Отчёт по лабораторной работе №5

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

Запускаем ВМ через рабочий каталог. На ВМ server входим под собственным пользователем и переходим в режим суперпользователя. В каталоге /etc/ssl создаем каталог private (рис. 1):

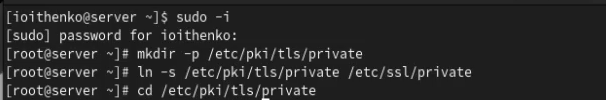


Рис. 1: создание каталога

Генерируем ключ и сертификат (рис. 2), введя следующую команду: openssl req -x509 -nodes -newkey rsa:2048 -keyout www.ioithenko.net.key -out www.ioithenko.net.crt

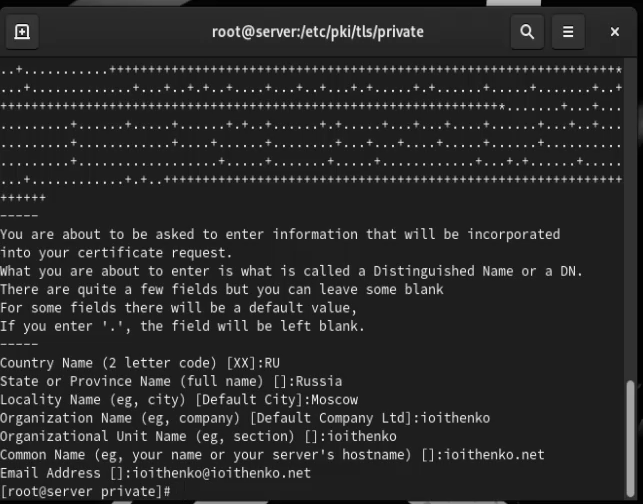


Рис. 2: Заполнение сертификата

Сгенерированные ключ и сертификат появляются в соответствующем каталоге /etc/ssl/private. Копируем сертификат в каталог /etc/ssl/certs (рис. 3)

Содержимое каталогов /etc/ssl/private и /etc/ssl/certs

Рис. 3: Содержимое каталогов /etc/ssl/private и /etc/ssl/certs

Редактируем конфигурационный файл /etc/httpd/conf.d/www.ioithenko.net (рис. 4)

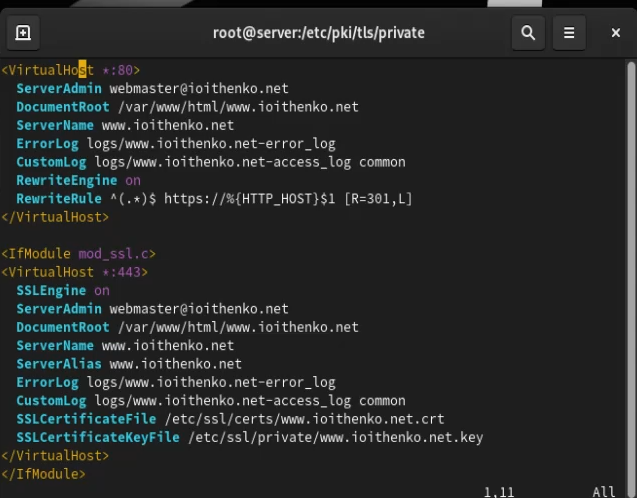


Рис. 4: Редактирование файла /etc/httpd/conf.d/www.ioithenko.net

Вносим изменения в настройки межсетевого экрана на сервере, перезапускаем веб-сервер (рис. 5)

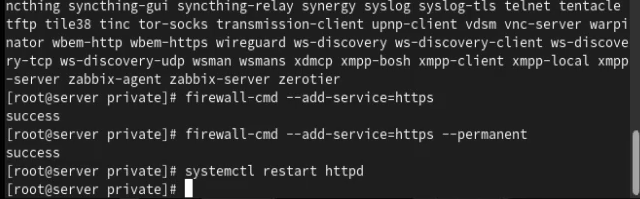


Рис. 5: Внесение изменений в настройки межсетевого экрана, перезапуск веб-сервера

На ВМ client открываем в браузере страницу www.ioithenko.net с сообщением о незащищенности соединения (рис. 6). Добавив страницу в исключения, просматриваем информацию о сертификате (рис. 7), (рис. 8).

