



РОССИЙСКИЙ ФОРУМ  
МИКРОЭЛЕКТРОНИКА 2025



ФЕДЕРАЛЬНАЯ  
ТЕРРИТОРИЯ  
«СИРИУС»



21–27  
сентября 2025

Оптимизация архитектуры системы  
распределения квантовозащищенных  
ключей для мобильных потребителей

СПБ

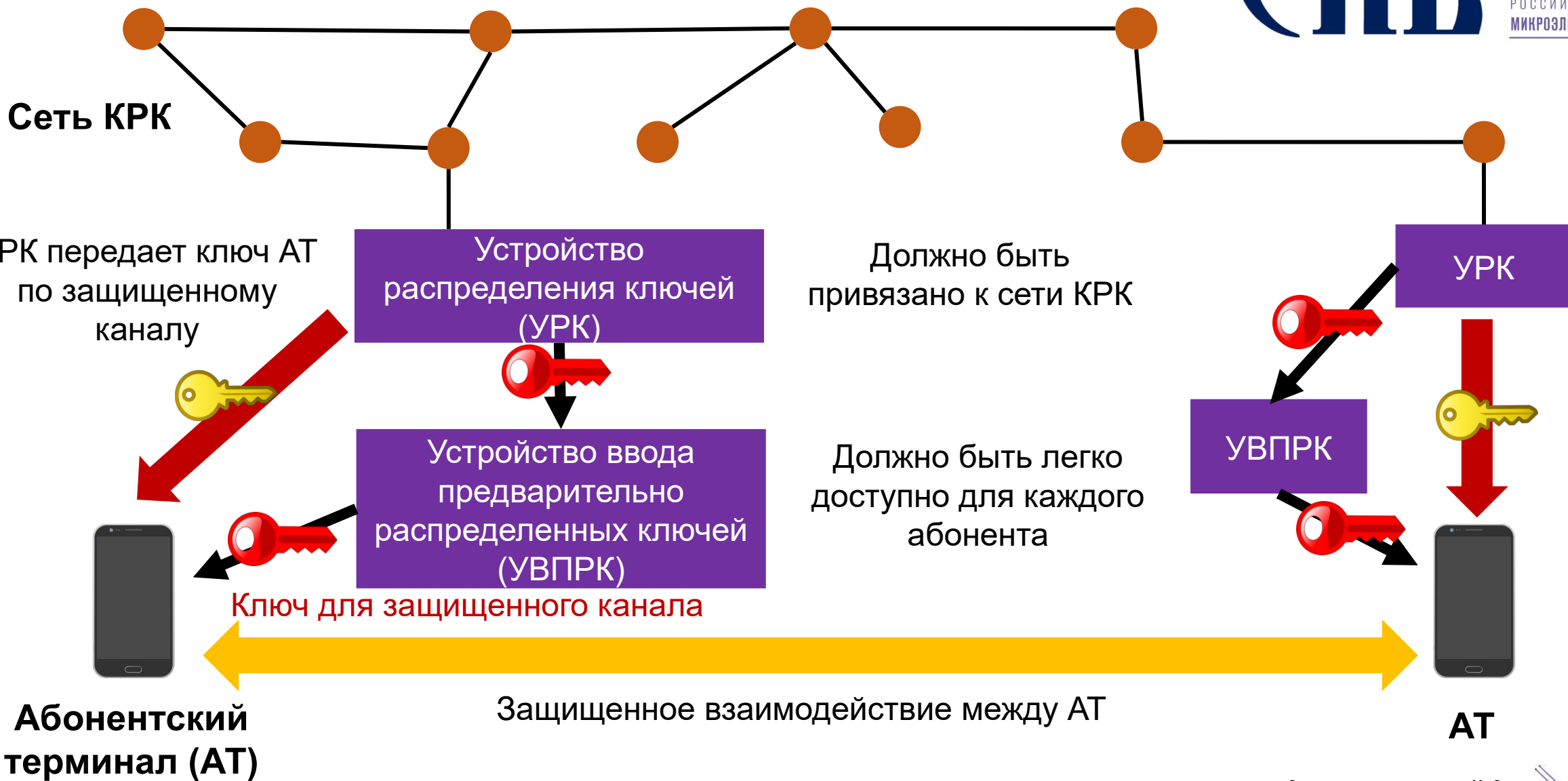
*Герасимова А.Г., Емельянов В.М., Росликов А.Н., Третникова Е.Н.*

*ООО «Системы практической безопасности»*

# МОБИЛЬНЫЕ ПОТРЕБИТЕЛИ КВАНТОВОЗАЩИЩЕННЫХ КЛЮЧЕЙ



# ВЫРАБОТКА И РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ



# ПОЛУЧЕНИЕ КЛЮЧЕЙ АБОНЕНТСКИМИ ТЕРМИНАЛАМИ ОТ УРК



В зависимости от порядка согласования идентификатора/метки КЗК между АТ, запрос КЗК АТ Б может выполняться:

- 1) **одновременно** с запросом КЗК АТ А при предварительном согласовании метки КЗК между АТ;
- 2) **после** получения КЗК АТ А и передачи от АТ А устройству АТ Б идентификатора КЗК.

