конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2023»

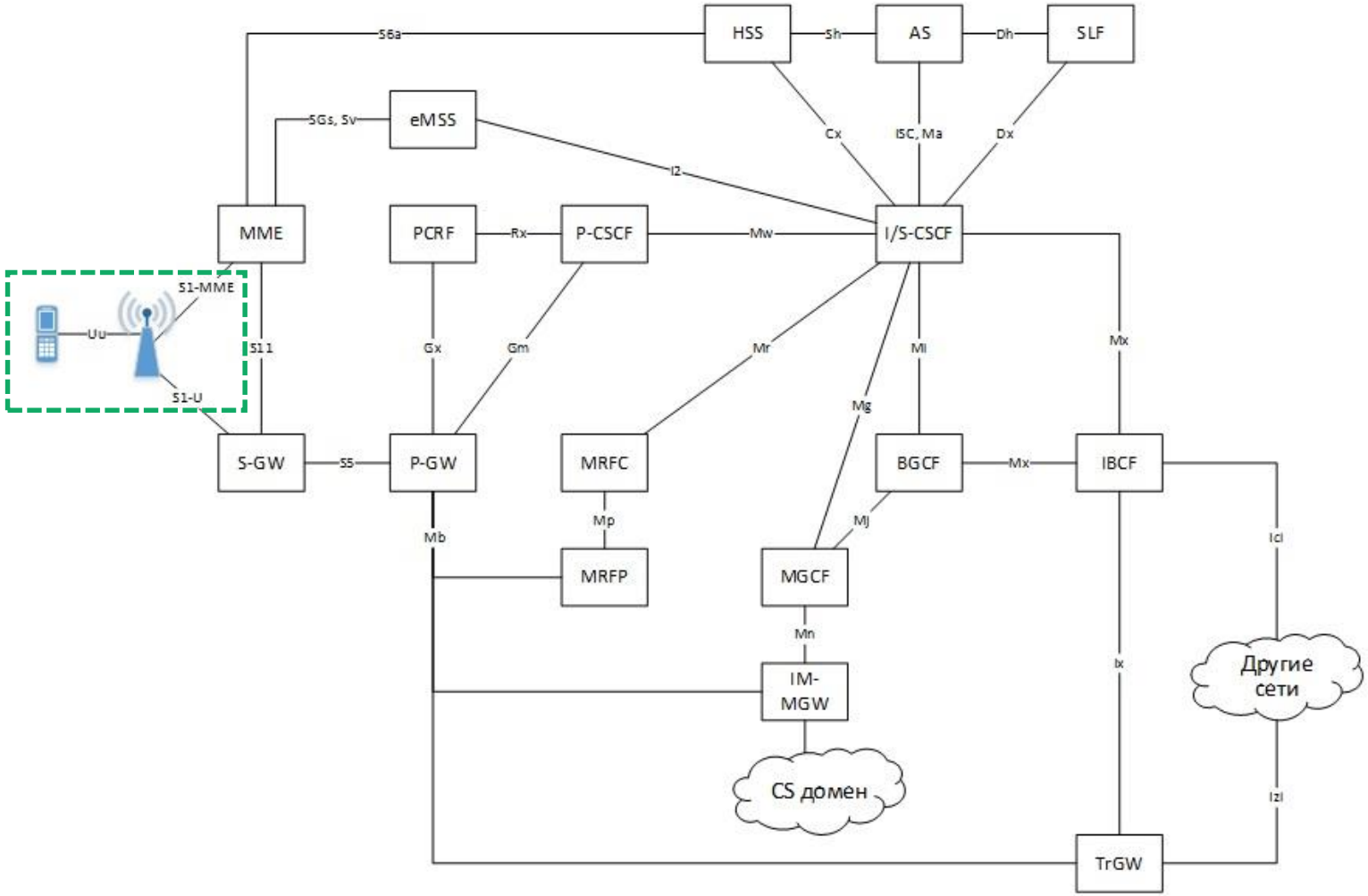
# Квантовое распределение ключей для обеспечения сквозной безопасности в подвижных сетей радиосвязи