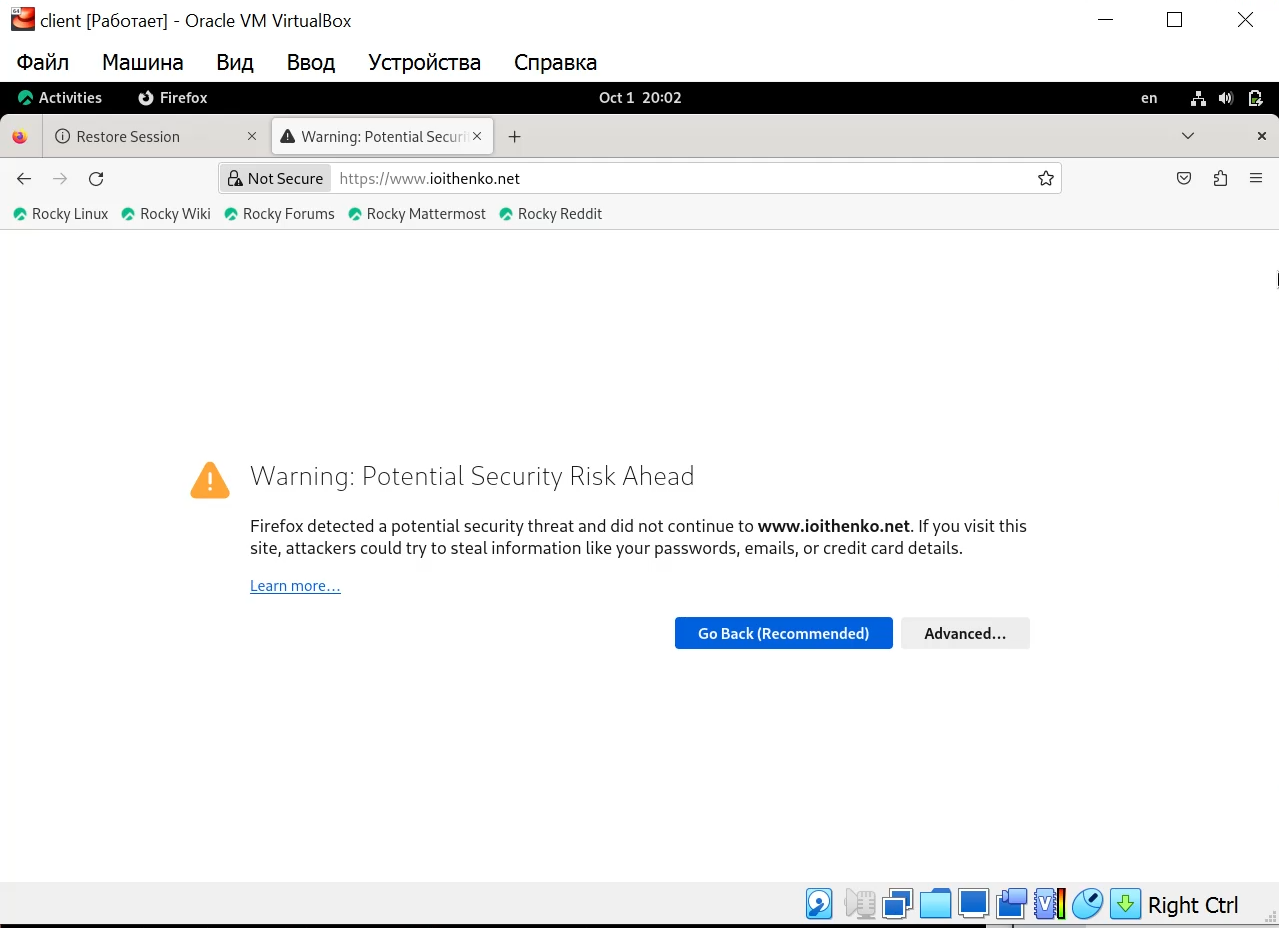


Рис. 6: Сообщение о незащищенности соединения

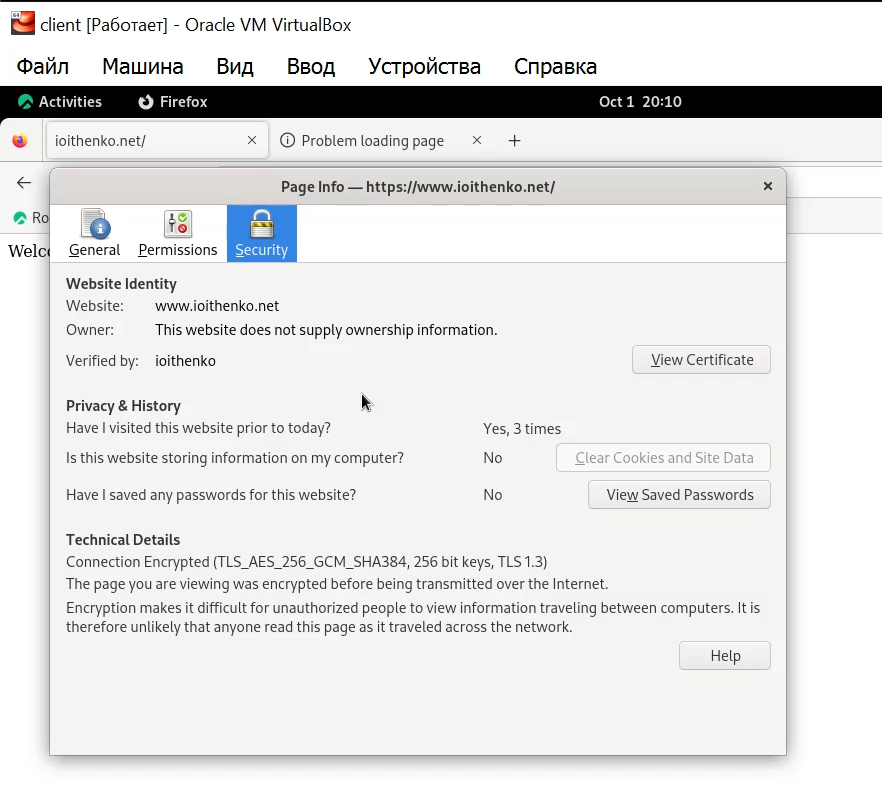


Рис. 7: Информация о веб-странице

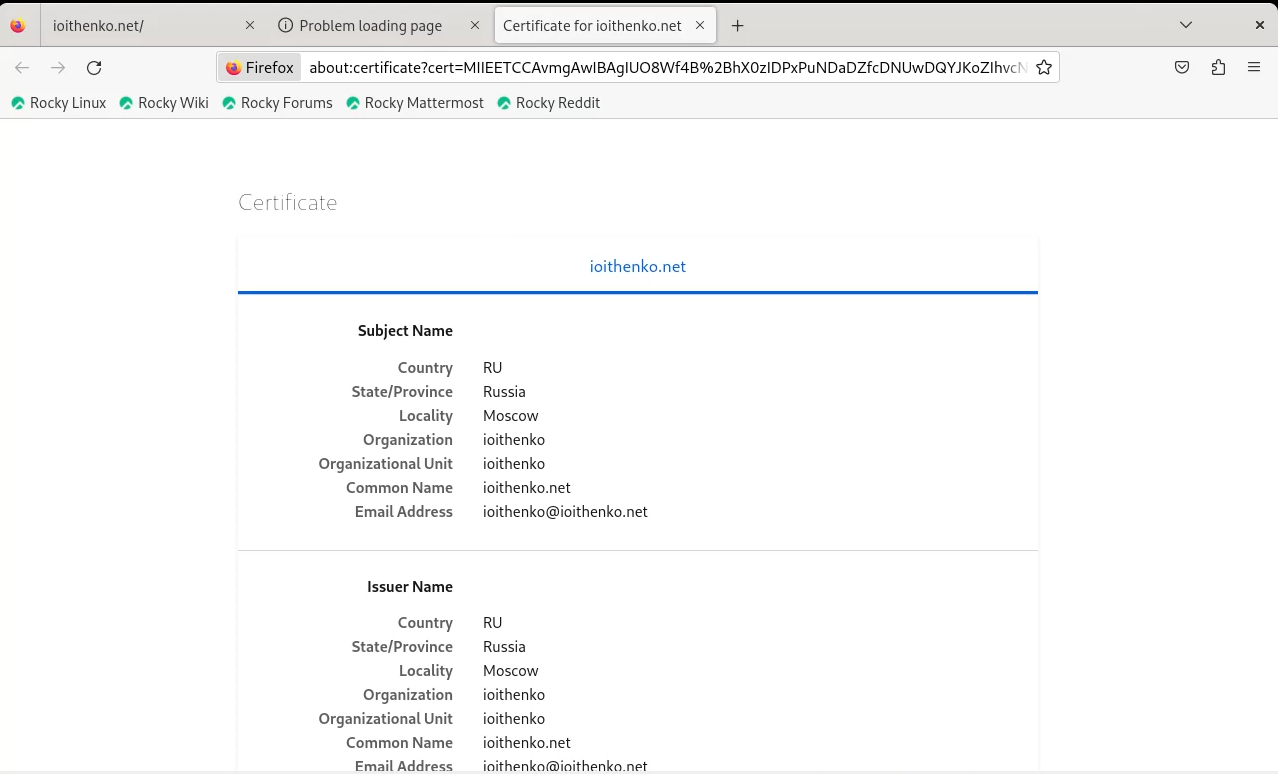


Рис. 8: Содержимое сертификата

Устанавливаю пакеты для работы с PHP: dnf -y install php (рис. 9).

