О перспективах использования систем квантового распределения ключей в государственных информационных системах

Науменко Антон Павлович, к.ф.-м.н.

Зам. генерального директора –
директор по развитию

конференция РусКрипто

26 марта 2026 года

anton.naumenko@infotecs.ru

Введение

Системы КРК (ККС ВРК) позволяют защититься как от перспективных угроз в виде появления нарушителя с квантовым вычислителем так и от актуальных угроз связанных с влиянием человеческого фактора на безопасность ключевого материала

Квантовый нарушитель

Нарушитель 2 категории

Угрозы информационной безопасности с учетом человеческого фактора

Инциденты информационной безопасности (далее – **ИБ**), связанные с действиями внутреннего нарушителя согласно статистическим исследованиям*, составляют до **15%** от общего количества, причем до **3%** связаны с действиями **привилегированного** пользователя/администратора безопасности.

Применение **ККС ВРК** позволяет **защитить** ключевой материал от действий внутренних нарушителей и **парировать** угрозы информационной безопасности

- УБИ.067 «Угроза неправомерного ознакомления с защищаемой информацией»
- УБИ.086 «Угроза несанкционированного изменения аутентификационной информации»
- УБИ.088 «Угроза несанкционированного копирования защищаемой информации»
- УБИ.156 «Угроза утраты носителей информации»
- УБИ.160 «Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации»
- УБИ.179 «Угроза несанкционированной модификации защищаемой информации»
- УБИ.187 «Угроза несанкционированного воздействия на средство защиты информации»

* Аналитический отчет. Утечки данных вследствие действий внутренних нарушителей. Мир-Россия 2022-2025. InfoWatch, 2025 год

Оценка вероятности компрометации системы по вине администратора

Критерий оценки, подразумевающий, что вся система будет скомпрометирована в случае утечки ключевого материала по вине любого администратора безопасности:

$$P_{\text{утечки}} = 1 - \left(1 - P_{\text{адм}}\right)^{N_{\text{адм}}} \leq P_{\text{крит}}$$

- $P_{\text{адм}}$ – вероятность утечки ключевого материала в результате умышленных/неумышленных действий администратора (оценивается экспертным методом)
- $N_{\text{адм}}$ – количество администраторов в ИС
- $P_{\text{крит}}$ – критическая величина вероятности утечки информации по вине администраторов, определяемая оператором/владельцем ИС

Предложения по оценке актуальности квантовой угрозы

При разработке модели угроз и нарушителя оператор/владелец ГИС должен определить **актуальность квантовой угрозы**

Данное решение может быть принято в результате **экспертной оценки специалистов** в области квантовых вычислений или на основе информации, представляемой профильными подразделениями или специалистами владельца информации или оператора

Во время экспертной оценки должен быть проведен **анализ открытых источников в области квантовых вычислений**, а также построен **прогноз времени появления квантового вычислителя**, обладающего необходимыми вычислительными способностями для реализации квантовой угрозы с учетом:

- **планируемого срока эксплуатации ИС и**
- **времени, в течение которого обрабатываемая информация сохраняет ценность**

Предложения по оценке актуальности квантовой угрозы

Вычислительные способности квантового вычислителя определяются оценкой доступного количества **логических кубит**. Для данной оценки рекомендуется использовать приближенную формулу для поверхностных кодов:

$$n_{logical} \approx n_{physical} \times \left(4 \log \left(\frac{\sqrt{10} P_{physical} / P_{logical}}{P_{threshold} / P_{physical}} \right) + 1 \right)^{-2},$$

- $n_{logical}$ – количество логических кубитов,
- $n_{physical}$ – количество физических кубитов;
- $P_{physical}$ – вероятность ошибки квантового гейта, реализованного физическими кубитами;
- $P_{logical}$ – допустимая вероятность ошибки квантового гейта, реализованного логическими кубитами;
- $P_{threshold} \leq 10^{-2}$ – пороговая вероятность ошибки для работы поверхностных кодов.

