Учебный курс
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЙ»

Тема :
Волоконно-оптические (технические) каналы утечки информации

Модуль 1:
Перехват трафика в волоконно-оптических коммуникациях

Лектор:

кфмн, доцент Гришачев Владимир Васильевич

Программа 1 модуля курса

ЛЕКЦИИ

I. Сценарии перехват трафика и их анализ

II. Способы и техника перехвата трафика

III. Методы защиты трафика

IV. Коллоквиум

Лекция 7-8

«Методы защиты трафика»

1. Общая характеристика методов защиты трафика;
2. Охрана периметра кабеля;
3. Мониторинг состояния оптического тракта;
4. Программно-аппаратная защита трафика;
5. Адаптированные методы кодировки для защиты информации при передаче по оптическим сетям;
6. Классическая и квантовая криптография.

1. Общая характеристика методов защиты трафика

- **Методы защиты информации сетях связи**

- построение ТСЗИ от перехват в ВОСПИ основано на анализе возможностей нарушителя и физико-технических особенностях волоконно-оптических каналов связи

преимущества оптического волокна и кабеля как транспортной среды для информации связаны с

- ✓ возможностью построения транспортной среды из полностью диэлектрических материалов;
- ✓ высокой скоростью передачи информации при низком уровне шумов;
- ✓ ограниченностью дистанционных методов съема информации;
- ✓ возможностью конвергенции транспортных и измерительных сетей;
- ✓ высокая удаленность друг от друга активных сетевых элементов;

1. Общая характеристика методов защиты трафика

- **Сравнительный анализ методов защиты информации сетях связи**

- Требования к методам защиты трафика от перехвата в телекоммуникациях
  1. Защита трафика должна проводиться на больших дальностях (от 500 км и более)
  2. Защиты трафика на участках как без, так и с активными элементами сети

- Требования к методам защиты трафика от перехвата в локальных сетях
  1. Защита трафика должна проводиться на дальностях (до 500 км)
  2. Защиты трафика на участках без активных элементов сети

Выбор метода защиты связан с техническими возможностями и значимостью защищаемой информации

1. Общая характеристика методов защиты трафика

- **Методы защиты информации сетях связи**

- ТСЗИ от перехват в ВОСПИ можно разделить на несколько типов

1. Охрана периметра оптического кабеля
2. Мониторинг состояния оптического тракта
3. Программно-аппаратная защита трафика
4. Адаптированные к оптической сети методы защиты
5. Классическая и квантовая криптография

2. Охрана периметра кабеля

○ Характеристика методов защиты трафика охраной кабеля

этап подхода к оптическому кабелю и волокну

❖ оптический кабель может быть использован как среда для передачи информации оптическими сигналами и как среда для измерений воздействий и полей оптическим зондирующим излучением.

- совмещение двух данных функций в одном кабеле позволяет реализовать функцию защиты от перехвата следующими способами

1. Контроль намерений нарушителя по его действиям вблизи кабеля
2. Контроль состояния защитных покрытий/оболочек кабеля на предмет преднамеренного разрушения
3. Защита кабеля от разрушения защитных покрытий/оболочек кабеля
4. Защита волокна от НСИ путем отвода оптических излучений

2. Охрана периметра кабеля

- **Контроль намерений нарушителя по его действиям вблизи кабеля**

- действия нарушителя сопровождаются вибро-акустическими сигналами, воздействующими на волокно оптического кабеля и вызывающими в нем паразитные модуляции параметров оптического излучения;

  - на данных свойствах оптического кабеля функционируют распределенные волоконно-оптические системы охраны периметра объектов;

  - промышленно выпускается много подобных систем, в том числе в России:

    1. Волоконно-оптическая периметральная система охраны «ВОРОН™» ООО «Прикладная радиофизика» www.neurophotonica.ru
    2. Волоконно-оптическая система охраны «СОВА» Инновационный центр «Оптика» www.centroptic.ru
    3. Оптоволоконная распределенная система вибромониторинга и охраны периметра ООО «Оптолекс» www.optolex.ru
    4. Когерентный рефлектометр «Дунай» ООО «Т8» www.t8.ru

2. Охрана периметра кабеля

- **Контроль намерений нарушителя по его действиям вблизи кабеля**

- принципы функционирования волоконно-оптических систем охраны периметра (ВОСОП) основаны на регистрации виброакустических колебаний окружающей среды методами
  1. регистрации межмодовой интерференции
  2. регистрации спекл-структуры
  3. двух лучевой интерференции
  4. датчиками на брэгговских решетках
  5. когерентной рефлектометрии

- ВОСОП в системе защиты трафика:
  - ✓ периметром является оптический кабель
  - ✓ чувствительным волокном является волокно телекоммуникационного кабеля (выделенное или используемое для передачи трафика)

2. Охрана периметра кабеля

- **Контроль намерений нарушителя по его действиям вблизи кабеля**

❖*Когерентный рефлектометр ДУНАЙ (ООО Т8, Москва, www.t8.ru)* распределенный датчик вибрации и акустических воздействий на основе когерентного рекфлектометра для систем безопасности

Принципы работы

В волокно периодически с частотой 2 кГц вводятся короткие (200 нс) оптические импульсы и анализируются изменения в интерференционной картине сигнала обратного рассеяния

