Отчет по оценке безопасности TLS и криптографических средств

Команда оценки безопасности

2026-01-29

Резюме

Реализация TLS, защищающая оцениваемое веб-приложение, была проанализирована в соответствии с текущими лучшими практиками индустрии и регулятивными рекомендациями (2025–2026). Конфигурация демонстрирует **высокий уровень безопасности**, включая предпочтение современных версий протоколов, надежные криптографические примитивы, принудительное обеспечение Perfect Forward Secrecy и устойчивость к известным атакам на уровне протокола.

> **Ключевой вывод**: В ходе оценки не было выявлено критических, высоких или средних рисков. Незначительные возможности усиления защиты с низким уровнем риска документированы для полноты картины.

Общий рейтинг риска: Очень низкий

С точки зрения бизнес-рисков, текущая конфигурация TLS не создает существенных рисков для конфиденциальности, целостности или доступности.

.

Параметры оценки

Параметр	Детали
Цель	Веб-приложение (HTTPS-конечная точка)
Область оценки	Конфигурация Transport Layer Security (TLS), криптографическая стойкость, поддержка протоколов и наборов шифров
Тип оценки	Неинтрузивная, внешняя, основанная на анализе конфигурации
Методологическая база	NIST SP 800-52r2 (основной), Рекомендации Mozilla по серверному TLS (современный профиль, редакция 2025), Рекомендации NCSC по TLS, OWASP Transport Layer Security Cheat Sheet

Используемые инструменты

- **Nmap** (NSE: ssl-enum-ciphers, ssl-cert, ssl-enum-protocols)
- **sslscan / testssl.sh**
- **Qualys SSL Labs** (перекрестная проверка)

.

Соответствие стандартам и нормативным требованиям

Данная оценка проводилась в соответствии со следующими авторитетными стандартами и отраслевыми рекомендациями:

- **NIST SP 800-52 Revision 2** — Руководство по выбору, настройке и использованию реализаций TLS (основной справочник)
- **Генератор конфигурации Mozilla SSL** — современный профиль совместимости (2025)
- **Руководство UK NCSC по TLS** — рекомендуемые профили
- **OWASP Transport Layer Security Cheat Sheet**
- **Лучшие практики Cloudflare TLS** (информационно)

Ключевые требования выполнены или превышены

TLS 1.3 обязателен и предпочтителен для всех современных клиентов

TLS 1.2 включен только как ограниченный, безопасный резерв

Отсутствие устаревших протоколов (TLS 1.1, 1.0, SSLv3/v2 отключены)

Perfect Forward Secrecy обеспечивается через ECDHE с современными эллиптическими кривыми

Наборы шифров AEAD (AES-GCM, ChaCha20-Poly1305) используются исключительно

.

Анализ поддержки протоколов TLS

Версия протокола	Статус	Оценка
TLS 1.3	Включен	Предпочтительный; наиболее безопасный и эффективный
TLS 1.2	Включен	Безопасный резерв со строгим контролем шифров
TLS 1.1	× Отключен	Соответствует требованиям
TLS 1.0	× Отключен	Соответствует требованиям
SSLv3 / SSLv2	× Отключен	Соответствует требованиям

Заключение

TLS 1.3 последовательно согласовывался для всех протестированных современных клиентов. TLS 1.2 наблюдался только в сценариях совместимости и ограничен сильными наборами шифров. Небезопасные или устаревшие версии протоколов не поддерживаются. Данная конфигурация соответствует рекомендациям NIST, Mozilla Modern и NCSC для 2025–2026 годов.

.

Оценка наборов шифров

Наборы шифров TLS 1.3

Наблюдаемый порядок предпочтений сервера:

1. **TLS_AES_128_GCM_SHA256**
2. **TLS_CHACHA20_POLY1305_SHA256**
3. **TLS_AES_256_GCM_SHA384**

Наборы шифров TLS 1.2

Только PFS, предпочитаемые сервером:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-CHACHA20-POLY1305

Сводная оценка

Криптографическая стойкость: Все поддерживаемые наборы шифров реализуют AEAD (аутентифицированное шифрование с дополнительными данными)

- Слабые, анонимные, основанные на CBC, SHA-1 или экспортные шифры не включены
- Порядок шифров сервера демонстрирует оптимальный баланс между производительностью и безопасностью
- ChaCha20-Poly1305 приоритизирован для мобильных устройств и сред с низкой энтропией
- AES-GCM оптимизирован для аппаратно-ускоренных платформ
- Perfect Forward Secrecy обеспечивается для всех согласованных соединений

.