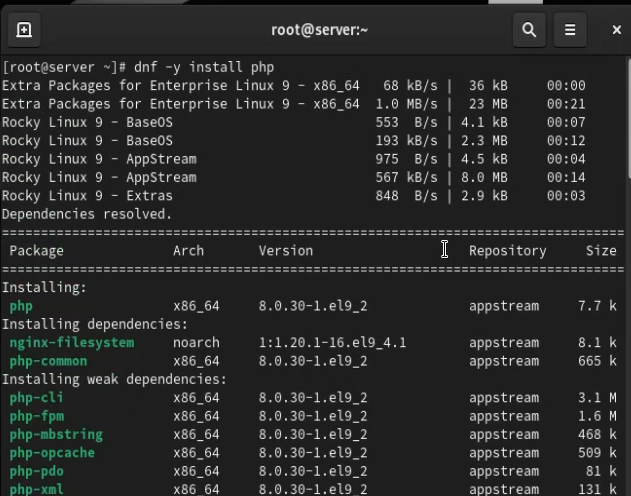


Рис. 9: PHP

В каталоге /var/www/html/www.ioithenko.net заменяю index.html на index.php.

Редактирую index.php (рис. 10).

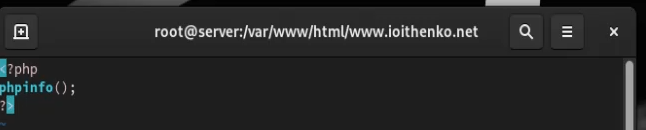


Рис. 10: Редактирование index.php

Корректирую права доступа в каталог с веб-контентом, восстанавливаю контекст безопасности в SELinux, перезагружаю HTTP-сервер (рис. 11).

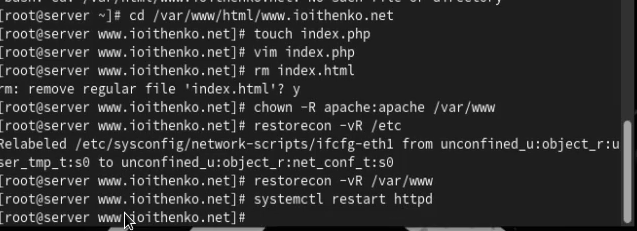


Рис. 11: Права доступа, контекст безопасности

На ВМ client ввожу в адресную строку браузера www.ioithenko.net и вижу веб-страницу с информацией об используемой версии PHP (рис. 12).

