РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

О подходах к снижению эксплуатационных издержек при использовании систем квантового распределения ключей с доверенными промежуточными узлами (ДПУ)

А.П Науменко, И.М. Арбеков, С.Н. Молотков

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2025
20 марта 2025

Anton.Naumenko@infotecs.ru

СФБ ЛАБ

”Курица не птица, логарифм не бесконечность”
(расхожий афоризм физиков-математиков)

”Курица не птица, логарифм не бесконечность”
(расхожий афоризм физиков-математиков)

- Системы КРК позволяют обеспечить стороны квантовыми ключами, обладающими заданным уровнем секретности

”Курица не птица, логарифм не бесконечность”
(расхожий афоризм физиков-математиков)

- Системы КРК позволяют обеспечить стороны квантовыми ключами, обладающими заданным уровнем секретности
- Для аутентификации участников КРК необходим предраспределенный ключ, который доставляется на физических носителях. При окончании срока действия необходима его смена

”Курица не птица, логарифм не бесконечность”
(расхожий афоризм физиков-математиков)

- Системы КРК позволяют обеспечить стороны квантовыми ключами, обладающими заданным уровнем секретности
- Для аутентификации участников КРК необходим предраспределенный ключ, который доставляется на физических носителях. При окончании срока действия необходима его смена
- Максимальное расстояние распределения ключей $\approx$ 100 км

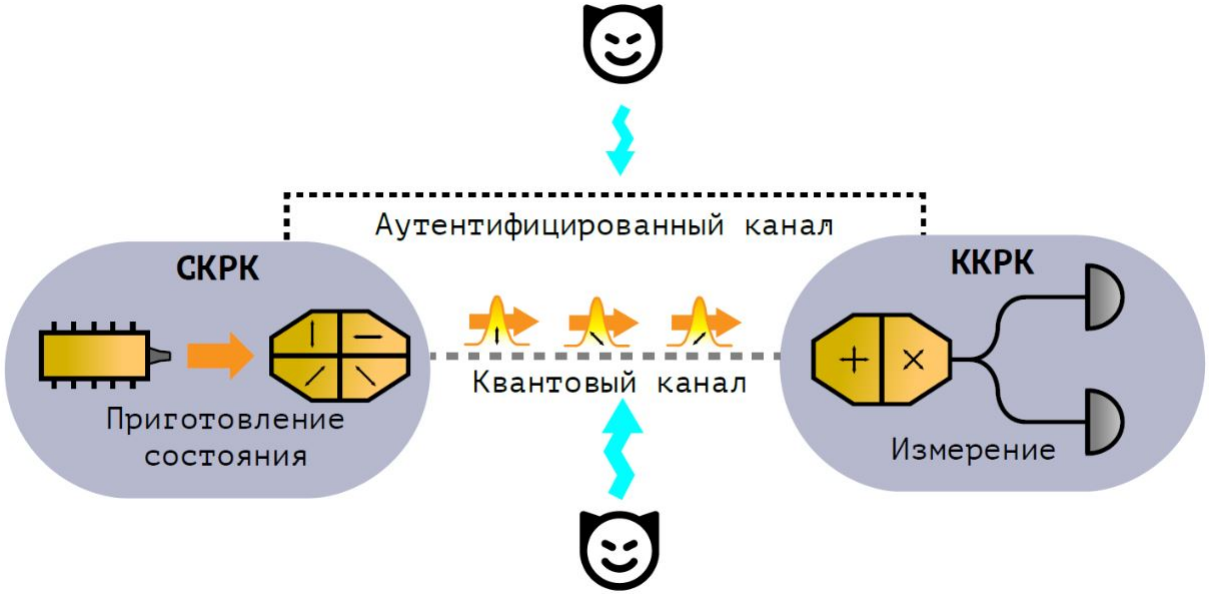
”Курица не птица, логарифм не бесконечность”
(расхожий афоризм физиков-математиков)

- Системы КРК позволяют обеспечить стороны квантовыми ключами, обладающими заданным уровнем секретности
- Для аутентификации участников КРК необходим предраспределенный ключ, который доставляется на физических носителях. При окончании срока действия необходима его смена
- Максимальное расстояние распределения ключей $\approx$ 100 км

Как распределить квантовые ключи на большие расстояния с одним предраспределенным ключом аутентификации?

