УДК 004.056.55

Шкуренков Егор Сергеевич, студент
Шишов Олег Алексеевич, ассистент кафедры безопасности информационных технологий
(РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва)
Egor S. Shkurenkov, student
Oleg A. Shishov, assistant lecturer, Department of Information Technology Security
(Gubkin University, Moscow)

ОЦЕНКА ГОТОВНОСТИ ВЕБ-САЙТОВ К ПЕРЕХОДУ НА ПОСТКВАНТОВУЮ КРИПТОГРАФИЮ ПО ДАННЫМ АКТИВНОГО СКАНИРОВАНИЯ ПРОТОКОЛА TLS

ASSESSING THE READINESS OF WEBSITES FOR POST-QUANTUM CRYPTOGRAPHY BASED ON ACTIVE TLS SCANNING

Аннотация. Сканированием двух выборок по 500 доменов рейтинга Tranco оценена доля сайтов, поддерживающих гибридный постквантовый обмен ключами X25519MLKEM768 в TLS 1.3: 52,8 % в мировой выборке и 13,6 % в зоне .ru. Каждый четвёртый сайт .ru не поддерживает TLS 1.3.

Abstract. Two samples of 500 Tranco domains were scanned to estimate the share of sites supporting the hybrid post-quantum key exchange X25519MLKEM768 in TLS 1.3: 52.8% globally and 13.6% in the .ru zone. Every fourth .ru site does not support TLS 1.3.

Защищённая передача информации в сети Интернет основана на протоколе TLS, обеспечивающем конфиденциальность и целостность данных [1]. Стойкость используемых в нём алгоритмов обмена ключами на эллиптических кривых опирается на вычислительную сложность задач, которые могут быть эффективно решены квантовым компьютером. Развитие квантовых вычислений [2] превращает эту угрозу из теоретической в практическую, причём её учёт необходим уже при проектировании систем, срок службы которых велик [3]. Особую опасность представляет стратегия «перехватить сейчас — расшифровать позже»: трафик, записанный сегодня, может быть расшифрован после появления достаточно мощного квантового компьютера.

Ответом на угрозу стали постквантовые алгоритмы, в частности механизм инкапсуляции ключа ML-KEM, стандартизированный NIST в документе FIPS 203. На практике его применяют в гибридном режиме совместно с классическим обменом X25519: соединение остаётся стойким,

пока не взломан хотя бы один из механизмов. Гибридная композиция классических и постквантовых алгоритмов предлагается и в отечественных криптографических схемах [4]. Цель работы — оценить, какая доля популярных веб-сайтов уже поддерживает гибридный постквантовый обмен ключами, и сравнить мировой сегмент с российским.

Выборки сформированы по рейтингу популярных доменов Tranco [5] (список N2PGW): первые 500 доменов рейтинга («мировая выборка») и первые 500 доменов в зоне .ru. Каждый домен проверялся клиентом OpenSSL 3.5, предлагавшим серверу группы X25519MLKEM768 и X25519; фиксировались версия протокола и выбранная сервером группа обмена ключами. Такой активный опрос конфигурации сервера аналогичен подходу средств автоматизированного аудита безопасности [6]. Дополнительно по опубликованным диапазонам адресов определялось, обслуживается ли сайт сетью доставки контента Cloudflare. Сканирование выполнено 29.09.2026; результаты обработаны открытыми инструментами анализа данных, применимость которых к прикладным задачам показана в [7], тогда как коммерческие инструменты [8] для выборки такого объёма избыточны. Результаты приведены в таблице 1.

Таблица 1 – Поддержка постквантового обмена ключами

Показатель	**Мировая выборка**	**Зона .ru**
Проверено доменов	500	500
Установлено соединение TLS	379	418
Только TLS 1.2, % от доступных	16,1	24,9
Поддерживают X25519MLKEM768, % от доступных	52,8	13,6
То же, % от поддерживающих TLS 1.3	62,9	18,2
Из них обслуживаются Cloudflare	49 из 200	4 из 57

В мировой выборке гибридный постквантовый обмен ключами согласуют 52,8 % доступных сайтов, в зоне .ru — 13,6 %, т. е. почти вчетверо меньше. Разрыв объясняется не только выбором алгоритмов, но и устаревшей инфраструктурой: 24,9 % доступных сайтов в зоне .ru не поддерживают TLS 1.3, без которого постквантовый обмен ключами невозможен (в мировой выборке — 16,1 %).