# ВАРИАНТЫ АРХИТЕКТУРЫ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ



## Централизованная архитектура

- Имеется малое количество УРК (типовой вариант: основной и резервный)
- Все УРК обслуживают всех абонентов. Каждый абонент может обратиться к любому из УРК для получения ключа связи с другим абонентом
- Все используемые абонентами КЗК фактически являются «локальными». Сеть КРК обеспечивает синхронную выработку и распределение ключей в УРК

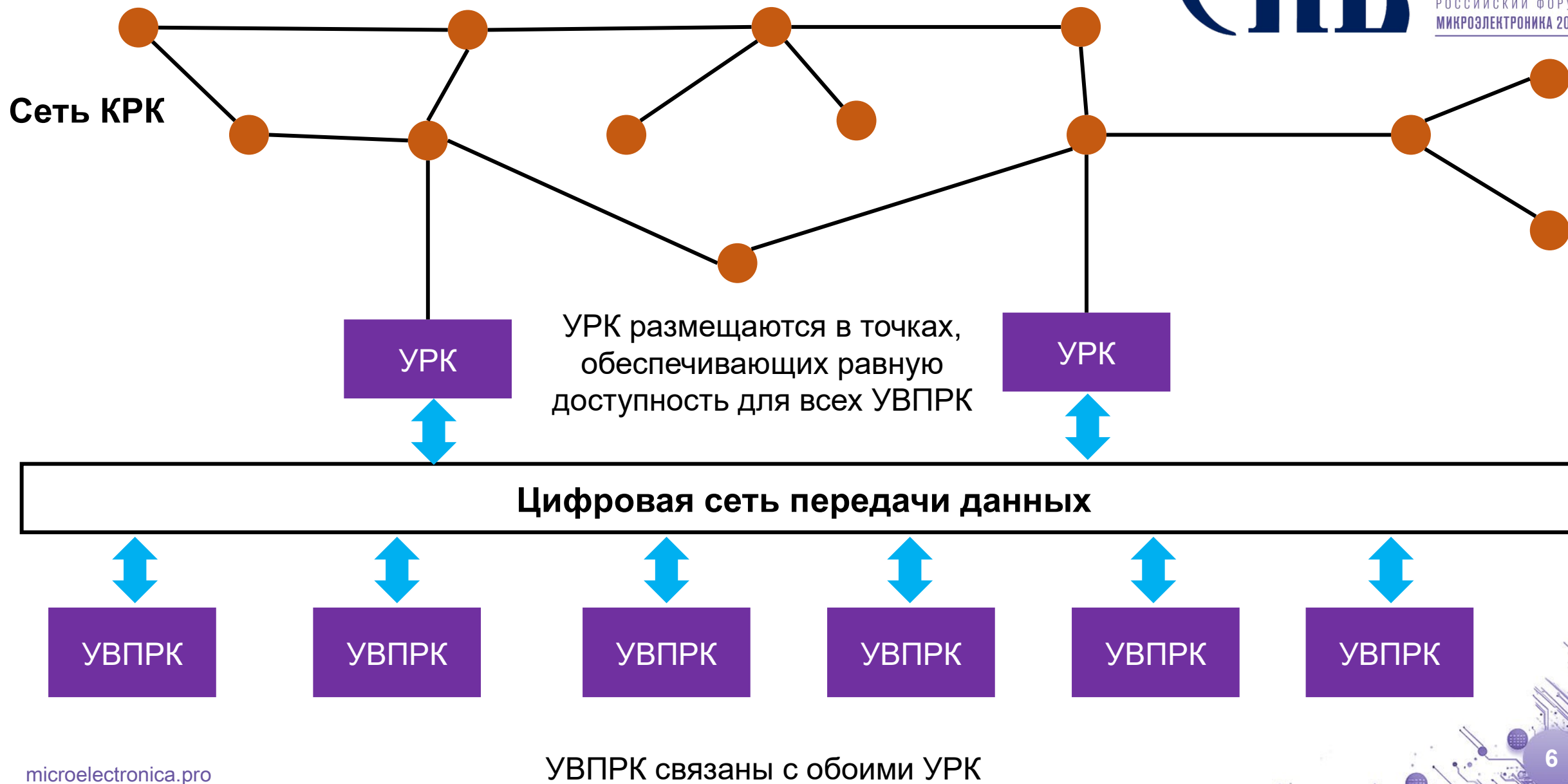
## Децентрализованная архитектура

- Имеется большое количество УРК
- Каждый УРК обслуживает только своих абонентов. Для получения ключа связи с другим абонентом запрашивающий ключ абонент должен обращаться к своему УРК
- Сеть КРК не используется при реализации в УРК функции резервирования КЗК, предназначенных для использования парами абонентов