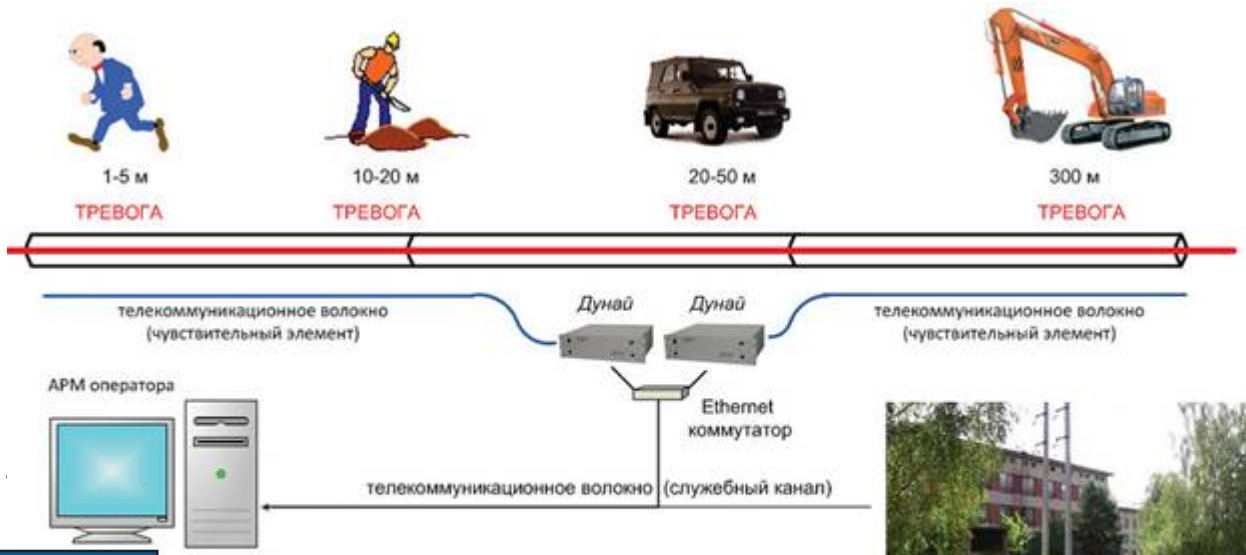


Иллюстрация работы распределенного датчика вибрации сигнала от идущего человека

Параметр	Значение
Тип оптического волокна	SMF-28
Максимальная длина волокна	40 км
Разрешаюшая способность	10 м
Диапазон регистрируемых частот (40 км)	10 Гц–1,2 кГц
Диапазон регистрируемых частот (10 км)	10 Гц–5 кГц

2. Охрана периметра кабеля

- **Контроль намерений нарушителя по его действиям вблизи кабеля**

❖ возможности волоконно-оптической системы охраны периметра (ВОСОП) в защите трафика

✓ используется для контроля действий возможных нарушителей в реальном времени на расстоянии до 100 м от кабеля;

✓ дальность обнаружения действий нарушителя по кабелю не превышает 100 км (в пределе действия рефлектометра не более 250 км);

✓ используется одно из волокон кабеля, возможно использование волокна передающего трафик при подключении ВОСОП путем мультиплексирования информационного сигнала и сигнала зондирования с разделением по длине волны;

✓ используется только в пределах «видимости» одной секции волокна:

за пределы секции, отделяемой активным оборудованием, зондирующее излучение не проникает;

2. Охрана периметра кабеля

○ Контроль состояния защитных оболочек кабеля

❖ специальная защита кабеля

основная угроза трафику исходит от физического контакта с волокном кабеля, даже с помощью дистанционных методов при не разрушенной защитной оболочке реализация перехвата связана с большими трудностями по формированию информативных излучений

в структуру оптического кабеля вводятся элементы, препятствующие разрушению и проникновению внутрь кабеля для последующего получения доступа к волокну

- ✓ усиленное бронирование
- ✓ защитное покрытие/оболочка с само разрушающимися при воздействии свойствами
- ✓ воздействие на кабель регистрируется ТСЗИ не волоконно-оптическими методами

2. Охрана периметра кабеля

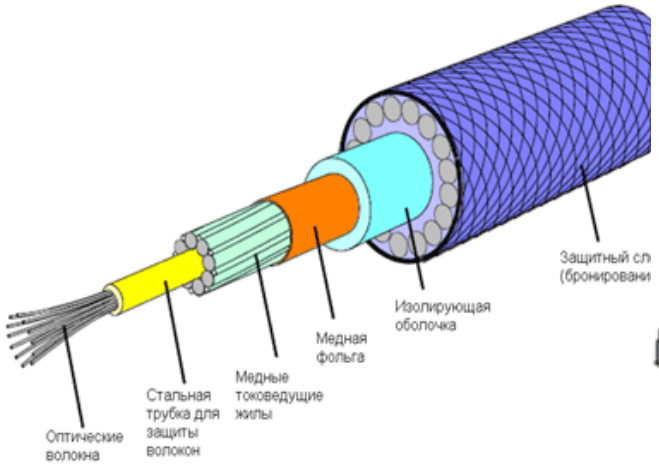
○ Контроль состояния защитных оболочек кабеля

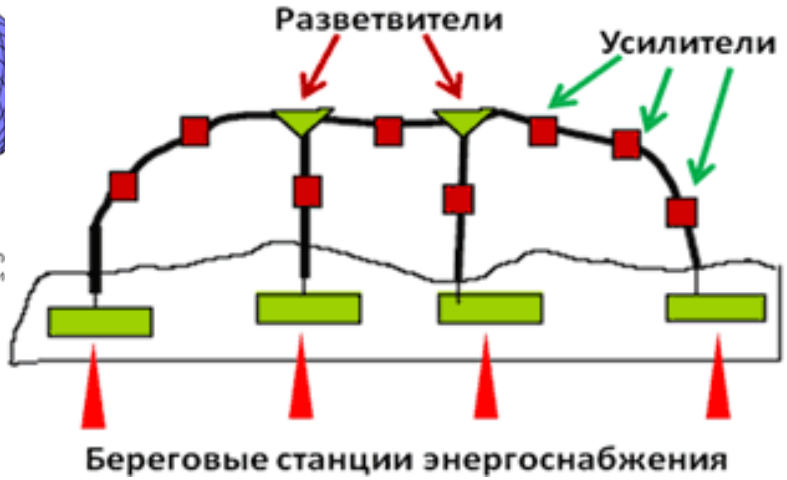
❖ подводный кабель под высоким напряжением

- защитные оболочки кабеля имеют прочную механическую защиту, содержащую металлическую оболочку;

- в кабеле для подводного монтажа металлическая оболочка используется для электрического питания оптических усилителей, на которую подается высокое напряжение;

- в зависимости от длины подводной части напряжение достигает нескольких 10 кВ.