КРК с одним предраспределенным ключом

Схема КРК



Квантовый канал – передача квантовых состояний, кодирующих логические биты

Аутентифицированный (служебный) канал – передача информации для реализации протокола КРК, требуется предраспределённый ключ

Секретность КК, один сеанс

СФБ ЛАБ

Теорема

Для одного сеанса КРК секретность ключа оценивается, как

$$\frac{1}{2}\left\|\rho^{Real}-\rho^{Ideal}\right\|_1 \leq \varepsilon_{Aut}+\varepsilon_{QKD}$$

ρ^{Real} – матрица плотности – реальный сеанс КРК,
ρ^{Ideal} – матрица плотности – идеальный сеанс КРК,
ε_{Aut} – качество предраспределенного ключа аутентификации,
ε_{QKD} – качество квантового ключа,
$\|\rho\| = \sum_{i,j}\left|\rho_{i,j}\right|$ – следовое расстояние (норма матрицы).

КРК, *N* сеансов

- В каждом сеансе КРК требуется обеспечить *аутентичность* служебного канала.

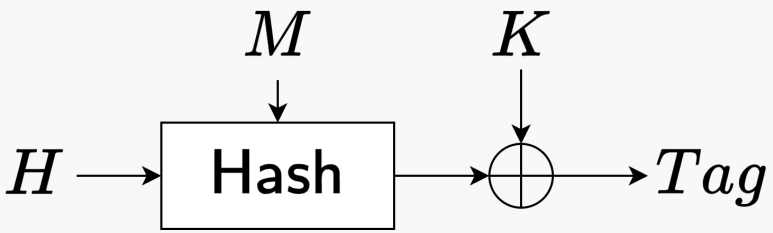
КРК, N сеансов

- В каждом сеансе КРК требуется обеспечить *аутентичность* служебного канала.
- Часть порождаемого в сеансе КРК квантового ключа используется для теоретико-информационной аутентификации в следующем сеансе.

КРК, N сеансов

- В каждом сеансе КРК требуется обеспечить *аутентичность* служебного канала.
- Часть порождаемого в сеансе КРК квантового ключа используется для теоретико-информационной аутентификации в следующем сеансе.

ТИ схема имитозащиты (Картера-Вегмана)



H – долговременный ключ
K – одноразовый ключ (квантовый)
Hash – хэш-функция специального вида

КРК, N сеансов

СФБ ЛАБ

Теорема

Для N-го сеанса

$$\frac{1}{2} \| \rho^{Real} - \rho^{Ideal} \|_1 \leq \varepsilon_{Aut} + N\varepsilon_{QKD} \leq \varepsilon_{crit}$$

N – число сеансов КРК,
ρ^{Real} – матрица плотности – реальный сеанс КРК,
ρ^{Ideal} – матрица плотности – идеальный сеанс КРК,
ε_{Aut} – качество предраспределенного ключа аутентификации,
ε_{QKD} – качество квантового ключа,
ε_{crit} – заданный уровень качества квантового ключа.

КРК, N сеансов

Для заданного уровня качества квантового ключа ε_{crit}

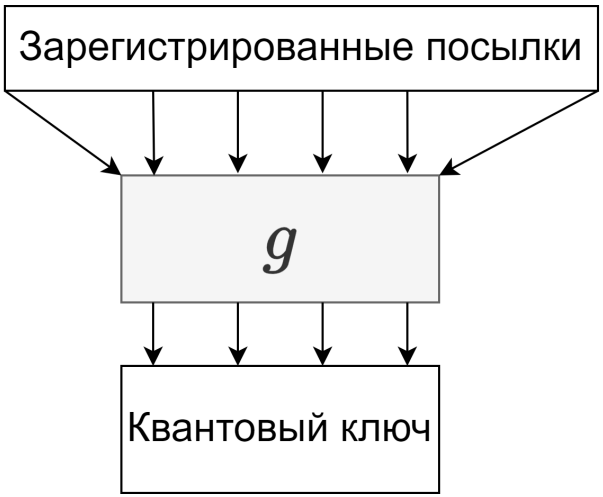
$$\varepsilon_{QKD} \leq \frac{\varepsilon_{crit}}{N}.$$