## АКТУАЛЬНЫЕ ВОПРОСЫ

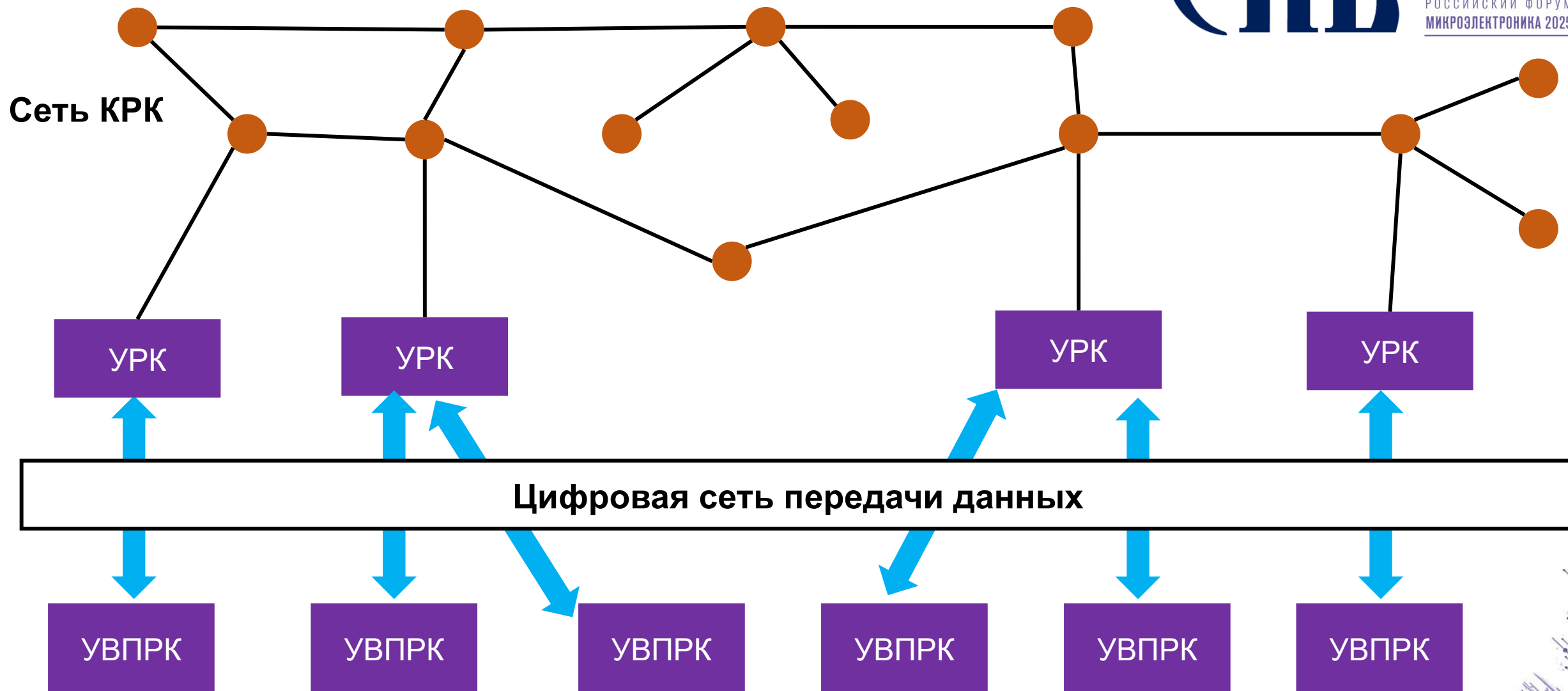
- Устойчивость системы распределения ключей к сбоям и отказам элементов сети КРК
- Влияние топологии сети КРК на характеристики системы