В.М. Емельянов[1], А.Г. Герасимова[1], Шкоркина[1], С.А. Новичков[2]
[1]ООО «Системы практической безопасности»
[2]АНО ОВО «Сколковский институт науки и технологий» (Сколтех)

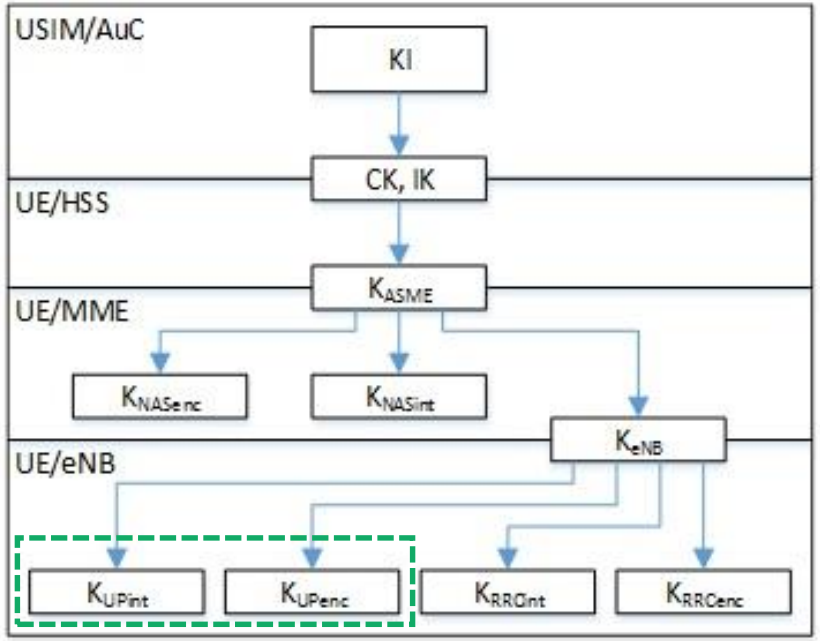
# Шифрование и имитозащита пользовательских данных в сетях подвижной радиосвязи 4G и 5G