КРК, N сеансов

Для заданного уровня качества квантового ключа ε_{crit}

$$\varepsilon_{QKD} \leq \frac{\varepsilon_{crit}}{N}.$$

Малость ε_{QKD} достигается хэшированием (хэш-функция 2-ого порядка) n-битных зарегистрированных посылок квантовых состояний в квантовый ключ заданной длины

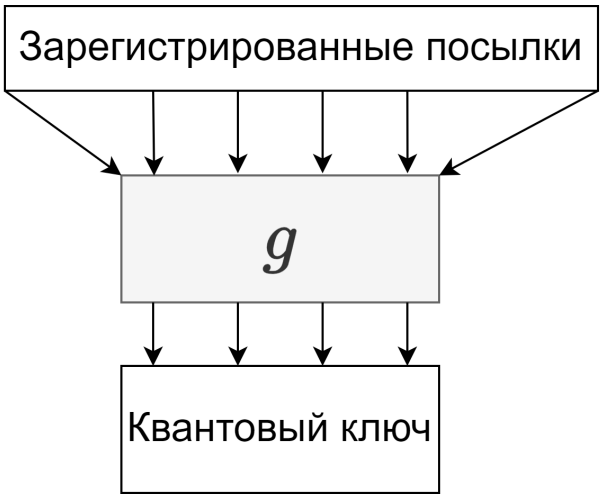


КРК, N сеансов

Для заданного уровня качества квантового ключа ε_{crit}

$$\varepsilon_{QKD} \leq \frac{\varepsilon_{crit}}{N}.$$

Малость ε_{QKD} достигается хэшированием (хэш-функция 2-ого порядка) n-битных зарегистрированных посылок квантовых состояний в квантовый ключ заданной длины



Чем меньше требуемое ε_{QKD}, тем больше требуется число n

КРК, N сеансов. Основной результат

СФБ ЛАБ

Теорема

Число n зарегистрированных посылок квантовых состояний на приемной стороне оценивается, как

$$n \propto \log(N) + \log\left(\frac{1}{\varepsilon_{crit}}\right)$$

N – число сеансов КРК

ε_{crit} – заданный уровень качества квантового ключа

$a \propto b$ – прямая пропорциональность, т.е. $\exists c_1, c_2 : \; c_1 b \leq a \leq c_2 b$

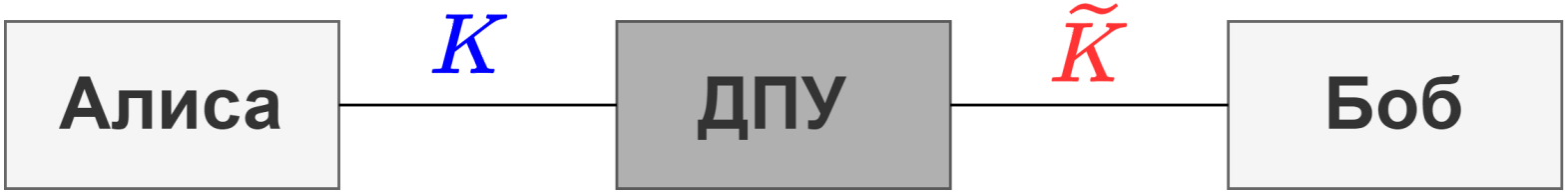
Распределение ключей на большие расстояния

Из-за неидеальности квантового канала ограничено максимальное расстояние распределения ключей ≈ 100 км

Из-за неидеальности квантового канала ограничено максимальное расстояние распределения ключей ≈ 100 км

Как распределить ключ на большее расстояние?