Оценка ресурсов квантового противника для атак на алгоритмы электронной подписи и открытого распределения ключей

Битовая длина модуля p	Количество логических кубитов	Количество квантовых гейтов	Источник
256	2338	$8{,}79 \cdot 10^{11}$	[1]
	2124	$4{,}98 \cdot 10^{10}$	[2]
	2619	$2{,}31 \cdot 10^{11}$	
	2871	$5{,}75 \cdot 10^{11}$	
	2326	$8{,}34 \cdot 10^{10}$	[3]
	2052	$2{,}81 \cdot 10^{11}$	[4]
512	4727	$7{,}96 \cdot 10^{12}$	[1]
	4258	$5{,}44 \cdot 10^{10}$	[2]
	5273	$1{,}07 \cdot 10^{12}$	
	5789	$2{,}03 \cdot 10^{11}$	
	4100	$2{,}06 \cdot 10^{12}$	[4]

Угроза: применение алгоритма Шора для ЭК для атак на алгоритм электронной подписи, алгоритм согласования ключей и протоколы, их использующие

ГОСТ 34.10-2018

восстановление закрытого ключа по открытому:

$$Q = [d]P$$

восстановление закрытого ключа по значению подписи:

$$\zeta = r \parallel s,\ d = \left(s - kH(msg)\right) \cdot r^{-1} \bmod q,$$
$$C = [k]P = (x_C, y_C),\ r = x_C$$

VKO (P 50.1.113-2016)

восстановление закрытого ключа по открытому:

$$K(x,y,UKM) = (m/q \cdot UKM \cdot x \bmod q)(y \cdot P)$$

[1] Roetteler, Martin, Michael Naehrig, Krysta M. Svore, and Kristin Lauter. «Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms»

[2] Häner, Thomas, Samuel Jaques, Michael Naehrig, Martin Roetteler, and Mathias Soeken. «Improved Quantum Circuits for Elliptic Curve Discrete Logarithms»

[3] Gouzien E., Ruiz D., Regent F.M., Guillaud J., Sangouard, N., «Performance Analysis of a Repetition Cat Code Architecture: Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits»

[4] Денисенко Д.В., Никитенкова М.Н., «О реализации ГОСТ 34.10-2018, ГОСТ 34.11-2018 и ГОСТ 34.12-2018 в виде квантовых схем с минимальным количеством кубитов»

Оценка ресурсов квантового нарушителя для атак на блочные шифры

Алгоритм	Количество логических кубитов	Количество квантовых гейтов	Источник
Магма	546	$4{,}03 \cdot 10^{44}$	[5]
	2369	$2{,}01 \cdot 10^{44}$	
	321	$2{,}80 \cdot 10^{46}$	[6] (квантовая схема шифра)
Кузнечик	1793	$4{,}03 \cdot 10^{44}$	[5]
	14976	$2{,}47 \cdot 10^{44}$	

Угроза: применение алгоритма Гровера для атак на алгоритм блочные шифры и режимы их работы

ГОСТ 34.12-2018, ГОСТ 34.13-2018

восстановление закрытого ключа по выборке известных пар **ОТ/ШТ** $(P_1,C_1),\ldots,(P_u,C_u)$

$u=4$ для алгоритма «Магма», **$u=2$** для алгоритма «Кузнечик»

[5] Денисенко Д.В., Маршалко Г.Б., Никитенкова М.В., Рудской В.И., Шишкин В.А. «Оценка сложности реализации алгоритма Гровера для перебора ключей алгоритмов блочного шифрования ГОСТ Р 34.12-2015». Журнал экспериментальной и теоретической физики. 2019. Т. 128. № 4. С. 552-559

[6] Денисенко Д.В., Никитенкова М.Н., «О реализации ГОСТ 34.10-2018, ГОСТ 34.11-2018 и ГОСТ 34.12-2018 в виде квантовых схем с минимальным количеством кубитов»

Оценка ресурсов квантового нарушителя для атак на парольную аутентификацию

Алгоритм	Количество логических кубитов	Количество квантовых гейтов	Источник
Стрибог	1537	$2{,}39 \cdot 10^8 \cdot 2^{|pass|/2}$	[7] (квантовая схема хэш-функции)

С учетом рекомендованных ТК26 параметров для алгоритма PBKDF2: алфавит мощности **156** символов, длина пароля **32** символа, число итераций $\mathbf{c = 8{,}3 \cdot 10^6}$, сложность перебора пароля алгоритмом Гровера составляет $\mathbf{2{,}75 \cdot 10^{50}}$ квантовых операций.

