Федеральная целевая программа
«Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014—2020 годы»

Соглашение
14.582.21.0009 **от __.__.201__**

на период 2015 - 2017 гг.

Тема: *Создание опытного образца квантового устройства безопасной передачи данных*

Руководитель проекта: *руководитель группы квантовых коммуникаций, Ю.В. Курочкин*

Информационно-телекоммуникационные системы

Участники проекта

Получатель субсидии: *ООО* «Международный центр квантовой оптики и квантовых технологий»

- *Целью организации являются фундаментальные и прикладные исследования в области квантовых технологий*

Индустриальный (или международный) партнёр: *ООО КуРэйт*

- *Малое инновационное предприятие, целью которого является развитие и коммерциализация квантовых устройства безопасной передачи данных при финансовой поддержке «Газпромбанк» (Акционерное общество).*

Соисполнитель (-и):

- Задача ООО «ФемтоВижн» - выполнение работ по ПНИ-1 «Разработка полупроводниковых детекторов одиночных фотонов для длины волны оптоволоконного стандарта связи»
- Задача ООО «ДЕФАН» - выполнение работ по ПНИ-2 «Разработка алгоритмов по обработке квантового ключа»
- Задача ООО «Акронис» - выполнение работ по ПНИ-3 «Разработка устройства сопряжения существующих линий связи с системами квантового распределения ключа»

Связанные соглашения комплексного проекта

1. *Все соглашения в подготовке к подписанию*
2. *<Номер, период действия и тема связанного Соглашения (1.3) о предоставлении субсидии. Организация – получатель субсидии по связанному Соглашению.>*
3. *<Номер, период действия и тема связанного Соглашения (1.3) о предоставлении субсидии. Организация – получатель субсидии по связанному Соглашению.>*
4. *…*

Цели и задачи проекта

- *Целью ПНИЭР является создание опытного образца квантового устройства безопасной передачи данных.*
- *Так же целью настоящих ПНИЭР, реализуемых в рамках комплексного проекта, является обеспечение индустриального партнера новым оборудованием передачи ключей, позволяющим обеспечить более высокий уровень конфиденциальности передачи данных. Новое оборудование позволит обеспечить долгосрочную конфиденциальность переданных данных при условии роста вычислительных мощностей в будущем. В результате проекта в Российской Федерации должно появиться собственное оборудование на основе квантового распределения ключа.*
- *Достижение вышеуказанных целей обеспечивается с использованием результатов прикладных научных исследований, выполняемых в период 2015-2016.*
    - *ПНИ-1 «Разработка полупроводниковых детекторов одиночных фотонов для длины волны оптоволоконного стандарта связи» (Шифр: 2015-14-579-0148);*
    - *ПНИ-2 «Разработка алгоритмов по обработке квантового ключа» (Шифр: 2015-14-579-0149);*
    - *ПНИ-3 «Разработка устройства сопряжения существующих линий связи с системами квантового распределения ключа» (Шифр: 2015-14-579-0150).*

Цели и задачи ПНИ-1, ПНИ-2 и ПНИ-3

- *Основной целью настоящих прикладных научных исследований (ПНИ-1), реализуемых в рамках комплексного проекта, является обеспечение исполнителя ПНИЭР полупроводниковыми детекторами одиночных фотонов.*
- *Основной целью настоящих ПНИ-2, реализуемых в рамках комплексного проекта, является обеспечение исполнителя ПНИ-3 алгоритмами и экспериментальным программным обеспечением, используемыми в рамках ПНИ-3 с последующей передачей результатов ПНИ-3 исполнителю ПНИЭР*
- *Обеспечение исполнителя ПНИЭР блоком сопряжения существующих линий связи (оптоволоконной линии связи потребителя) с блоком передачи квантового устройства безопасной передачи данных (ПРД) и блоком приема квантового устройства безопасной передачи данных (ПРМ).*

Актуальность проекта, его соответствие приоритетам деятельности профильных федеральных ведомств и технологических платформ