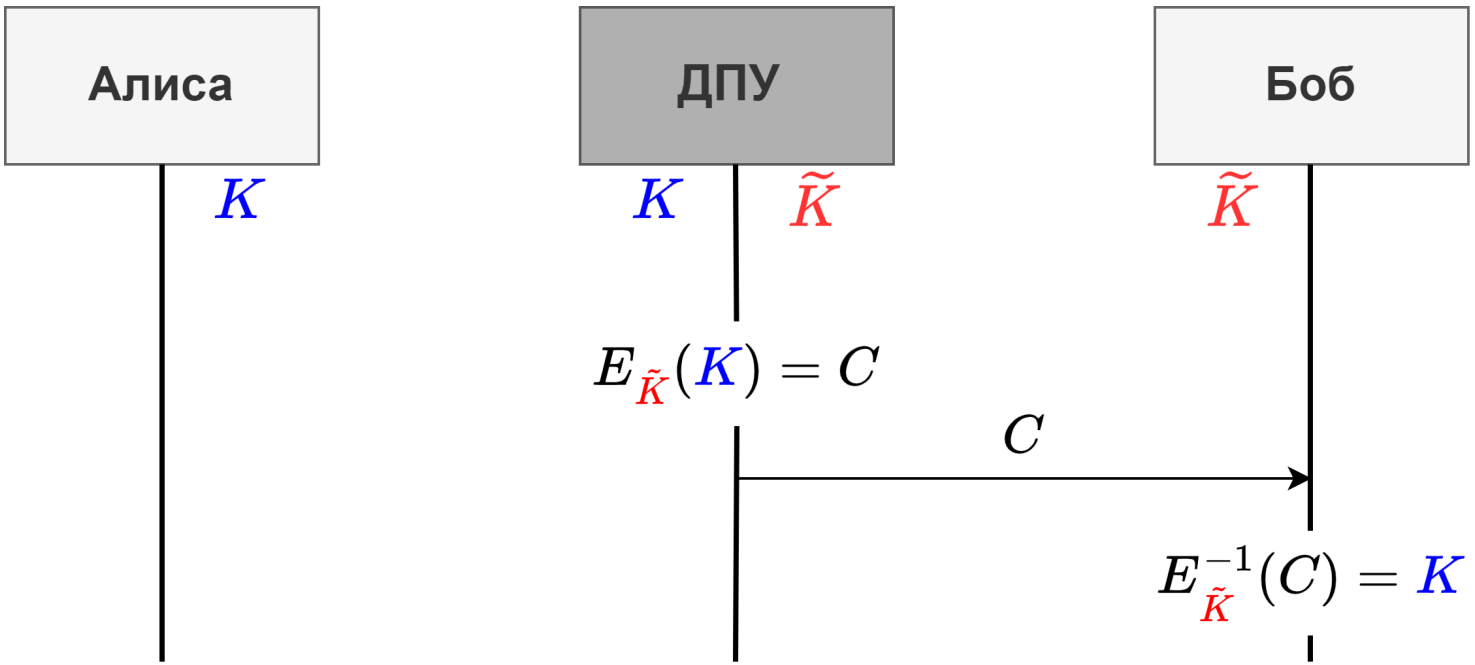
Доверенный промежуточный узел



Задача

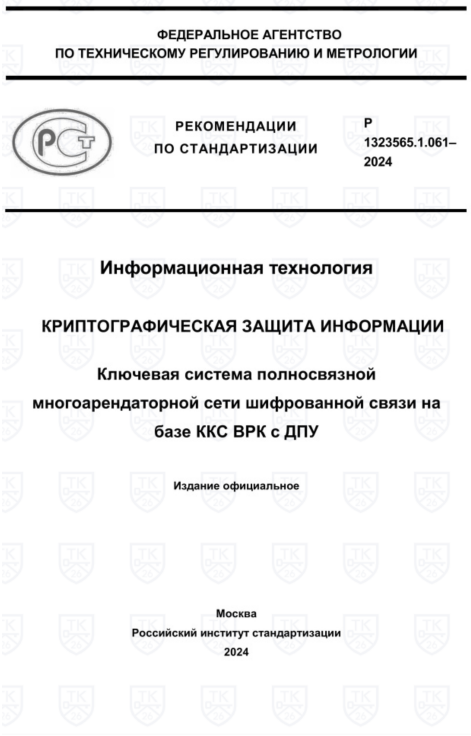
Выработать общий целевой (квантовозащищенный) ключ между сторонами **Алиса** и **Боб**

