УДК 004.738.5

Белеевский Дмитрий Александрович

студент

2 курс, факультет «Комплексной безопасности ТЭК»

РГУ нефти и газа (НИУ) имени И.М. Губкина

Россия, г. Москва

Лебедев Никита Кириллович

студент

2 курс, факультет «Комплексной безопасности ТЭК»

РГУ нефти и газа (НИУ) имени И.М. Губкина

Россия, г. Москва

НАСТРОЙКА СЕРВЕРА APACHE, НА БАЗЕ ОТЕЧЕСТВЕННЫХ СРЕДСТВ ЗАЩИТЫ, В ИНФРАСТРУКТУРЕ ОС АЛЬТ

Аннотация: *В статье рассматривается практическая методика развёртывания и защищённой настройки веб-сервера Apache (служба httpd2) в ОС ALT Server 10.4 с применением отечественных криптографических средств (CryptoPro CSP) для организации HTTPS с использованием ГОСТ-алгоритмов. Описаны этапы установки и базовой конфигурации Apache, генерации ключевого контейнера и запроса PKCS#10 (CSR), получения и установки серверного сертификата через тестовый УЦ, подключение SSL-модуля и параметров виртуального хоста, а также проверка работоспособности защищённого соединения средствами CSP и браузером; приведены типовые проблемы (цепочка доверия, доступ процесса веб-сервера к контейнеру ключа, настройки портов/Listen) и рекомендации по их устранению.*

Ключевые слова: *Apache (httpd2), ALT Server, CryptoPro CSP, ГОСТ TLS, mod_ssl, сертификат, контейнер ключей (HDIMAGE).*

Annotation: *The article describes a practical method for deploying and securely configuring the Apache web server (httpd2 service) in the ALT Server 10.4 operating system using domestic cryptographic tools (CryptoPro CSP) to implement HTTPS using GOST algorithms. The article describes the steps of installing and configuring Apache, generating a key container and a PKCS#10 (CSR) request, obtaining and installing a server certificate through a test CA, connecting the SSL module and configuring virtual host settings, as well as testing the secure connection using CSP and a browser. The article also provides common issues (trust chain, web server process access to the key container, and port/Listen settings) and recommendations for resolving them.*

Keywords: *Apache (httpd2), ALT Server, CryptoPro CSP, GOST TLS, mod_ssl, certificate, key container (HDIMAGE).*

Введение

В условиях цифровизации и роста доли онлайн-сервисов веб-инфраструктура становится критическим элементом корпоративных и государственных ИТ-систем. Передача учетных данных и служебной информации без шифрования делает обмен уязвимым для перехвата и подмены трафика, поэтому защищённый доступ по HTTPS на базе TLS рассматривается как базовый механизм обеспечения конфиденциальности, целостности и аутентичности взаимодействия клиента и сервера. На практике одним из наиболее распространённых веб-серверов остаётся Apache HTTP Server, где поддержка TLS реализуется через модуль mod_ssl и параметры виртуальных хостов.

В условиях санкционных ограничений и политики импортозамещения для ряда организаций дополнительно актуально применение отечественных (в том числе сертифицированных) криптографических средств и ГОСТ-алгоритмов при построении защищённых каналов связи. Для Linux-платформ поддержку TLS с ГОСТ для Apache обеспечивает CryptoPro CSP, предоставляя бинарный модуль mod_ssl и инструменты управления контейнерами ключей и сертификатами. Криптографическая основа опирается на действующие стандарты ГОСТ, включая ГОСТ Р 34.10-2012 (электронная подпись) и ГОСТ Р 34.11-2012 (функция хэширования).

Актуальность исследования обусловлена необходимостью воспроизводимой методики настройки Apache в инфраструктуре ОС Альт (ALT Server), где служба Apache администрируется как httpd2 и используется модульная структура конфигурации (включение портов, модулей и виртуальных хостов через каталоги). Это требует корректной интеграции веб-сервера с отечественными средствами защиты: создание ключевого контейнера, формирование PKCS#10-запроса, установка сертификата и цепочки доверия, включение TLS-параметров и проверка рукопожатия.

В соответствии с требованиями регуляторов (ФСТЭК России, ГКРЦ) к защите информации в государственных информационных системах, применяемые меры должны обеспечивать безопасность на всех этапах обработки данных, включая передачу по протоколу HTTPS. При настройке веб-серверов необходимо руководствоваться отраслевыми стандартами и рекомендациями, такими как OWASP Top 10 [7], CIS Benchmarks for Apache [4] и другими документами, определяющими типовые уязвимости и методы защиты [3]. Кроме того, в контексте импортозамещения актуальны исследования, посвящённые миграции на отечественное программное обеспечение, например, работы [4], [5], в которых анализируются проблемы и перспективы перехода на российские платформы и средства защиты информации.

В рамках данной работы развёртывание выполнялось на локальном адресе (127.0.0.1) с использованием сертификата публичного Тестового УЦ «КриптоПро». Такой подход обусловлен отсутствием доступа к платным сертификатам ведомственных удостоверяющих центров и необходимостью демонстрации принципов настройки в лабораторных условиях. При этом все ключевые этапы - генерация ключевого контейнера, формирование запроса PKCS#10, установка сертификата и конфигурирование mod_ssl - полностью соответствуют процедуре, применяемой в реальной корпоративной инфраструктуре. Для перехода к продуктивной эксплуатации достаточно заменить тестовый сертификат на сертификат, выпущенный доверенным УЦ организации, и обеспечить доступ к серверу из внешней сети, что не требует изменения рассмотренной методики.

Объект исследования - процесс развёртывания и эксплуатации защищённого веб-сервиса на базе Apache (httpd2) в операционной системе ALT Server.

Предмет исследования - особенности интеграции криптопровайдера CryptoPro CSP в конфигурационную среду Apache для организации HTTPS-соединений с использованием ГОСТ-алгоритмов (включая генерацию ключевого контейнера, выпуск и установку сертификата X.509, настройку mod_ssl и обеспечение доступа процесса к ключевому материалу).

Целью исследования является разработка и апробация практического алгоритма настройки сервера Apache (httpd2) в ОС Альт с использованием отечественных средств защиты для организации защищённого доступа по HTTPS, а также формирование рекомендаций по диагностике типовых ошибок (доверие к цепочке, доступ процесса к ключевому контейнеру, параметры портов и TLS).

Литературный обзор

В качестве базового источника по включению HTTPS в Apache выступает официальная документация модуля mod_ssl, где описаны ключевые директивы (SSLEngine, SSLCertificateFile/KeyFile, SSLCipherSuite и др.), а также общая логика построения SSL-виртуальных хостов [1]. Этот источник задаёт «каноническую» модель настройки TLS на уровне Apache и позволяет корректно интерпретировать журнальные сообщения и ошибки конфигурации при подключении сертификатов и выборе параметров шифрования.