Угроза: применение алгоритма Гровера для атак на механизмы парольной аутентификации на основе хэш-функции

ГОСТ 34.11-2018, PBKDF2 (Р 1323565.1.040– 2022)

восстановление пароля по хэш-значению

$$h = H(pass,salt)$$

[7] Денисенко Д.В., Никитенкова М.Н., «О реализации ГОСТ 34.10-2018, ГОСТ 34.11-2018 и ГОСТ 34.12-2018 в виде квантовых схем с минимальным количеством кубитов»

Использованием ККС ВРК для решения проблем с нагрузкой на ключ

При использовании алгоритма ГОСТ 34.12-2018 **«Магма»** в режимах работы по ГОСТ 34.13-2018 допускается обрабатывать порядка $\leq 2^{31}$ блоков данных

(суммарно с учетом количества и длины сообщений)

Системы ККС ВРК позволяют обеспечить регулярную и быструю сменяемость ключей при высоких скоростях работы

Скорость, Гбит/с	Частота смены ключа, сек
1	137
25	5,4
100	1,37
1200	0,114

Альтернативой является использование **BBB-режимов** с улучшенными оценками нагрузки на ключ, например AEAD-режимов MXP и MXP2*

BBB (Beyond the Birthday Bound) – режимы, стойкие при пересечении «границы дней рождения» ($2^{n/2}$)

* Кирюхин В.А. “AEAD-mode MXP – beyond the birthday bound without loss of efficiency” (CTCrypt’25); MXP2 – на CTCrypt’26

Угрозы информационной безопасности с учетом человеческого фактора и появления перспективных квантовых вычислителей

Рассматриваются следующие классы угроз в отношении криптографических алгоритмов:

угрозы, связанные с электронной подписью (ГОСТ 34.10-2018)

- компрометация ключа подписи
- подделка электронной подписи

угрозы, связанные с распределением ключей (VKO)

- компрометация секретного ключа одной из сторон
- компрометация распределяемого ключа
- атака типа «человек посередине» (нарушитель вырабатывает независимые ключи с двумя сторонами)

угрозы, связанные с нарушением конфиденциальности при использовании режимов шифрования (ГОСТ 34.13-2018)

- компрометация секретного ключа шифрования

угрозы, связанные с нарушением целостности при использовании режимов имитозащиты (ГОСТ 34.13-2018)

- компрометация секретного ключа имитозащиты
- навязывание ложных данных

угрозы, связанные с (парольной) аутентификацией (алгоритмы, основанные на хэш-функции ГОСТ 34.11-2018)

- компрометация фактора аутентификации (пароля)
- ложная аутентификация

Угрозы информационной безопасности с учетом появления перспективных квантовых вычислителей

С появлением квантовых вычислителей **перспективными** угрозами информационной безопасности можно считать атаки на **следующие криптографические механизмы:**

- схема цифровой подписи, реализованная в соответствии с ГОСТ 34.10-2018
- протоколы выработки общего секретного ключа, реализованные в соответствии с ГОСТ Р 50.1.113-2016, ГОСТ Р 1323565.1.048-2023, ГОСТ Р 1323565.1.004-2017