ДПУ. Идея



Алиса и **Боб** после передачи ключа через доверенный узел имеют целевой ключ K

Текущее состояние дел



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

Р
1323565.1.061–
2024

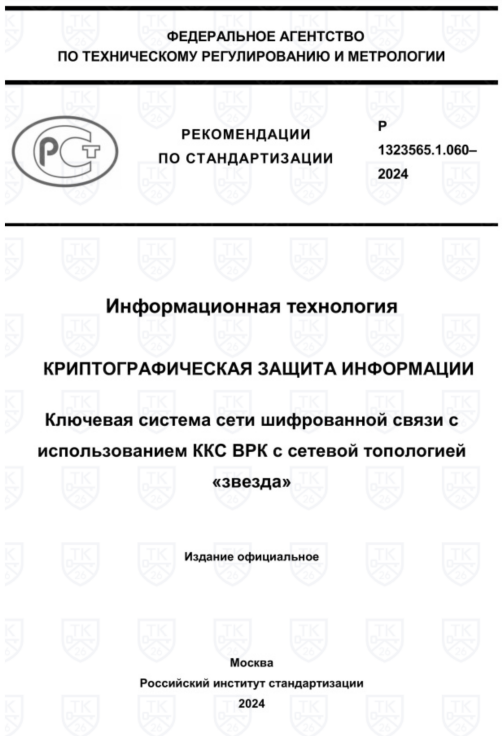
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ

Издание официальное

Москва
Российский институт стандартизации
2024



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

Р
1323565.1.060–
2024

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

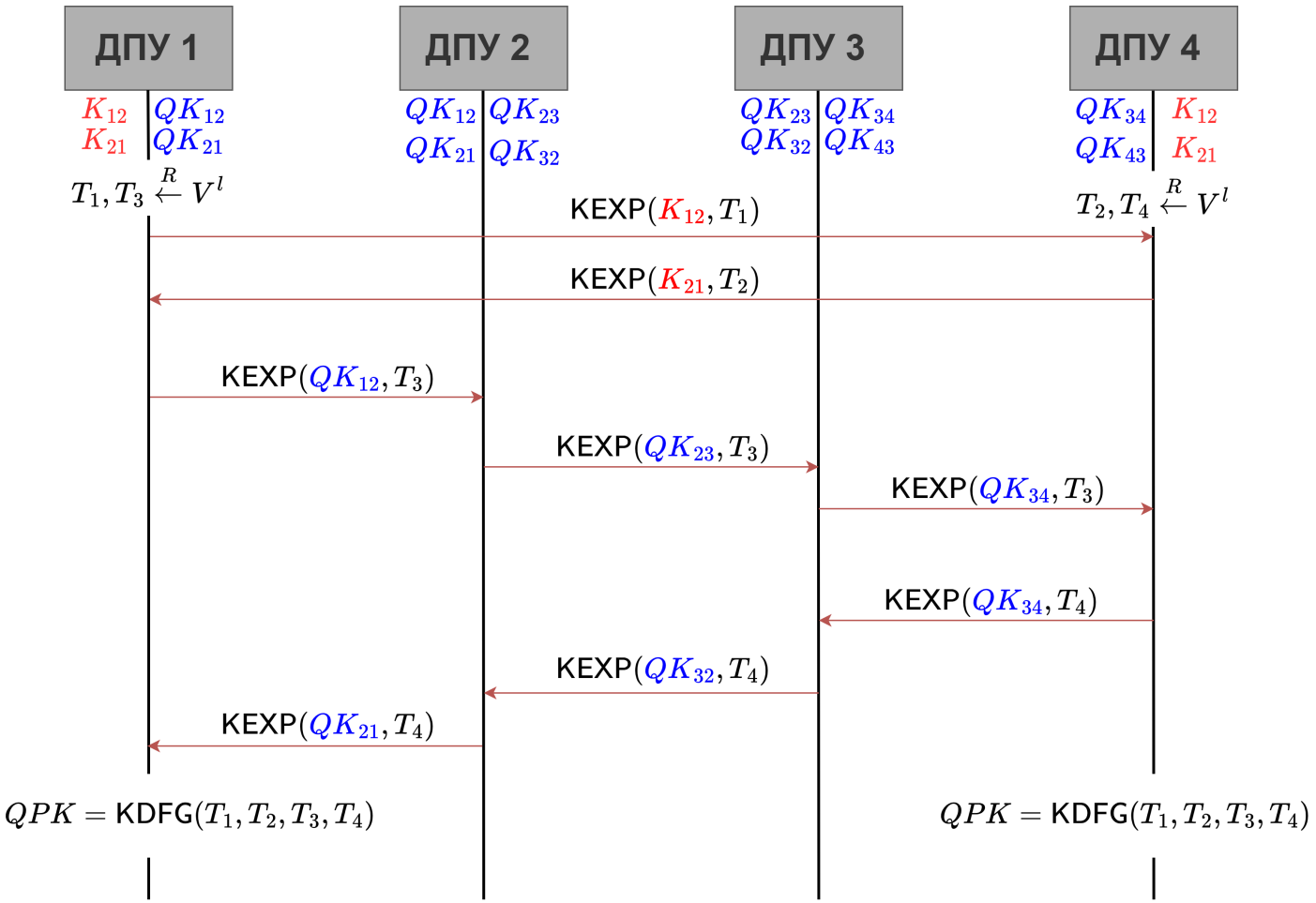
Ключевая система сети шифрованной связи с использованием ККС ВРК с сетевой топологией «звезда»