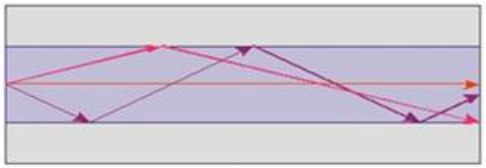
✓ это естественная защита от действий нарушителя по разрушению кабеля

2. Охрана периметра кабеля

- **Защита волокна от НСИ путем отвода оптических излучений**

- специальные волокна с защитой от НСИ

  основные способы отвода излучения из волокна или регистрации проходящего излучения связаны с волокнами со стандартной структурой: ступенчатое или градиентное распределение показателя преломления от сердцевины к оболочке

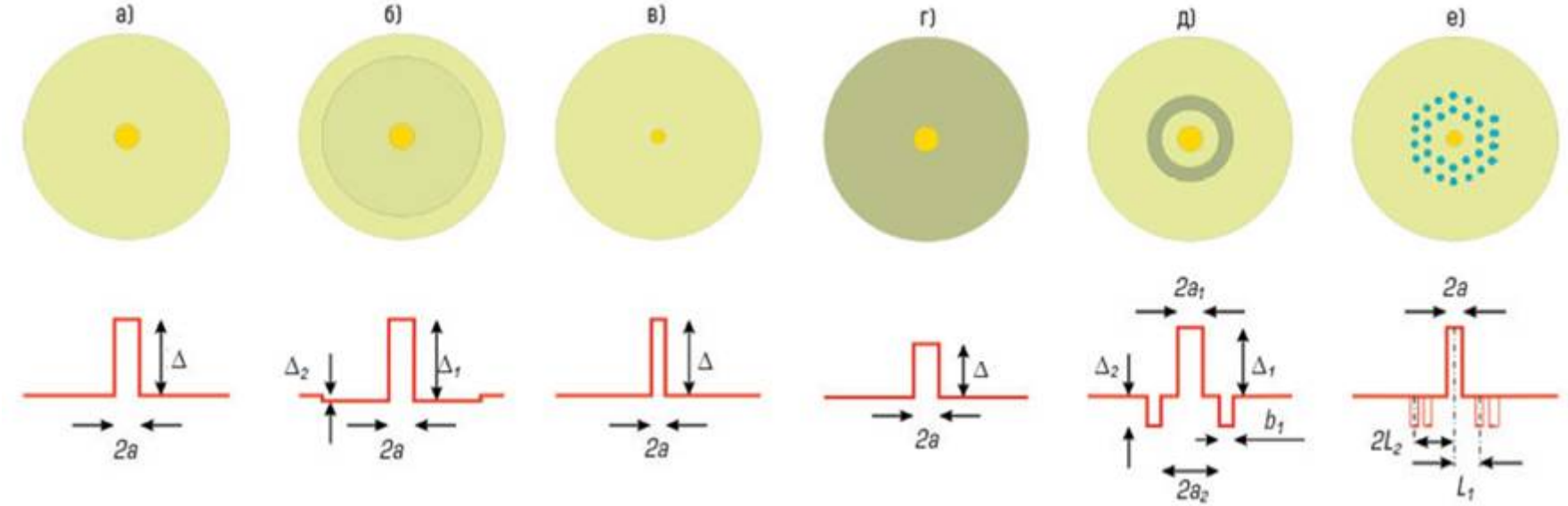


2. Охрана периметра кабеля

- **Защита волокна от НСИ путем отвода оптических излучений**

❖ специальные волокна с защитой от НСИ

применение оптоволокна со сложным распределением показателя преломления:
а — волокно с традиционным ступенчатым профилем показателя преломления; *б* — волокно с дипрессированной оболочкой; *в* — волокно с уменьшенной сердцевиной и, соответственно, уменьшенным диаметром модового поля; *г* — волокно с уменьшенным показателем преломления оболочки; *д* — волокно, с кольцевой «траншеей» в оболочке; *е* — микроструктурированное волокно HAF (Holed Assisted Fiber) с уменьшенными потерями на изгибах