- Квантовое распределение ключа позволяет реализовать абсолютно безопасную передачу данных между двумя легитимными пользователями линии связи. Принципиальная невозможность незаметного прослушивания основана на фундаментальных законах физики.
- В основе технологии квантового распределения ключа лежит принцип квантового распределения ключа, который гарантированно не известна никому, за исключением передатчика и приемника. Данная технология востребована в Российском банковском секторе. В 2016-2018гг. в США и Китае будут созданы национальные сети передачи данных, защищенных квантовой криптографией, вт.ч. Для специальных приложений. Ожидается потребность строительства в России протяженных государственных сетей, защищенных технологией квантовой криптографии. Полный цикл разработки, испытаний и освоения техники потребителем по опыту зарубежных коллег требует не менее пяти лет, поэтому создание опытного образца должно вестись уже сейчас.
- Создание таких сетей является важнейшим вызовом России в плане технологий безопасной передачи данных.
- Получено письмо от ФОИВ Министерства связи и массовых коммуникаций Российской Федерации, как инициатора ПНИЭР.
- Проект поддержан профильной технологической платформы "Фотоника".
- АО «Газпробанк» подтверждает готовность участвовать в финансировании проекта. Сформирован бизнес-план данного комплексного проекта. Потребителем продукции планируется банковский сектор.

Приложение: Как взломать канал связи?

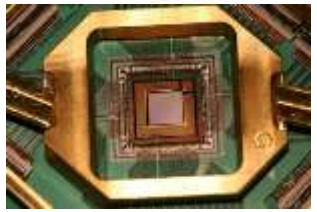
- Прибор для прослушки оптоволокна можно заказать за $200 в интернете.

- Согласно последним утечкам, АНБ успешно взломало ряд криптоалгоритмов и сотрудничает с провайдерами решений в области «безопасности».

- Безопасность основного ассимметричного алгоритма шифрования — RSA — основана на сложности вычислений и отсутствии алгоритмов дешифровки.

- Слабое место — передача ключа. Если канал связи был скомпрометирован, то единственный способ восстановить безопасность — передать новый ключ шифрования физически «из рук в руки».

- Квантовый компьютер потенциально может обесценить RSA и существенно ослабить остальные шифры.



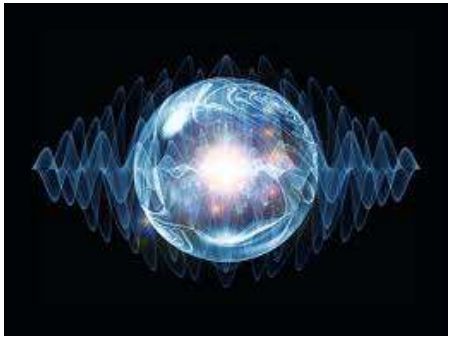
Приложение: Квантовая криптография – абсолютная надежность, гарантированная законами физики

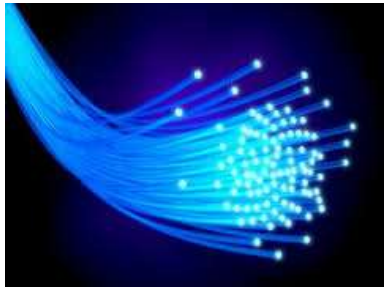
Концепция

- Информация кодируется в квантовом состоянии отдельных фотонов
- Постулаты квантовой механики
  - Фотон неделим
  - Квантовое состояние одной частицы нельзя скопировать
  - Измерение меняет или уничтожает состояние
- Если канал подслушивается, это гарантированно обнаруживается на основе фундаментальных законов физики

Характеристики

- Можно использовать существующие оптические линии связи
- Rack-mountable. Прибор может быть установлен в обычном датацентре
- Поддержка различных алгоритмов шифрования, возможность добавления новых
- Plug-and-Play. Не требует тонкой настройки, обслуживается рядовым сетевым инженером
- Скорость передачи ключа 10 кбит/с (коммерческие продукты на данный момент)
- Дальность передачи до 25-100 км
- Требует выделенного оптоволокна (работа в одном канале с классической связью ухудшает соотношение сигнал/шум, снижая дальность)

