



XV симпозиум

Современные тенденции в криптографии

STCrypT 2026



КОД
безопасности



О комбинации постквантовых механизмов и режимов работы блочных шифров для задач защиты информации на носителях и в облачных хранилищах

А.М. Коренева¹, С.С. Минаков², М.В. Поляков^{1,3} и Г.В. Фирсов^{1,3}

¹ Код Безопасности, ²Академия криптографии РФ, ³НИЯУ МИФИ

**г. Минск
04.06.2026**

ПРОБЛЕМАТИКА

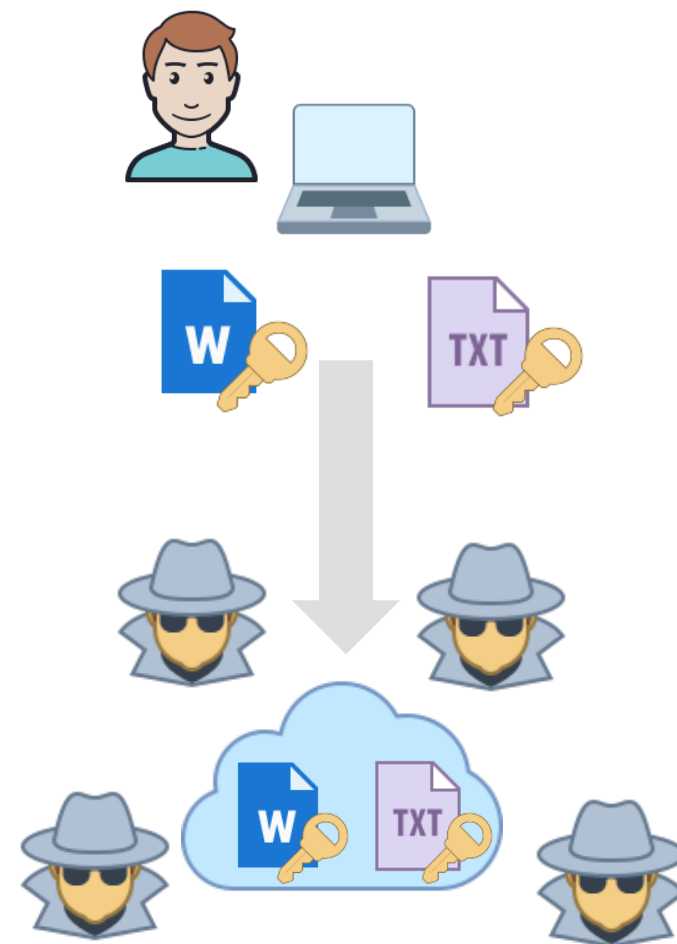
Шифрование данных на стороне клиента –

возможное решение для защиты данных, размещаемых в «облаках»:

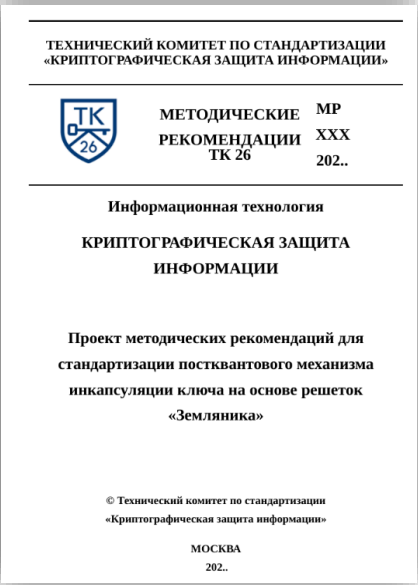
- ✓ при передаче по публичному каналу связи;
- ✓ при хранении на удалённых серверах «облачного» провайдера.

Использование постквантовых механизмов для выработки и защищённого хранения ключей доступа к мастер-ключу шифрования данных может парировать квантовую угрозу при облачном хранении данных.

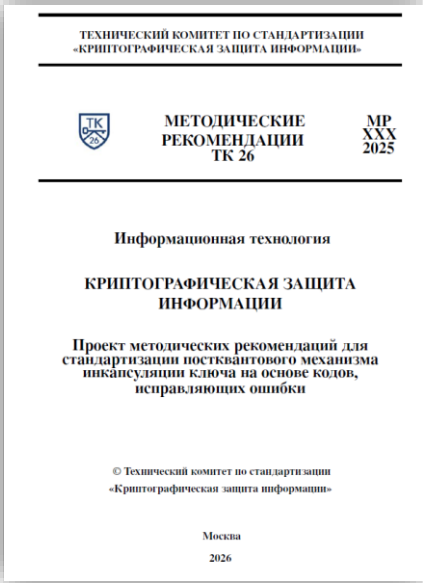
Комбинированную схему (постквантовые механизмы + симметричные конструкции) удобно применить и к шифрованию носителей с блочно-ориентированной структурой.