# ЦЕНТРАЛИЗОВАННАЯ АРХИТЕКТУРА



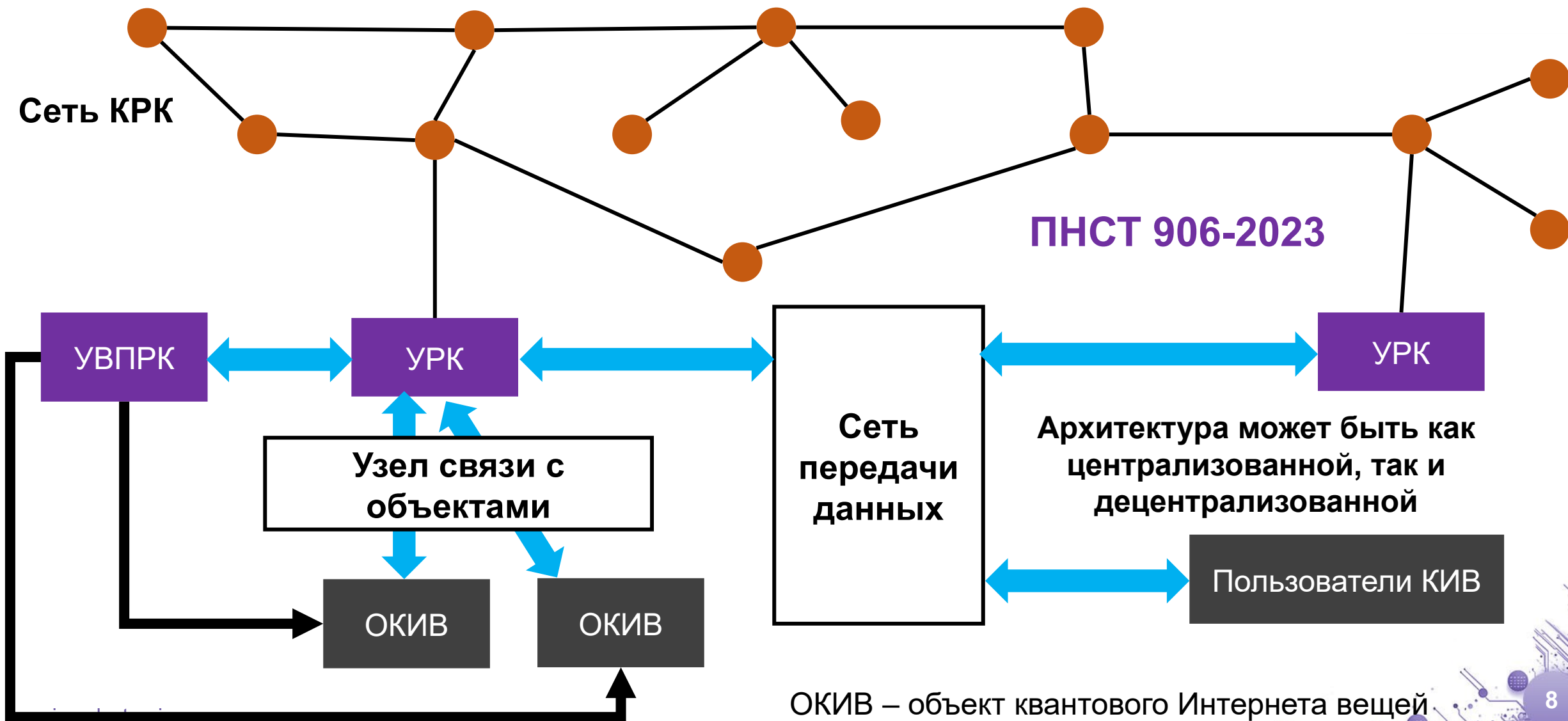
# ДЕЦЕНТРАЛИЗОВАННАЯ АРХИТЕКТУРА

СПБ



УВПРК привязаны к ближайшему УРК

# СИСТЕМА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ КВАНТОВОГО ИНТЕРНЕТА ВЕЩЕЙ (КИВ)



# МОДЕЛИРОВАНИЕ ОТКАЗОВ В СЕТИ КРК И АНАЛИЗ НАДЕЖНОСТИ



## ЭТАП 1

- Генерация сети случайной топологии
- Размещение УРК

Сеть представляется как простой неориентированный связный граф, причем достаточно разреженный

## ЭТАП 2

- Удаление ребер графа случайным образом
- Анализ связности и длины квантового маршрута между УРК