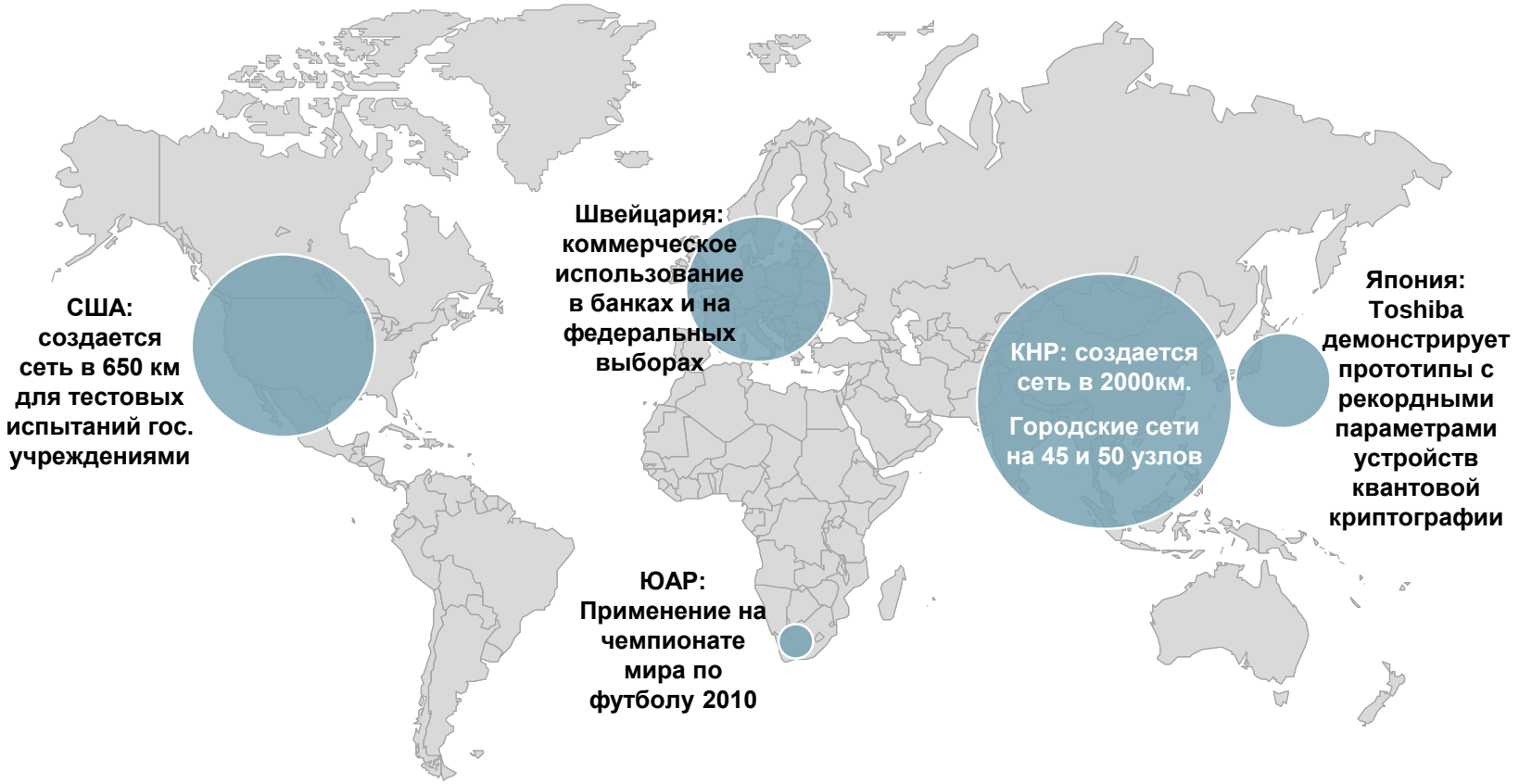




Приложение: Квантовая криптография решает проблемы, невозможные для классических схем

	Преимущества	Проблемы
Одноразовый код (курьер)	• Максимальная защита	Необходим способ защищенного распределения секретных ключей • Дорого и неудобно
Криптография с открытым ключом (например RSA)	• Использует вычислительную сложность некоторых задач (например, факторизация больших чисел) • Защита не доказана, но проверена практически • Применима для большинства задач, кроме самых важных	• Потенциально взламывается квантовым компьютером • Есть угроза появления новых алгоритмов
Квантовая криптография	• Обеспечивает защищенное распределение секретных ключей по открытым каналам связи • Защита гарантируется фундаментальными законами физики	• **Ограничена длина пролета (усилить сигнал нельзя)** • **Требует выделенного волокна**