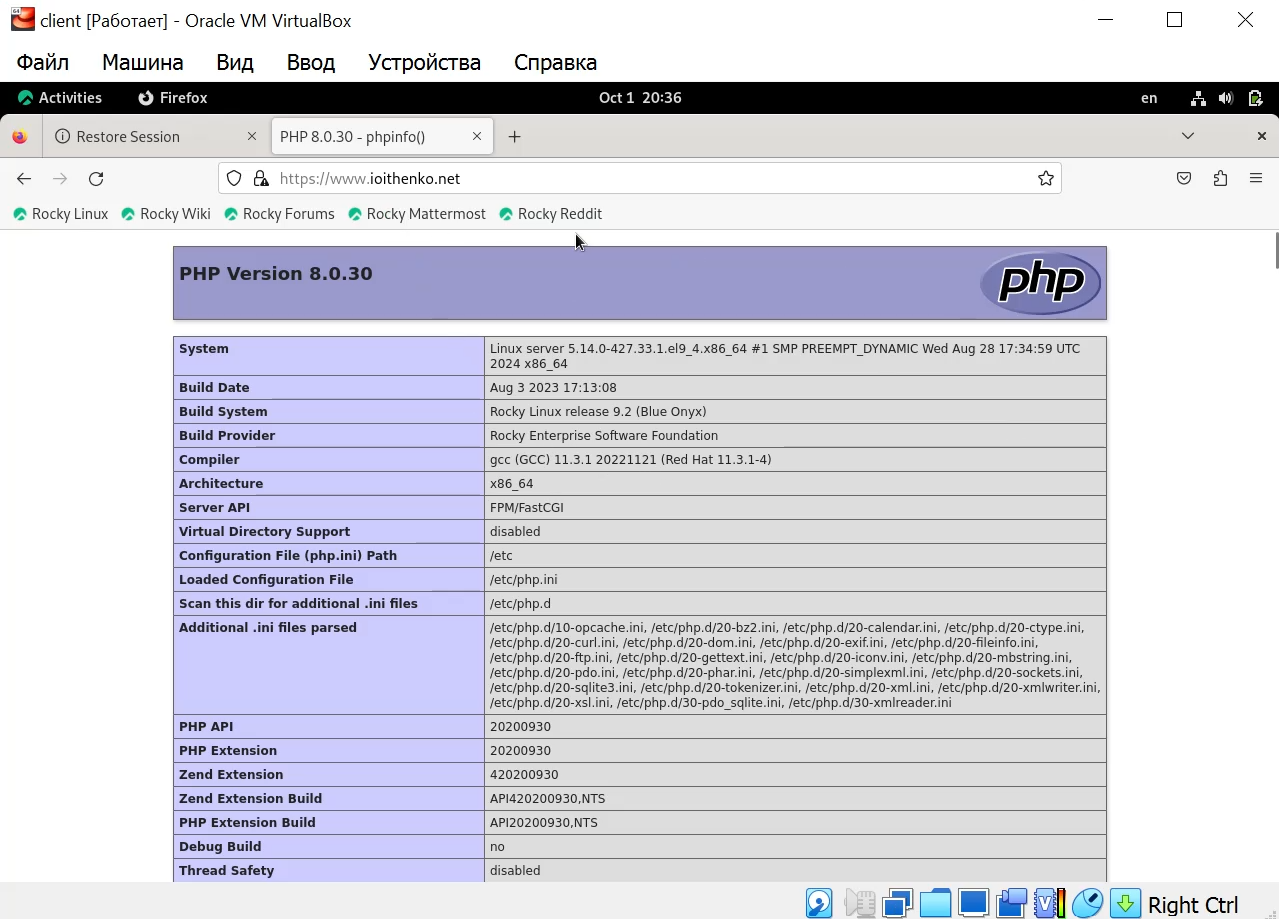


Рис. 12: Веб-страница с информацией об используемой версии PHP

На ВМ server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую в соответствующие каталоги конфигурационные файлы (рис. 13).

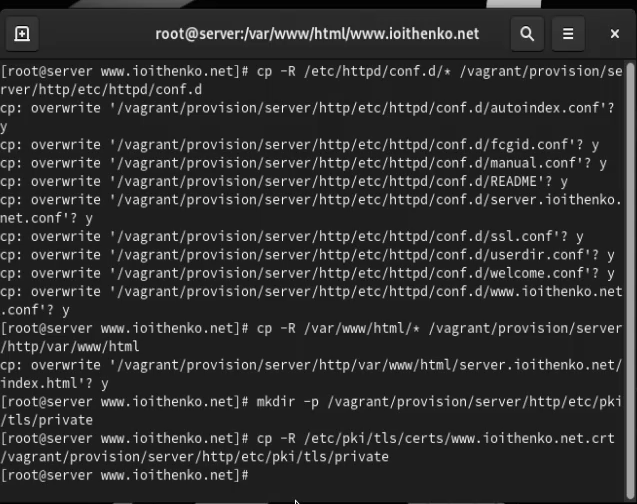


Рис. 13: Внутреннее окружение

В скрипт /vagrant/provision/server/http.sh вношу изменения, добавив установку PHP и настройку межсетевого экрана для работы с https (рис. 14).