Платформенная специфика ОС Альт отражена в руководстве BaseALT по разделу HTTP(S), где приводится типовой сценарий установки Apache (httpd2), запуск службы, проверка статуса и размещение стартовой страницы [2]. Дополняет его ALT Linux Wiki, фиксирующая дебин-подобную структуру конфигурации httpd2 (каталоги mods/sites/ports/extra available/enabled) и практику включения компонентов через символьные ссылки [3]. В совокупности эти источники важны для воспроизводимости стенда: они показывают, где именно в Альт корректно подключать модуль SSL, как объявлять порты Listen и как организовывать файлы виртуальных хостов, чтобы изменения не конфликтовали с системной схемой конфигурации.

Ключевой особенностью рассматриваемой темы является применение отечественной криптографии (ГОСТ) в составе TLS. Документация CryptoPro прямо указывает, что поддержка TLS с ГОСТ для Apache обеспечивается использованием бинарного модуля mod_ssl из состава CryptoPro CSP, то есть интеграция выполняется не «чистым» OpenSSL-стеком, а через вызовы функций СКЗИ [4]. Это обстоятельство определяет требования к программной среде и объясняет, почему при одинаковой конфигурации Apache результаты могут отличаться в зависимости от установленного криптопровайдера и доступных механизмов работы с ключами.

Практическая часть работ с ключевым материалом и сертификатами опирается на штатные инструменты CryptoPro: CryptCP используется для формирования запросов PKCS#10 (CSR) и выполнения операций с сертификатами/контейнерами [5], а certmgr - для установки сертификатов и цепочек доверия в хранилища, экспорта и просмотра атрибутов, включая привязку закрытого ключа (PrivateKey Link) [6]. Эти источники важны тем, что переводят задачу из «общей» настройки Apache в конкретные шаги управления контейнером ключей и жизненным циклом сертификата в инфраструктуре CSP, что на практике часто является причиной сбоев TLS-рукопожатия.

Таким образом, анализ литературы показывает, что корректная настройка Apache в ОС Альт с отечественными средствами защиты требует согласования трёх уровней: системного (схема конфигурации httpd2 и управление сервисом) [2–3], прикладного (директивы mod_ssl и параметры виртуального хоста) [1], и криптографического (CSP-инструменты, контейнер ключей, цепочка доверия и профиль ГОСТ-TLS) [4–10]. Важно учитывать, что ГОСТ-профиль стандартизован для TLS 1.2, поэтому при тестах контролируют версию протокола и выбранные шифры [7].

Версия	Год	Краткое назначение
1.3.42	февраль 2010	Первая версия, получившая поддержку DSO (динамически загружаемых модулей) и экспериментальную поддержку Windows
2.0.65	Июль 2013	Представила гибридную многопоточную/многопроцессную модель обработки запросов (MPM), поддержку IPv6 и фильтрацию ввода-вывода
2.2.34	Июль 2017	Внедрила Apache Portable Runtime (APR) 1.0 API, промышленную систему кэширования и встроенную поддержку протокола AJP
2.4.65	Июль 2025	Оптимизирована для облачных сред благодаря асинхронному вводу-выводу, сниженному потреблению памяти, динамической настройке обратного прокси и более гибким механизмам авторизации , при этом остаётся актуальной и поддерживаемой версией .

Таблица 1 – Версии Apache HTTP Server.

Ключевой отличительной особенностью ГОСТ-HTTPS является зависимость не только от директив Apache, но и от корректной интеграции с отечественным криптопровайдером. Документация КриптоПро фиксирует, что для Linux-систем решение «TLS с ГОСТ на nginx/Apache» включает модуль mod_ssl для Apache определённых версий и тем самым задаёт официальный механизм реализации ГОСТ-TLS на стороне веб-сервера [7]. Это означает, что при настройке HTTPS необходимо учитывать совместимость версий Apache и компонентов CSP, а также корректную подготовку ключевого материала в контейнере.

Отдельный блок литературы посвящён криптографическим стандартам, определяющим алгоритмическую основу сертификатов и рукопожатия: ГОСТ Р 34.10-2012 описывает процессы формирования/проверки электронной подписи [3], а ГОСТ Р 34.11-2012 - функцию хэширования [4]. Для практической реализации этих алгоритмов в интернет-протоколах используется профильная спецификация IETF: RFC 7836 делает параметры ГОСТ-алгоритмов доступными для внедрения в криптопротоколах [9], а RFC 9189 задаёт профиль TLS 1.2 с ГОСТ-алгоритмами и определяет наборы шифров и связанные параметры совместимости реализаций [8].

Практические шаги выпуска и установки сертификата в инфраструктуре CryptoPro подробно раскрываются через утилиты CSP: CryptCP применяется для формирования запроса PKCS#10 (CSR) и операций с криптообъектами [6], а certmgr - для установки/экспорта сертификатов и цепочек доверия, а также контроля привязки закрытого ключа (PrivateKey Link) [5]. Эти источники важны тем, что объясняют типовые причины ошибок TLS-рукопожатия в реальных стендах: неверно установленная цепочка доверия, отсутствие привязки сертификата к контейнеру, либо недоступность контейнера для процесса веб-сервера.Общие принципы включения TLS в Apache и назначение mod_ssl закреплены в официальной документации Apache, что позволяет сопоставлять параметры виртуального хоста и требования криптопрофиля ГОСТ-TLS [10].

На основе обзора литературы можно сформулировать основную гипотезу исследования:

1. Предполагается, что разработанная методика настройки httpd2 в ОС Альт (включающая интеграцию CryptoPro mod_ssl и сертификата ГОСТ) обеспечит функционирование HTTPS по ГОСТ-TLS, если будут выполнены требования к генерации ключевого контейнера, корректности цепочки сертификатов и правам доступа веб-сервера.

Методы исследования

Работа выполнена в лабораторной среде на виртуальном сервере ALT Server 10.4. Методика направлена на пошаговую настройку Apache (служба httpd2) и проверку HTTPS при использовании отечественных средств защиты CryptoPro CSP (ГОСТ-TLS).

Сначала выполнялся вход на сервер и проверка доступности удалённого администрирования по SSH. На этом шаге важно убедиться, что стенд действительно доступен и можно продолжать работу без «ручного доступа» через панель хостинга. Также на раннем этапе полезно сразу увидеть в логах SSH попытки входа - это помогает понять, правильно ли настроены учётные данные и нет ли лишних проблем с доступом, которые потом будут отвлекать от основной темы.

