

Лабораторная работа №5

Расширенная настройка HTTP-сервера Apache

Андреева Софья Владимировна

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
4	Выводы	16
5	Контрольные вопросы	17

Список иллюстраций

3.1	Создание каталога private	6
3.2	Генерация ключа и сертификата	6
3.3	Наличие ключа в каталоге	7
3.4	Наличие сертификата в каталоге	8
3.5	Содержимое	9
3.6	Редактирование файла	10
3.7	Настройка межсетевого экрана на сервере	11
3.8	Сообщение о незащищенности на сайте	12
3.9	Содержание сертификата	12
3.10	Установка пакетов для работы с php	13
3.11	Права доступа и контекст безопасности в SELinux	13
3.12	Содержание сайта	14
3.13	Внесения изменений в настройки внутреннего окружения	14
3.14	Редактирование скрипта	15

1 Цель работы

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

2 Задание

1. Сгенерировать криптографический ключ и самоподписанный сертификат безопасности для возможности перехода веб-сервера от работы через протокол HTTP к работе через протокол HTTPS;
2. Настроить веб-сервер для работы с PHP;
3. Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке HTTP-сервера во внутреннем окружении виртуальной машины server.

(CSR);

- параметр `-nodes` указывает OpenSSL, что нужно пропустить шифрование сертификата SSL с использованием парольной фразы, т.е. позволить Apache читать файл без какого-либо вмешательства пользователя (без ввода пароля при попытке доступа к странице, в частности);
- параметр `-newkey rsa: 2048` указывает, что одновременно создаются новый ключ и новый сертификат, причём используется 2048-битный ключ RSA;
- параметр `-keyout` указывает, где хранить сгенерированный файл закрытого ключа при создании;
- параметр `-out` указывает, где разместить созданный сертификат SSL. Далее требуется заполнить сертификат:

Сгенерированные ключ и сертификат появились в соответствующем каталогах `/etc/ssl/private` и `/etc/ssl/certs`.

Левая панель	Файл	Команда	Настройки	Правая
< /etc/ssl/private .[^]>				
	Имя	Размер	Дата правки	
	/..	-BBERX-	сен 24 07:11	
	localhost.key	1704	сен 23 06:38	
	www.svandreeva.net.crt	1484	сен 24 06:59	
	www.svandreeva.net.key	1704	сен 24 06:58	

Рис. 3.3: Наличие ключа в каталоге

/etc/ssl/certs				.[^]>	
Имя	Размер	Дата	правки		
@f249de83.0	91	сен	4 17:55		
@f30dd6ad.0	88	сен	4 17:55		
@f387163d.0	71	сен	4 17:55		
@f39fc864.0	65	сен	4 17:55		
@f459871d.0	70	сен	4 17:55		
@f51bb24c.0	67	сен	4 17:55		
@f8fc53da.0	73	сен	4 17:55		
@fa5da96b.0	67	сен	4 17:55		
@fb5fa911.0	67	сен	4 17:55		
@fb717492.0	88	сен	4 17:55		
@fc5a8f99.0	88	сен	4 17:55		
@fd08c599.0	67	сен	4 17:55		
@fd64f3fc.0	67	сен	4 17:55		
@fde84897.0	59	сен	4 17:55		
@fe8a2cd8.0	66	сен	4 17:55		
@feffd413.0	70	сен	4 17:55		
@ff34af3f.0	96	сен	4 17:55		
@ffa7f1eb.0	71	сен	4 17:55		
localhost.crt	3932	сен	23 06:38		
www.svandreeva.net.crt	1485	сен	24 07:11		
www.svandreeva.net.crt					