Проекты, реализующие технологию квантовой криптографии в мире



Проекты квантовой криптографии переходят из PR плоскости в прикладные решения

Соглашение № *14.582.21.0009*

Квантовой криптография предоставляет секретные ключи для кодирования существующим оборудованием

Основа квантовой криптографии – квантовые свойства частиц

Информация кодирует состояние (поляризацию) единичного фотона

Основы квантовой механики

- Фотон невозможно разделить
- Квантовое состояние одиночной частицы невозможно скопировать
- Измерение уничтожает или изменяет состояние

⇒ **Перехват создаст ошибки в передаваемом сообщении и будет обнаружен**

Но что происходит при попытке взлома?

- Перехватчик может перехватывать фотоны, измерять их и отправлять заново в том же состоянии или производить любые неразрушающие измерения, не запрещенные законами физики.

⇒ **Передача не ортогональных квантовых состояний делает невозможным узнать все об этом состоянии, если есть только один квант.**

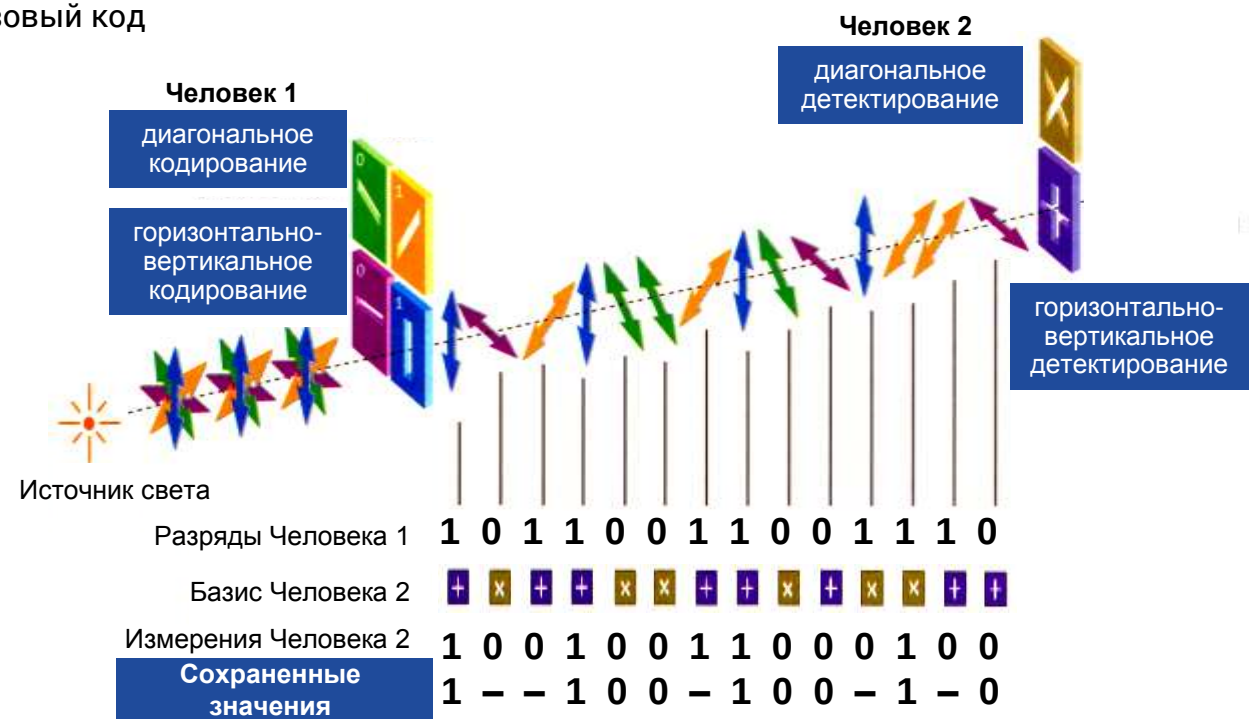
⇒ **Любая попытка измерений вносит шумы, которые обнаруживаются**

Первый протокол квантовой криптографии BB84

Передача сообщения

- Отправитель выбирает случайное значение разряда: 0 или 1
- Отправитель выбирает случайным образом между двумя способами кодирования: 