А также на **производные криптографические механизмы:**

- Схема формирования и проверки кода проверки в соответствии с ГОСТ Р 1323565.1.062-2025
- Протокол обмена ключами в сети Интернет версии 2 (IKEv2) в соответствии с ГОСТ Р 1323565.1.048-2023
- Криптографический протокол OpenID Connect в соответствии с МР 26.2.002-2024 в режиме использования протокола выработки общего секретного ключа
- Протокол получения актуальных статусов сертификатов OCSP в соответствии с ГОСТ Р 1323565.1.059-2024
- Криптографический протокол аутентификации между интегральной схемой карты и терминалом в соответствии с ГОСТ Р 1323565.1.013-2017
- Схема формирования и проверки в профиле EMV сертификатов открытых ключей платежных систем в соответствии с ГОСТ Р 1323565.1.015-2018
- Схема оффлайновой аутентификации платежного приложения в соответствии с ГОСТ Р 1323565.1.016-2018
- Криптографический протокол аутентификации и выработки общего ключа для контрольных устройств автотранспорта в соответствии с ГОСТ Р 1323565.1.018-2018
- Криптографический протокол TLS 1.2 в соответствии с ГОСТ Р 1323565.1.020-2020
- Криптографический протокол TLS 1.3 в соответствии с ГОСТ Р 1323565.1.043-2022
- Криптографический протокол DLMS в соответствии с ГОСТ Р 1323565.1.032-2020
- Протокол сообщений на основе XML-документа в соответствии с ГОСТ Р 1323565.1.033-2020
- Протокол штампов времени TSP в соответствии с ГОСТ Р 1323565.1.044-2022

Меры обеспечения безопасности реализованные с помощью криптографических механизмов

№	Мера обеспечения безопасности
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах
РСБ.7	Защита информации о событиях безопасности
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

* Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014

Меры обеспечения безопасности реализованные с помощью криптографических механизмов

№	Мера обеспечения безопасности
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны
ЗИС 15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации
ЗИС 20	Защита беспроводных соединений, применяемых в информационной системе
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе

* Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014

Сценарии использования

В зависимости от специфики информационной системы, в том числе ГИС и объектов КИИ, могут возникнуть следующие схемы развертывания ККС ВРК:

в рамках одной контролируемой зоны (КЗ)

данная схема предполагает использования ККС ВРК для повышения защищенности ИС от человеческого фактора

в рамках нескольких контролируемых зон

данная схема предполагает использования ККС ВРК для повышения защищенности ИС от человеческого фактора и нарушителя с квантовым вычислителем

путем сопряжения с магистральной квантовой сети доверенных промежуточных узлов (МКС ДПУ)

данная схема предполагает использования ККС ВРК для связи распределенных ИС (сегментов ИС) в федеральном масштабе

Схема развертывания ККС ВРК между сегментами территориально распределенной ГИС (между разными ГИС)

- При схеме развертывания в рамках нескольких контролируемых зон ККС ВРК применяется для организации **защищенного взаимодействия**.
- При этом каждая развернутая ККС ВРК в рамках своего сегмента ГИС позволяет выполнять функции, соответствующие схеме развертывания в рамках одного объекта ГИС.
- В связи с этим, осуществляется **минимизация угроз** со стороны внутреннего нарушителя и обеспечение **гарантированной** смены ключей для средств защиты на всех узлах сети.