Рис. 3.4: Наличие сертификата в каталоге


```
--/etc/ssl/private/www.svandreeva.net.crt
-----BEGIN CERTIFICATE-----
MIIEGzCCAwwOgAwIBAgIUD6bVxB0jjsqn0ym4w1efumHLVy14wDQYJKoZIhvcNAQEL
BQAwgZwwCzAJBgNVBAYTA1JVMQ8wDQYDVQQIDAZScXNzXWExZDZANBgNVBACMBk1v
c2NvdzETMBEGA1UECgwKc3ZhbmRyZWV2Y2ETMBEGA1UECwwKc3ZhbmRyZWV2Y2EX
MBUAGA1UEAwwOc3ZhbmRyZWV2Y2YS5uZXQxKDAMBgkqhkiG9w0BCQEWEQXN2YW5kcmVl
dmFAC3ZhbmRyZWV2Y2YS5uZXQwHhcNMjU0OTI0MDY1OTU1WbcNMjU0MDY1OTU1
WjCBNDLMkAkgA1UEBHMCLUx0ZDZANBgNVBAgMBG1lc3NpY2ETPMAGGA1UEBwwGTW9z
Y293MRMwEQYDVQQKDApzdmdFuZHZJLXZlXHMwEQYDVQQKDApzdmdFuZHZJLXZlXHMrcw
FQYDVQQDDA5zdmdFuZHZJLXZlXHM5ldDEoMCYGCSCGSIb3B0QDEJARYZc3ZhbmRyZWV2
YUBzdmdFuZHZJLXZlXHM5ldDCCASiWdQYJKoZIhvcNAQEBBQADgGEPADCCAQoCggEB
ANiEWkELCZt3r4UNgNZN89eyaxSHCNsm00kIRXPKPiFRZi31fwSNeuFCY1DrLQ
Mn5m7SN+Aw96enu3wiXNMd1iYgUN8X4KYUnuuVchoZ84w34z6QBvY21BCj0MQ8e6
DrqQIT9DeQ1F2vqqBm1Ai9VX4SAfZa6fvWh+SfY/qz00IQBDxehR6GhSjXp4S2f
+HqN0q8NBcBk9rJcNIAGEJoAwNgblUav3NHefk6sBZZCad/smNH6qI6vZk2r
WztthtQG0Z26tCkuQb3ty6wif8RAqQNBa8QmBJhw2138HFahwCX5s48G+OwwE907mpf
ya0HwMWNjqtQH/5QipKV38CAwEAANtmFEwHQYDVR00BBYEFi+LBYrO30EuZWZ/
r5GcQEo4wqSxMB8GA1UdIwQYMBaAFi+LBYrO30EuZWZ/r5GcQEo4wqSxMA8GA1Ud
EwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAGlNcb3plKtv8RjE3SjgCGcD
SGdHEt9vDiyAcgt/or7Lqqi/F7G010C4nfwpj8Ia1nKEJSHZml7KctmYZUzpzp1RX
VSYw1sIUNthoLgA93+idLzYm3WMHPwItW22RWgTmXsyMPtmdpdku7joKV5jZgMDK3
GfY8zHy/R9gEa9Qhm2os0n7wyvsfUW3g/ufocj+/PpnH4uTRpqjJ7gP1qY4iRjBI
fVPIsytjndST/YKLvjVxZx3/Lh6FMu3gYHmfAPTq6nutcNKKMYXhX9LRNismNPN
bvReOxp4L6XBIMSyECY+3RrJzcK2w+0TMVWDCAfq5S26dU8LQu9BopgJ/hu9MI=
-----END CERTIFICATE-----
```

Рис. 3.5: Содержимое

Для перехода веб-сервера `www.svandreeva.net` на функционирование через протокол HTTPS требуется изменить его конфигурационный файл. Перейдем в каталог с конфигурационными файлами: `cd /etc/httpd/conf.d`

Откроем на редактирование файл `/etc/httpd/conf.d/www.svandreeva.net.conf` и заменим его содержимое на следующее:

```
<VirtualHost *:80>
```

ServerAdmin webmaster@svandreeva.net

```
DocumentRoot /var/www/html/www.svandreeva.net
```