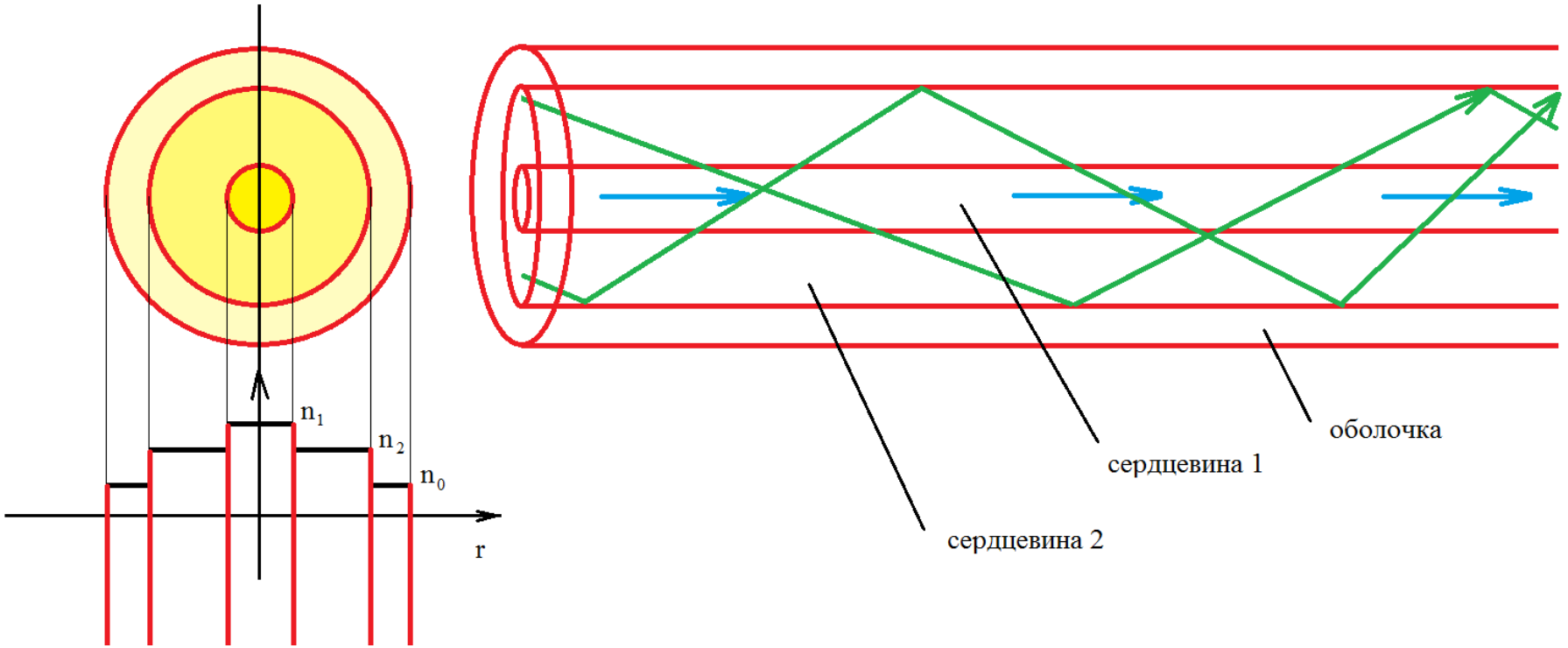


2. Охрана периметра кабеля

- **Защита волокна от НСИ путем отвода оптических излучений**

- специальные волокна с защитой от НСИ

  ступенчатое волокно со сдвоенными концентрическими сердцевинами для защищаемого трафика (1) и с защитным шумовым излучением (2)

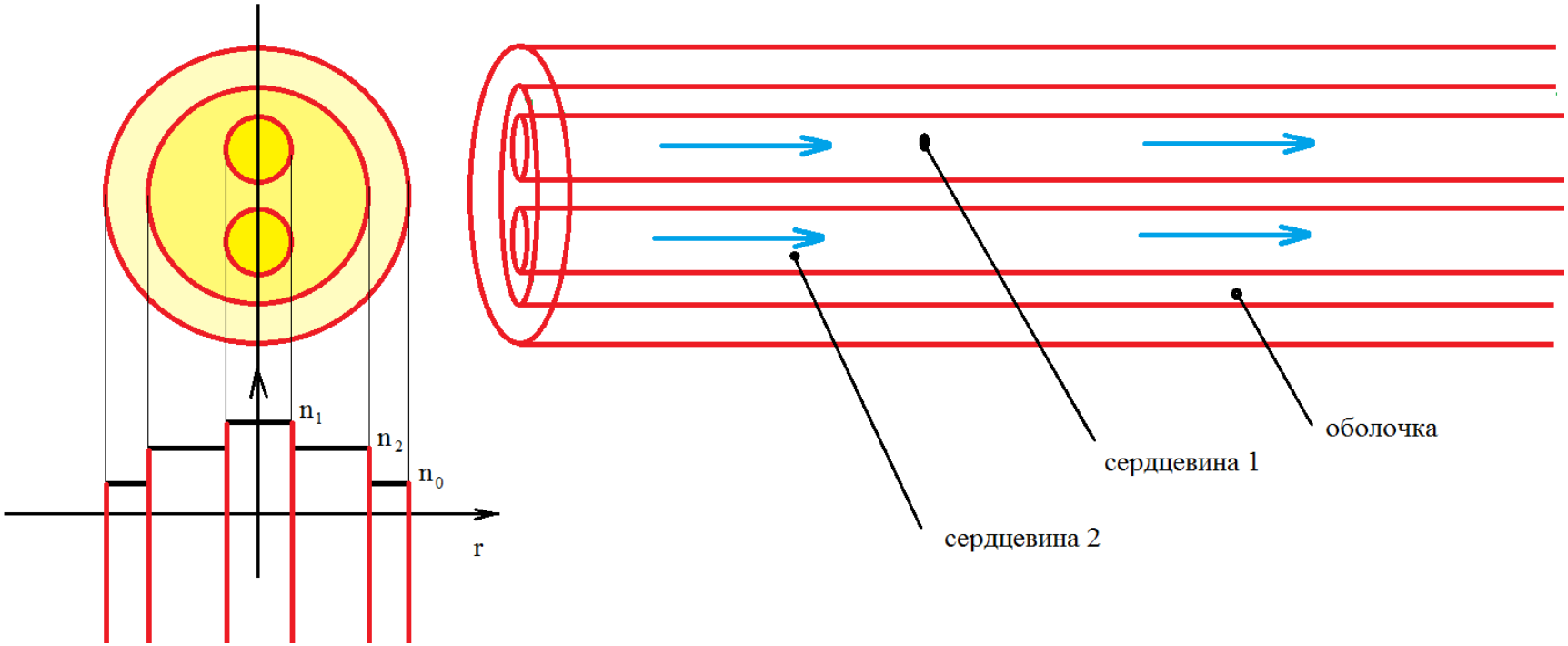


2. Охрана периметра кабеля

- **Защита волокна от НСИ путем отвода оптических излучений**

- специальные волокна с защитой от НСИ

  ступенчатое волокно со сдвоенными разнесенными сердцевинами 1 и 2 для защищаемого трафика



2. Охрана периметра кабеля

- **Выводы**

1. ВОСОП применимо для защиты локальных сетей, так как охраняемый периметр ограничен дальностью действия системы;

2. Другие методы защиты применимы как в телекоммуникациях, так и локальной связи, но эффективность защиты связывается только со сложностью выполнения работ по нарушению защитных свойств;

3. Подобные системы защиты являются неотъемлемой частью монтируемой кабельной системы и первым рубежом защиты трафика;

