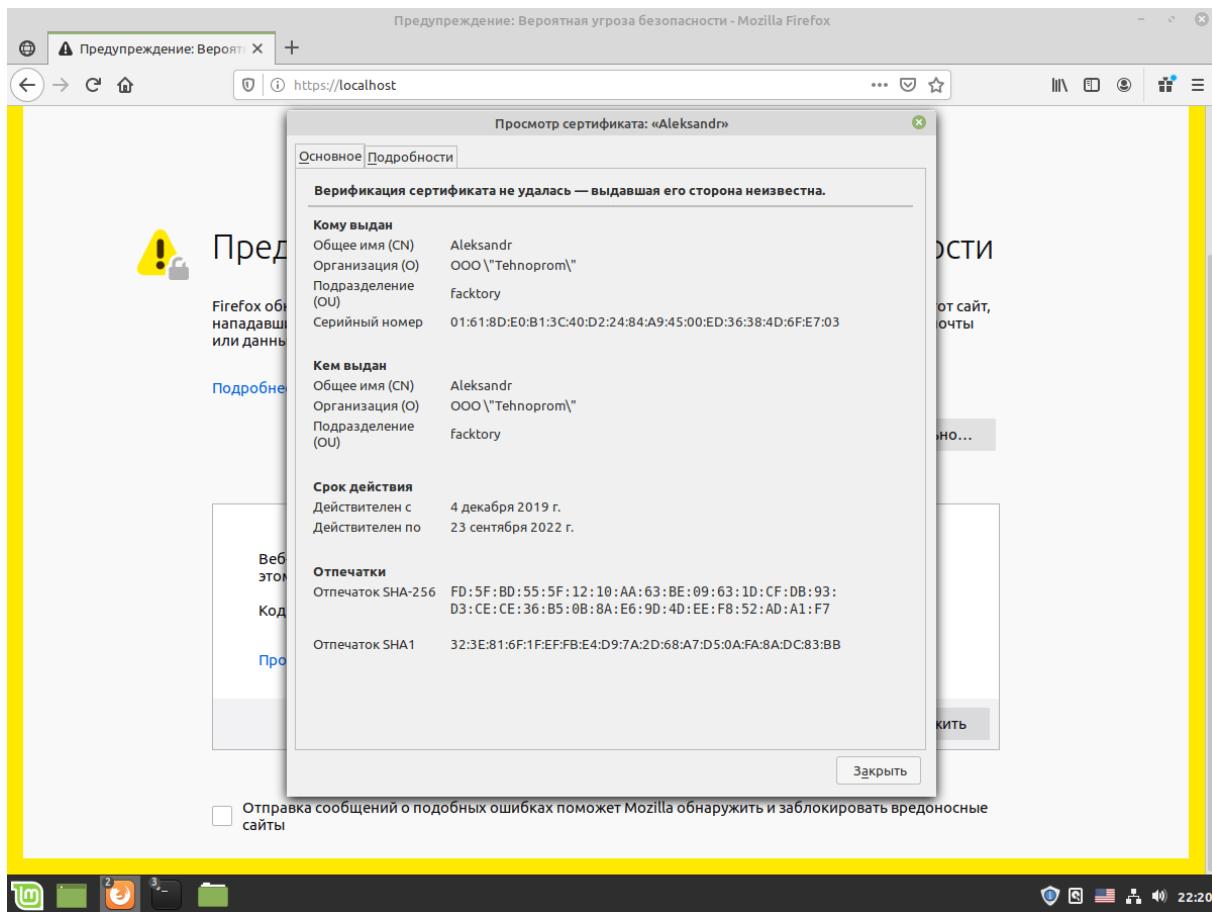
ServerAdmin webmaster@localhost
DocumentRoot /var/www/tehnopr
#Index index.php index.html i
SSLCertificateFile /etc/apache2/cert
SSLCertificateKeyFile /etc/apache2/cert$ sudo a2enmod proxy
[sudo] пароль для usr:
# Available loglevels: trace8|Enabling module proxy.
# error, crit, alert, emerg. To activate the new configuration, you need to run:
# It is also possible to config systemctl restart apache2
# modules, e.g.
#LogLevel info ssl:warn
LogLevel warn
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

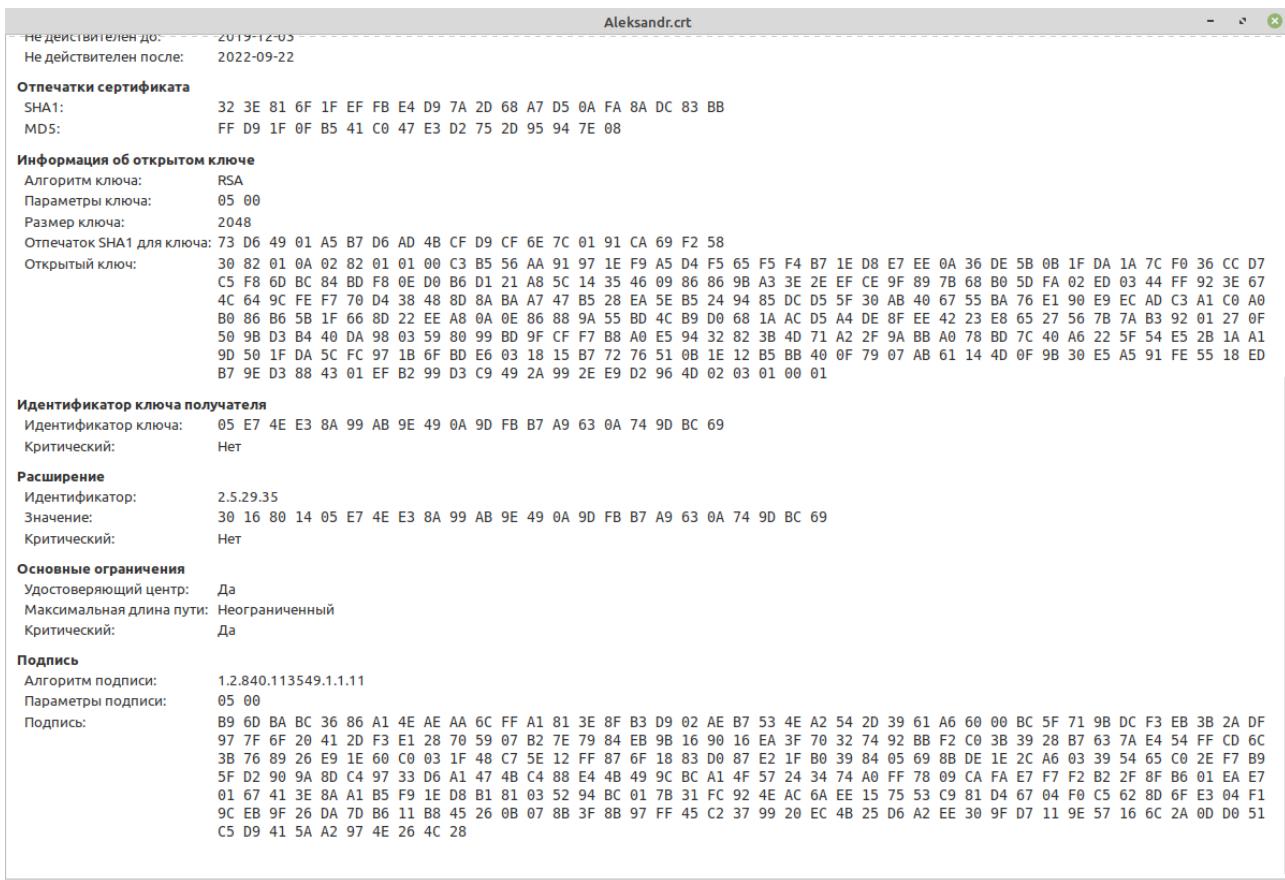
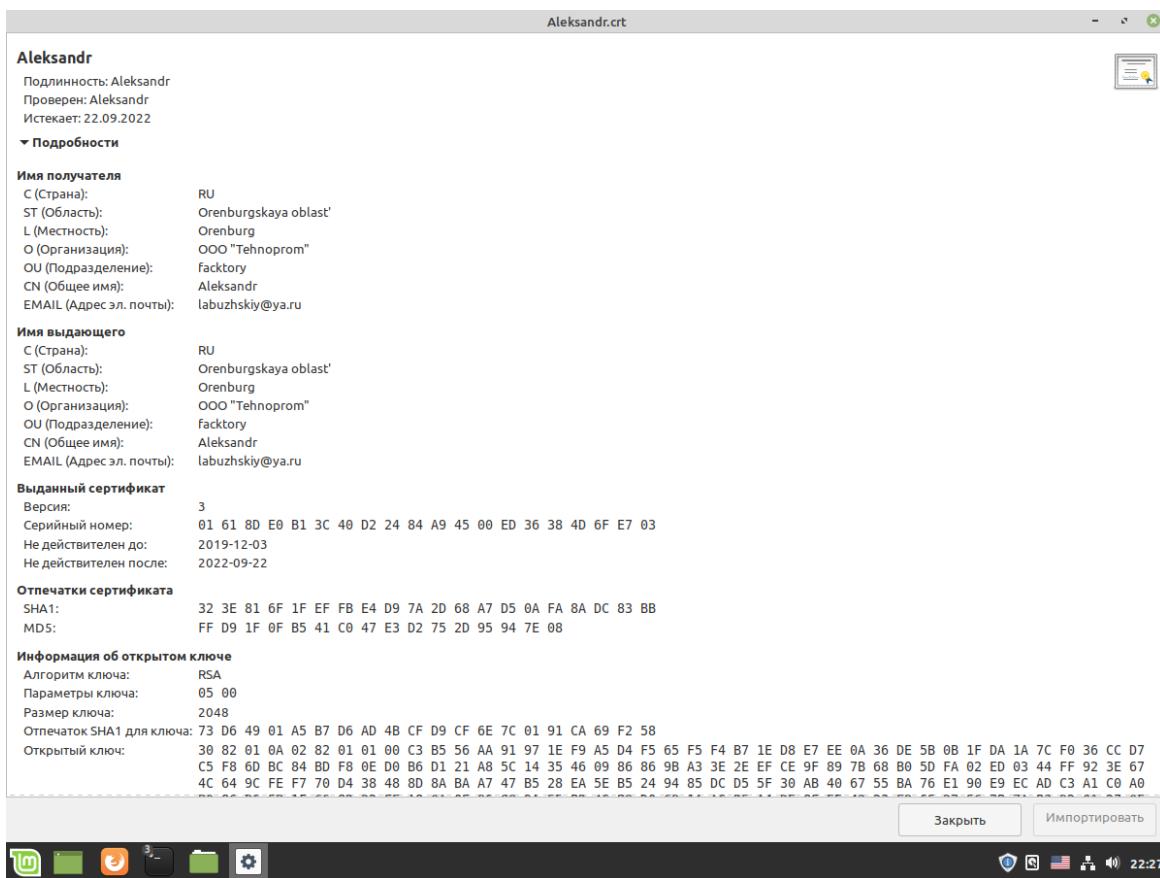
# For most configuration file
# enabled or disabled at a global
# include a line for only one
# following line enables the
# after it has been globally
#Include conf-available/serve
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4
```

перезапустив apache2, переходим в веб-браузере по адресу <https://localhost> и видим, что наш самоподписанный сертификат работает.







phpinfo() - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

phpinfo()

Главная / Технопром catalog2.pdf

https://127.0.0.1/phpinfo.php

PHP Version 7.2.24-Ubuntu0.18.04.1

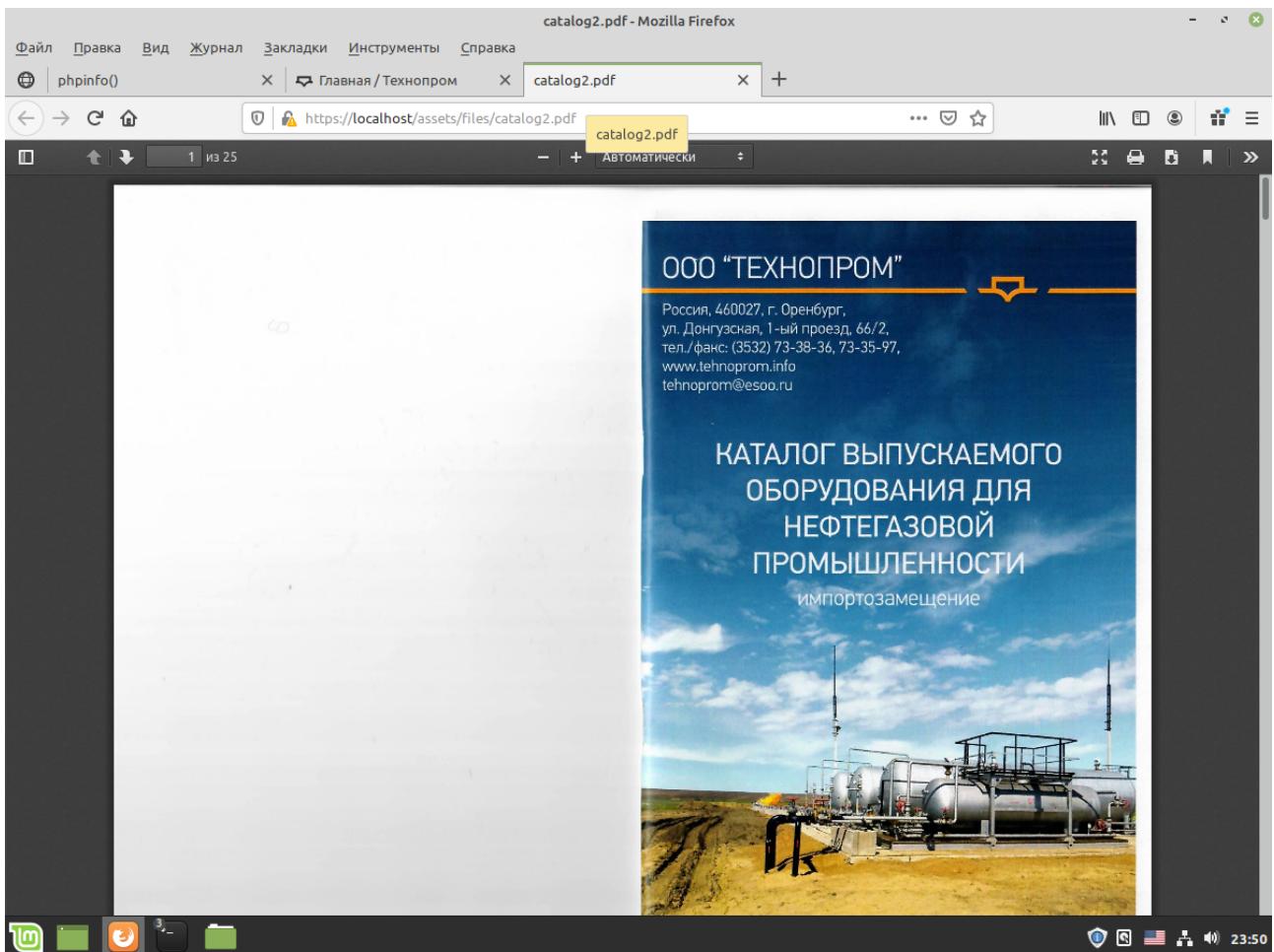


System	Linux vb 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26 12:20:02 UTC 2019 x86_64