ServerName www.svandreeva.net

ServerAlias www.svandreeva.net

```
ErrorLog logs/www.svandreeva.net-error_log
```

```
CustomLog logs/www.svandreeva.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@svandreeva.net
    DocumentRoot /var/www/html/www.svandreeva.net
    ServerName www.svandreeva.net
    ServerAlias www.svandreeva.net
    ErrorLog logs/www.svandreeva.net-error_log
    CustomLog logs/www.svandreeva.net-access_log common
    SSLCertificateFile /etc/ssl/certs/www.svandreeva.net.crt
    SSLCertificateKeyFile /etc/ssl/private/www.svandreeva.net.key
</VirtualHost>
</IfModule>

```



```

root@server:/etc/httpd/c
<VirtualHost *:80>
    ServerAdmin webmaster@svandreeva.net
    DocumentRoot /var/www/html/www.svandreeva.net
    ServerName www.svandreeva.net
    ServerAlias www.svandreeva.net
    ErrorLog logs/www.svandreeva.net-error_log
    CustomLog logs/www.svandreeva.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@svandreeva.net
    DocumentRoot /var/www/html/www.svandreeva.net
    ServerName www.svandreeva.net
    ServerAlias www.svandreeva.net
    ErrorLog logs/www.svandreeva.net-error_log
    CustomLog logs/www.svandreeva.net-access_log common
    SSLCertificateFile /etc/ssl/certs/www.svandreeva.net.crt
    SSLCertificateKeyFile /etc/ssl/private/www.svandreeva.net.key
</VirtualHost>
</IfModule>

```

Рис. 3.6: Редактирование файла

Внесем изменения в настройки межсетевого экрана на сервере, разрешив ра-

боту с https. Перезапустим веб-сервер, исправив синтаксические ошибки, допущенные при редактировании файла: `systemctl restart httpd`.

```
[root@server.svandreeva.net conf.d]# firewall-cmd --add-service=https
success
[root@server.svandreeva.net conf.d]# firewall-cmd --add-service=https --permanent
success
[root@server.svandreeva.net conf.d]# firewall-cmd --reload
success
[root@server.svandreeva.net conf.d]# systemctl restart httpd
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for details.
[root@server.svandreeva.net conf.d]# systemctl status httpd.service
* httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: failed (Result: exit-code) since Wed 2025-09-24 07:07:52 UTC; 25s ago
     Duration: 19min 4.392s
   Invocation: c6ea259999ee4715aa4e24046ed97f8d
     Docs: man:httpd.service(8)
   Process: 11473 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited, status=1/FAILURE)
   Main PID: 11473 (code=exited, status=1/FAILURE)
   Status: "Reading configuration..."
   Memory peak: 3.4M
   CPU: 84ms

сен 24 07:07:51 server.svandreeva.net systemd[1]: Starting httpd.service - The Apache HTTP Server...
сен 24 07:07:52 server.svandreeva.net (httpd)[11473]: httpd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
сен 24 07:07:52 server.svandreeva.net httpd[11473]: AH00526: Syntax error on line 22 of /etc/httpd/conf.d/www.svandreeva.net.conf:
сен 24 07:07:52 server.svandreeva.net httpd[11473]: SSLCertificateFile: file '/etc/ssl/certs/www.svandreeva.net.crt' does not exist or is empty
сен 24 07:07:52 server.svandreeva.net systemd[1]: httpd.service: Main process exited, code=exited, status=1/FAILURE
сен 24 07:07:52 server.svandreeva.net systemd[1]: httpd.service: Failed with result 'exit-code'.
сен 24 07:07:52 server.svandreeva.net systemd[1]: Failed to start httpd.service - The Apache HTTP Server.
[root@server.svandreeva.net conf.d]# nano /etc/ssl/certs/www.svandreeva.net.crt
[root@server.svandreeva.net conf.d]# cp /etc/ssl/private/www.svandreeva.net.crt /etc/ssl/cert/
cp: cannot stat '/etc/ssl/cert/': Это не каталог
[root@server.svandreeva.net conf.d]# cp /etc/ssl/private/www.svandreeva.net.crt /etc/ssl/cert/
cp: cannot stat '/etc/ssl/private/www.svandreeva.net.crt': Это не каталог
[root@server.svandreeva.net conf.d]# nano /etc/ssl/cert/
[root@server.svandreeva.net conf.d]# vim /etc/ssl/cert/
[root@server.svandreeva.net conf.d]# vim /etc/ssl/certs/www.svandreeva.net.crt
[root@server.svandreeva.net conf.d]# systemctl restart httpd
```