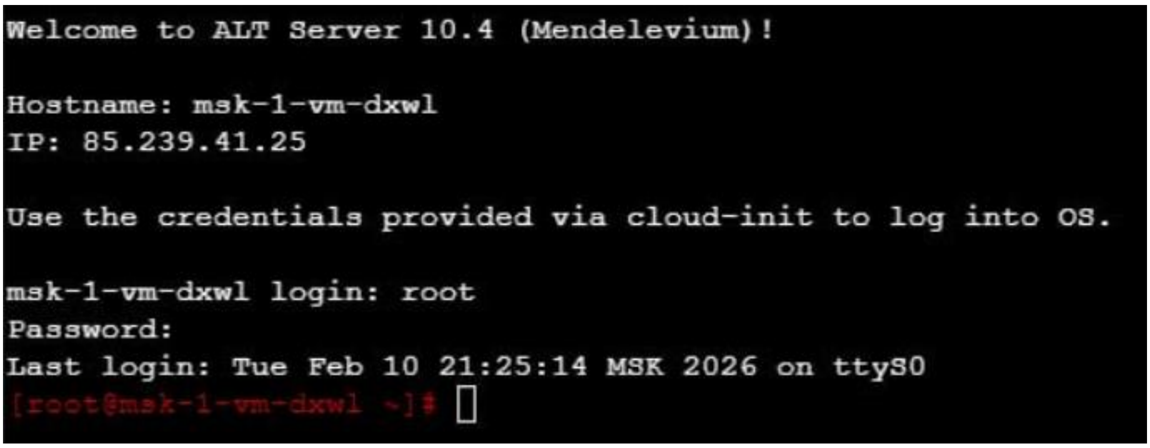
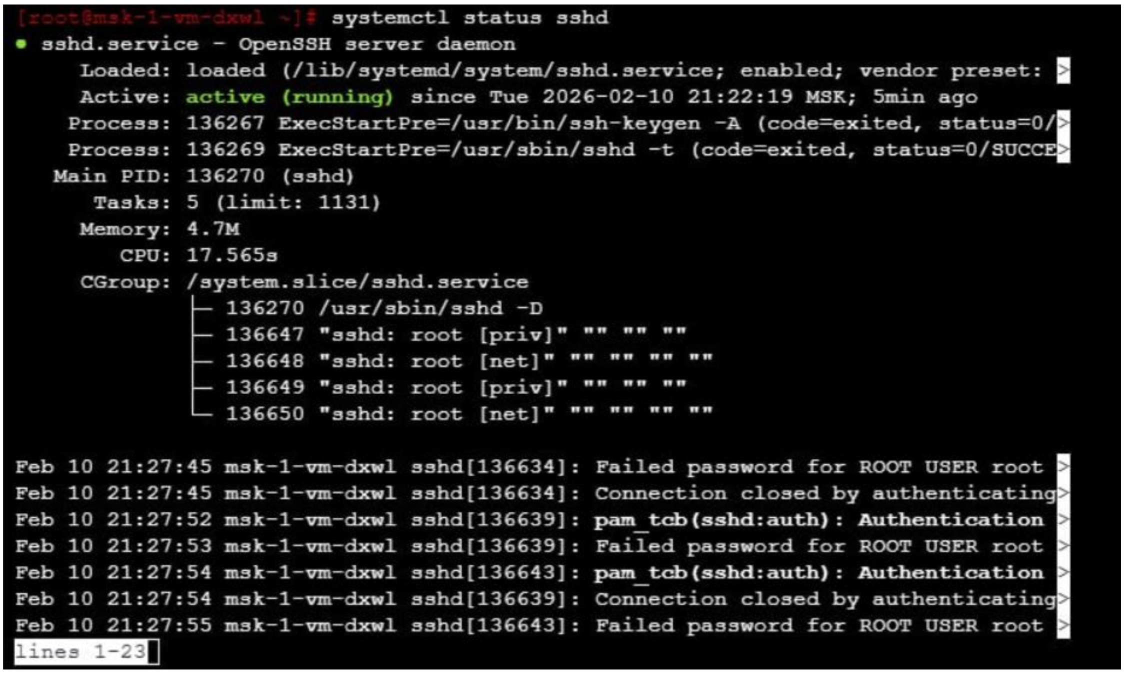


Рисунок 1 – Вход в ALT Server 10.4 под root

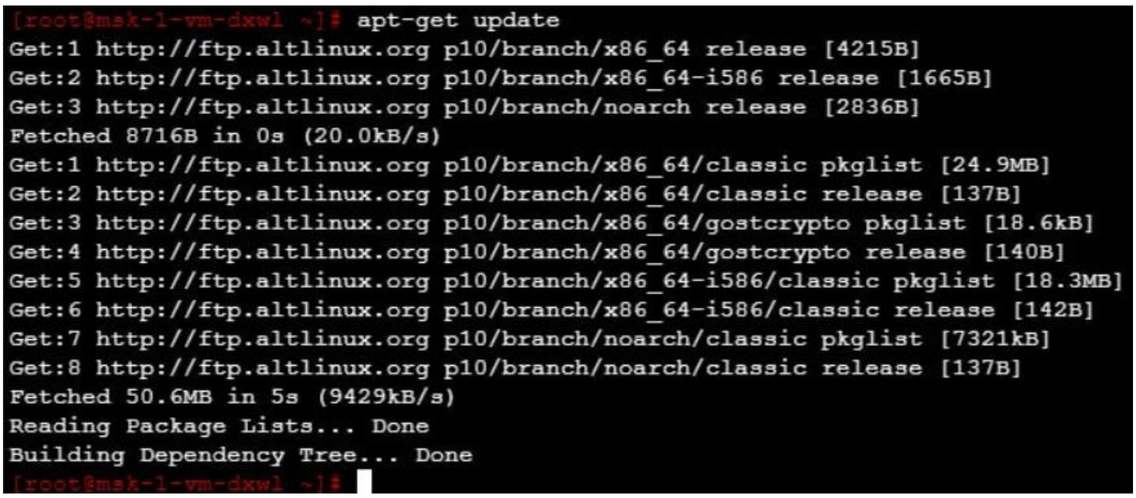


```
[root@msk-1-vm-dxwl ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: >
     Active: active (running) since Tue 2026-02-10 21:22:19 MSK; 5min ago
    Process: 136267 ExecStartPre=/usr/bin/ssh-keygen -A (code=exited, status=0/>
    Process: 136269 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCE>
   Main PID: 136270 (sshd)
      Tasks: 5 (limit: 1131)
     Memory: 4.7M
        CPU: 17.565s
     CGroup: /system.slice/sshd.service
             ├─ 136270 /usr/sbin/sshd -D
             ├─ 136647 "sshd: root [priv]" "" "" ""
             ├─ 136648 "sshd: root [net]" "" "" "" ""
             ├─ 136649 "sshd: root [priv]" "" "" ""
             └─ 136650 "sshd: root [net]" "" "" "" ""

Feb 10 21:27:45 msk-1-vm-dxwl sshd[136634]: Failed password for ROOT USER root >
Feb 10 21:27:45 msk-1-vm-dxwl sshd[136634]: Connection closed by authenticating>
Feb 10 21:27:52 msk-1-vm-dxwl sshd[136639]: pam_tcb(sshd:auth): Authentication >
Feb 10 21:27:53 msk-1-vm-dxwl sshd[136639]: Failed password for ROOT USER root >
Feb 10 21:27:54 msk-1-vm-dxwl sshd[136643]: pam_tcb(sshd:auth): Authentication >
Feb 10 21:27:54 msk-1-vm-dxwl sshd[136639]: Connection closed by authenticating>
Feb 10 21:27:55 msk-1-vm-dxwl sshd[136643]: Failed password for ROOT USER root >
lines 1-23
```