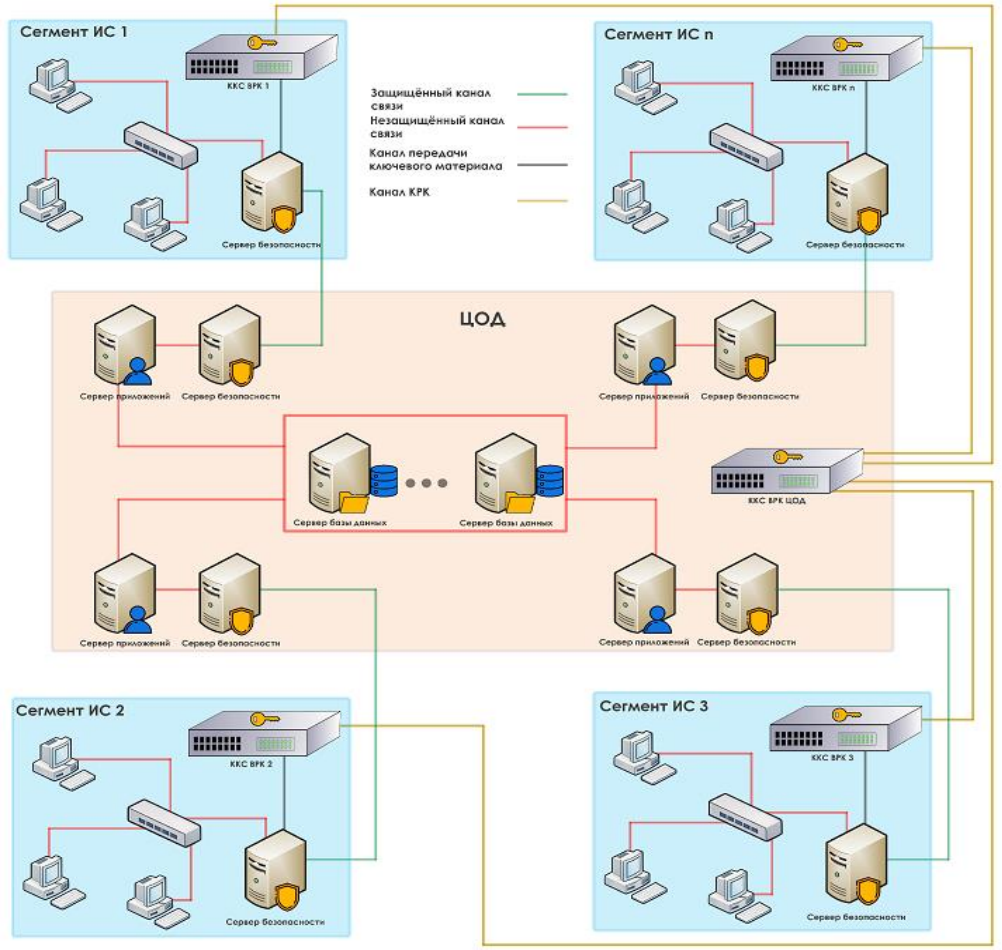


Схема развертывания ККС ВРК для организации защищенного взаимодействия с ЦОД

Схема развертывания ККС ВРК с использованием магистральной квантовой сети

Данная схема развертывания предназначена для:

1. Использования ККС ВРК при организации доверенного канала передачи информации между **сегментами одной ГИС**, в том числе распределенных в федеральном масштабе;
2. Использования ККС ВРК при организации защищённого взаимодействия **между любыми ГИС (сегментами разных ГИС), подключенных к МКС ДПУ**. Данный сценарий позволяет значительно облегчить ввод в эксплуатацию новых ГИС и подключения их к системам межведомственного электронного взаимодействия;
3. Создания **общей информационно-коммуникационной сети** (сегмента Интернета), защищенной на симметричных ключах.