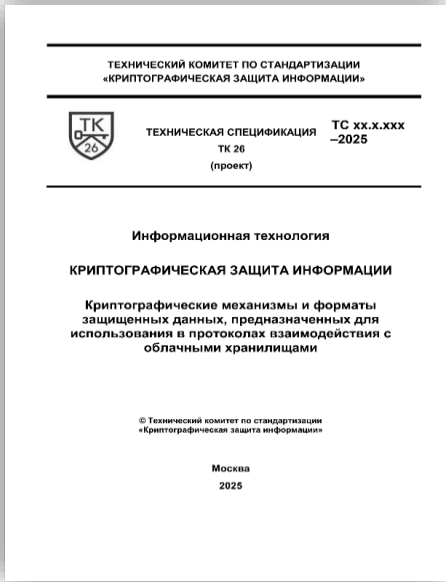
НАУЧНО-ТЕХНИЧЕСКИЙ ЗАДЕЛ В РФ



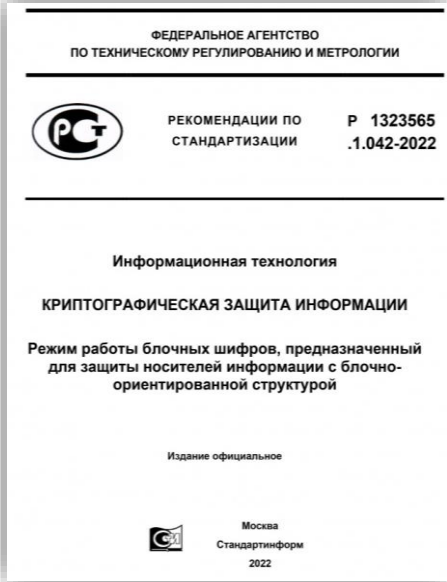
КЕМ (МИК)
Земляника
(проект)



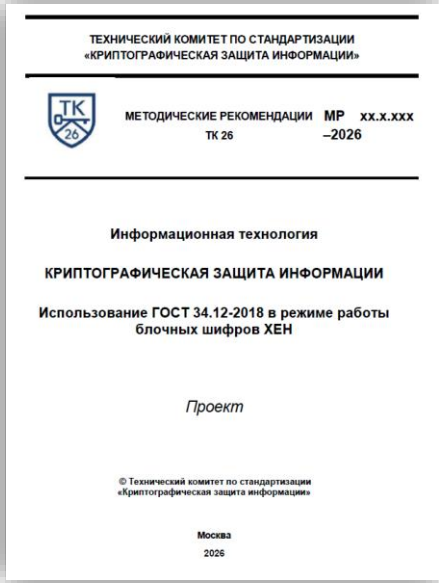
КЕМ (МИК)
Кодиеум
(проект)



Криптографические
механизмы и форматы
данных в протоколах
взаимодействия с
облачными
хранилищами
(проект)



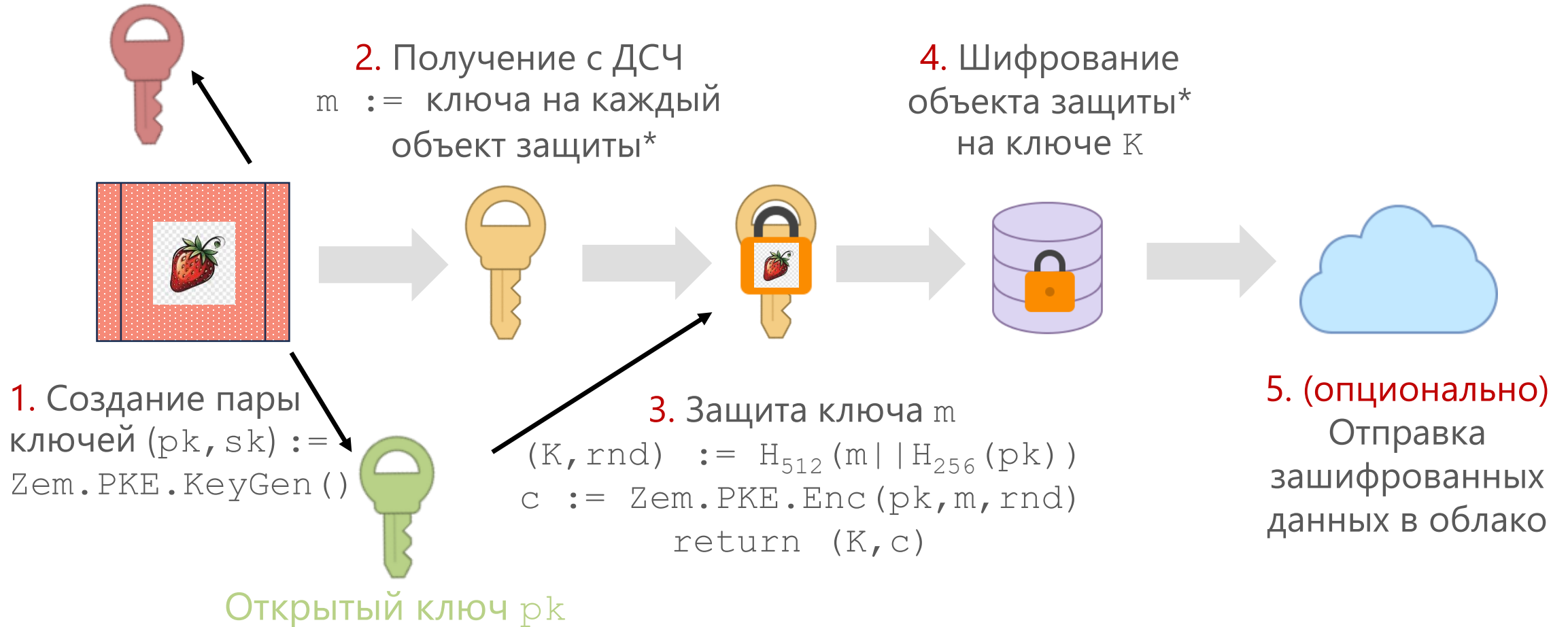
Режим DEC
(рекомендации по
стандартизации)