Рисунок 2 – Проверка службы SSH

Затем система приводилась в рабочее состояние: обновлялись индексы пакетов, выполнялась попытка обновления ОС и ставились базовые утилиты (редактор, средства загрузки и сетевые инструменты). Этот этап нужен не «для галочки»: без актуальных списков пакетов часто возникают ошибки установки, а без утилит (nano, curl, wget) сложно проверять доступность веб-сервиса и редактировать конфиги. В ходе подготовки отдельно фиксировалась проблема нехватки места в кэше APT, потому что в реальной настройке такие ограничения реально встречаются и напрямую влияют на возможность поставить нужные пакеты (Apache, зависимости, компоненты CryptoPro)



```
[root@msk-1-vm-dxwl ~]# apt-get update
Get:1 http://ftp.altlinux.org p10/branch/x86_64 release [4215B]
Get:2 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Get:3 http://ftp.altlinux.org p10/branch/noarch release [2836B]
Fetched 8716B in 0s (20.0kB/s)
Get:1 http://ftp.altlinux.org p10/branch/x86_64/classic pkglist [24.9MB]
Get:2 http://ftp.altlinux.org p10/branch/x86_64/classic release [137B]
Get:3 http://ftp.altlinux.org p10/branch/x86_64/gostcrypto pkglist [18.6kB]
Get:4 http://ftp.altlinux.org p10/branch/x86_64/gostcrypto release [140B]
Get:5 http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist [18.3MB]
Get:6 http://ftp.altlinux.org p10/branch/x86_64-i586/classic release [142B]
Get:7 http://ftp.altlinux.org p10/branch/noarch/classic pkglist [7321kB]
Get:8 http://ftp.altlinux.org p10/branch/noarch/classic release [137B]
Fetched 50.6MB in 5s (9429kB/s)
Reading Package Lists... Done
Building Dependency Tree... Done
[root@msk-1-vm-dxwl ~]#
```

Рисунок 3 – Обновление индексов пакетов: apt-get update

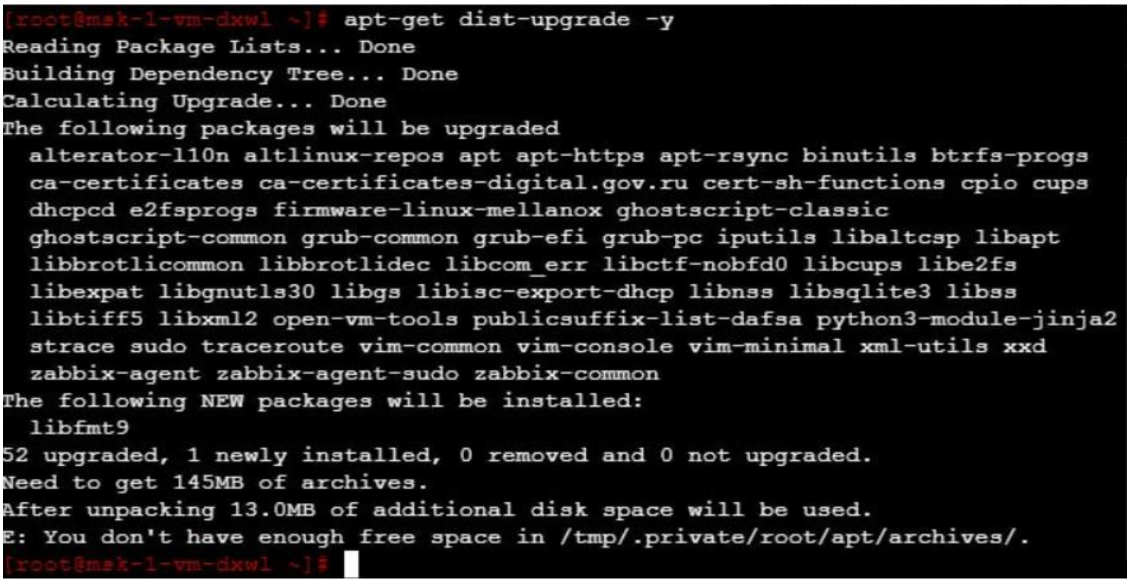


Рисунок 4 – Попытка обновления ОС

После этого задавался правильный часовой пояс, чтобы время в логах сервера и временные метки сертификатов отображались корректно. Это особенно важно для TLS: если время отличается, браузер может ругаться на срок действия сертификата, а в логах Apache и системных логах будет неудобно сопоставлять события по времени.

Рисунок 5 – Настройка часового пояса

Далее устанавливался Apache и запускался как сервис **httpd2** (в ALT отсутствует unit httpd.service). На этом шаге я специально зафиксировал различие в названии службы, потому что многие инструкции в интернете ориентируются на «httpd/apache2», а в ALT это именно httpd2 - и это влияет на команды управления (enable, restart, status). После запуска контролировался статус службы: важно убедиться, что Apache реально поднялся, не упал с ошибкой и готов обслуживать запросы.