Рис. 3.7: Настройка межсетевого экрана на сервере

На виртуальной машине client в строке браузера введем название веб-сервера `www.user.net` и убедимся, что произойдёт автоматическое переключение на работу по протоколу HTTPS. На открывшейся странице с сообщением о незащищённости соединения нажмем кнопку «Дополнительно», затем добавим адрес сервера в постоянные исключения. Затем просмотрим содержание сертификата.

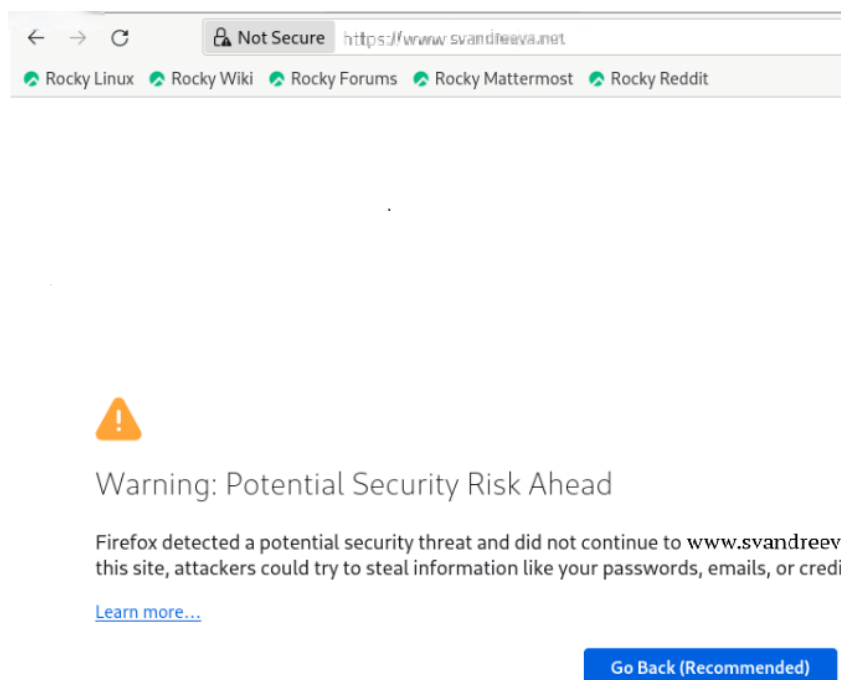


Рис. 3.8: Сообщение о незащищенности на сайте

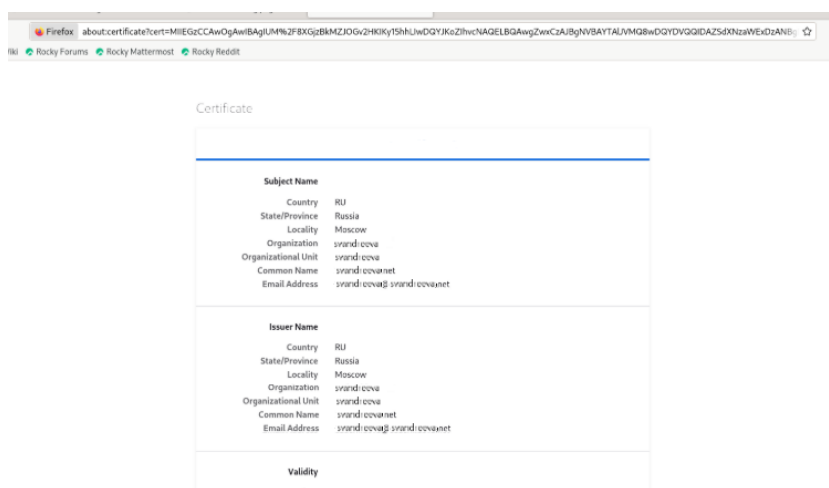


Рис. 3.9: Содержание сертификата

Конфигурирование HTTP-сервера для работы с PHP

Установим пакеты для работы с PHP: `dnf -y install php`

```

Total download size: 8.3 M
Installed size: 50 M
Downloading Packages:
(1/10): php-8.3.19-1.el10_0.x86_64.rpm                                43 kB/s | 11 kB  00:00
(2/10): nginxfilesystem-1.26.3-1.el10.noarch.rpm                    39 kB/s | 11 kB  00:00
(3/10): capstone-5.0.1-6.el10.x86_64.rpm                           1.7 MB/s | 1.9 MB  00:00
(4/10): php-common-8.3.19-1.el10_0.x86_64.rpm                      880 kB/s | 713 kB  00:00
(5/10): php-cli-8.3.19-1.el10_0.x86_64.rpm                         3.9 MB/s | 7.6 MB  00:00
(6/10): php-fpm-8.3.19-1.el10_0.x86_64.rpm                         2.2 MB/s | 1.9 MB  00:00
(7/10): php-mbstring-8.3.19-1.el10_0.x86_64.rpm                   1.3 MB/s | 571 kB  00:00
(8/10): php-opcache-8.3.19-1.el10_0.x86_64.rpm                     1.0 MB/s | 357 kB  00:00
(9/10): php-pdo-8.3.19-1.el10_0.x86_64.rpm                         644 kB/s | 88 kB  00:00
(10/10): php-xsl-8.3.19-1.el10_0.x86_64.rpm                       1.3 MB/s | 149 kB  00:00
-----
Total: 4.2 MB/s | 6.3 MB  00:01

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : php-common-8.3.19-1.el10_0.x86_64                1/1