# Обеспечение безопасности пользовательских данных в сетях подвижной радиосвязи 4G

## Архитектура сети



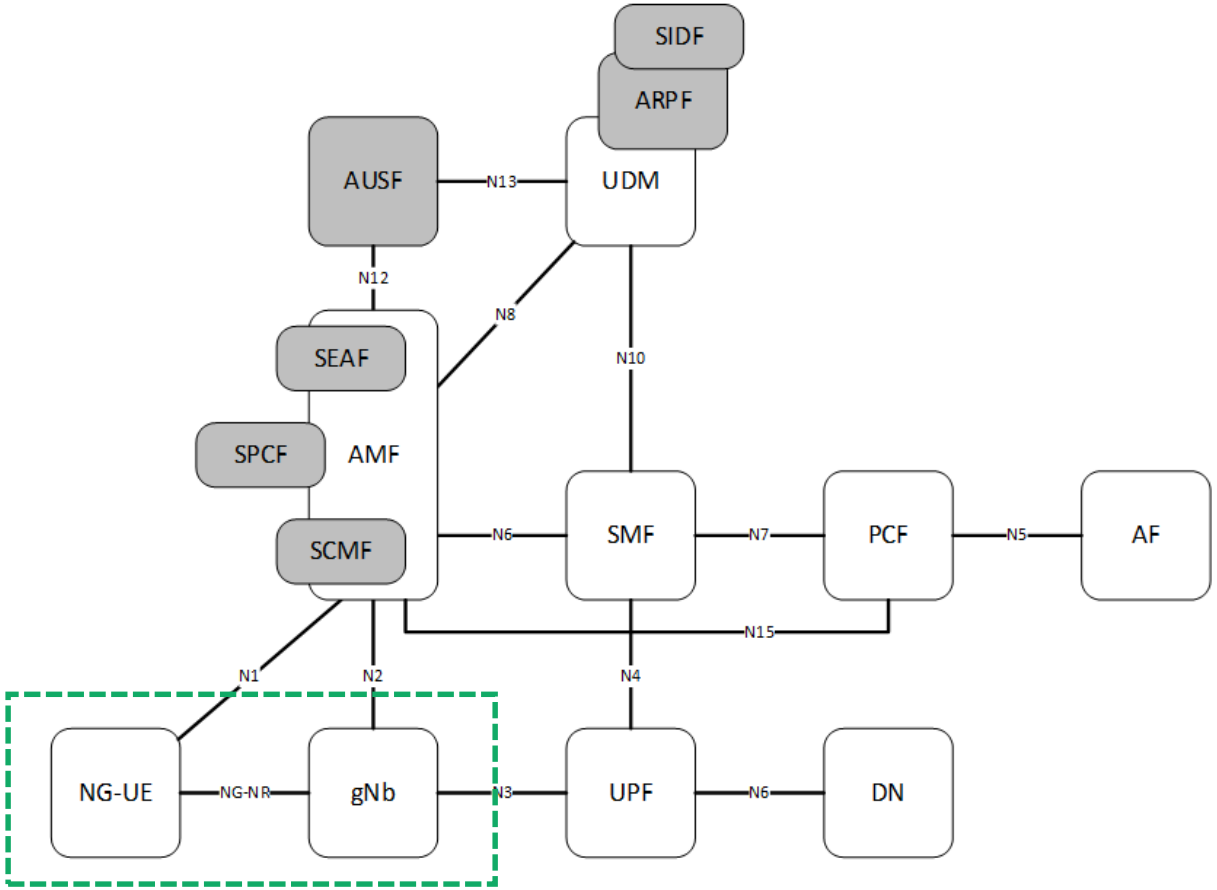

## Иерархия ключей



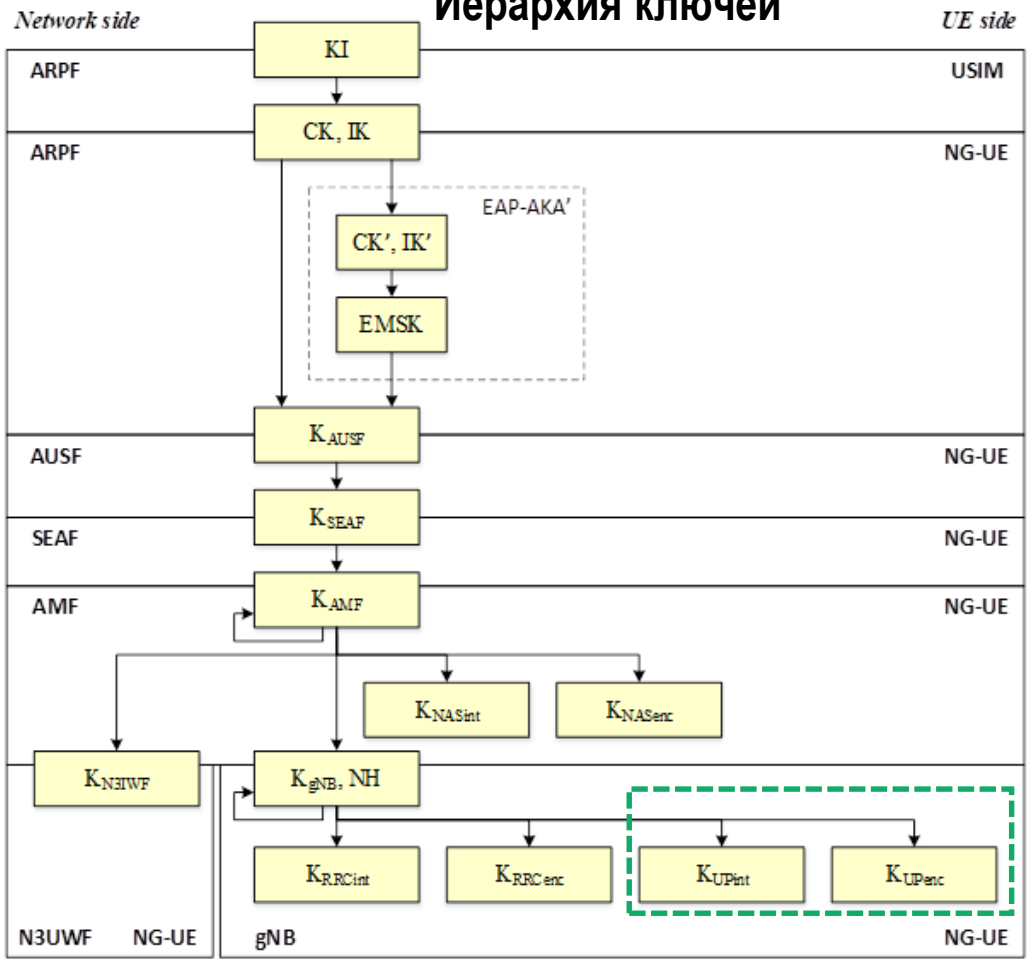

**В сетях 3G для тех же целей используются ключи CK, IK, в сетях