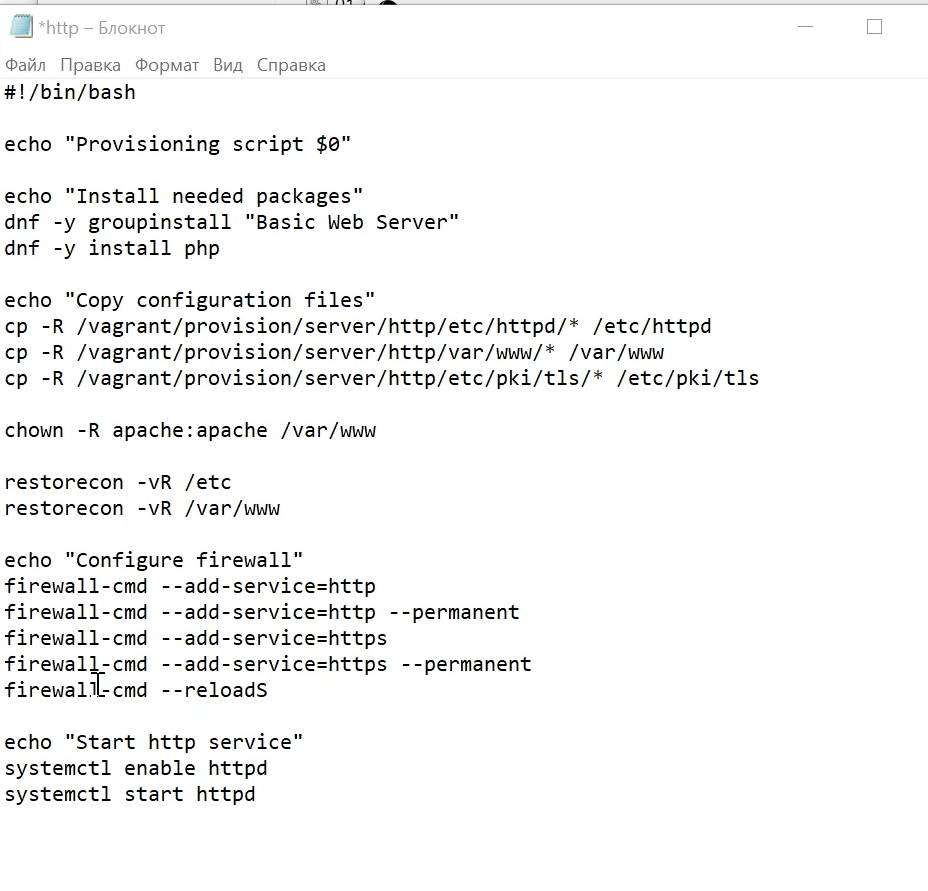


Рис. 14: Внесение изменений в скрипт http.sh

# 3 Выводы

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

# 4 Ответы на контрольные вопросы

1. В чём отличие HTTP от HTTPS?

**HTTP** (HyperText Transfer Protocol) – это протокол передачи данных, который используется для передачи информации между клиентом (например, веб-браузером) и сервером. Однако он не обеспечивает шифрование данных, что делает их уязвимыми к перехвату злоумышленниками.

**HTTPS** (HyperText Transfer Protocol Secure) - это расширение протокола HTTP с добавлением шифрования, обеспечивающее безопасную передачу данных между клиентом и сервером. Протокол HTTPS использует SSL (Secure Sockets Layer) или более современный TLS (Transport Layer Security) для шифрования данных.

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

Шифрование данных: при использовании HTTPS данные, передаваемые между клиентом и сервером, шифруются, что делает их невозможными для прочтения злоумышленниками, перехватывающими трафик.

Идентификация сервера: сервер предоставляет цифровой сертификат, подтверждающий его легитимность. Этот сертификат выдается сертификационным центром и содержит информацию о владельце сертификата, публичный ключ для шифрования и подпись, подтверждающую подлинность сертификата.

1. Что такое сертификационный центр?

Сертификационный центр (Центр сертификации) - это доверенная сторона, которая выдает цифровые сертификаты, подтверждающие подлинность владельца сертификата. Пример: Одним из известных сертификационных центров является “Let’s Encrypt”. Он предоставляет бесплатные SSL- сертификаты, которые используются для обеспечения безопасного соединения на множестве веб-сайтов. Владельцы веб-сайтов могут получить сертификат от Let’s Encrypt, чтобы обеспечить шифрование и подтвердить свою легитимность в онлайн-среде.