РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2025

ФЕДЕРАЛЬНАЯ ТЕРРИТОРИЯ «СИРИУС»

21–27 сентября 2025

Особенности систем квантового распределения ключей с учетом актуальных подходов к защите информации

СФБ ЛАБ

Введение

Системы КРК последнее десятилетие активно развиваются в нашей стране и за рубежом. Вместе с тем, основная практическая функция указанных систем на данный момент – снабжение ключами надлежащего криптографического качества существующих и/или перспективных средств криптографической защиты информации (СКЗИ)

Для СКЗИ как и вообще для защиты информации (информационной безопасности) в России разработан и успешно применяется уже более 20 лет подход к нормативному регулированию.

Основные документы в области нормативного регулирования КРК (1)

СФБ ЛАБ

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2025

Доктрина информационной безопасности РФ (Указ Президента № 646)

Стратегия национальной безопасности Российской Федерации (Указ Президента № 400)

№ 152-ФЗ «О персональных данных» — федеральный закон, регулирующий деятельность по обработке (использованию) персональных данных

Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 года (Распоряжение Правительства № 1856-р)

Положение ПКЗ-2005 (Приказ ФСБ № 66)

«О безопасности критической информационной инфраструктуры Российской Федерации» (№ 187-ФЗ)

Стратегия развития отрасли связи до 2035 года (Распоряжение Правительства № 3339-р)

«Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ)

Основные документы в области нормативного регулирования КРК (2)

«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Приказ ФСТЭК № 17)

«Инструкция об организации и обеспечении безопасности…» (Приказ ФАПСИ № 13)

Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Методика оценки угроз безопасности информации (ФСТЭК)

«Требования о защите информации, содержащейся в государственных информационных системах…» (Приказ ФСТЭК № 117)

Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных…»

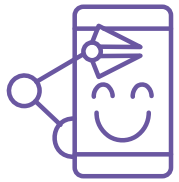
Методические рекомендации 8 Центра ФСБ России № 149/7/2/6-432

Р 1323565.1.012 2017 «Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»

Особенности систем КРК (1)

Во-первых, системы КРК обеспечивают высокую степень автоматизации процессов выработки и распределения ключей для СКЗИ-потребителей.

- В частности, корректно спроектированная система КРК после своего запуска может функционировать полностью в автоматическим режиме, причем администратор системы не будет иметь доступа к формируемым и распределяемым ключам (так называемая, безлюдная технология снабжения ключами)
- На данный момент в большинстве ИС администратор системы не предполагается нарушителем, что, к сожалению, не может быть надежно гарантировано – у территориально распределенной ИС могут быть сотни администраторов



Особенности систем КРК (2)

Во-вторых, в силу естественных предположений о возможностях нарушителя при рассмотрении атак на систему КРК класса КС3 (наиболее представленный на данный момент на рынке тип систем КРК), для многих атак может быть показана защищенность и по более высокому классу с учетом Р 1323565.1.012 2017

- Соответственно, с использованием систем КРК возможно формирование ключей, криптографическое качество которых достаточно для использования в СКЗИ любого класса, что способствует повышению уровня защищенности информационной системы в целом.

Особенности систем КРК (3)

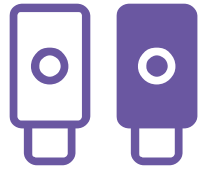
В-третьих, при использовании системы КРК может быть теоретически доказана достаточность однократного ввода ключей на произвольный с практической точки зрения период времени (например, 10 лет) без угрозы компрометации в связи с долговременным хранением введенного ключа (фактически, данный ключ может быть полностью заменен за несколько минут в ходе реализации протокола КРК).

- Соответственно, отпадает необходимость в проведении плановой смены мастер-ключей СКЗИ (процедура должна проводиться с заданной периодичностью, обычно раз в 15 месяцев), что не только позволяет снизить нагрузку на ответственных за ввод ключей сотрудников и понизить требования к их квалификации, но и повышает надежность работы с ключами для информационной системы.

Подробнее см. в докладе
А.П. Науменко «О подходах к снижению эксплуатационных издержек при использовании систем квантового распределения ключей с доверенными промежуточными узлами (ДПУ)» (РусКрипто’2025)

Особенности систем КРК (4)

В-четвертых, системы КРК позволяют формировать новые ключи даже теоретически не связанные с ранее выработанными, что в полной мере обеспечивает контроль рисков, связанных с нагрузкой на криптографические ключи и все возрастающим объемом защищаемых данных.



- Вырабатываемые системой КРК ключи обладают теоретической стойкостью – являются ε-секретными, т.е. отличимы от «идеальных» равновероятных ключей не более чем на малую величину ε
  - Для достижения теоретической ε-секретности все исходные случайные последовательности должны вырабатываться истинным источником случайности – физическим генератором случайных чисел (ФГСЧ).
  - Целесообразно использовать высокоскоростной квантовый генератор случайных чисел (КГСЧ), случайность выхода которого гарантируется законами квантовой механики
- Например, для блочного шифра ГОСТ 34.12-2018 «Магма» в стандартных режимах работы допускается обрабатывать на одном ключе не более 2^{32} блоков (34,3 Гбайт) данных (или меньше при предъявлении более строгих требований к безопасности).
- Системы КРК используются для обеспечения возможности регулярной «бесшовной» смены ключей

Возможности нарушителя (1)

Нарушитель способен проводить атаки на протокол, взаимодействуя с квантовыми состояниями в канале

Часть атак можно провести с использованием стандартного телекоммуникационного оборудования, другая часть требует специальных разработок, что соответствует классу КВ.