3. Мониторинг состояния оптического тракта

- **Характеристика методов защиты трафика мониторингом сети**

этап работы с оптическим каналом

- действия нарушителя по перехвату трафика направлены на получения доступа к оптическим информационным сигналам и сопровождающих их информативным сигналам;

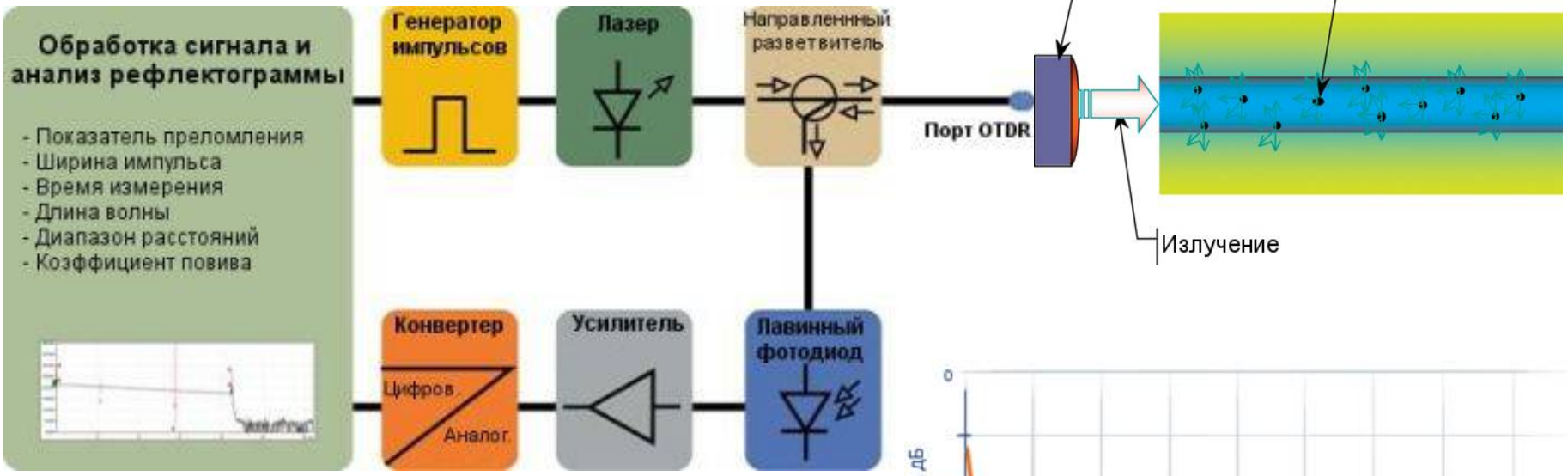
  в результате данных действий изменяются параметры сети, что может выявляться следующими методами

1. Рефлектометрией оптических волокон на предмет возможных изменений в сети;
2. Контроль временных параметров прохождения сигнала;
3. Контроль оптического бюджета в оптическом канале;
4. Контроль оптических параметров сигнала;

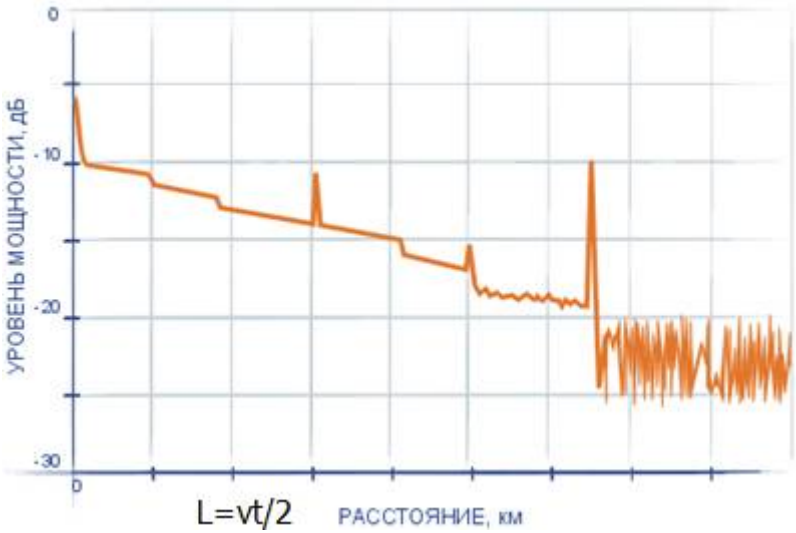
3. Мониторинг состояния оптического тракта

○ Рефлектометрия оптических волокон

❖Optical Time Domain Reflectometer, OTDR



Импульсная оптическая рефлектометрия волокон –
это область измерительной техники, которая основывается на получении информации об измеряемой линии по анализу её реакции на зондирующее (возмущающее) воздействие,
с возможностью определения расстояния до неоднородности в канале: $L=vt/2$,
v – скорость распространения света в волокне,
t - время от отправления до возвращения оптического импульса

