

Инновационные направления исследований в области телекоммуникаций в Республике Узбекистан

*А. Мирхабибов
начальник НИД связи и информатизации ГУП «UNICON.UZ»
Тел.: +998 71 2359366
e-mail: amirhabibov@unicon.uz*

План проведения НИР 2011-2012 гг.

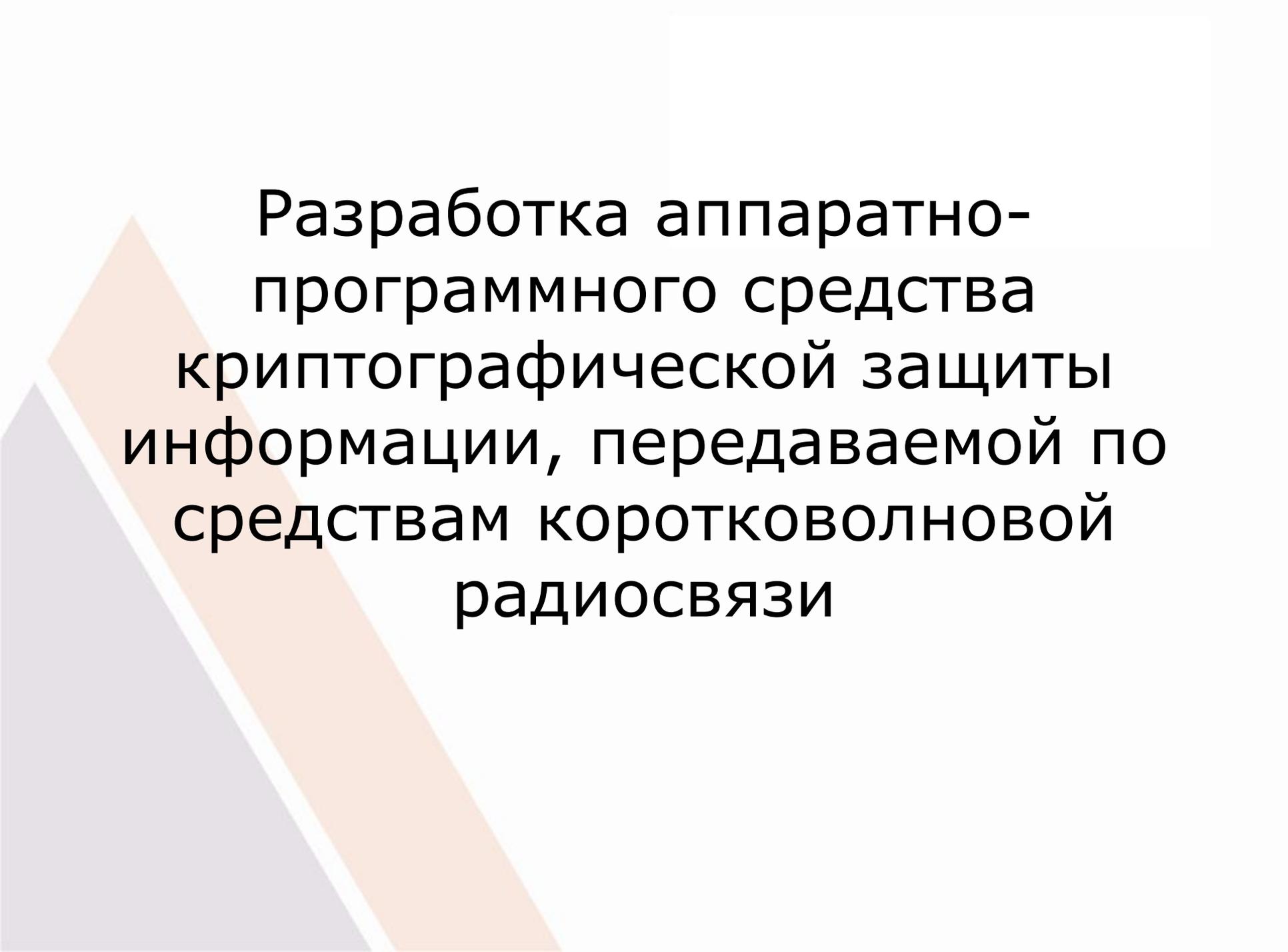
- Разработка аппаратно-программного средства криптографической защиты информации, передаваемой по средствам коротковолновой радиосвязи
- Разработка и исследование алгоритмов коллективной электронной цифровой подписи на базе неявных эллиптических кривых
- Разработка и исследование алгоритмов распределения ключей на базе неявных эллиптических кривых