- Отправитель готовит одиночный фотон, кодирует значение разряда в его поляризации, и отправляет Получателю
- Получатель измеряет полученный фотон с помощью поляризационного светоделителя, случайным образом настроенного на вертикально-горизонтальное или диагональное кодирование
- Получатель получит верное значение, только если использует ту же схему кодирования, что и Отправитель
- После передачи большого числа разрядов Отправитель и Получатель обмениваются (по открытому каналу) схемами кодирования каждого разряда. Так как передача происходила на одиночных фотонах, потенциальный перехватчик не может иметь полной информации о состояниях
- Отправитель и Получатель выкидывают те случаи, в которых они использовали разные схемы кодирования
- После этого у Отправителя и Получателя остаются идентичные, секретные последовательности разрядов, то есть одноразовый код



Квантовая криптография позволяет обнаружить перехват

Что произойдет в случае попытки перехвата?

- Перехватчик не знает базиса кодирования отправителя (горизонтально-вертикальный или диагональный)
- Перехватчик может детектировать, а затем пересылать фотоны только в случайном базисе, при этом его знания о состоянии конкретного фотона будут не полными, так как для полного измерения нужна серия экспериментов
- Между секретными ключами отправителя и адресата возникнут расхождения
- Перехват будет обнаружен

Основные ожидаемые результаты ПНИЭР

- Основной результат ПНИЭР – достижение РФ уровня ведущих разработок по созданию телекоммуникационного оборудования нового поколения на основе квантового распределения ключа
- Будет создано отечественное устройство квантового распределения ключа, состоящее из приемника и передатчика, стабильно работающих в существующих линиях связи (стандартное одномодовое оптоволокно 1550 нм).
- Будет произведен поиск путей улучшения параметров предельной дальности и скорости передачи квантового ключа, а также решений, позволяющих обеспечить надежность работы образца в существующих линиях связи. Переданный квантовый ключ будет использоваться для кодирования данных.
- В результате будет создан образец устройства квантовой криптографии, где новые технические решения обеспечат параметры работы выше зарубежных коммерческих образцов на данный момент и на уровне ожидаемых коммерческих продуктов конкурентов в 2018 году.

Прогнозную оценку ожидаемых масштабов можно сделать на основе следующих данных:

- На данный момент швейцарская компания ID Quantique успешно продает в банковском секторе устройство квантовой криптографии «Cerberis», которая обеспечивает генерацию квантового ключа со скоростью менее 10 кбит/с на расстояние 25-80 км.
- В США и Китае активно идет строительство протяжённых междугородних сетей и городских сетей, состоящих из десятков серверов каждая. Стоимость одного импортного устройства с устройством сопряжения и подключением составляет порядка 300 000 Евро.
- Согласно исследованию, представленному на сайте http://companiesandmarkets.com, мировой рынок квантовой криптографии будет составлять 1 миллиард долларов США к 2018 году.
- В анализе рынка квантовой криптографии, который был сделан Institute for Quantum Computing, мировой рынок квантовой криптографии будет иметь экспоненциальный рост и к 2023 достигнет 5 миллиардов долларов, а к 2029 - уже 20 миллиардов
- Создание отечественного устройства позволит России занять 5-10% мирового рынка квантовой криптографии.

Ожидаемые результаты ПНИ-1, ПНИ-2 и ПНИ-3

- *ПНИ-1:* должен быть разработан образец детектора одиночных фотонов готовый для коммерческого использования в составе квантового устройства безопасной передачи данных;
- ПНИ-2: Будут разработаны алгоритмы обработки квантового ключа для реализации в ПНИ-3, а также создано экспериментальное программное обеспечение, реализующего данные алгоритмы
- ПНИ-3: Будет создан блок устройства квантовой криптографии, реализующий классическую обработку квантового ключа путем коммуникации между приемником и передатчиком. Блок будет иметь возможность универсального подключения, как к оптоволоконной сети, так и с использованием стандарта Ethernet. Блок должен быть встраиваться в основное устройство квантовой криптографии;