GSM- Kc**

# Обеспечение безопасности пользовательских данных в сетях подвижной радиосвязи 5G

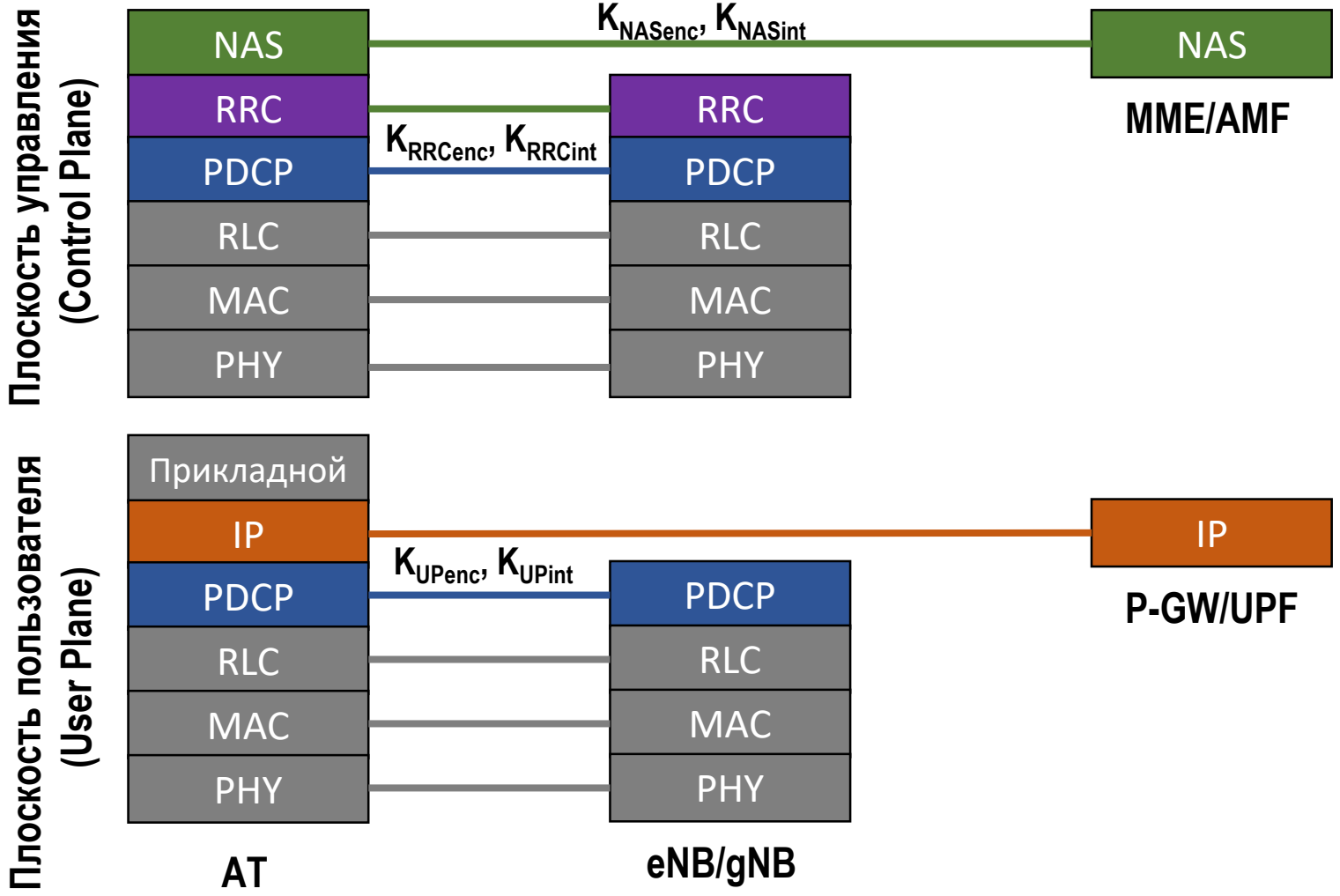
## Архитектура сети




## Иерархия ключей



# Шифрование и имитозащита пользовательских данных в сетях подвижной радиосвязи 4G и 5G