Тип атаки\Класс СКЗИ	КС3	КВ
Атаки на протокол ККС ВРК		
Непрозрачная атака («прием-перепосыл», Opaque)	+	+
Прозрачная индивидуальная атака (Translucent)	-	+
Коллективная атака (Collective)	-	+
Когерентная атака (Joint)	-	+
Атака с разделением по числу фотонов (PNS)	-	+
Атака со светоделителем (Beam Splitting)	+	+
Атака с измерениями с определенным исходом (UM)	+	+

Возможности нарушителя (2)

Нарушитель способен проводить атаки на техническую реализацию, пользуясь несовершенствами оборудования легитимных пользователей

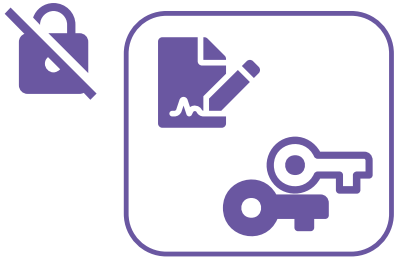
Часть атак можно провести с использованием стандартного телекоммуникационного оборудования без дополнительных сведений о СКЗИ, другая часть требует знаний о функциональных параметрах составных частей СКЗИ, что отвечает классу КВ.

Тип атаки\Класс СКЗИ	КС3	КВ
Атаки на техническую реализацию ККС ВРК		
Атака активного оптического зондирования (Trojan Horse)	+	+
Атака пассивного оптического зондирования (Backflash)	-	+
Атаки считывания сигналов (ПЭМИН)	-	+
Атака с ослеплением детекторов одиночных фотонов (Detector Blinding)	+	+
Атака на спаде строба (After Gate)	-	+
Атака с рассогласованием эффективностей детекторов (Detector Efficiency Mismatch, Time Shift)	-	+
Атака с лазерным повреждением (Laser Damage)	+*	+*
Атака с затравочным излучением (Laser Seeding, Induced Photorefraction)	+*	+*

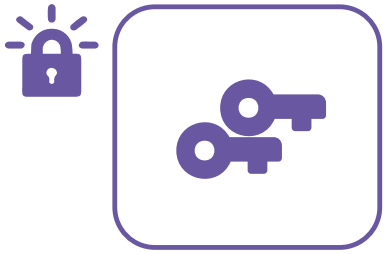
*Для получения информации нарушителю необходимо комбинировать атаку с другими типами атак

Квантовая угроза (1)

Квантовая угроза состоит в том, что имеются основания предполагать, что в обозримом будущем будет разработан квантовый вычислитель достаточной производительности, способный решать задачи, сложность которых лежит в основе стойкости целого ряда промышленно используемых в России и в мире асимметричных криптосистем.



электронная подпись и протоколы открытого распределения ключей типа Диффи-Хеллмана

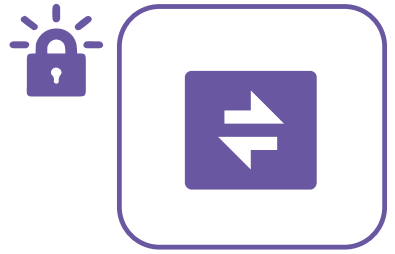


шифрование, контроль целостности/имитозащита, хэширование

При этом по современным представлениям системы симметричной криптографии останутся стойкими (при необходимости повышения стойкости достаточно будет двукратного увеличения длин ключей и/или выходов хэш-функций).

Квантовая угроза (2)

Учет квантовой угрозы необходим, в первую очередь, в системах, использующих асимметричные криптографические механизмы, в частности такие, где для защиты каналов связи применяются протоколы TLS и IPsec, использующие для установления общих ключей шифрования каналов протокол Диффи-Хеллмана.



Замена в таких системах асимметричных протоколов выработки ключей на протоколы КРК

- обеспечит защиту от квантовой угрозы
- и при этом не потребует изменений других этапов реализации «классических» криптографических протоколов, что удобно с точки зрения эксплуатации

Квантовая угроза (3)

Например, при встраивании постквантовых механизмов инкапсуляции ключей (KEM) в протокол TLS Handshake потребуется:

- пересмотреть стандартную структуру протокола (включая формат заголовков пакетов)
- провести дополнительные исследования безопасности протокола

Увеличенные размеры параметров, присущие постквантовым механизмам, также приводят к увеличению объемов трафика.

При использовании ключей, вырабатываемых системой КРК, возможно использование режима TLS «предраспределенные» ключи. Это не потребует значимых изменений структуры протокола.

Заключение

1. **Особенности** систем КРК наводят на мысль о целесообразности их использования в территориально распределенных системах, в первую очередь государственных (ГИС), в качестве меры, направленной на обеспечение гарантированно надежной (и не зависящей от человеческого фактора, безлюдной) работы с криптографическими ключами при любых возникающих сейчас и в обозримой перспективе нагрузках на ключи, в т.ч. с учетом перспективных угроз (в частности, квантовой угрозы).

2. **Целесообразно** применять системы КРК в тех ИС, для которых в рамках модели угроз требования противодействия нарушителю типа Н3 (класс КС3 СКЗИ) дополнены дополнительными требованиями по работе с ключами (например, в случае, когда ИС признана объектом КИИ).

СПАСИБО ЗА ВНИМАНИЕ!

Науменко Антон Павлович

Зам. начальника отдела специальных исследований и разработок
ООО «СФБ Лаб», АО «ИнфоТеКС»

+7 (916) 987-44-83

anton.naumenko@infotecs.ru

MICROELECTRONICA.PRO

ПОДПИСЫВАЙТЕСЬ И БУДЬТЕ В КУРСЕ ВСЕХ ПОСЛЕДНИХ НОВОСТЕЙ!

ВАШ ЛИЧНЫЙ КАБИНЕТ

Rutube

VK Видео