  Installing     : php-cli-8.3.19-1.el10_0.x86_64                  1/14
  Installing     : php-mbstring-8.3.19-1.el10_0.x86_64              2/14
  Installing     : php-pdo-8.3.19-1.el10_0.x86_64                  3/14
  Installing     : php-xsl-8.3.19-1.el10_0.x86_64                  4/14
  Installing     : php-xml-8.3.19-1.el10_0.x86_64                   5/14
  Running scriptlet: nginxfilesystem-2:1.26.3-1.el10.noarch        6/14
  Installing     : nginxfilesystem-2:1.26.3-1.el10.noarch          6/14
  Installing     : php-fpm-8.3.19-1.el10_0.x86_64                  7/14
  Running scriptlet: php-fpm-8.3.19-1.el10_0.x86_64                 7/14
  Installing     : capstone-5.0.1-6.el10.x86_64                    8/14
  Installing     : php-opcache-8.3.19-1.el10_0.x86_64              9/14
  Installing     : php-8.3.19-1.el10_0.x86_64                     10/14
  Running scriptlet: php-8.3.19-1.el10_0.x86_64                     10/14

Installed:
capstone-5.0.1-6.el10.x86_64      nginxfilesystem-2:1.26.3-1.el10.noarch      php-8.3.19-1.el10_0.x86_64      php-cli-8.3.19-1.el10_0.x86_64
php-common-8.3.19-1.el10_0.x86_64  php-fpm-8.3.19-1.el10_0.x86_64             php-mbstring-8.3.19-1.el10_0.x86_64  php-opcache-8.3.19-1.el10_0.x86_64
php-pdo-8.3.19-1.el10_0.x86_64     php-xml-8.3.19-1.el10_0.x86_64

Complete!
[root@server svandreeva.net ~]# cd /var/www/html/www.svandreeva.net

```

Рис. 3.10: Установка пакетов для работы с php

В каталоге `/var/www/html/www.svandreeva.net` заменим файл `index.html` на `index.php` следующего содержания:

```

<?php
phpinfo();
?>

```

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

Восстановим контекст безопасности в SELinux:

```

restorecon -vR /etc
restorecon -vR /var/www