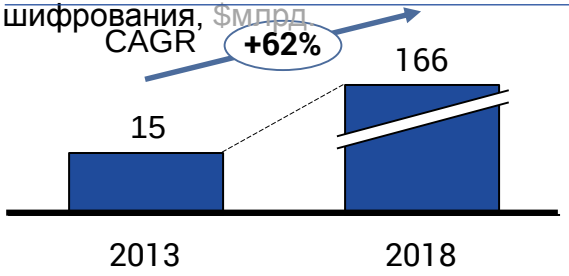
Приложение: Рынок и основные игроки

Производители коммерческих продуктов квантовой

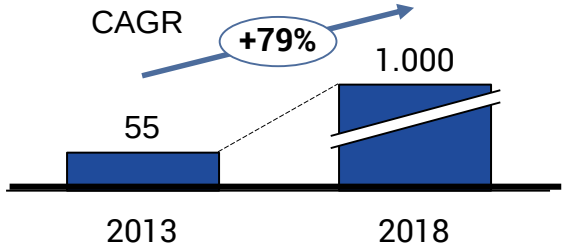
Компания	Продукт	Цена	Расстояние, км	Скорость, Kbits
Id Quantique (Швейцария)	Cerberis	$ 300 000 с установкой	25	1
MagiQ (США)	QPN	$ 100 000	50	3,5
SequreNet (Франция)	Cyngus	?	20	10

Объемы рынка классической и квантовой криптографии

Рынок классического аппаратного шифрования, $млрд.



Рынок квантовой криптографии, $млн.

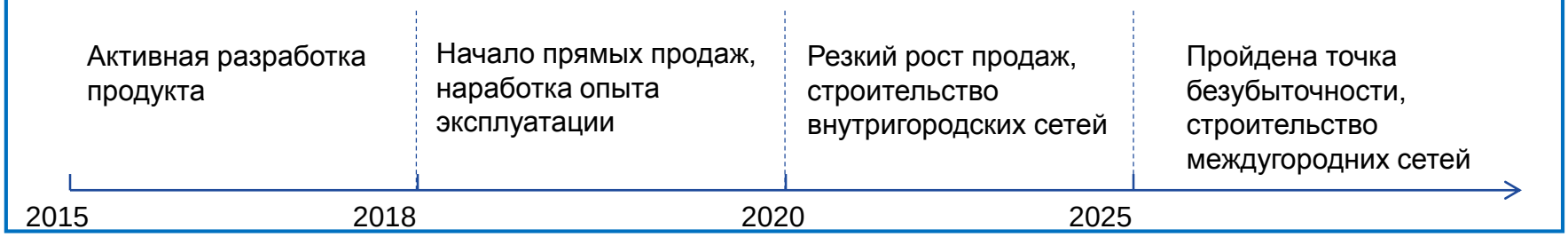


Кроме того, основные игроки в области ИТ и телекоммуникаций активно занимаются R&D разработками в области телекоммуникационных сете нового поколения на основе технологии квантовой криптографии.

Все зарубежные разработки проходят сертификацию в своих странах.

План коммерциализации

Краткий план выхода на рынок



Продукты

Разрабатываемые продукты

- Установки квантовой криптографии для университетов
- Установки квантовой криптографии для корпораций
- Детекторы высокой эффективности
- Детекторы низкой стоимости

Потребители

Детекторы

Биомедицинское оборудование:
- Потоковые цитометры
- ДНК-ридеры
- Томографы
- SPECT