Конфигурация обмена ключами и криптографии

Компонент	Конфигурация	Оценка
Обмен ключами	X25519 (предпочтительный), secp256r1	Безопасный и производительный
Аутентификация	ECDSA (предпочтительный), RSA-2048/3072	Соответствует требованиям
Симметричное шифрование	AES-GCM, ChaCha20-Poly1305	Безопасный AEAD
Длина ключа	256-битные кривые, 2048/3072-битный RSA	Рекомендовано индустрией

Техническое примечание: X25519 правильно предпочитается для обмена ключами, обеспечивая улучшенную производительность и устойчивость к атакам по побочным каналам по сравнению с традиционными кривыми NIST P-256.

.

Оценка уязвимостей безопасности

Устойчивость к атакам понижения версии и устаревшим атакам

Были проверены следующие средства защиты от атак понижения версии и устаревших атак:

- **TLS_FALLBACK_SCSV** поддерживается
- **Отсутствие путей понижения** к слабым наборам шифров TLS 1.2
- **Защита от понижения TLS 1.3** правильно обеспечивается
- **Невозможность согласования устаревших шифров**

Результат: Конфигурация устойчива к известным атакам понижения версии и устаревшим атакам протокола, включая POODLE, Logjam и попытки понижения, инициированные клиентом.

Проверка известных уязвимостей

Уязвимость	Статус
Heartbleed	Не уязвим
BEAST	Смягчено
CRIME	Неприменимо
POODLE	Не уязвим
Logjam	Не уязвим
Sweet32	Не уязвим

Заключение: В ходе тестирования не было обнаружено эксплуатируемых уязвимостей на уровне TLS.

.

Рекомендации и возможности усиления защиты

Следующие пункты представляют возможности усиления защиты с **низким уровнем риска**, которые могут дополнительно укрепить позицию TLS:

🔍 Дополнительные улучшения

1. **HSTS Preload**
   - Текущее состояние: Заголовок HSTS присутствует
   - Улучшение: Подать домен в списки предварительной загрузки браузеров
   - Преимущество: Дополнительное снижение риска понижения версии и MITM при первом подключении
2. **OCSP Must-Staple**
   - Текущее состояние: Сертификат не включает OCSP Must-Staple
   - Улучшение: Включить это расширение

- Преимущество: Улучшить надежность проверки отзыва и конфиденциальность пользователей

3. **Время жизни сессионных билетов**
   - Текущее состояние: Зашифрованные сессионные билеты поддерживаются с прямой секретностью
   - Улучшение: Рассмотреть сокращение времени жизни билетов до ≤ 24 часов
   - Условие: Если политики ротации ключей позволяют
4. **Цепочка доверия сертификатов**
   - Текущее состояние: Действительная цепочка сертификатов, выданная доверенным публичным CA
   - Примечание: Облачное завершение TLS и интегрированные средства управления WAF обеспечивают дополнительную эшелонированную защиту

.

Сводка оценки рисков

Категория риска	Рейтинг	Обоснование
Конфиденциальность	Очень низкий	Сильное шифрование с современными шифрами AEAD
Целостность	Очень низкий	Аутентифицированное шифрование предотвращает подделку
Доступность	Очень низкий	Надежная поддержка протоколов обеспечивает подключение
Общий риск TLS	**Очень низкий**	**Комплексные средства безопасности на месте**

.

Заключение

Оцениваемая конфигурация TLS отражает **текущие лучшие практики** для высокозащищенных веб-приложений в 2026 году. Реализация демонстрирует:

- **Предпочтение современных протоколов**: TLS 1.3 приоритизирован с безопасным резервом TLS 1.2
- **Сильная криптография**: Наборы шифров AEAD с обменом ключами X25519
- **Устойчивость к атакам**: Защита от известных уязвимостей протокола
- **Операционная зрелость**: Правильное упорядочение шифров и управление безопасностью

Вывод оценки: Срочные меры по исправлению не требуются. Реализация документированных рекомендаций по усилению защиты с низким уровнем риска дополнительно поднимет конфигурацию до образцового уровня безопасности.

.

Метаданные оценки

Поле	Значение

Поле	Значение
Подготовлено для	Портфолио публичной безопасности / Демонстрация аудита
Классификация оценки	Информационная / Валидация лучших практик
Дата оценки	Январь 2026
Версия документа	1.0
Следующий обзор	Январь 2027

Данный документ представляет комплексную техническую оценку средств безопасности TLS и предназначен для специалистов по безопасности и технических аудиторов.