**Безопасность пользовательских данных обеспечивается на двух участках:**

1. **Абонентский терминал (AT, UE) – базовая станция (eNB/gNB), то есть в сети радиодоступа**
2. **При передаче информации через транспортные сети**

**Стандартные механизмы 3GPP не обеспечивают сквозную (end-to-end) безопасность.**

# Вопросы обеспечения сквозной (end-to-end) безопасности пользовательских данных

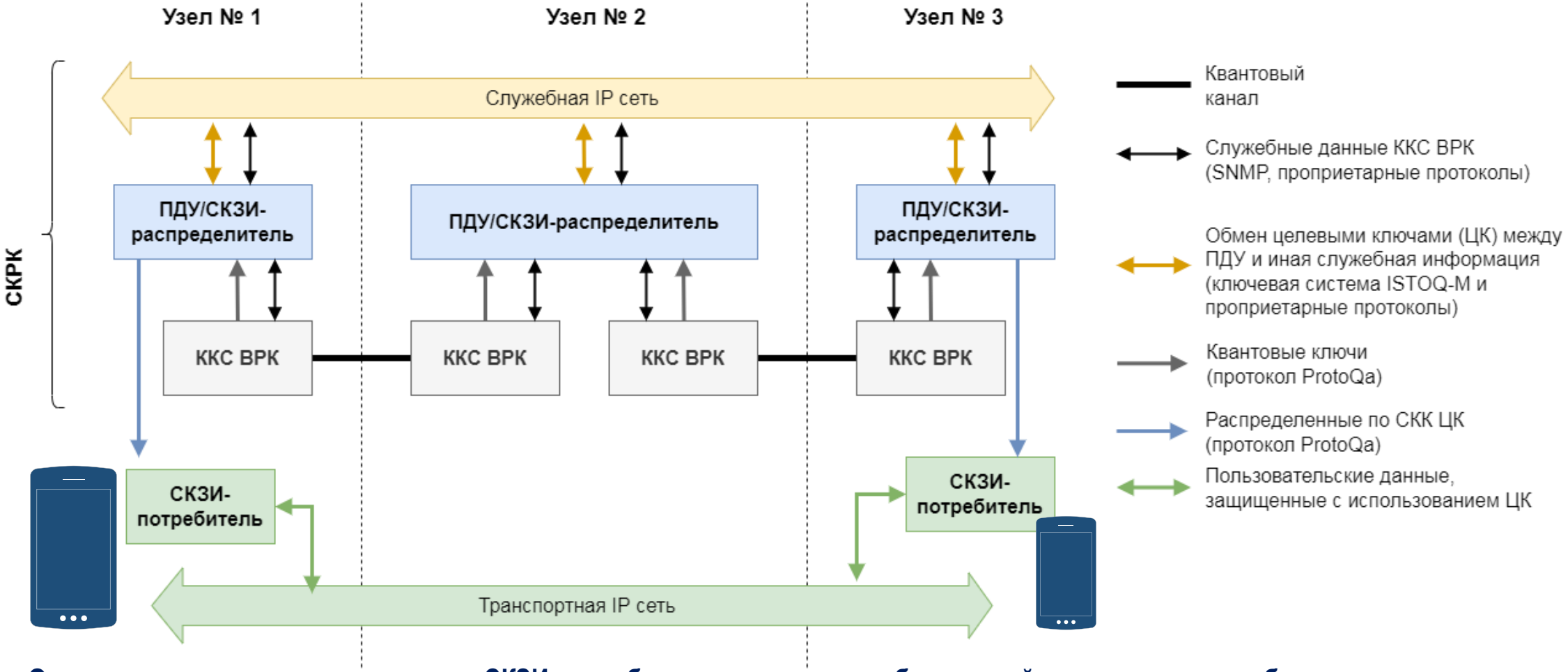
Для обеспечения взаимной аутентификации и защиты трафика между парой абонентов могут применяться механизмы, основанные на:

- симметричном распределении ключей;
- открытом распределении ключей (ОРК).

Основной проблемой для симметричных протоколов распределения ключей является наличие общего доверенного центра распределения ключей, что на практике не всегда реализуемо при большом числе абонентов. Схема ОРК является более гибкой, позволяя организовать иерархию из удостоверяющих центров, и успешно применяется для взаимной аутентификации в сетях, имеющих сотни миллионов абонентов. Квантовое распределение ключей Тем не менее, существующие потенциальные уязвимости для асимметричных криптографических алгоритмов со стороны квантовых вычислительных машин делают актуальным рассмотрение альтернативных методов распределения ключей.

**Квантовое распределение ключей** позволяет организовать симметричное распределение ключей между большим числом удаленных объектов и их смену.

# Использование КРК для защиты пользовательских данных

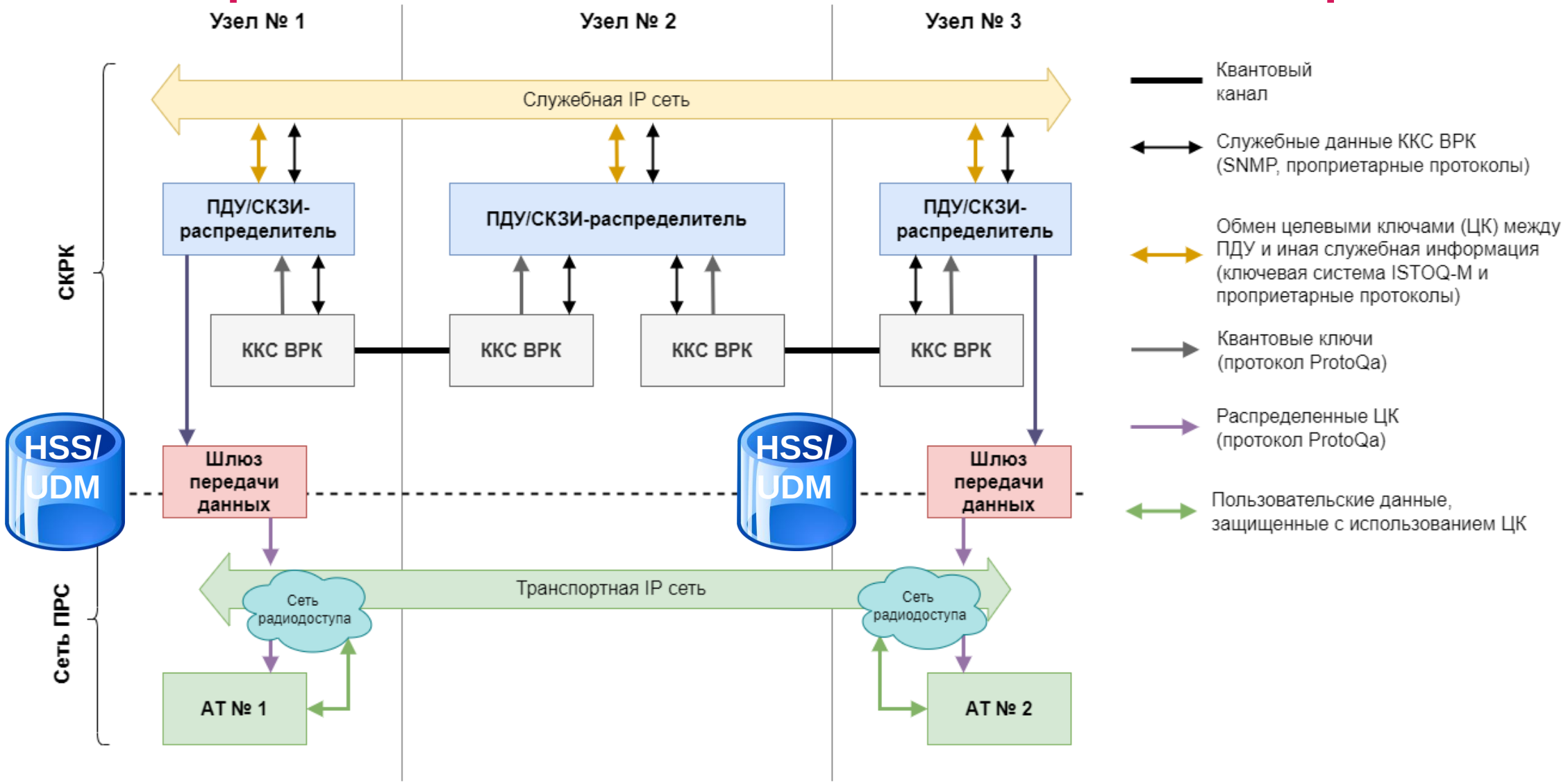



**Основная сложность в случае, когда СКЗИ-потребителем становится абонентский терминал – его мобильность**

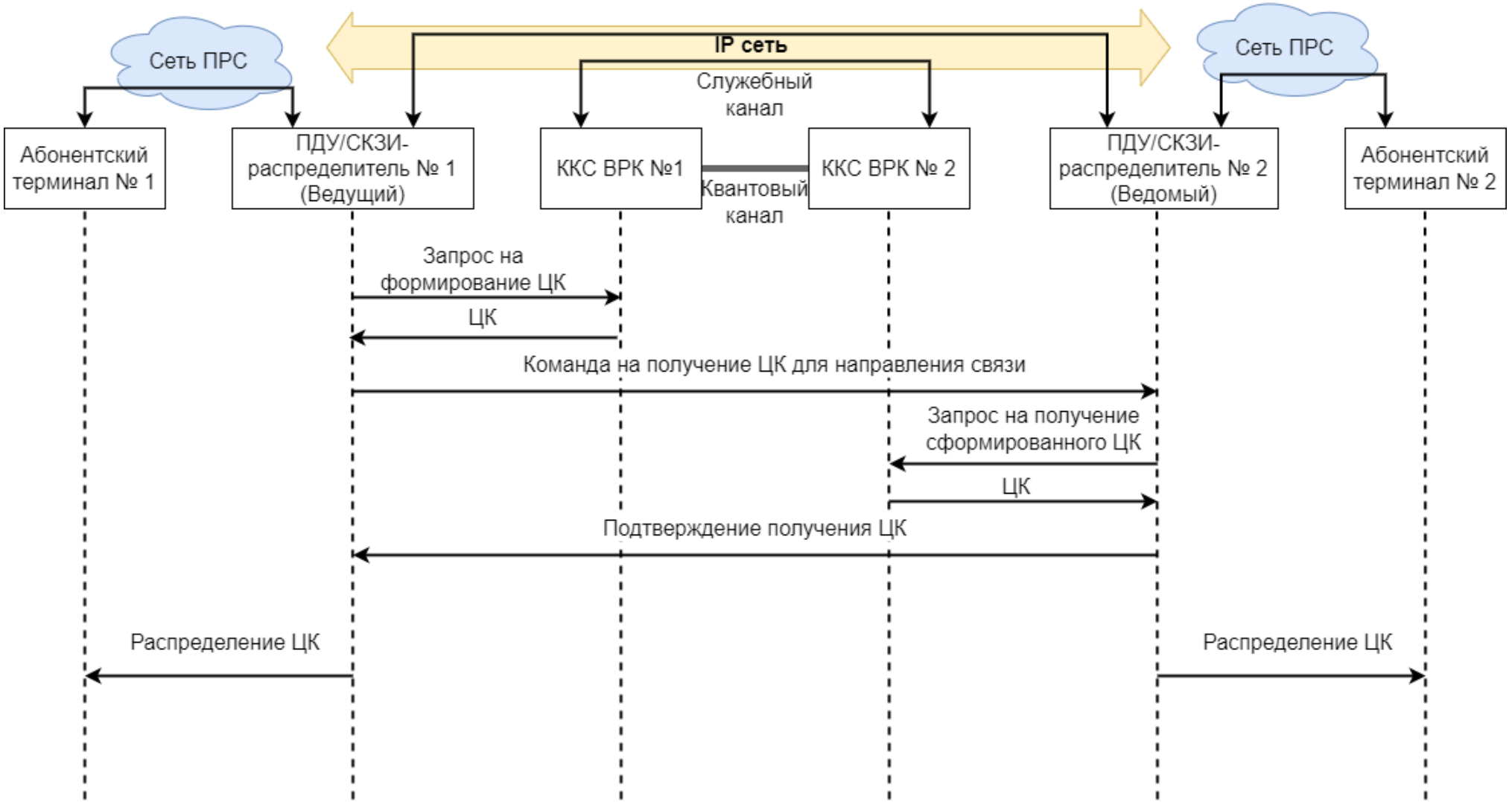
# Требования к доверенным центрам распределения квантовых ключей

1. Доверенный центр распределения должен обеспечивать получение целевых ключей от аппаратуры выработки квантовых ключ, их распределение между парами абонентов и доведение до каждого абонентского устройства.
2. Доверенный центр распределения должен быть реализован в составе СКЗИ-распределителя.