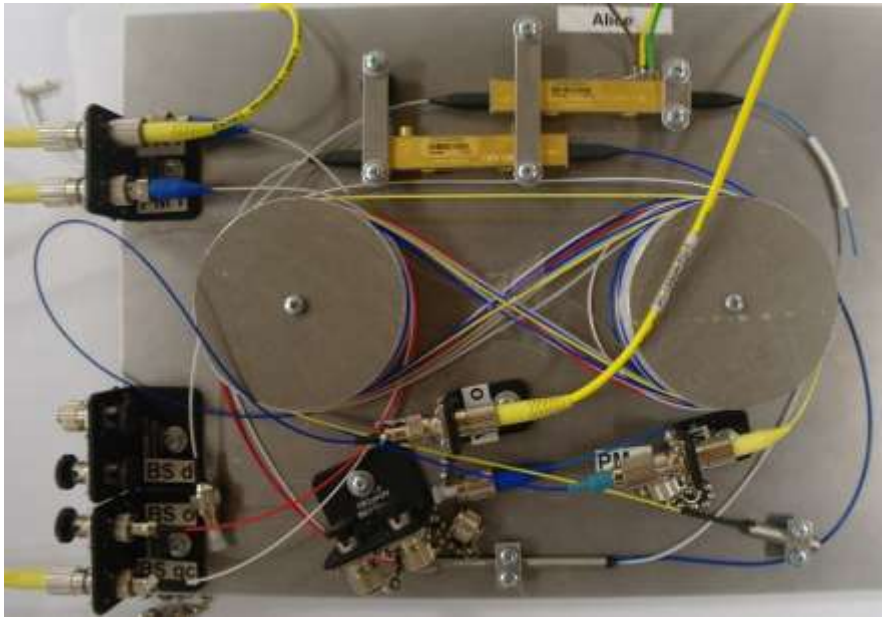
Установки криптографии

- Госструктуры
- Финансовые организации
- Корпорации
- Средний бизнес
- Университеты

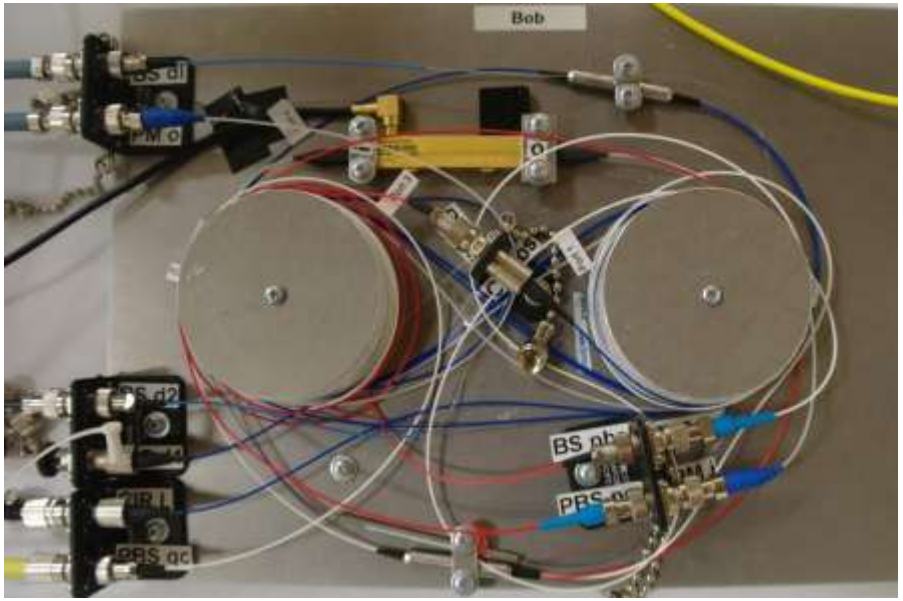
Результаты исследовательской работы, полученные в 2015 г.

Первый этап ПНИЭР подготовительный, на этом этапе выполняется макетирование.

- *ПНИЭР: Разработаны и испытаны макеты интерферометров передатчика и приемника (Отчет – ЭКД, методики испытаний и результаты испытаний)*