Этапы 1 и 2 повторяются многократно для получения надежных оценок

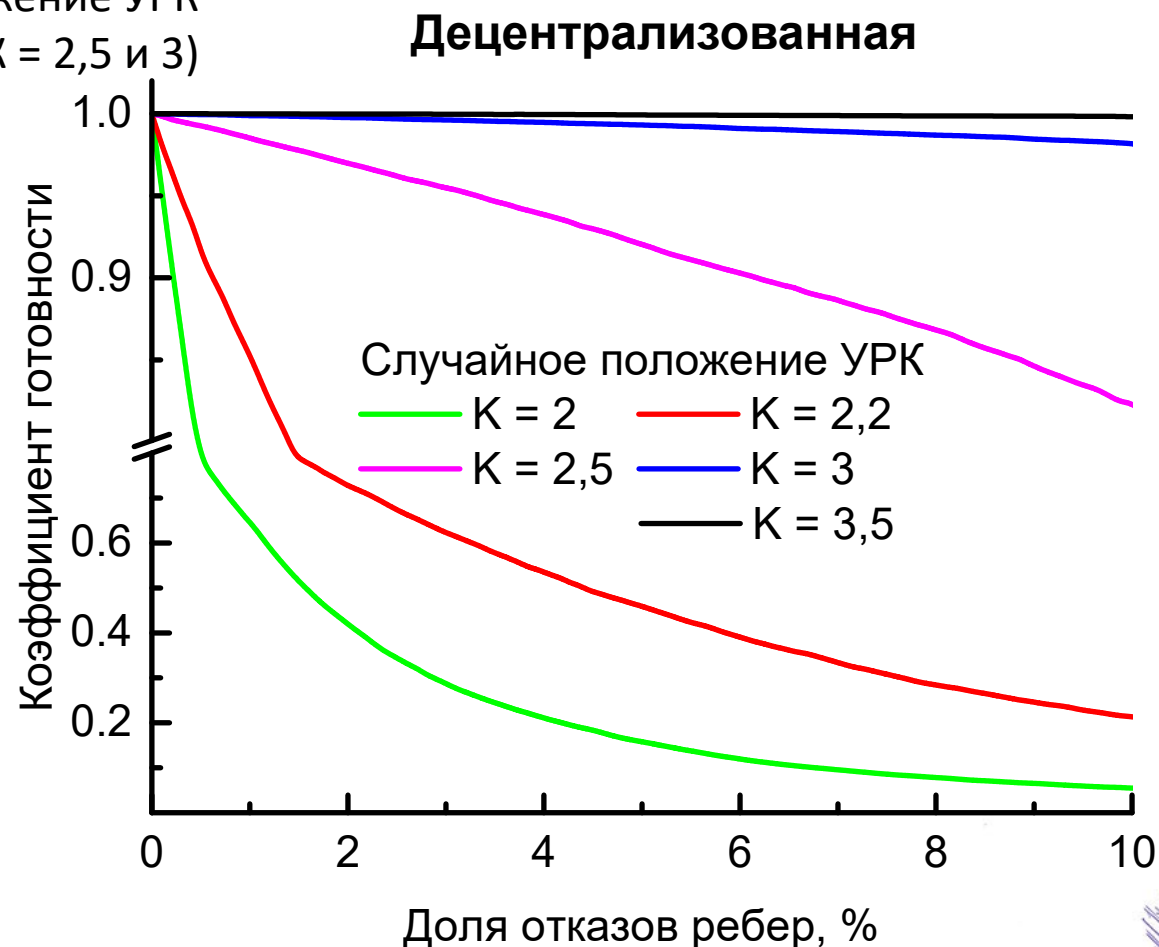
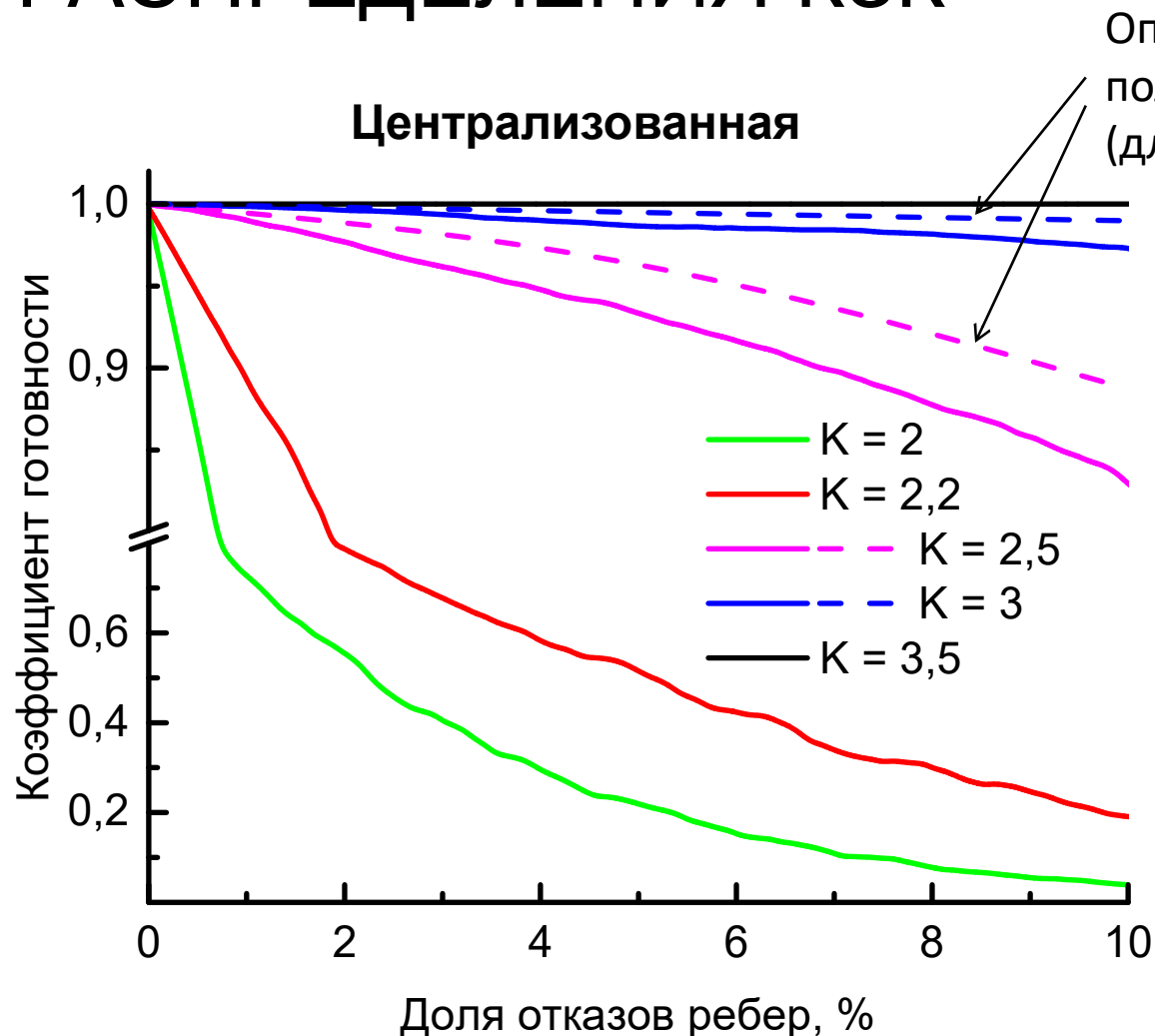
## ЭТАП 3

- Расчет статистики
- Формирование усредненных оценок

Расчеты были выполнены для разных вариантов топологии:

- ячеистой (при разных значениях средней степени вершины)
- кольцевой
- линейной

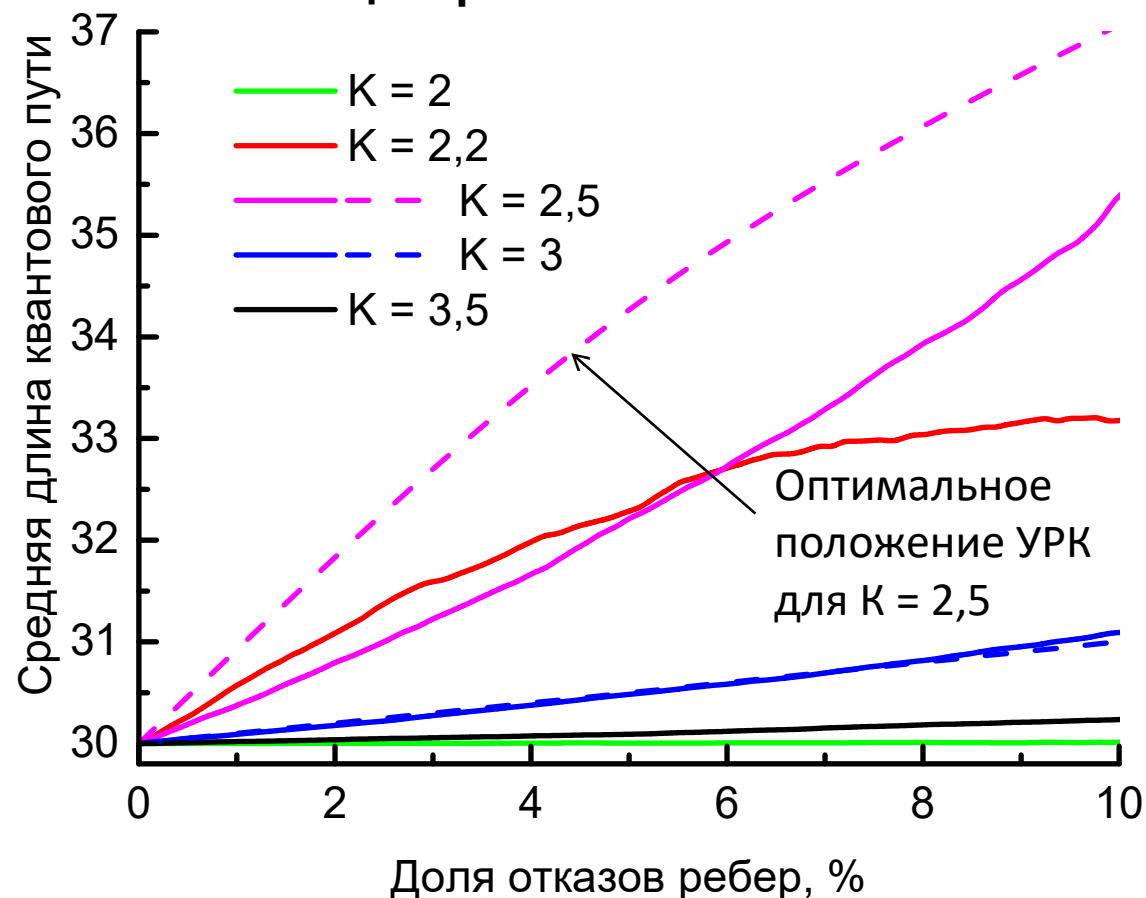
# КОЭФФИЦИЕНТ ГОТОВНОСТИ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ КЗК



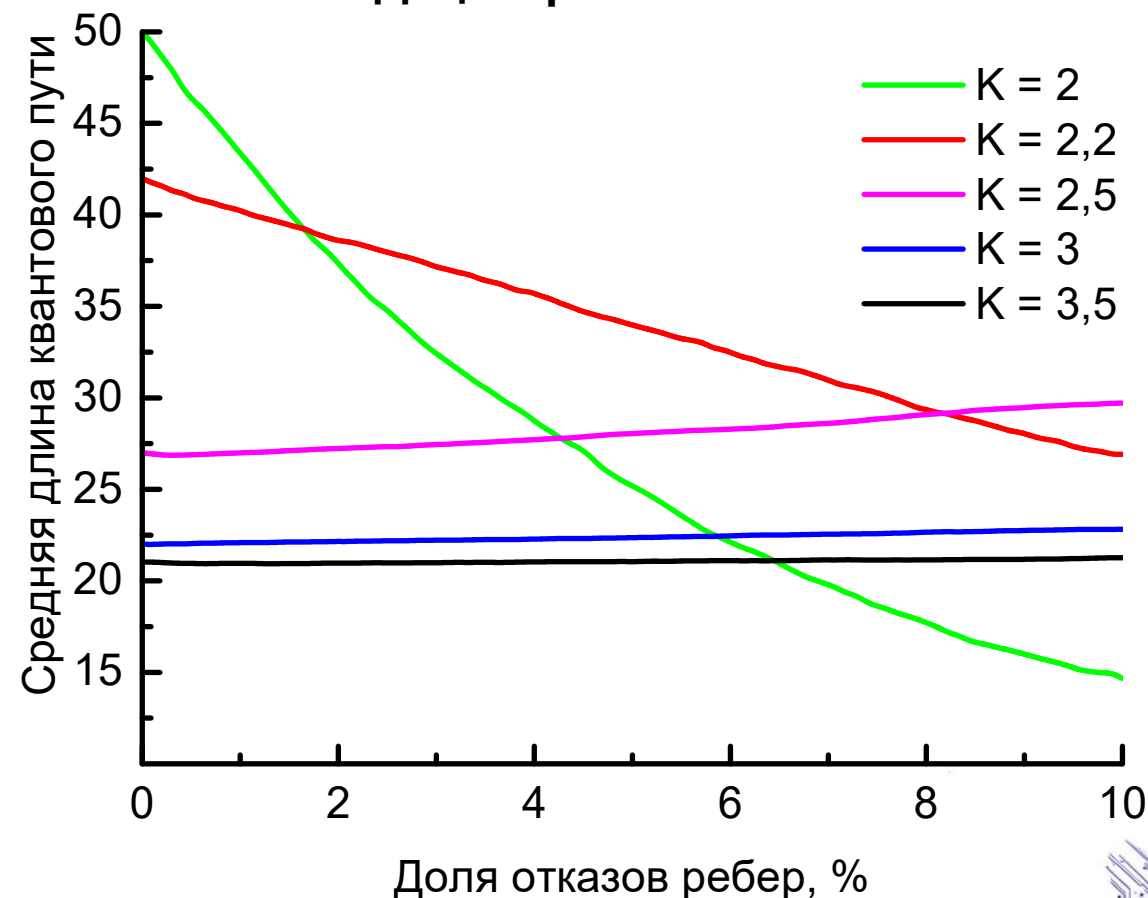
Сеть ячеистой топологии, 961 узел  
 $K$  – средняя степень вершины