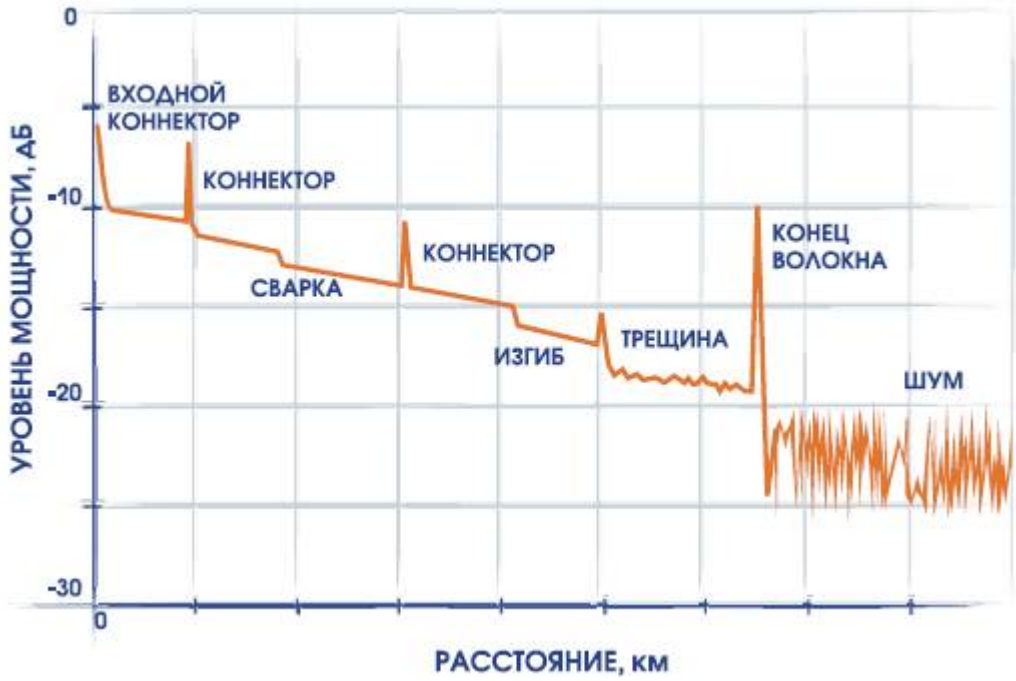


3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон**

❖Optical Time Domain Reflectometer, OTDR

с помощью рефлектометра можно определить полную величину потерь в линии, местоположение обрыва волокон, участки линии с большими значениями потерь, коэффициенты отражения от соединительных разъемов и т.д.