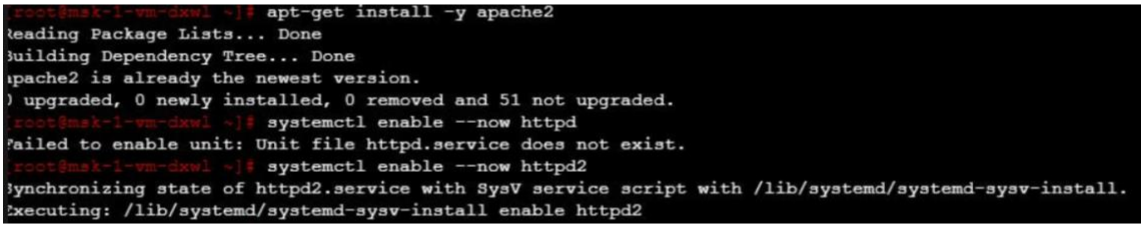


Рисунок 6 – Установка Apache

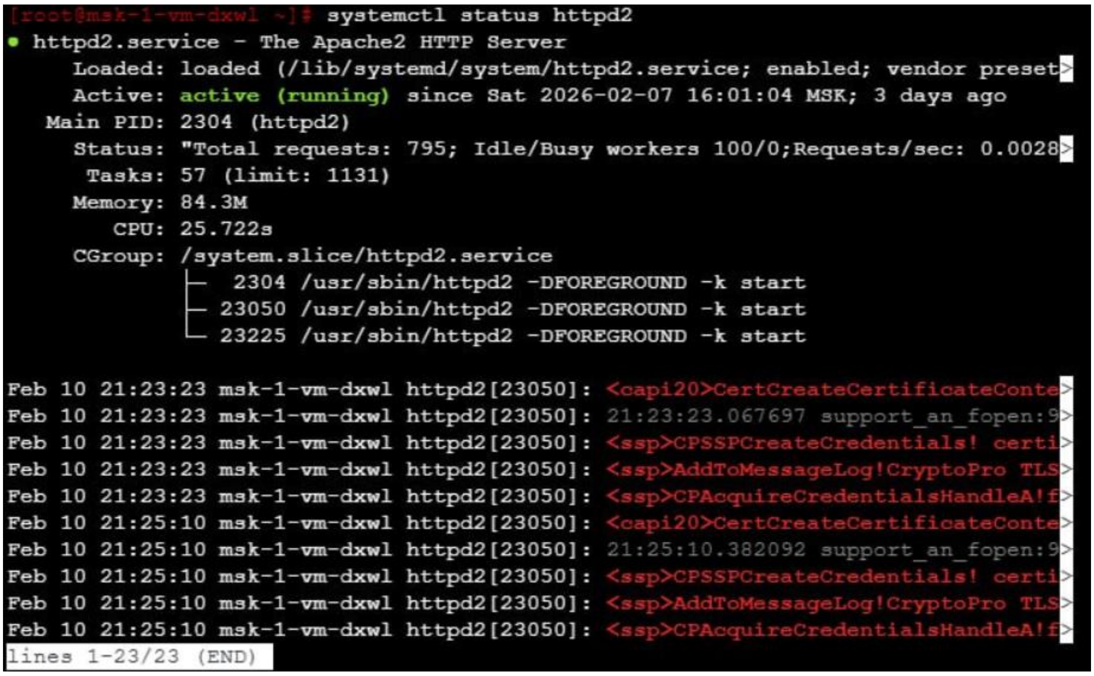


Рисунок 7 – Проверка состояния Apache

Чтобы проверить, что веб-часть работает ещё до настройки TLS, создавалась тестовая страница «Hello world» в каталоге /var/www/html. Это простой, но полезный приём: если потом возникают проблемы с HTTPS, можно сразу понимать - проблема в шифровании/сертификате или вообще в работе Apache/DocumentRoot.

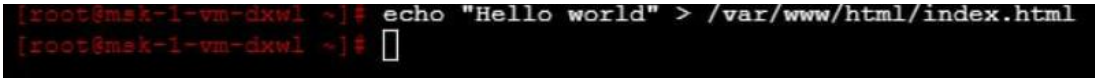


Рисунок 8 – Создание тестовой страницы: запись «Hello world»

Следующий блок методики - организация портов и логики доступа. Чтобы разделить «обычный» HTTP-бэкенд и защищённый контур, портовая схема httpd2 настраивалась отдельно: backend переводился на локальный адрес 127.0.0.1:8080, а HTTPS-часть тестировалась на 127.0.0.1:8443. Такой подход помогает отладке: можно отдельно проверить, что Apache отдаёт страницу по HTTP локально, и отдельно - что TLS-контур не конфликтует с другими службами и не мешает основной части. Для исключения конфликтов отключались дефолтные конфиги портов, после чего повторно проверялись активные директивы Listen. По сути, это «чистка окружения», чтобы не было ситуации, когда Apache слушает сразу несколько портов из разных конфигов и поведение становится непредсказуемым.

```
[root@msk-1-vm-dxwl ~]# rm -f /etc/httpd2/conf/ports-enabled/00-ports.conf
f <<'EOF'-1-vm-dxwl ~]# cat > /etc/httpd2/conf/ports-enabled/10-backend-8080.conf
> Listen 127.0.0.1:8080
> EOF
[root@msk-1-vm-dxwl ~]#
```

Рисунок 9 – Настройка backend-порта

```
[root@msk-1-vm-dxwl ~]# ls -l /etc/httpd2/conf/ports-enabled/
total 0
lrwxrwxrwx 1 root root 28 Jan 27 15:22 http.conf -> ../ports-available/http.conf
lrwxrwxrwx 1 root root 27 Jan 27 17:27 ssl.conf -> ../ports-available/ssl.conf
[root@msk-1-vm-dxwl ~]# rm -f /etc/httpd2/conf/ports-enabled/http.conf
[root@msk-1-vm-dxwl ~]# rm -f /etc/httpd2/conf/ports-enabled/ssl.conf
[root@msk-1-vm-dxwl ~]# grep -R "^[[:space:]]*Listen" /etc/httpd2
/etc/httpd2/conf/ports-available/http.conf:Listen 80
/etc/httpd2/conf/ports-available/http-localhost-8088.conf:Listen localhost:8088
/etc/httpd2/conf/ports-available/ssl.conf:Listen 443
/etc/httpd2/conf/ports-available/https.conf:    Listen 443
/etc/httpd2/conf/original/ports-available/http.conf:Listen 80
/etc/httpd2/conf/original/ports-available/https.conf:   Listen 443
/etc/httpd2/conf/ports.conf:Listen 127.0.0.1:8443
[root@msk-1-vm-dxwl ~]#
[root@msk-1-vm-dxwl ~]#
```

Рисунок 10 – Отключение дефолтных портов

После настройки портов я переходил к основной части работы - интеграции отечественных средств защиты. Сначала проверялась установка CryptoPro CSP: наличие утилит в каталоге /opt/cprocsp/bin/amd64 показывает, что базовые компоненты CSP действительно присутствуют [7]. Затем через csptest фиксировались версия CSP и доступные ГОСТ-алгоритмы [7]. Этот шаг нужен, чтобы заранее понимать: поддерживается ли нужная криптография на стенде и не придётся ли «искать проблему» в Apache, когда на самом деле её причина в CSP или в отсутствии нужных алгоритмов.

```
[root@msk-1-vm-dxwl ~]# /opt/cprocsp/bin/amd64/csptest -enum -info
CSP (Type:80) v5.0.10011 KC1 Release Ver:5.0.12600 OS:Linux CPU:AMD64 FastCode:READY:AVX,AVX2.
CryptAcquireContext succeeded.HCRYPTPROV: 132707411
GetProvParam(...PP_ENUMALGS...) until it returns false
   Algid     Bits     Type      NameLen    AlgName
________________________________________________________
 0000661eh  256    Encrypt        14     GOST 28147-89
 00008021h  256    Hash           18     GR 34.11-2012 256
 00002e49h  512    Signature      18     GR 34.10-2012 256
 0000aa46h  512    Exchange       18     DH 34.10-2012 256
 0000aa47h  512    Exchange       18     DH 34.10-2012 256
 0000801fh  32     Hash           18     GOST 28147-89 MAC
 00006630h  256    Encrypt        14     GR 34.12-15 M
 00006631h  256    Encrypt        14     GR 34.12-15 K
 0000803ch  64     Hash           18     GR 34.13-15 M MAC
 0000803dh  128    Hash           18     GR 34.13-15 K MAC
 00008034h  256    Hash           20     GR34.11-12 256 HMAC
Cycle exit when getting data. 11 items found. Level completed without problems.
Total: SYS: 0.020 sec USR: 0.000 sec UTC: 0.050 sec
```