Проверка гипотезы о том, что постквантовую защиту обеспечивают в основном сети доставки контента, её не подтвердила: из 200 сайтов мировой выборки с поддержкой X25519MLKEM768 лишь 49 обслуживаются Cloudflare, в зоне .ru — 4 из 57. Следовательно, основную часть постквантовой поддержки обеспечивают собственные серверы владельцев сайтов, обновившие криптографические библиотеки. При этом все сайты, обслуживаемые Cloudflare и поддерживающие TLS 1.3, согласовали постквантовую группу: перенос сайта на современную инфраструктуру сразу даёт такую защиту.

Ограничения исследования: выборки включают только популярные домены; часть доменов рейтинга не обслуживает веб-сайты, поэтому анализ ведётся по доступным сайтам; поддержка российских криптографических алгоритмов в TLS не проверялась, так как требует специализированного клиента. Для организаций практический вывод состоит в необходимости инвентаризации серверов, не поддерживающих TLS 1.3, и планирования их обновления; экономическое обоснование такого обновления выполняется по методикам оценки эффективности цифровой трансформации [9]. Отслеживание требований к компетенциям специалистов в этой области может выполняться средствами анализа вакансий [10].

Список литературы

1. Мельников, В. А. Исследование существующих методов и технологий обеспечения защищенной передачи информации / В. А. Мельников // Цифровое общество: образование, экономика, технологии : Материалы III Международной научно-практической конференции, Новокузнецк, 18–19 марта 2025 года. – Москва: ООО "Актуальность.РФ", 2025. – С. 299-304. – EDN OYPKNT.
2. Казанцев, И. С. Перспективы развития квантовых вычислений / И. С. Казанцев, В. А. Мельников, А. А. Першина // Интеллектуальные технологии в эргодизайне и когнитивных науках : сборник материалов всероссийской научно-практической онлайн-конференции с международным участием, Брянск, 10–11 июня 2025 года. – Брянск: Брянский государственный технический университет, 2025. – С. 122-130. – EDN QVDUSI.
3. Сундеев, П. В. Функциональная устойчивость распределенного реестра в условиях появления новой квантовой угрозы / П. В. Сундеев // Вопросы кибербезопасности. – 2025. – № 3 (67). – С. 83-89.
4. Минаков, С. С. Схема криптографической защиты данных облачных хранилищ с возможностью расширения квантовозависимыми ключами и постквантовыми алгоритмами / С. С. Минаков, С. В. Тихов, А. А. Цупак // Вопросы кибербезопасности. – 2025. – № 6 (70). – С. 88-100.
5. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation / V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob [et al.] // Proceedings 2019 Network and Distributed System Security Symposium. – 2019. – DOI 10.14722/ndss.2019.23386.
6. Мельников, В. А. Инструменты для аудита безопасности на ALT Linux на примере Lynis / В. А. Мельников, А. А. Першина // Глобальные научные тренды: междисциплинарные исследования : Сборник статей II Международной научно-практической конференции, Саратов, 25 марта 2025 года. Часть 1. – Саратов: ООО Издательство "Кубик", 2025. – С. 90-102. – EDN DBAKYT.
7. Мельников, В. А. Анализ применимости открытых инструментов работы с алгоритмами Data Mining для решения задач анализа экономических дан-

ных / В. А. Мельников, А. А. Першина, Н. А. Савченко // Актуальные проблемы нефти и газа : Сборник трудов VII Всероссийской молодежной научной конференции, Москва, 16–18 октября 2024 года. – Москва: Институт проблем нефти и газа РАН, 2024. – С. 360-361. – EDN UIKEBJ.
8. Мельников, В. А. Оценка коммерческих инструментов работы с алгоритмами Data Mining / В. А. Мельников, А. А. Першина, Н. А. Савченко // Губкинский университет в решении вопросов нефтегазовой отрасли России : Тезисы докладов VIII Региональной научно-технической конференции, посвященной 100-летию профессора Ю.П. Желтова, Москва, 07–11 октября 2024 года. – Москва: Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, 2024. – С. 434-435. – EDN SJRFEZ.
9. Мельников, В. А. Анализ современных методик оценки экономической эффективности цифровой трансформации / В. А. Мельников, А. А. Мельникова // Цифровое общество: образование, экономика, технологии : Сборник трудов IV Международной научно-практической конференции, Новокузнецк, 18–19 марта 2026 года. – Москва: ООО "Актуальность.РФ", 2026. – С. 188-194. – EDN NGHSYH.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2026662602 Российская Федерация. Интеллектуальный анализатор цифровых компетенций вакансий : заявл. 17.04.2026 : опубл. 29.04.2026 / В. А. Мельников, А. А. Мельникова. – EDN XUTTOK.