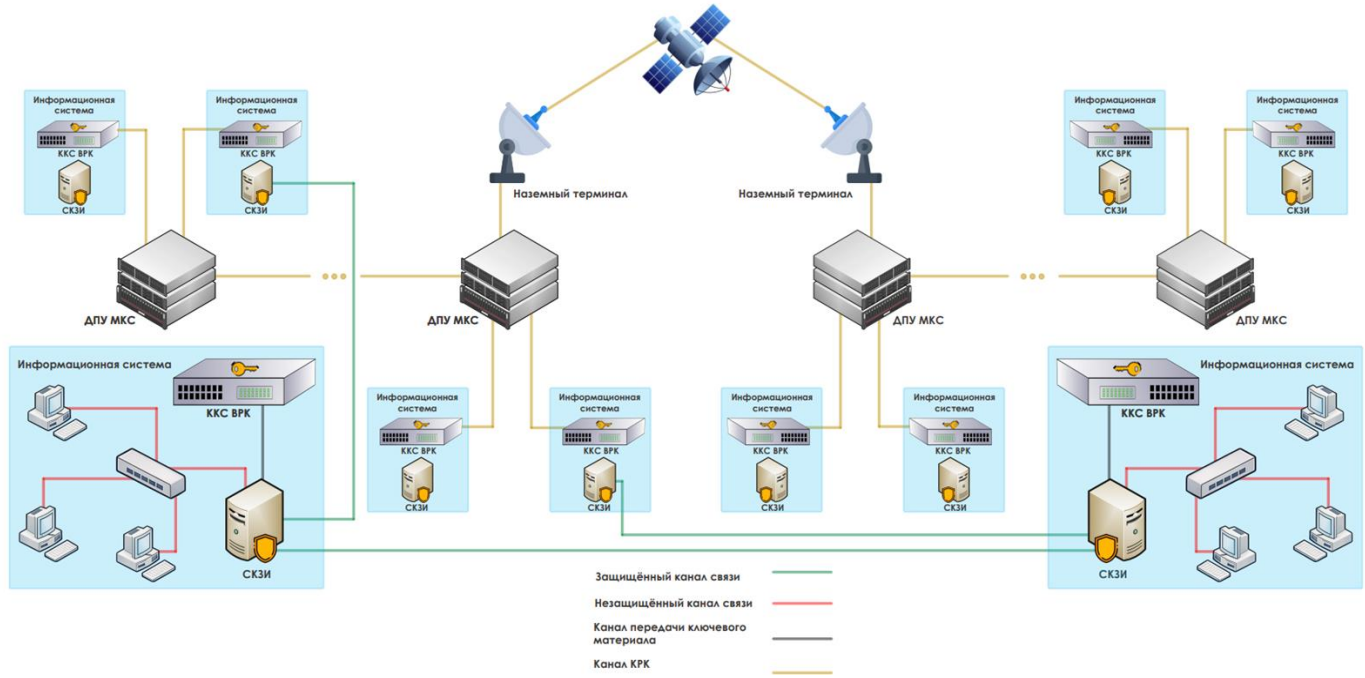
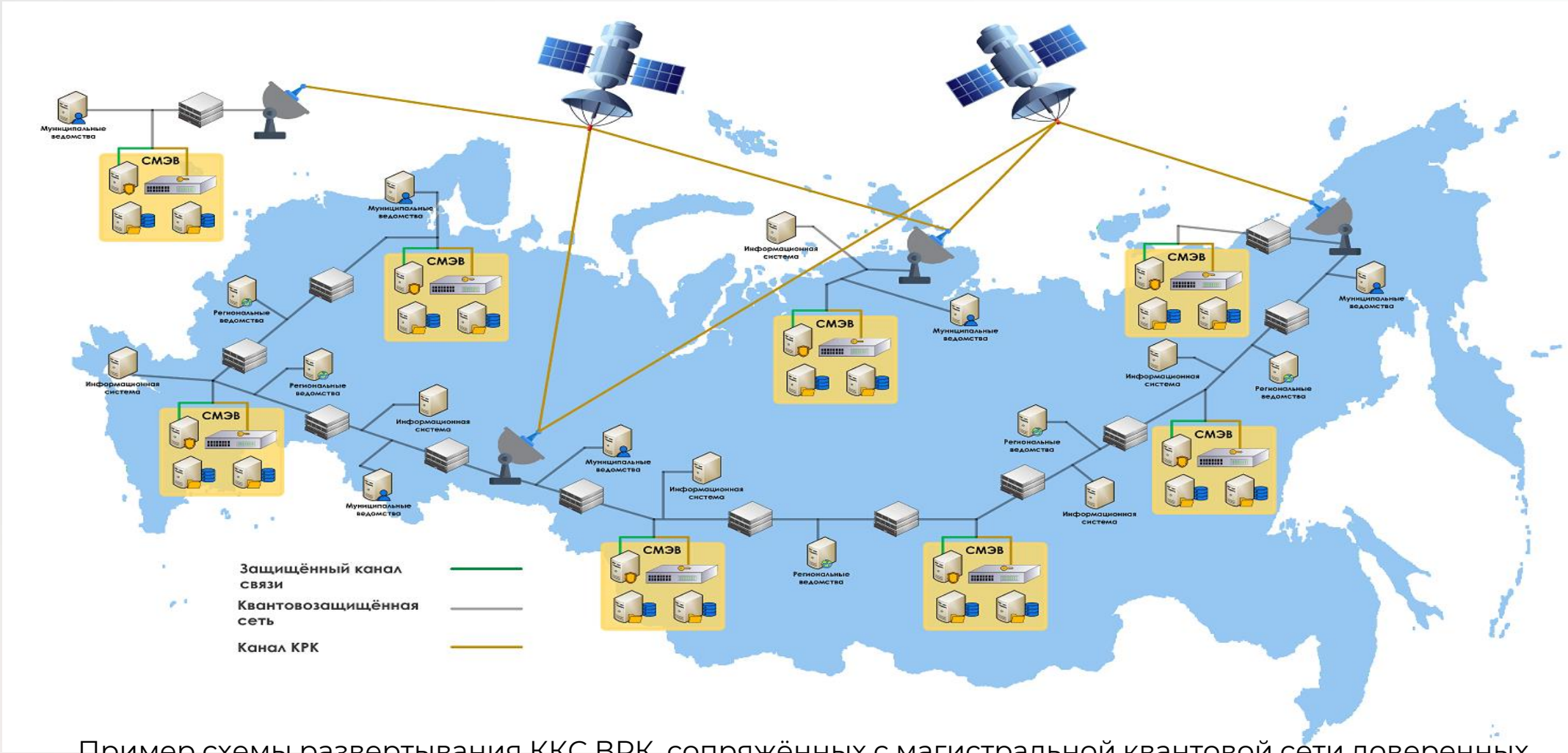