Режим ХЕН
(проект)

ПРЕДЛАГАЕМАЯ КРИПТОГРАФИЧЕСКАЯ СХЕМА

Закрытый ключ sk



* объектом защиты могут быть: файл, контейнер, раздел диска, носитель информации

ЗАЧЕМ?

1. В СКЗИ распространена **практика защиты секретного ключа симметричной криптосистемы на сеансовом ключе**, выработанном по протоколу Диффи-Хеллмана.
2. Стойкость протокола Диффи-Хеллмана основана на вычислительной сложности решения **задачи дискретного логарифмирования в некоторой абелевой группе**. Эта задача считается вычислительно трудной для классических вычислителей, однако уже **более 30 лет известен эффективный квантовый алгоритм её решения**.
3. Это приводит к тому, что известные криптографические схемы, в которых используется протокол Диффи-Хеллмана, **становятся потенциально уязвимыми** в условиях развития квантовых вычислений.
4. Видится целесообразным встраивание **квантово-устойчивых** альтернатив в известные криптографические схемы.

ВЫВОДЫ и НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

- ❑ Представлена криптографическая схема с постквантовым механизмом защиты секретных ключей блочных шифров для повышения защищённости информации на носителях с блочно-ориентированной структурой и в облачных хранилищах.
- ❑ В подобных схемах представляет интерес замена ДСЧ на «облегчённые» методы с использованием личностного (IBE) или атрибутного (ABE) шифрования.
- ❑ Ведутся исследования постквантовых протоколов согласования ключа (на основе *коммутативных* изогений эллиптических кривых, CSIDH), допускающих меньшие длины общих параметров и более лёгкую интеграцию в существующие инфраструктуры.

Спасибо за внимание!

Коренева Алиса Михайловна, a.koreneva@securitycode.ru

Минаков Сергей Сергеевич, s.minakov@tc26.ru

Поляков Михаил Вадимович, m.polyakov@securitycode.ru

Фирсов Георгий Валентинович, g.firsov@securitycode.ru

НАУЧНЫЕ РАБОТЫ ПО ТЕМЕ

1. **Zelenetsky, A.** Zemlyanika–Module-LWE based KEM with the power-of-two modulus, explicit rejection and revisited decapsulation failures / A. Zelenetsky, P. Klyucharev // Journal of Computer Virology and Hacking Techniques. – 2025. – Vol. 21, No. 1. – P. 32. – DOI 10.1007/s11416-025-00576-y.
2. **Минаков, С. С.** О возможности применения постквантовых алгоритмов и квантовозависимых ключей в схеме криптографической защиты облачных хранилищ / С. С. Минаков // Кибернетика и информационная безопасность "КИБ-2025" : Сборник научных трудов Третьей Всероссийской научно-технической конференции. В 2-х томах, Москва, 03–04 декабря 2025 года. – Москва: Национальный исследовательский ядерный университет МИФИ, 2025. – С. 24-29. – EDN: OJPAFR.
3. **Коренева, А. М.** Постквантовая симметричная криптография на основе блочных шифров: известные результаты и актуальные направления исследований / А. М. Коренева, С. П. Панасенко, Г. В. Фирсов // Прикладная дискретная математика. Приложение. – 2025. – № 18. – С. 146-152. – DOI 10.17223/2226308X/18/30.
4. **Firsov, G.** On improved security bounds of one block ciphers mode of operation for protection of block-oriented system storage devices / G. Firsov, A. Koreneva // Journal of Computer Virology and Hacking Techniques. – 2024. – Vol. 20. – DOI 10.1007/s11416-024-00528-y.
5. **Коренева А.М., Минаков С.С., Фирсов Г.В.** О проблематике выбора режимов работы блочных шифров для защиты системного раздела диска // Материалы XXVIII Научно-практической конференции «РусКрипто'2026». URL: https://ruscrypto.ru/resource/archive/rc2026/files/09_koreneva_minakov_firsov.pdf (дата обращения 29.05.2026).
6. **Полякова П.А., Поляков М.В., Коренева А.М.** Обзор алгоритмов, построенных на основе коммутативных изогений суперсингулярных эллиптических кривых // Материалы XXVIII Научно-практической конференции «РусКрипто'2026». URL: https://ruscrypto.ru/program/sections/s_9.html (дата обращения 29.05.2026).