3. Доверенный центр должен быть доступен для абонента в любой момент времени по каналам связи.
4. Должен быть предусмотрен механизм ввода исходных ключей связи АТ с СКЗИ-распределителем. Соответствующие ключи должны передаваться абонентам способом, который обеспечивал бы конфиденциальность переданной информации, в том числе и сотрудников оператора ПРС.
5. С учётом реализации механизмов по п.2 и п.3 целесообразна гармонизация инфраструктуры квантовых сетей с инфраструктурой операторов ПРС. Как минимум, один доверенный центр распределения должен соответствовать одному домашнему регистру HLR/HSS/UDM.

# Схема сопряжения квантовой сети с сетью подвижной радиосвязи



# Генерация и распределение ключей



# Варианты распределения ключей связи АТ с СКЗИ-распределителем

| | Вариант распределения | Достоинства | Недостатки |
|---|---|---|---|
| 1 | В составе абонентского профиля | 1. Простая архитектура сети<br>2. Удобство получения КИ абонентом | Есть риск компрометации со стороны персонала сетей ПРС |
| 2 | Независимо от профиля на физическом носителе | Нет риска компрометации со стороны персонала сетей ПРС | Есть риск компрометации со КИ со стороны третьих лиц при доставке носителя |
| 3 | Независимо от профиля на физическом носителе в неизвлекаемом виде | Оптимальная защита КИ | Необходим специализированный носитель |

# Контактная информация

**Электронная почта:**

emelyanov@systempb.ru

**Телефон:**

+7 812 468-15-61

**Сайт:**

www.systempb.ru

skzi.ru