# ДЛИНА КВАНТОВОГО ПУТИ МЕЖДУ УРК В СИСТЕМЕ РАСПРЕДЕЛЕНИЯ КЗК

Централизованная

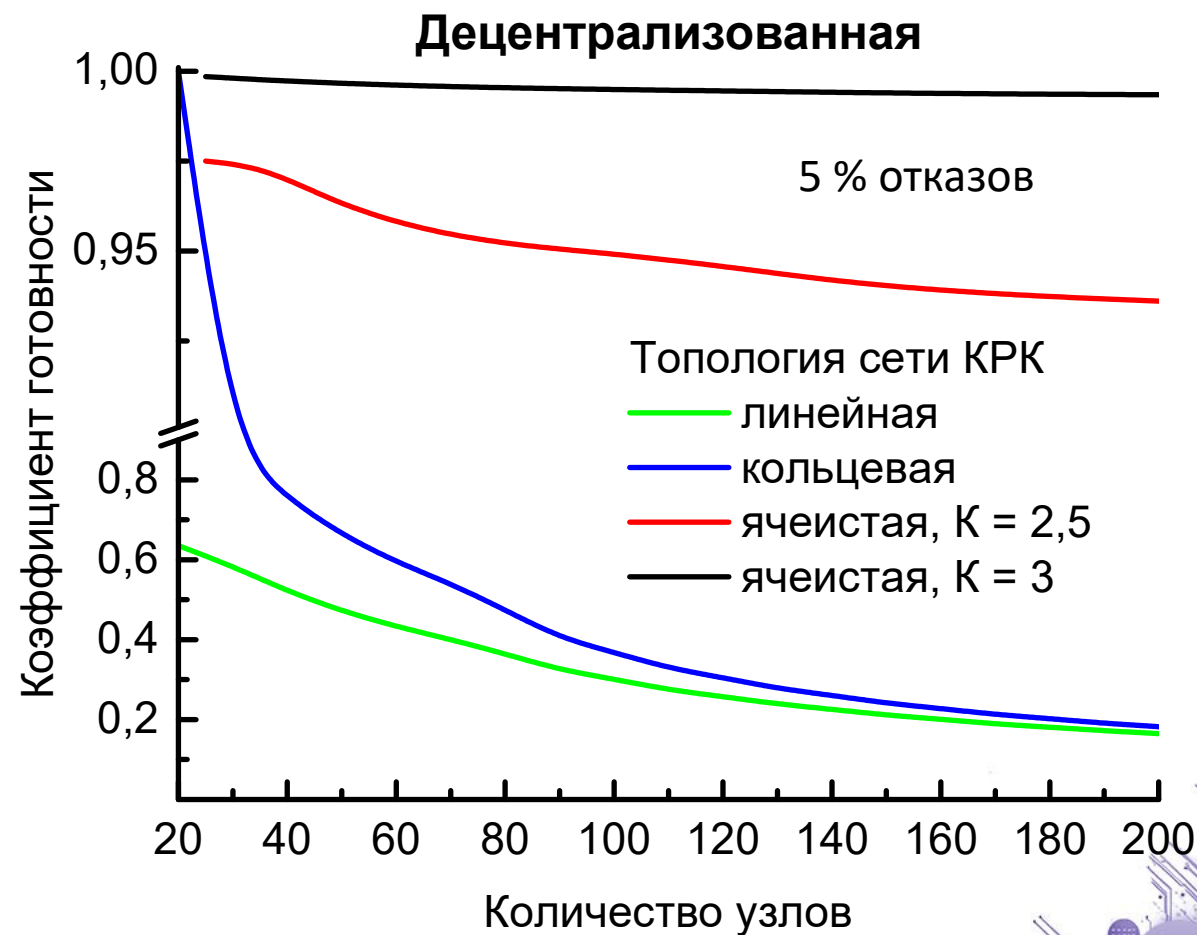
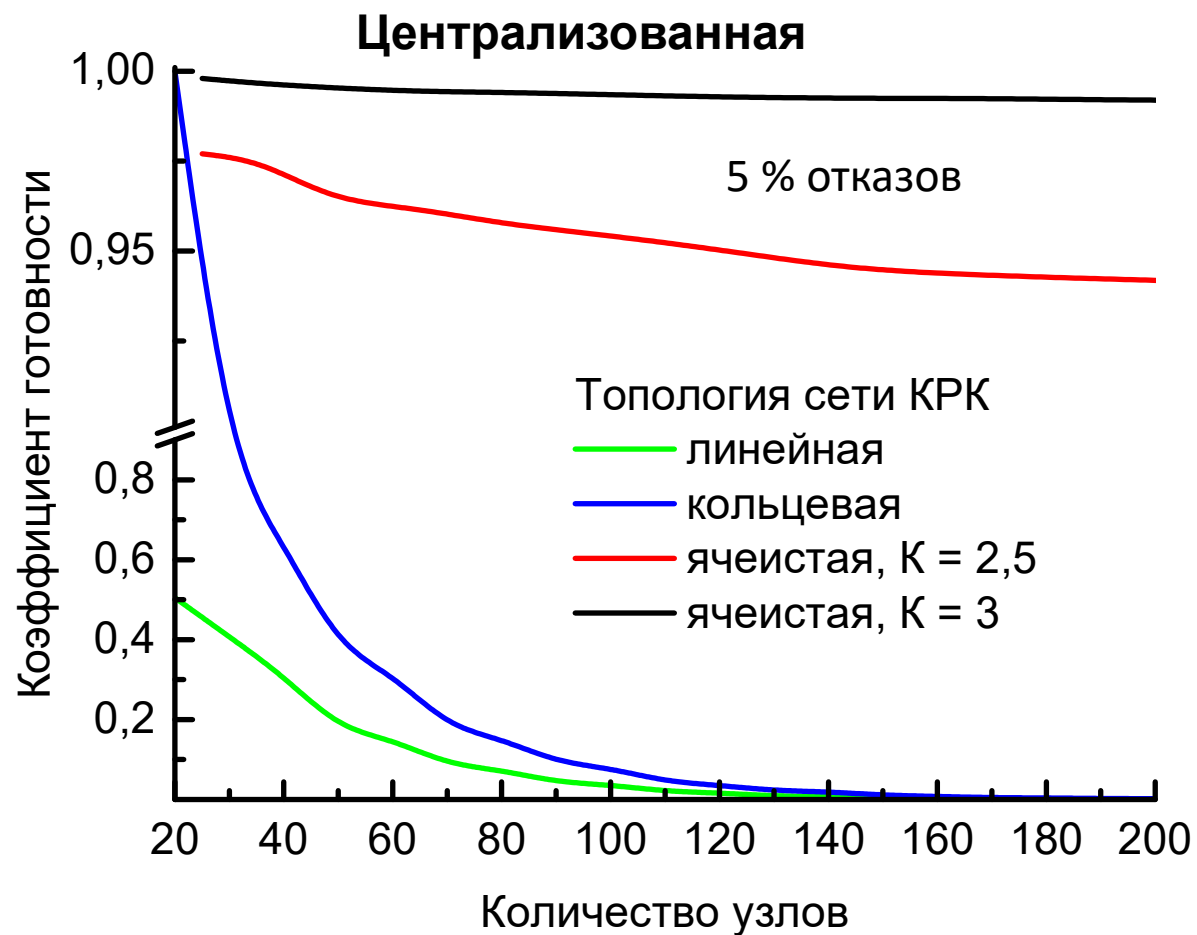