План проведения НИР 2011-2012 гг.

- Исследование проблем и путей развития универсального широкополосного доступа в Узбекистане
- Подготовка вкладов Администрации связи Республики Узбекистан для Всемирной ассамблеи стандартизации телекоммуникаций (WTSA-2012)

План проведения НИР 2011-2012 гг.

- Подготовка вклада Республики Узбекистан на Всемирную конференцию по международной электросвязи (WCIT-2012)
- Исследование и разработка методических основ технического регулирования в сфере связи и информатизации
- *Архитектурные, функциональные и экономические аспекты проектирования сетей следующего поколения*



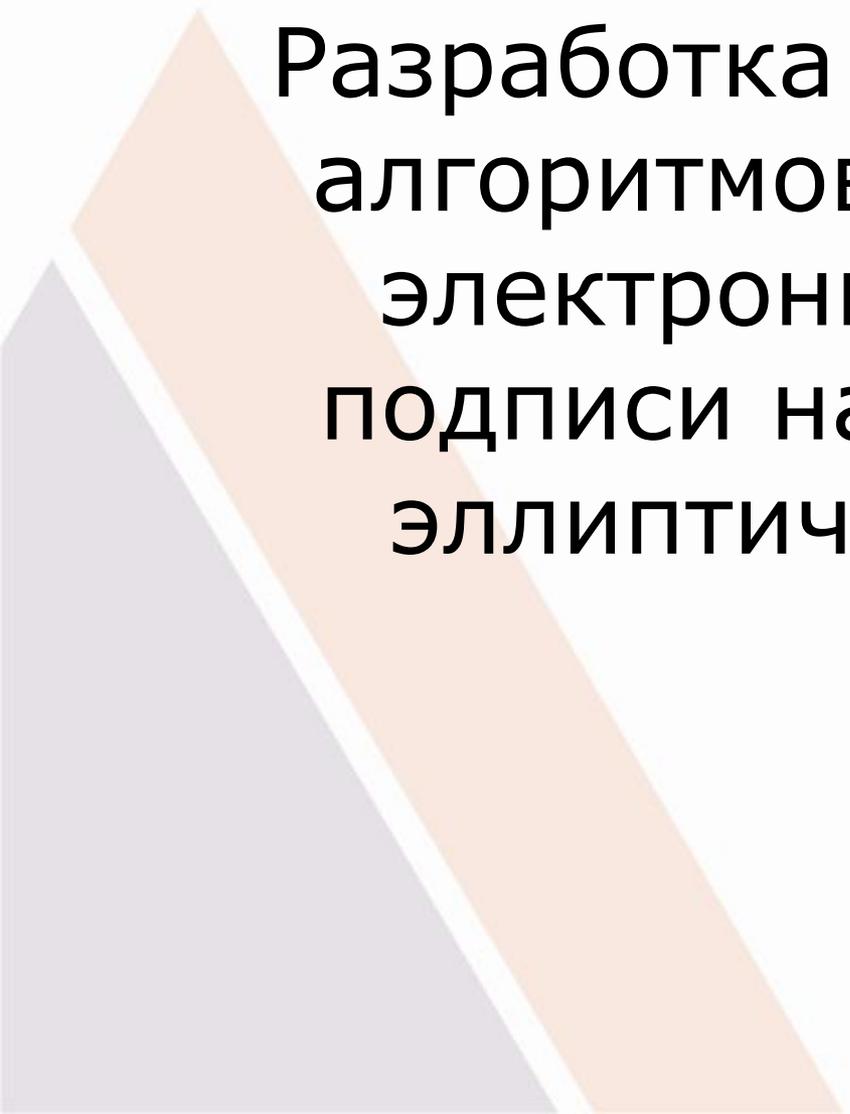
Разработка аппаратно-
программного средства
криптографической защиты
информации, передаваемой по
средствам коротковолновой
радиосвязи