Издание официальное

Москва
Российский институт стандартизации
2024

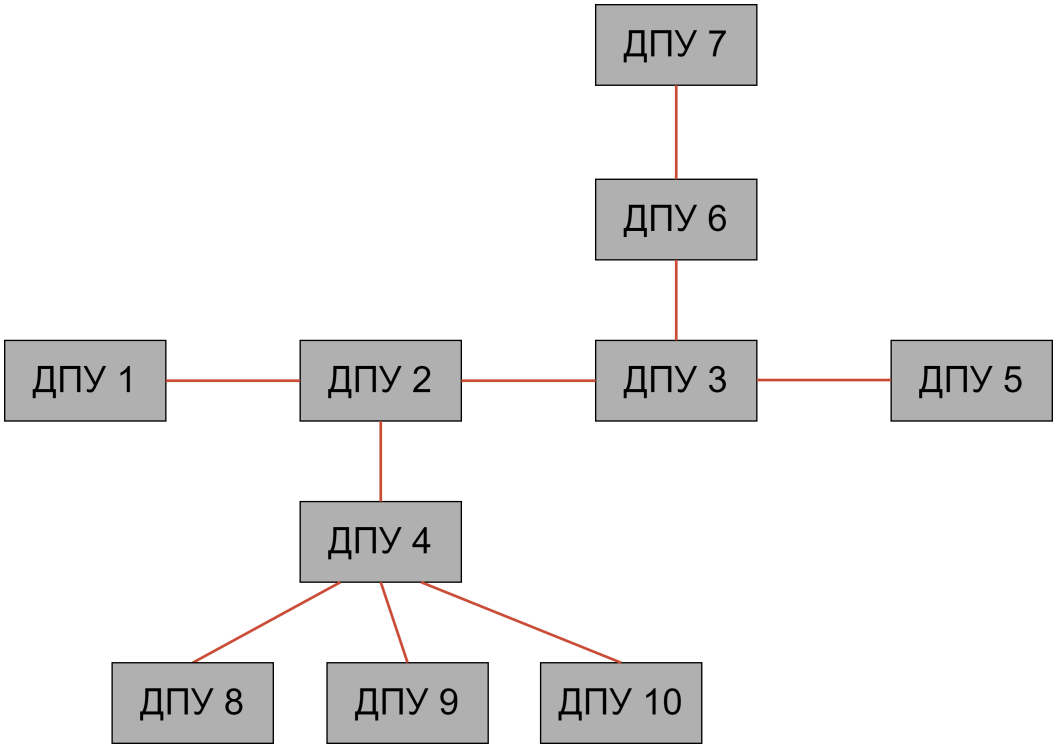
Р 1323565.1.060-2024 и Р 1323565.1.061-2024 описывают ключевые системы ISTOQ-A и ISTOQ-M, определяющие процесс **создания целевых ключей сети ДПУ** в топологии «звезда» и произвольной топологии соответственно