Децентрализованная



Сеть ячеистой топологии, 961 узел  
 $K$  – средняя степень вершины

# ВЛИЯНИЕ ТОПОЛОГИИ СЕТИ КРК НА ХАРАКТЕРИСТИКИ НАДЕЖНОСТИ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ КЗК



- ▶ Практически возможно построение системы как с централизованной, так и децентрализованной архитектурой. При этом характеристики надежности системы в большей степени определяются не ее архитектурой, а топологией сети КРК
- ▶ Ячеистая топология является естественной для сетей КРК. Коэффициент готовности системы распределения КЗК зависит от доли отказавших ребер сети КРК схожим образом в случае централизованной и децентрализованной архитектуры системы. При этом значения коэффициента готовности для централизованной архитектуры в случае оптимального выбора расположения УРК несколько выше
- ▶ Достижение высоких значений показателей надежности системы распределения КЗК возможно при значениях средней степени вершины сети КРК выше 2,5. При средней степени вершины 3 обеспечивается  $K_g > 0,97$  даже в случае отказов 10 % ребер сети КРК
- ▶ Надежность системы распределения КЗК, использующей сеть КРК ячеистой топологии, практически не зависит от количества узлов сети. При этом показатели надежности систем, использующих сети КРК сетей с линейной и кольцевой топологиями, быстро деградируют с увеличением количества узлов

# СПАСИБО ЗА ВНИМАНИЕ!

Емельянов Виктор Михайлович

Руководитель направления

ООО «Системы практической безопасности»



emelyanov@systempb.ru



MICROELECTRONICA.PRO



ПОДПИСЫВАЙТЕСЬ И БУДЬТЕ В КУРСЕ  
ВСЕХ ПОСЛЕДНИХ НОВОСТЕЙ!



ВАШ ЛИЧНЫЙ  
КАБИНЕТ



Rutube



VK Видео



РОССИЙСКИЙ ФОРУМ  
МИКРОЭЛЕКТРОНИКА 2025



21–27  
сентября 2025