Макет интерферометра передатчика



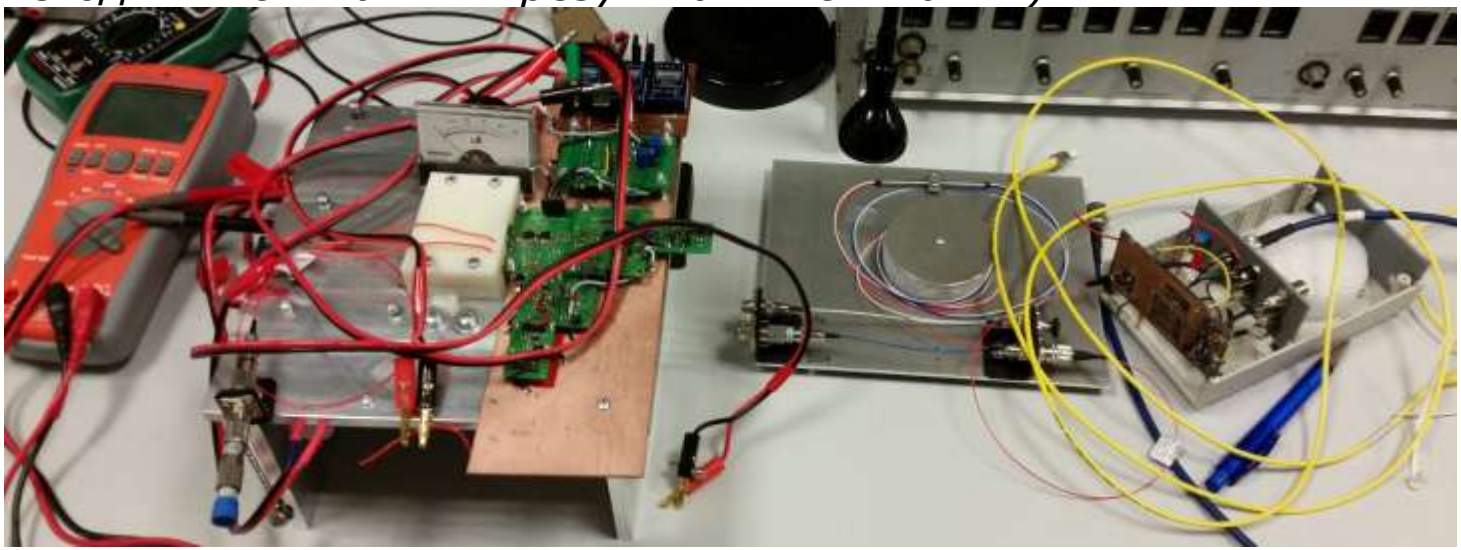
Макет интерферометра приемника

Соглашение № *14.582.21.0009*

Результаты исследовательской ПНИ-1, ПНИ-2 и ПНИ-3 работы, полученные в 2015 г.

Первый этап подготовительный, на этом этапе выполняется макетирование.

- *ПНИ-1: Разработан макет детектора одиночных фотонов (Отчет – ЭКД, методики испытаний и результаты испытаний).*



- *ПНИ-2: Разработаны первые версии алгоритмов (Описание алгоритмов).*
- *ПНИ-3: Разработаны эскизные и технические проекты ПО Блока, Разработаны проекты протоколов информационно-электрического взаимодействия (документация проектов).*

Состояние выполнения запланированных индикаторов

ТРЕБОВАНИЯ ПО ДОСТИЖЕНИЮ ЗНАЧЕНИЙ ПОКАЗАТЕЛЕЙ РЕЗУЛЬТАТИВНОСТИ ПРЕДОСТАВЛЕНИЯ СУБСИДИИ

Наименование	Единица измерения	2015 год	2016 год	2017 год
Индикаторы				
Число публикаций по результатам проекта в научных журналах, индексируемых в базе данных Scopus или в базе данных "Сеть науки" (WEB of Science)	единиц	0	2	2
Число патентных заявок, поданных по результатам проекта	единиц	0	1	1
Доля исследователей в возрасте до 39 лет в общей численности исследователей-участников проекта	процентов	50	50	50
Число завершенных проектов прикладных научно-исследовательских работ, готовых к переходу в стадию опытно-конструкторских работ (опытно-технологических работ)	процентов	0	0	1
Объем привлеченных внебюджетных средств	млн руб	17	27	40,5
Показатели				
Средний возраст исследователей – участников проекта (не более)	лет	40	40	40
Количество мероприятий по демонстрации и популяризации результатов и достижений науки, в которых приняла участие и представила результаты проекта организация - исполнитель проекта	единиц	0	2	3
Количество используемых при проведении исследований и разработок в рамках проекта уникальных научных установок	единиц	0	0	0
Количество используемых при проведении исследований и разработок объектов зарубежной инфраструктуры сектора исследований и разработок	единиц	0	0	0
Количество центров коллективного пользования научным оборудованием, научное оборудование которых использовалось при проведении исследований и разработок в рамках проекта	единиц	0	0	0
Число диссертаций на соискание ученых степеней, защищенных по результатам проекта	единиц	0	0	0

На данный момент идет подготовительная работа и ожидается получение средств Субсидии. Все показатели относятся к 2016-2017 годам.

По ПНИ-1, ПНИ-2 и ПНИ-3 на 2015 год патентных заявок и публикаций не запланировано

Спасибо за внимание!

Докладчик:

руководитель группы квантовых коммуникаций, Ю.В. Курочкин

Соглашение № *14.582.21.0009*