Схема развертывания ККС ВРК, сопряжённых с магистральной квантовой сети доверенных промежуточных узлов

Схема развертывания ККС ВРК с использованием магистральной квантовой сети



Пример схемы развертывания ККС ВРК, сопряжённых с магистральной квантовой сети доверенных промежуточных узлов для ГИС «Система электронного межведомственного взаимодействия», распределенной в федеральном масштабе

Рекомендации по парированию угроз со стороны квантового нарушителя с помощью ККС ВРК в ГИС

ККС ВРК рекомендуется использовать для парирования угроз **квантового нарушителя** для ГИС **первого класса защищённости (К1).**

Соответствие уровней значимости обрабатываемой информации, масштаба информационной системы и применения ККС ВРК для парирования угроз со стороны **квантового нарушителя**:

Уровень значимости информации (УЗ)	**Масштаб информационной системы (ИС, сегмента ИС)**		
	Федеральный	**Региональный**	**Объектовый**
Высокий уровень значимости (УЗ 1)	+	+	+
Средний уровень значимости (УЗ 2)	+	-	-
Низкий уровень значимости (УЗ 3)	-	-	-

Рекомендации по парированию угроз со стороны внутреннего нарушителя с помощью ККС ВРК в ГИС

ККС ВРК рекомендуется использовать для парирования угроз, приводящих к нарушению конфиденциальности ключевого материала со стороны **внутреннего нарушителя** в ГИС **первого и второго классов защищённости (К1 и К2).**

Соответствие уровней значимости обрабатываемой информации, масштаба информационной системы и применения ККС ВРК для парирования угроз со стороны **внутреннего нарушителя**

Уровень значимости информации (УЗ)	Масштаб информационной системы (ИС, сегмента ИС)		
	Федеральный	Региональный	Объектовый
Высокий уровень значимости (УЗ 1)	+	+	+
Средний уровень значимости (УЗ 2)	+	+	-
Низкий уровень значимости (УЗ 3)	+	-	-

Заключение

1. При разработке модели угроз и нарушителя оператор/владелец ГИС должен **определить актуальность квантовой угрозы**. Предложен методический подход к данной оценке

2. При разработке модели угроз и нарушителя оператор/владелец ГИС должен **определить актуальность угрозы**, что **администратор безопасности** (любое лицо, имеющее доступ к ключевой информации при выполнении своих должностных обязанностей) **является внутренним нарушителем**. Предложен вероятностный критерий оценки актуальности угрозы утечки ключевой информации для системы с множеством администраторов безопасности

3. **Системы КРК (ККС ВРК) целесообразно применять в ГИС** (и любых других ИС), **для которых признана актуальной хотя бы одна из угроз**, описанных в пункте 1 и 2

* более подробно предложенные подходы описаны в документе *"Методика оценки типовых угроз со стороны нарушителей и последствий при их реализации в отношении ГИС и ЗОКИИ, а также целесообразности использования в целях парирования данных угроз ККС ВРК"*

СПАСИБО ЗА ВНИМАНИЕ!

Науменко Антон Павлович, к.ф.-м.н.

Зам. генерального директора –
директор по развитию

конференция РусКрипто

26 марта 2026 года

anton.naumenko@infotecs.ru