```

Перезапустим HTTP-сервер: `systemctl restart httpd`

```

[root@server svandreeva.net www.svandreeva.net]# vim index.php
[root@server svandreeva.net www.svandreeva.net]# chown -R apache:apache /var/www
[root@server svandreeva.net www.svandreeva.net]# restorecon -vR /etc
[root@server svandreeva.net www.svandreeva.net]# restorecon -vR /var/www
bash: restorecon: команда не найдена...
[root@server svandreeva.net www.svandreeva.net]# restorecon -vR /var/www
[root@server svandreeva.net www.svandreeva.net]# systemctl restart httpd
[root@server svandreeva.net www.svandreeva.net]#

```

Рис. 3.11: Права доступа и контекст безопасности в SELinux

На виртуальной машине client в строке браузера введем название веб-сервера `www.svandreeva.net` и убедимся, что будет выведена страница с информацией об используемой на веб-сервере версии PHP.

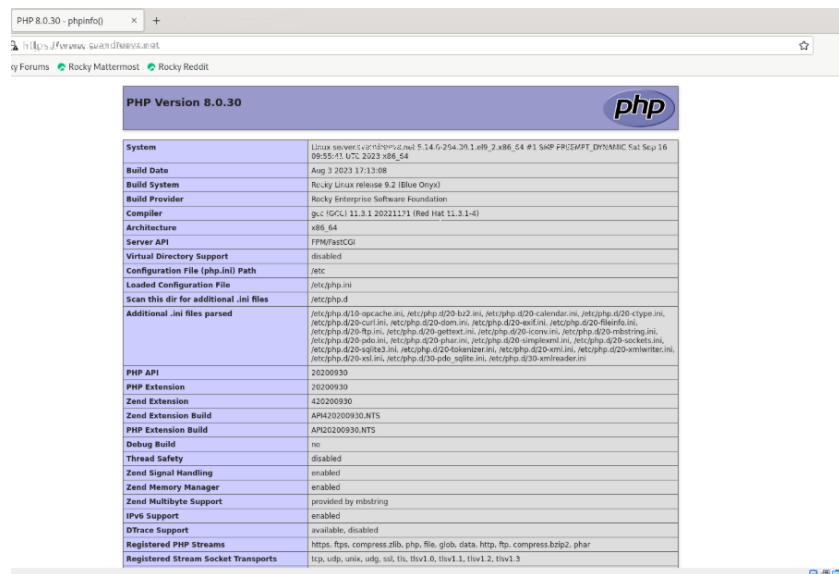


Рис. 3.12: Содержание сайта

Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/http` и в соответствующие каталоги скопируйте конфигурационные файлы:



Рис. 3.13: Внесения изменений в настройки внутреннего окружения

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

c https.



```
root@server:~ - sudo -i
#!/bin/bash
#
echo "Provisioning script $0"

echo "Install needed packages"
dnf -y groupinstall "Basic Web Server"

echo "Copy configuration files"
cp -R /vagrant/provision/server/http/etc/httpd/* /etc/httpd
cp -R /vagrant/provision/server/http/var/www/* /var/www
cp -R /vagrant/provision/server/http/etc/tls/* /etc/tls

chown -R apache:apache /var/www

restorecon -vR /etc
restorecon -vR /var/www

echo "Configure firewall"
firewall-cmd --add-service=http
firewall-cmd --add-service=http --permanent
echo "Start http service"
systemctl enable httpd
systemctl start httpd
~
~
```

Рис. 3.14: Редактирование скрипта

4 Выводы

в процессе выполнения данной лабораторной работы я приобрела практические навыки по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования PHP.

5 Контрольные вопросы

1. В чём отличие HTTP от HTTPS?

Отличие состоит в том, что HTTPS — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.

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

Улучшение безопасности при использовании HTTPS вместо HTTP достигается за счёт использования криптографических протоколов при организации HTTP-соединения и передачи по нему данных. Для шифрования может применяться протокол SSL (Secure Sockets Layer) или протокол TLS (Transport Layer Security). Оба протокола используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

3. Что такое сертификационный центр? Приведите пример.

Сертификационный центр (Certification authority, CA) представляет собой компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей.

Пример: IdenTrust, DigiCert.