Рисунок 11 – Проверка наличия утилит CryptoPro CSP

Далее создавался ключевой контейнер в хранилище HDIMAGE с паролем (как ближе к реальной эксплуатации) с использованием утилиты cryptcp [6]. Я выбрал вариант с паролем специально, потому что это типовая ситуация: закрытый ключ должен быть защищён, и именно из-за пароля/прав доступа часто возникают сложности при запуске веб-сервера (процессу нужно иметь доступ к ключу). После генерации контейнера формировался запрос на сертификат (CSR) в формате PKCS#10 также с помощью cryptcp [6]. Важно, что CSR создавался на основе уже созданного контейнера, то есть ключи не генерировались «внутри CSR», а использовались те, которые лежат в контейнере. Корректность CSR подтверждалась тем, что файл имеет PEM-вид с заголовком BEGIN NEW CERTIFICATE REQUEST - это означает, что запрос можно загружать в УЦ и он соответствует ожидаемому формату.

```
[root@msk-1-vm-dxwl ~]# /opt/cprocsp/bin/amd64/csptest -keyset -newkeyset \
>   -provtype 80 \
>   -cont "\\\\.\\HDIMAGE\\apachelab_tls"
CSP (Type:80) v5.0.10011 KC1 Release Ver:5.0.12600 OS:Linux CPU:AMD64 FastCode:READY:AVX,AVX2.
AcquireContext: OK. HCRYPTPROV: 1039242035
GetProvParam(PP_NAME): Crypto-Pro GOST R 34.10-2012 KC1 CSP
Container name: "apachelab_tls"
Signature key is not available.
Attempting to create a signature key...
Press keys to provide random data...
[.......................................................................]
фCrypto-Pro GOST R 34.10-2012 KC1 CSP requests new container password
New password:
Confirm password:
a signature key created.
Exchange key is not available.
Attempting to create an exchange key...
Press keys to provide random data...
[.......................................................................]
an exchange key created.
Keys in container:
  signature key
  exchange key
Extensions:
  OID: 1.2.643.2.2.37.3.9
  PrivKey: Not specified - 10.05.2027 19:45:06 (UTC)

  OID: 1.2.643.2.2.37.3.10
  PrivKey: Not specified - 10.05.2027 19:45:44 (UTC)
Total: SYS: 1.240 sec USR: 0.080 sec UTC: 57.350 sec
[ErrorCode: 0x00000000]
[root@msk-1-vm-dxwl ~]#
```

Рисунок 12 – Создание контейнера ключей (с паролем)

```
[root@msk-1-vm-dxwl ~]# /opt/cprocsp/bin/amd64/cryptcp -creatrqst \
>   -dn "CN=apachelab.ru" \
>   -provtype 80 \
>   -certusage "1.3.6.1.5.5.7.3.1" \
>   -ex \
>   -nokeygen \
>   -cont '\\.\HDIMAGE\apachelab_tls' \
>   apachelab.req
CryptCP 5.0 (c) "Crypto-Pro", 2002-2022.
Command prompt Utility for file signature and encryption.
Crypto-Pro GOST R 34.10-2012 KC1 CSP requests container password
Type password:
Request is saved in file.
[ErrorCode: 0x00000000]
```

Рисунок 13 – Формирование CSR

```
[root@msk-1-vm-dxwl ~]# ls -l apachelab.req
achelab.req
-rw-r--r-- 1 root root 452 Feb 10 22:56 apachelab.req
[root@msk-1-vm-dxwl ~]# head -n 5 apachelab.req
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBDzCBvQIBADAXMRUwEwYDVQQDDAxhcGFjaGVsYWIucnUwZjAfBggqhQMHAQEB
ATATBgcqhQMCAiQABggqhQMHAQECAgNDAARAQhNjM59XitGtEWLbLUgY8+zZ74W3
mLdM1G/B0n9btI7N8qz6dGcWx0uX9k1QRo1m7Dp3F6N+0Ct8XKLAXc3Gc6A3MDUG
CisGAQQBgjcCAQ4xJzAlMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA4GA1UdDwEB/wQE
[root@msk-1-vm-dxwl ~]#
```

Рисунок 14 - Проверка CSR

Получение сертификата выполнялось через Тестовый УЦ «КриптоПро» ГОСТ 2012. Тут методика была простой: перейти на портал УЦ, убедиться в требованиях к окружению, включить расширение CryptoPro и проверить, что плагин корректно работает (диагностика проходит и сертификат выбирается). Это нужно, чтобы не столкнуться с ситуацией, когда запрос сформирован правильно, но выпуск/установка сертификата тормозится из-за проблем на стороне клиента (браузер/плагин/сертификаты корня). После выпуска сертификата он устанавливался на сервер и подключался в конфигурации Apache (через SSL-контур).

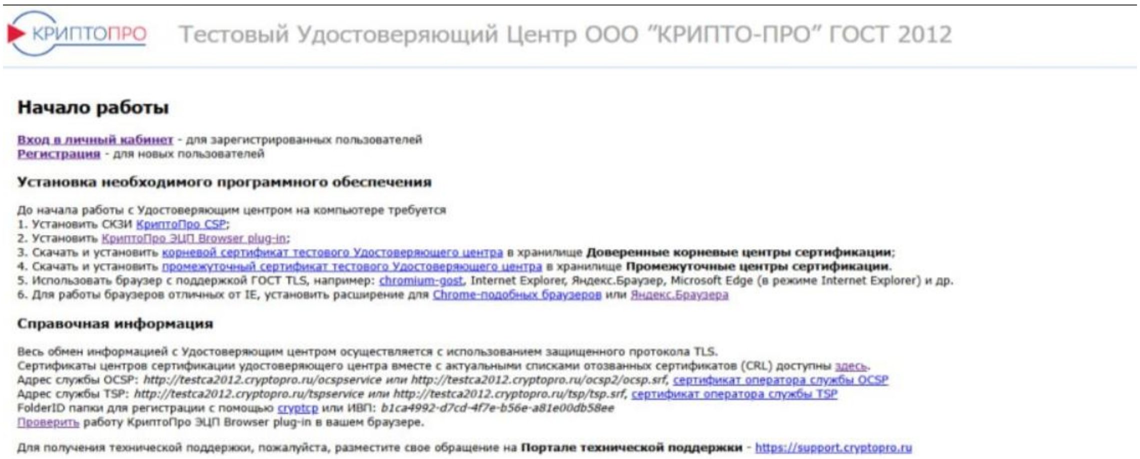


Рисунок 15 – Стартовая страница Тестового УЦ «КриптоПро» ГОСТ 2012

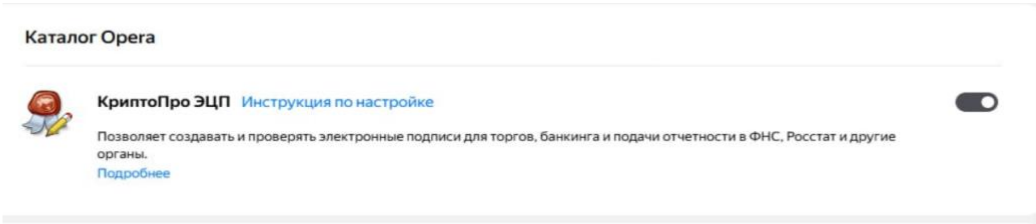


Рисунок 16 – Включение расширения Opera «CryptoPro Extension for CAdES Browser Plug-in».