Build Date	Oct 28 2019 12:07:07
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/15-xml.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-curl.ini, /etc/php/7.2/apache2/conf.d/20-dom.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gd.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mbstring.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-simplexml.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini, /etc/php/7.2/apache2/conf.d/20-wddx.ini, /etc/php/7.2/apache2/conf.d/20-xmireader.ini, /etc/php/7.2/apache2/conf.d/20-xsl.ini, /etc/php/7.2/apache2/conf.d/20-zip.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled

The screenshot shows the homepage of the Teploprom website. At the top, there's a navigation bar with links for 'Файл' (File), 'Правка' (Edit), 'Вид' (View), 'Журнал' (Journal), 'Закладки' (Bookmarks), 'Инструменты' (Tools), and 'Справка' (Help). The title bar says 'Главная / Технопром - Mozilla Firefox'. Below the navigation, there are two tabs: 'Главная / Технопром' and 'catalog2.pdf'. The main content area has six cards arranged in a grid:

- Каталог продукции**: An image of industrial equipment under a blue sky.
- Оставить заявку**: An image of a hand holding a tablet displaying a form.
- Свидетельства и сертификаты**: An image of a signed certificate or document.
- Нам доверяют**: An image of four business people shaking hands.
- Реализованные проекты**: An image of a yellow tape measure on a blueprint.
- Новости**: An image of a circular industrial structure with a blue box containing the word 'НОВОСТИ'.

At the bottom, there's a footer with several small logos and the text 'Наши партнеры' (Our partners).



На этом процедуре настройки сайта с самоподписаным сертификатом считаю завершённой, остаётся запросить подписание созданного нами самоподписанного сертификата в проверенном удостоверяющем центре сертификации. Копии архивов со сгенерированными файлами, а так же изменённые конфигурационные файлы Apache2 будут приложены к данной инструкции.

Примечание: проведении данной работы пользовался следующими источниками:
<https://losst.ru/ustanovka-lamp-ubuntu-18-04>

<https://habr.com/ru/post/352722/>