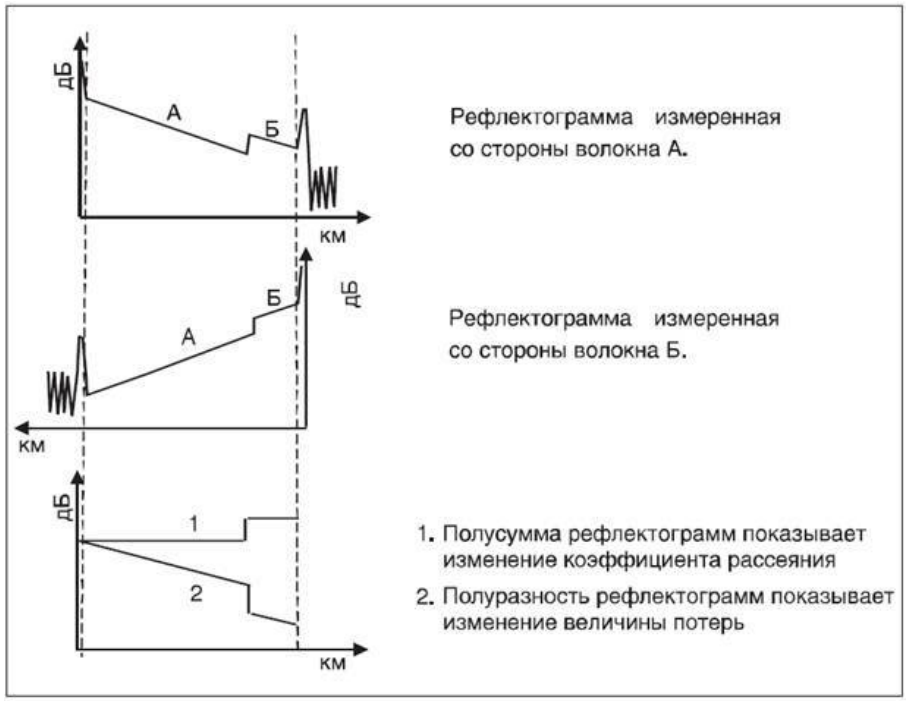


3. Мониторинг состояния оптического тракта

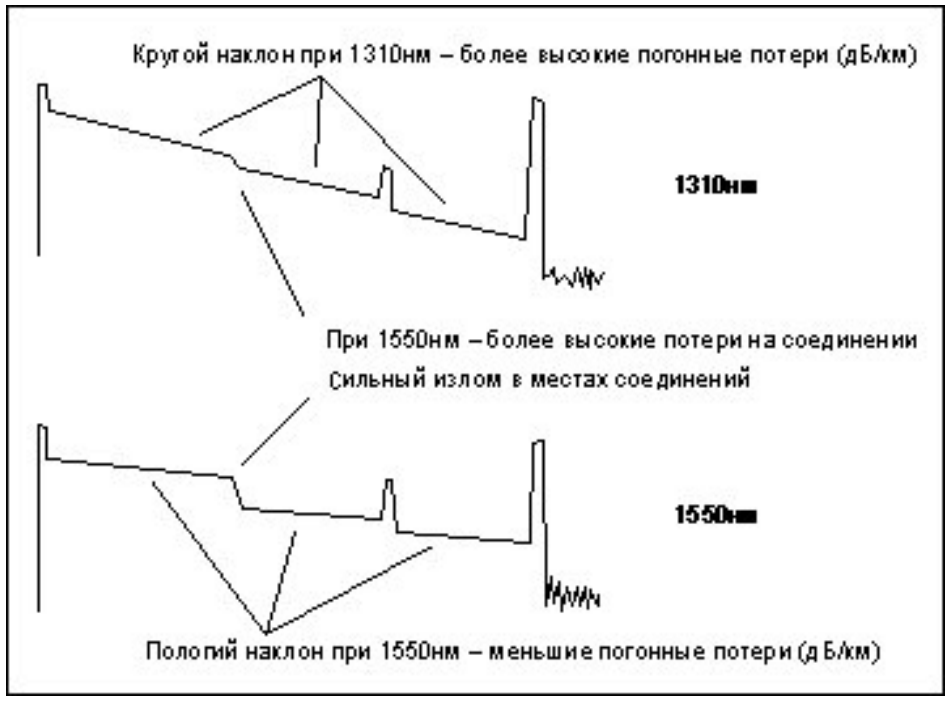
- **Рефлектометрия оптических волокон**

❖Optical Time Domain Reflectometer, OTDR

Виды оптических рефлектограмм



встречные рефлектограммы



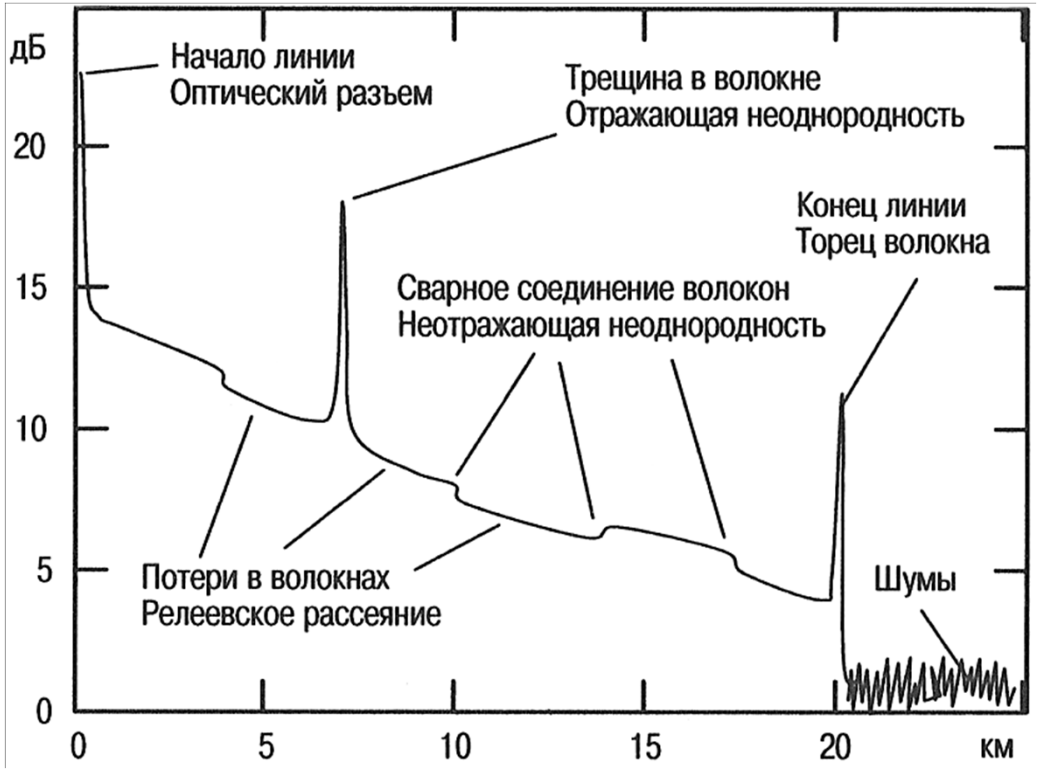
рефлектограммы на разных длинах волн

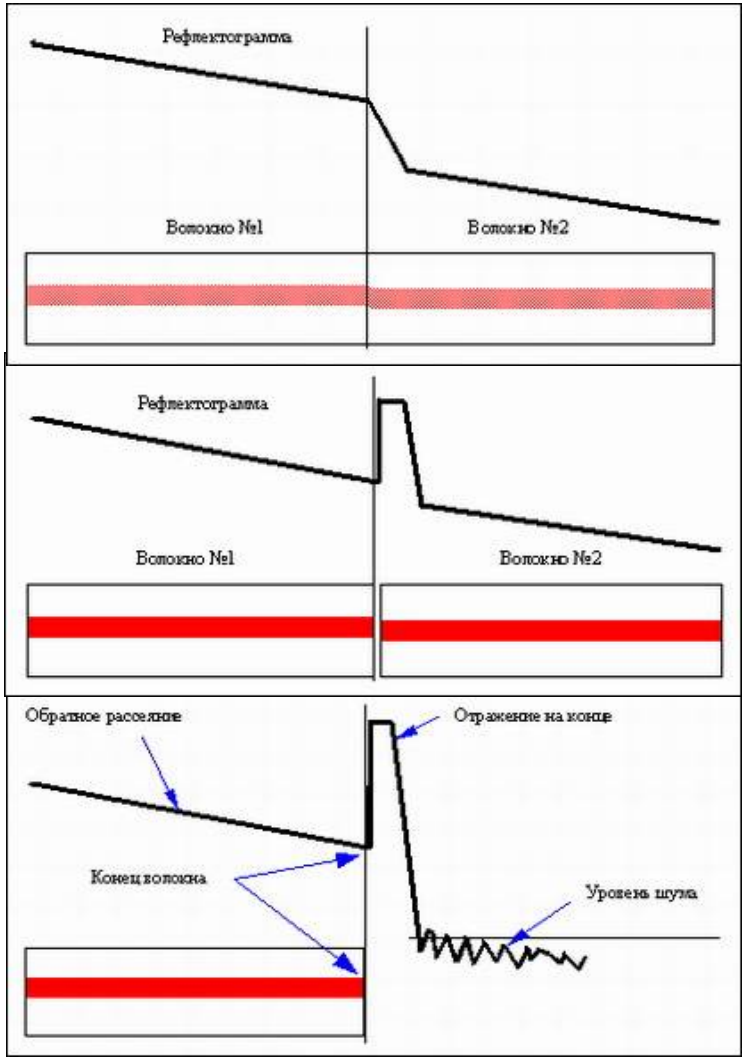
3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон**

❖Optical Time Domain Reflectometer, OTDR

виды дефектов на рефлектограммах





3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон**

❖Optical Time Domain Reflectometer, OTDR

оптический рефлектометр в системе мониторинга ВОЛС.

1. Программно-аппаратный комплекс "Сапфир" (НЕЛК, Москва).
2. Система мониторинга оптических волокон FIBERTEST (ИИТ, Беларусь).
3. Система мониторинга ВОЛС (КБПМ-ИБ, Москва).
4. Предложение по защите волоконно-оптических коммуникаций с помощью
   Remote Fiber Test System (RFTS),
   Optical Network Management System (ONMS)

от

Agilent Technologies – HP (**AccessFiber**); Wavetek Wandel&Goltermann (**Atlas**); GN Nettest (**Orion**); JDSU (**ONMS**); EXFO (**FiberVisor**) и другие

3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон**

❖программно-аппаратный комплекс «Сапфир»
НПЦ «НЕЛК» www.nelk.ru

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ ИЗМЕРЕНИЯ ПАРАМЕТРОВ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ (ВОСП) И ОЦЕНКИ ЗАЩИЩЕННОСТИ ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ «САПФИР»

3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: ПАК «Сапфир»**

Возможности

✓ В комплексе использованы возможности оптического тестера и рефлектометра.