Текущее состояние дел. ISTOQ-M



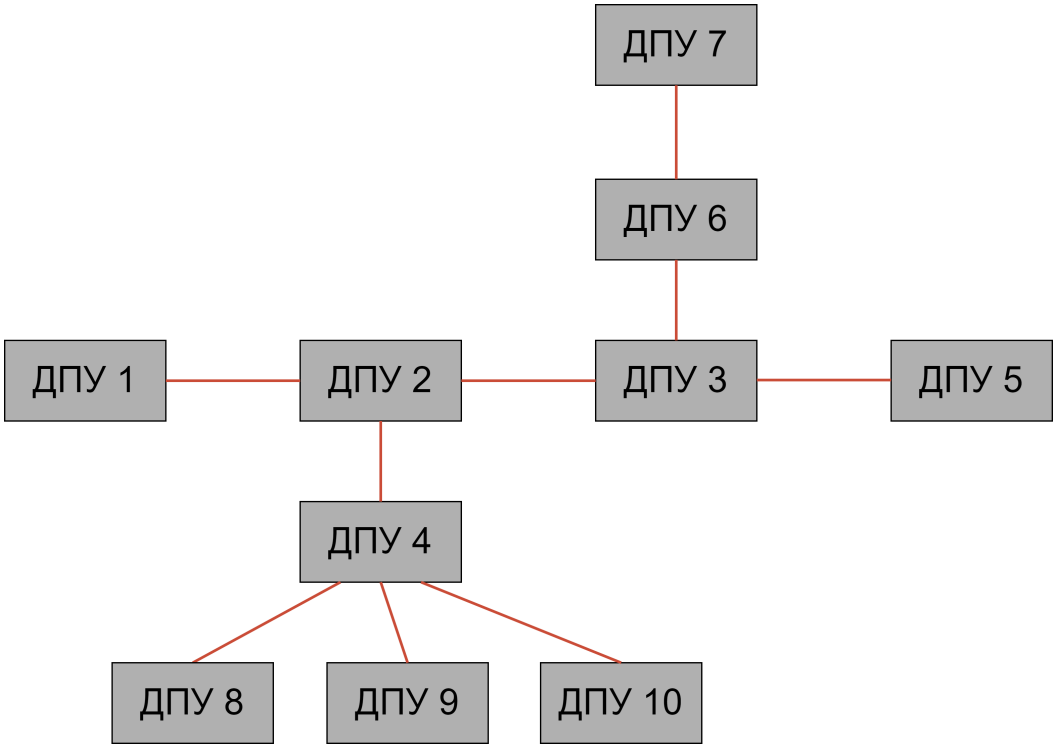
- K_{12},K_{21} – «классические» ключи
- QK_{12}, …. , QK_{43} – квантовые ключи
- QPK – целевой ключ