Цель и задачи работы

- Цель:
 - разработка собственного средства криптографической защиты передаваемой информации
- Задачи:
 - анализ методов и способов реализации аппаратно-программных средств криптографической защиты информации
 - разработка полнофункционального макетного образца
 - испытание разработанного аппаратно-программного средства криптографической защиты

Ожидаемый результат

- полностью работоспособный опытный образец, а также конструкторская, программная, техническая и эксплуатационная документация к нему



Разработка и исследование
алгоритмов коллективной
электронной цифровой
подписи на базе неявных
эллиптических кривых

Цель и задачи работы

- Цель:

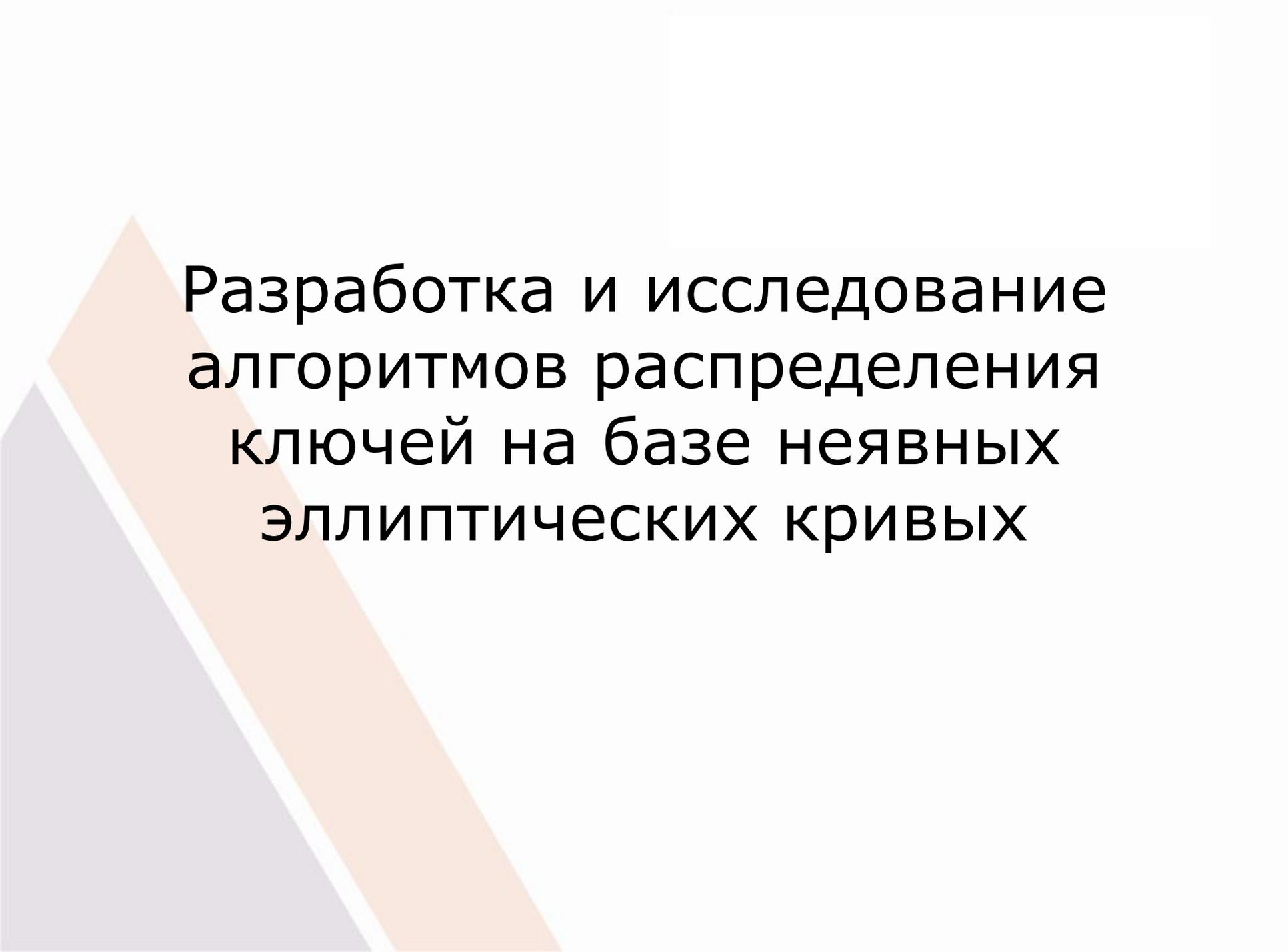
- разработка алгоритмов коллективной электронной цифровой подписи на базе неявных эллиптических кривых с увеличенной стойкостью