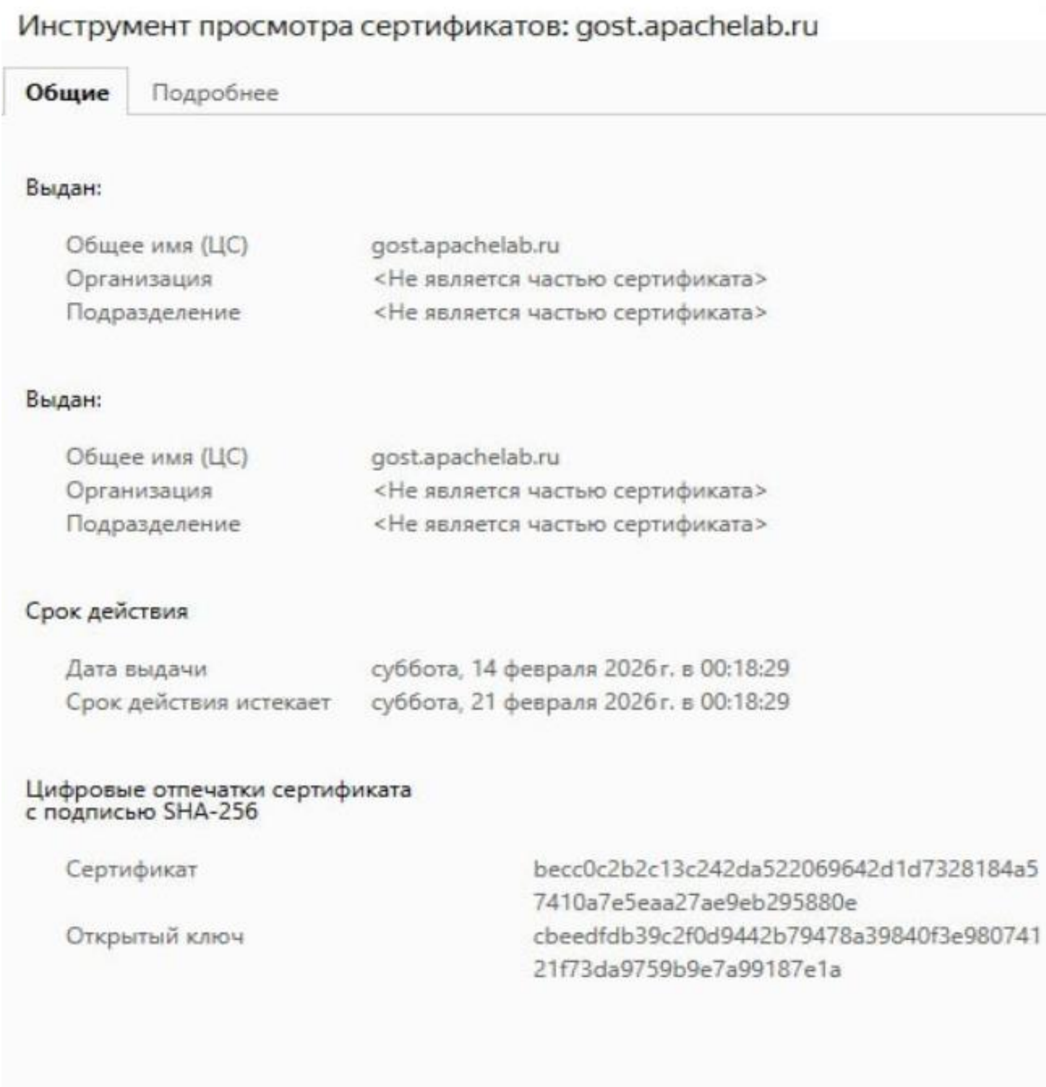


Рисунок 17 - Просмотр сведений TLS-сертификата сайта gost.apachelab.ru в браузере

Финальный контроль выполнялся со стороны клиента: открывалась страница по HTTPS на порту 8443 и просматривались параметры сертификата (срок действия, отпечатки). Смысл этого шага - подтвердить результат именно «глазами пользователя»: сервер реально отдаёт страницу по защищённому соединению, сертификат подхватывается, а в просмотре сертификата видно, что он относится к нужному домену и действует в указанные даты. Если на этом шаге возникают предупреждения, это тоже диагностический результат: чаще всего причина либо в доверии к цепочке, либо в том, что сертификат не полностью соответствует доменному имени/порту, либо есть ошибка в настройках TLS-части

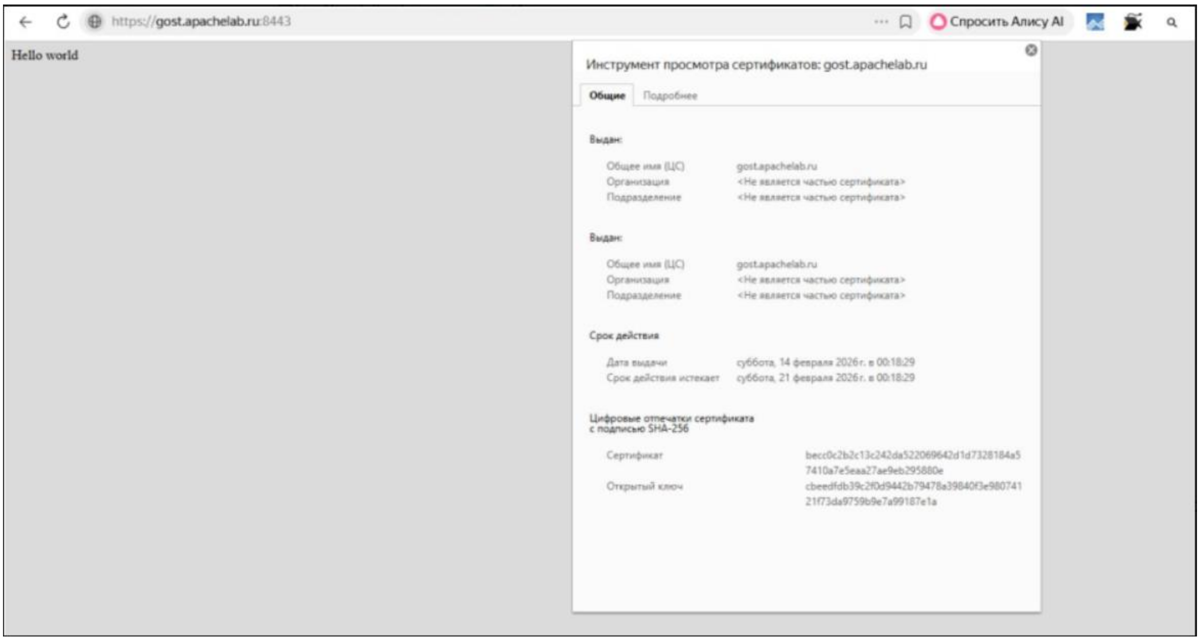


Рисунок 18 - Проверка HTTPS-доступности (страница «Hello world»)

В итоге методика исследования строится как последовательная цепочка проверок: сначала готовность системы и доступ к серверу, затем работоспособность Apache без шифрования, затем раздельная настройка портов, после чего - подготовка CryptoPro CSP, генерация контейнера и CSR, выпуск сертификата в отечественном УЦ и финальная проверка HTTPS в браузере. Такой подход удобен тем, что при ошибке можно быстро локализовать, где именно она возникла (ОС/Apache/порты/CSP/сертификат /клиентская проверка).