Текущее состояние дел



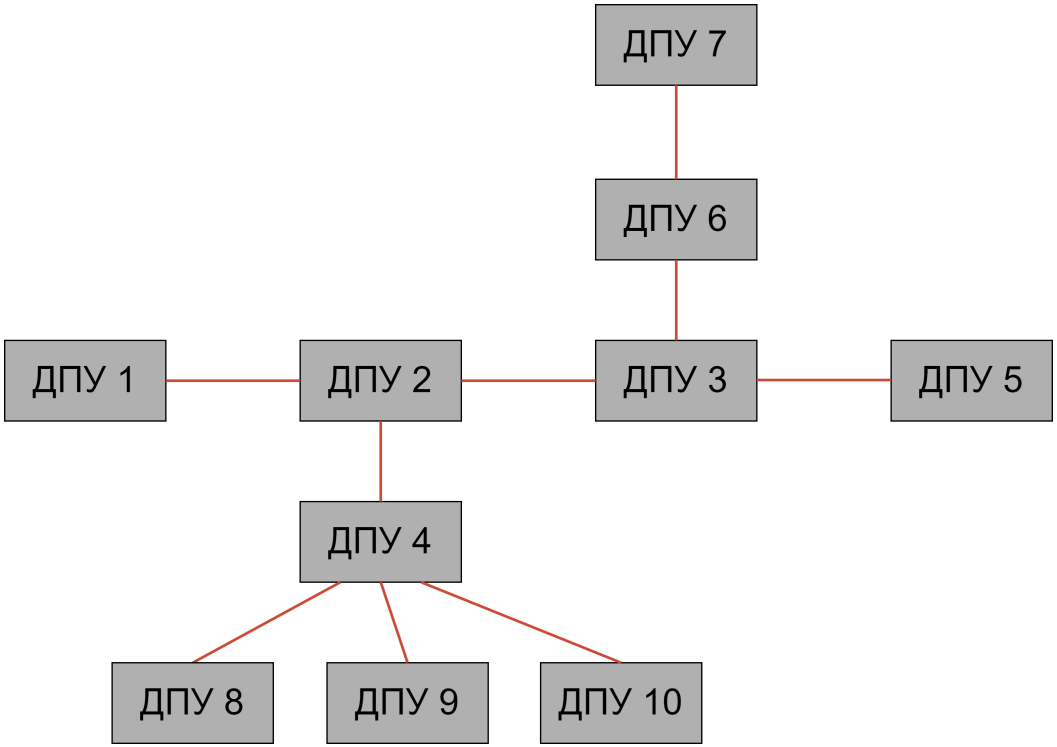
1. Администратор сети на каждый ДПУ вводит долговременный ключ для служебного канала

Текущее состояние дел



1. Администратор сети на каждый ДПУ вводит долговременный ключ для служебного канала
2. После окончания срока действия этих ключей Администратор загружает новые ключи

Текущее состояние дел



1. Администратор сети на каждый ДПУ вводит долговременный ключ для служебного канала
2. После окончания срока действия этих ключей Администратор загружает новые ключи

С ростом числа узлов и их географической удаленности своевременное обслуживание сети может быть затруднено!

Обеспечение КРК на большие расстояния с одним предраспределенным ключом

Основной результат для системы ДПУ

Теорема

Секретность квантового ключа для последнего N-ого сеанса

$$\frac{1}{2} \| \rho^{Real} - \rho^{Ideal} \|_1 \leq \varepsilon_{Aut} + N \cdot L \cdot \varepsilon_{QKD} \leq \varepsilon_{crit}$$

N – число сеансов КРК,
L – число ДПУ,
ε_{Aut} – качество *стартового* ключа аутентификации,
ε_{QKD} – качество квантового ключа,
ε_{crit} – заданный уровень качества квантового ключа.

Основной результат для системы ДПУ

Теорема

Число n зарегистрированных посылок квантовых состояний на приемной стороне оценивается, как

$$n \propto \log(N) + \log(L) + \log\left(\frac{1}{\varepsilon_{crit}}\right)$$

N – число сеансов КРК,
L – число ДПУ,
ε_{crit} – заданный уровень качества квантового ключа.

Заключение

Афоризм отражает фактическую ситуацию. Число физических ресурсов – число зарегистрированных квантовых состояний, **логарифмически** зависит от требуемого числа сеансов КРК, заданного числа ДПУ и уровня секретности ключей

Заключение

Афоризм отражает фактическую ситуацию. Число физических ресурсов – число зарегистрированных квантовых состояний, **логарифмически** зависит от требуемого числа сеансов КРК, заданного числа ДПУ и уровня секретности ключей

На текущем технологическом уровне возможно практически сколь угодно большое число сеансов КРК с использованием одного предраспределенного ключа

Благодарю за внимание!

А.П Науменко, И.М. Арбеков, С.Н. Молотков

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2025

20 марта 2025

Anton.Naumenko@infotecs.ru