- Задачи:

- анализ методов формирования и проверки коллективной электронной цифровой подписи
- разработка алгоритма и программы коллективной электронной цифровой подписи
- оценка стойкости и эффективности алгоритма и программы коллективной электронной цифровой подписи

Ожидаемый результат

- результаты НИР будут использованы для формирования коллективной электронной цифровой подписи и аутентификации в системах электронного документооборота и коллективных контрактах



Разработка и исследование алгоритмов распределения ключей на базе неявных эллиптических кривых

Цель и задачи работы

- Цель:

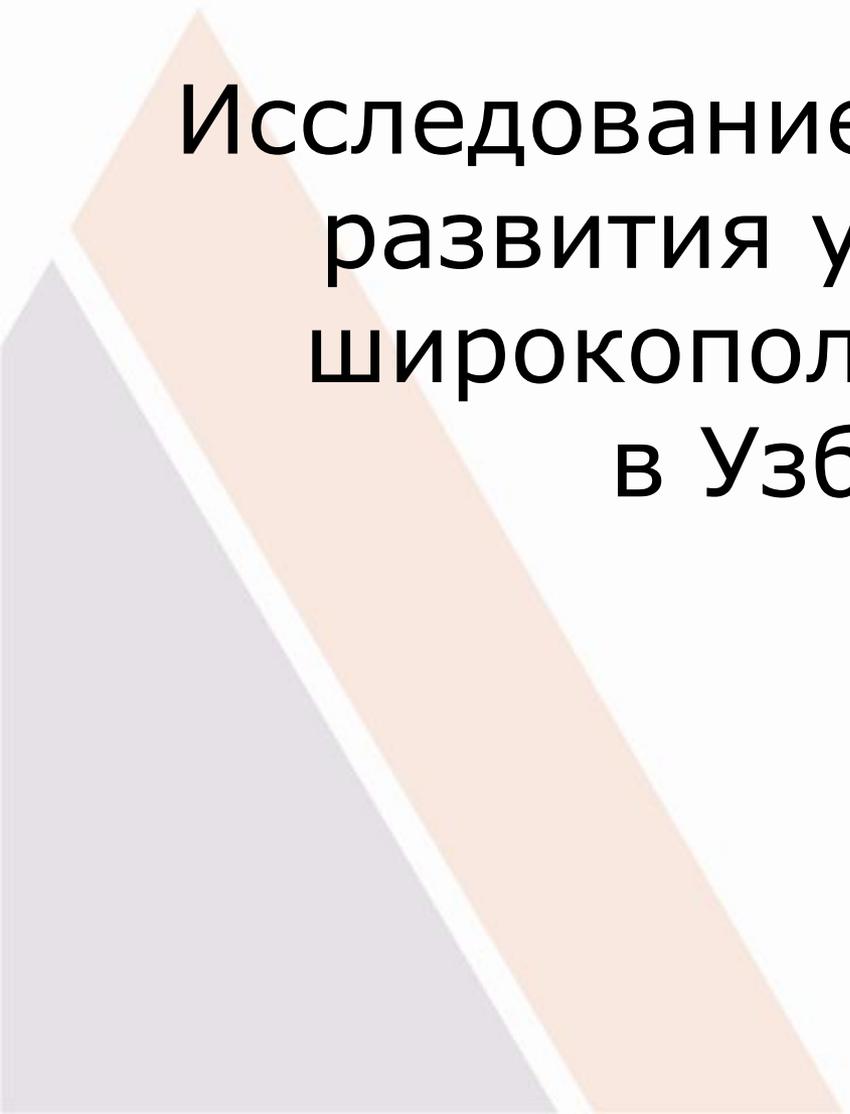
- разработка и исследование алгоритмов распределения ключей на базе неявных эллиптических кривых с увеличенной стойкостью