Результаты исследования

В ходе выполнения исследования была разработана и апробирована практическая методика настройки веб-сервера Apache (служба httpd2) в операционной системе ALT Server 10.4 с применением отечественных криптографических средств CryptoPro CSP для организации защищённого доступа по протоколу HTTPS с использованием ГОСТ-алгоритмов. Предложенный алгоритм включает последовательность шагов: подготовку инфраструктуры (обновление пакетов, настройка часового пояса), установку и базовую настройку Apache, конфигурирование портовой схемы, установку и проверку компонентов CryptoPro CSP, генерацию ключевого контейнера и запроса PKCS#10, получение сертификата через тестовый удостоверяющий центр, установку сертификата и цепочки доверия, а также финальную проверку защищённого соединения.

В процессе работы выявлен и систематизирован ряд типовых проблем, возникающих при развёртывании подобной конфигурации, а также сформулированы практические рекомендации по их диагностике и устранению:

1. Проблемы подготовки системы: недостаток свободного места в кэше пакетного менеджера APT может блокировать установку необходимых компонентов. Рекомендуется предварительно контролировать объём доступного дискового пространства и при необходимости очищать кэш.

2. Некорректная временная синхронизация: расхождение системного времени с актуальным приводит к ошибкам валидации сертификатов (предупреждения браузера о сроке действия). Перед настройкой TLS необходимо убедиться в правильности часового пояса и синхронизации времени.

3. Особенности имени службы Apache в ОС Альт: использование команды systemctl для управления httpd2 (а не httpd или apache2) является обязательным, иначе возможны сбои при запуске и проверке статуса

4. Конфликты портов и некорректная привязка Listen: при разделении HTTP- и HTTPS-контуров необходимо отключать стандартные конфигурации портов и явно задавать директивы Listen для нужных адресов и портов, иначе Apache может прослушивать нежелательные интерфейсы.

5. Доступ процесса веб-сервера к ключевому контейнеру: закрытый ключ должен быть доступен для чтения пользователем, от которого

работает Apache (обычно httpd2). При создании контейнера с паролем необходимо либо хранить пароль в защищённом виде, либо использовать хранилище, доступное процессу.

6. Цепочка доверия и установка сертификата: для корректного TLS-рукопожатия в хранилище сервера должны присутствовать все промежуточные и корневые сертификаты.
7. Проверка работоспособности: после настройки рекомендуется не только открыть страницу в браузере, но и проанализировать логи Apache (например, error_log) на предмет ошибок SSL

Разработанная методика ориентирована на лабораторные условия (локальный адрес, тестовый сертификат), однако все принципы и этапы конфигурации полностью соответствуют требованиям, предъявляемым к промышленной эксплуатации в государственных и корпоративных информационных системах. Для перехода в продуктивную среду достаточно заменить тестовый сертификат на сертификат, выпущенный доверенным удостоверяющим центром, обеспечить доступ к серверу из внешней сети и при необходимости дополнить настройки в соответствии с отраслевыми стандартами безопасности (CIS Benchmarks, рекомендации ФСТЭК).

Список литературы

1. ALT Linux Wiki. Apache2/Configs (схема конфигурации httpd2: mods/sites/ports/extra available/enabled) – URL: https://www.altlinux.org /Apache2/Configs (дата обращения: 16.01.2026)
2. BaseALT. Альт Сервер 10.2: HTTP(S) (раздел 72.5, настройка веб-сервера Apache/httpd2). – URL: https://docs.altlinux.org/ru-RU/alt-server/10.2/html/alt-server/http.html (дата обращения: 16.01.2026).
3. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной

цифровой подписи. – URL: https://protect.gost.ru/document.aspx?control=7&id=180151 (дата обращения: 16.01.2026).
4. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – URL: https://protect.gost.ru/document.aspx?control=7&id=180209 (дата обращения: 16.01.2026).
5. КриптоПро. certmgr (утилита управления сертификатами в составе CryptoPro CSP для UNIX-платформ, руководство, PDF). – URL: https://www.cryptopro.ru/sites/default/files/docs/csp36r3/certmgr.pdf (дата обращения: 16.01.2026).
6. КриптоПро. КриптоПро CSP. Приложение командной строки CryptCP (руководство, PDF). – URL: https://cryptopro.ru/sites/default/files/products/cryptcp/cryptcp_5.0.x.pdf (дата обращения: 16.01.2026).
7. КриптоПро. TLS с ГОСТ на nginx/Apache (требования и состав решения CryptoPro TLS/CSP). – URL: https://cryptopro.ru/products/csp/tls/gost-nginx-apache (дата обращения: 16.01.2026).
8. Уймин А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.
9. Smyshlyaev S., Belyavsky D., Alekseev E. GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2 // RFC 9189. – IETF, 2022. – URL: https://www.rfc-editor.org/rfc/rfc9189.html (дата обращения: 16.01.2026).
10. Smyshlyaev S. Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012 // RFC 7836. – IETF, 2016. – URL: https://www.rfc-editor.org/rfc/rfc7836.html (дата обращения: 16.01.2026).

References

1. ALT Linux Wiki. Apache2/Configs (httpd2 configuration scheme: mods/sites/ports/extra available/enabled) – URL: https://www.altlinux.org/Apache2/Configs (accessed on 16.01.2026)
2. BaseALT. Alt Server 10.2: HTTP(S) (section 72.5, configuring the Apache/httpd2 web server). – URL: https://docs.altlinux.org/ru-RU/alt-server/10.2/html/alt-server/http.html (accessed on 16.01.2026).
3. GOST R 34.10-2012. Information technology. Cryptographic protection of information. Processes for generating and verifying electronic digital signatures. – URL: https://protect.gost.ru/document.aspx?control=7&id=180151 (accessed on 16.01.2026).
4. GOST R 34.11-2012. Information technology. Cryptographic protection of information. Hash function. – URL: https://protect.gost.ru/document.aspx?control=7&id=180209 (accessed on 16.01.2026).
5. CryptoPro. certmgr (certificate management utility included in CryptoPro CSP for UNIX platforms, manual, PDF). – URL: https://www.cryptopro.ru/sites/default/files/docs/csp36r3/certmgr.pdf (accessed on 16.01.2026).
6. CryptPro. CryptPro CSP. CryptCP Command Line Application (manual, PDF). – URL: https://cryptopro.ru/sites/default/files/products/cryptcp/cryptcp_5.0.x.pdf (accessed on 16.01.2026).
7. CryptoPro. TLS with GOST on nginx/Apache (requirements and composition of the CryptoPro TLS/CSP solution). – URL: https://cryptopro.ru/products/csp/tls/gost-nginx-apache (accessed: 01/16/2026).
8. Uimin A. G. Basic level demonstration exam. Network and System Administration : A practical course. Textbook for universities / A. G. Uimin. Saint Petersburg : Lan Publishing House, 2024. 116 p. (Higher education). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.

9. Smyshlyaev S., Belyavsky D., Alekseev E. GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2 // RFC 9189. – IETF, 2022. – URL: https://www.rfc-editor.org/rfc/rfc9189.html (date of access: 01/16/2026).
10. Smyshlyaev S. Guidelines on the Cryptographic Algorithms to Accommodate the Use of Standards GOST R 34.10-2012 and GOST R 34.11-2012 // RFC 7836. – IETF, 2016. – URL: https://www.rfc-editor.org/rfc/rfc7836.html (accessed: 01/16/2026).