- Задачи:

- сравнительный анализ существующих международных алгоритмов распределения ключей
- разработка алгоритма распределения ключей на базе неявных эллиптических кривых
- разработка программы распределения ключей на базе неявных эллиптических кривых

Ожидаемый результат

- результаты данной НИР будут использованы для формирования электронной цифровой подписи и аутентификации в системах электронного документооборота и электронных платежных системах



Исследование проблем и путей развития универсального широкополосного доступа в Узбекистане

Цель и задачи работы

- Цель:

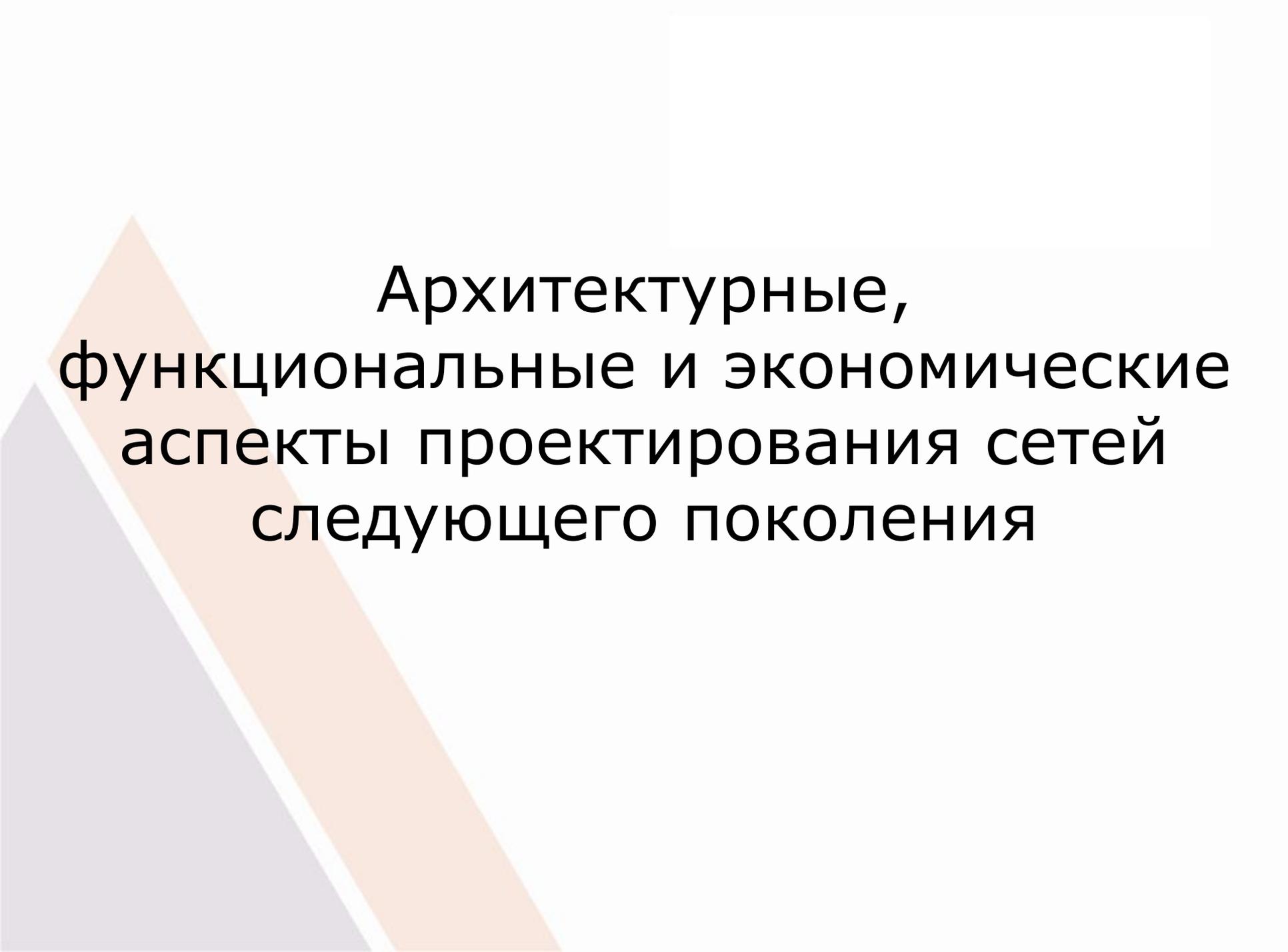
- разработка рекомендаций, которые в дальнейшем могут быть использованы при формировании национальной программы развития ШПД

- Задачи:

- исследование экономических и социальных преимуществ развития инфраструктуры ШПД
- формирование набора индикаторов развития инфраструктуры ШПД в Узбекистане
- исследование статистических показателей развития сетей ШПД в мире и в Узбекистане
- исследование национальных планов различных стран по внедрению универсальной услуги ШПД

Ожидаемый результат

- на основании результатов исследований планируется сформировать набор индикаторов состояния развития ШПД в Узбекистане и выработать рекомендации по внедрению и развитию универсальной услуги ШПД



Архитектурные,
функциональные и экономические
аспекты проектирования сетей
следующего поколения

Цель и задачи работы

- Цель:

- исследование архитектурных, функциональных и экономических аспектов проектирования и разработка целостной методики проектирования сетей последующего поколения (NGN)

- Задачи:

- анализ существующих методов и подходов к проектированию сетей NGN
- определение методов исследования характеристик сетей NGN
- исследование транспортной инфраструктуры, платформ реализации услуг и требований к качеству
- определение критериев разработки конкурентоспособного системного проекта

Ожидаемый результат

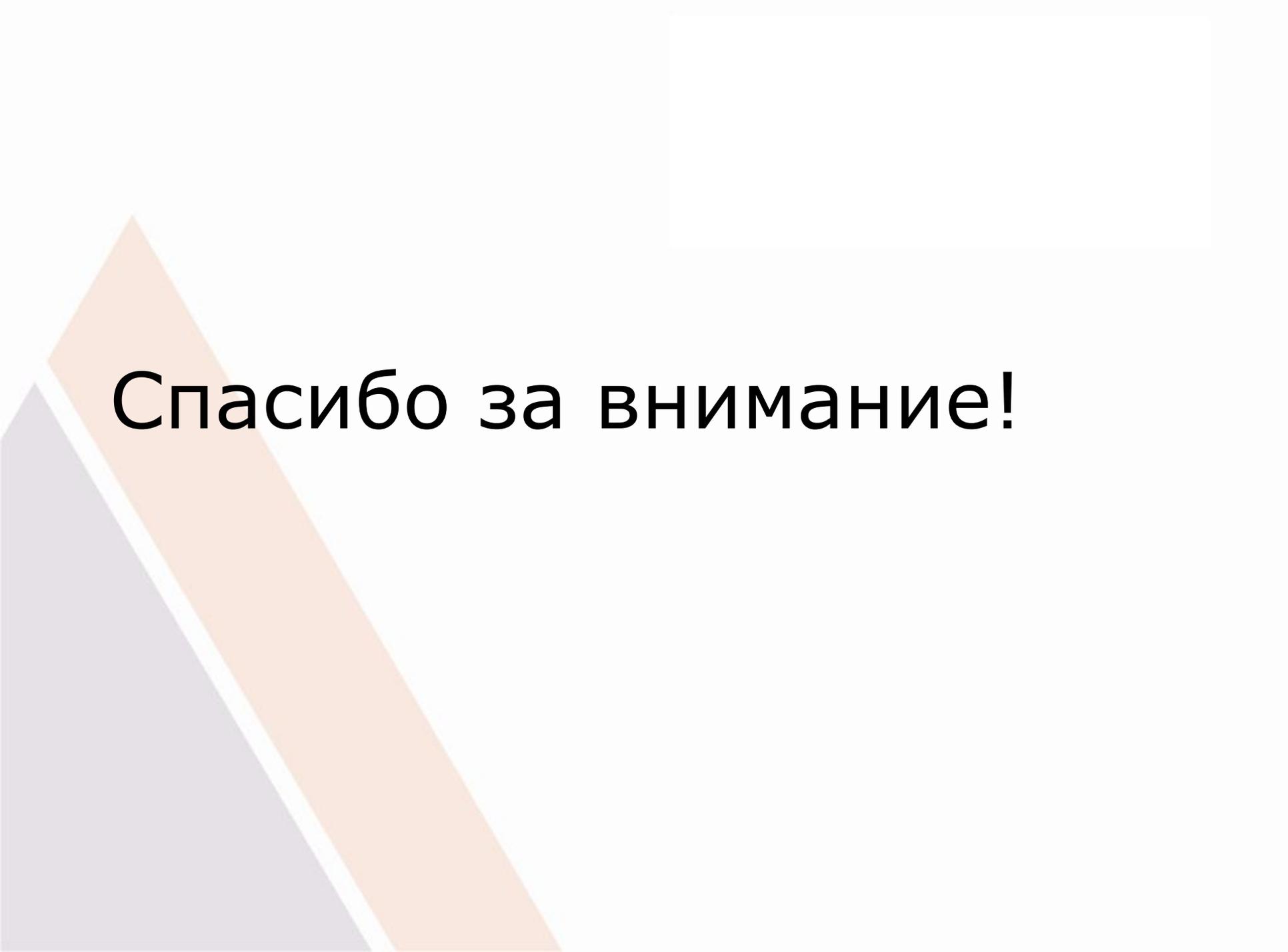
- в результате данной работы будут даны рекомендации по методологии проектирования сетей последующего поколения и предложения по определению рациональных параметров проектирования

Направления исследований

- разработка собственных средств криптографической защиты информации
- разработка алгоритмов коллективной ЭЦП и алгоритмов распределения ключей
- подготовка вкладов Республики Узбекистан на WAST-2012 и WCIT-2012

Направления исследований

- разработка рекомендаций по формированию системы технического регулирования
- разработка рекомендаций по внедрению универсального ШПД
- изучение особенностей проектирования NGN



Спасибо за внимание!