✓ Комплекс может определить как место обрыва, так и локализовать отражающие и не отражающие неоднородности волокна, включая те, которые вызваны поломкой кабеля.

✓ Комплекс может работать в автоматическом, автоматизированном и ручном режимах, в автоматическом режиме диапазон, ширина импульса, а также время усреднения устанавливаются автоматически.

✓ Автоматический режим идеально подходит для обслуживающего персонала, слабо знакомых с работой оптических измерительных приборов.

✓ Полуавтоматический режим позволяет пользователю устанавливать диапазон длины волокна, остальные параметры устанавливаются автоматически.

✓ Ручной режим предназначен для опытных пользователей.

✓ В комплексе используются сменные адаптеры, что позволяет подключать кабели с различными типами коннекторов.

3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: ПАК «Сапфир»**

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Длина волны	550±20 нм, доп. 850±20, 1310+20, 1625±10 нм
Динамический диапазон	30 дБ
Диапазон расстояний	20, 40, 80, 160 км
Длительность импульса	50, 100, 300, 1000, 3000,10000, 20000
Точность	±(1м+0.005% *расстояние+неточность индекса волокна)

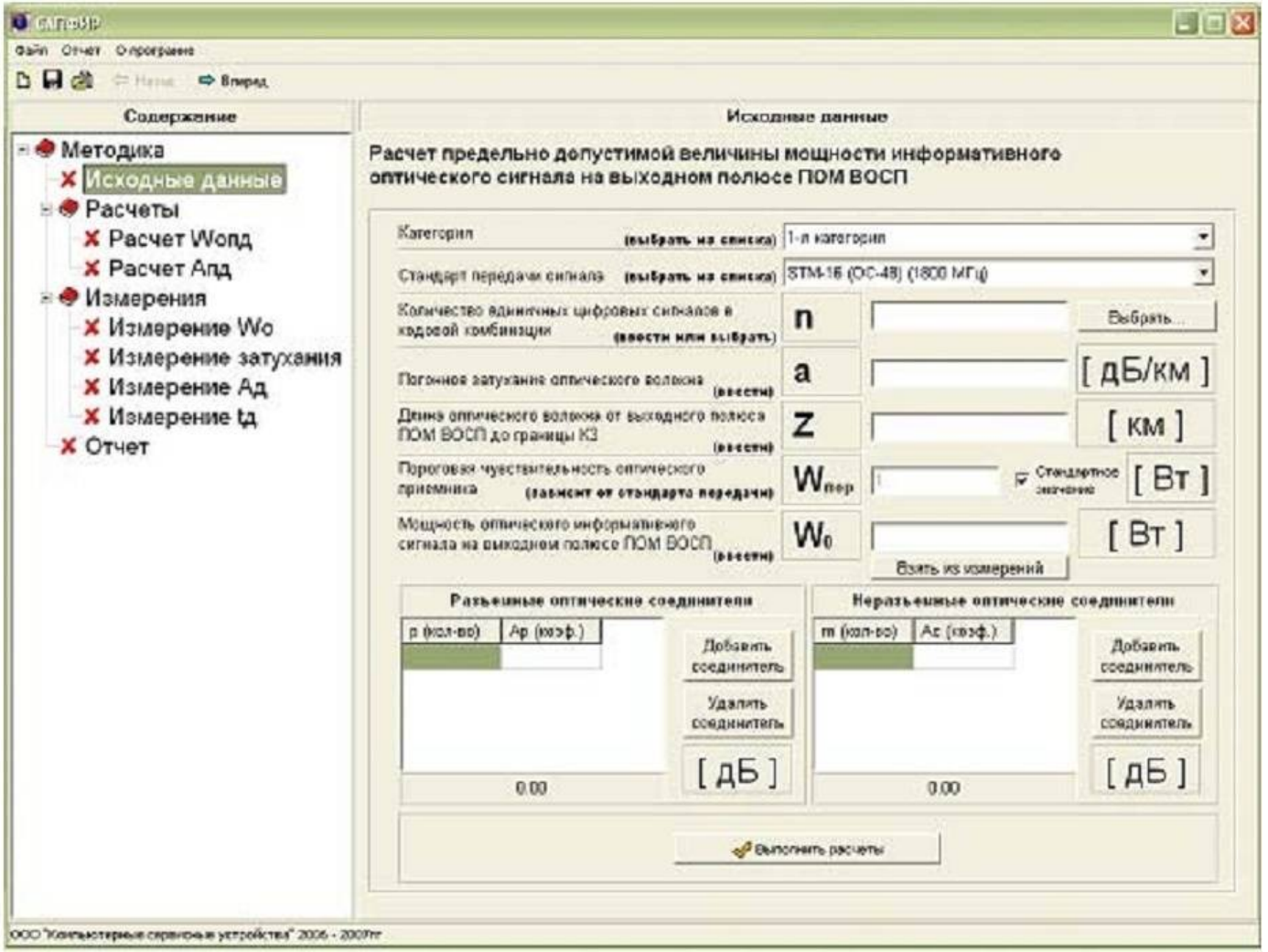
ОСОБЕННОСТИ

Микрорефлектометр; программируемый аттенюатор; адаптеры 6 шт.; оптические переключатели 2 шт.; портативный измеритель мощности; управляющая ПЭВМ типа ноутбук с сумкой для переноски; специальное программное обеспечение на CD-диске; кейс для переноски комплекса. Сертификат об утверждении типа средств измерений.

3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: ПАК «Сапфир»**

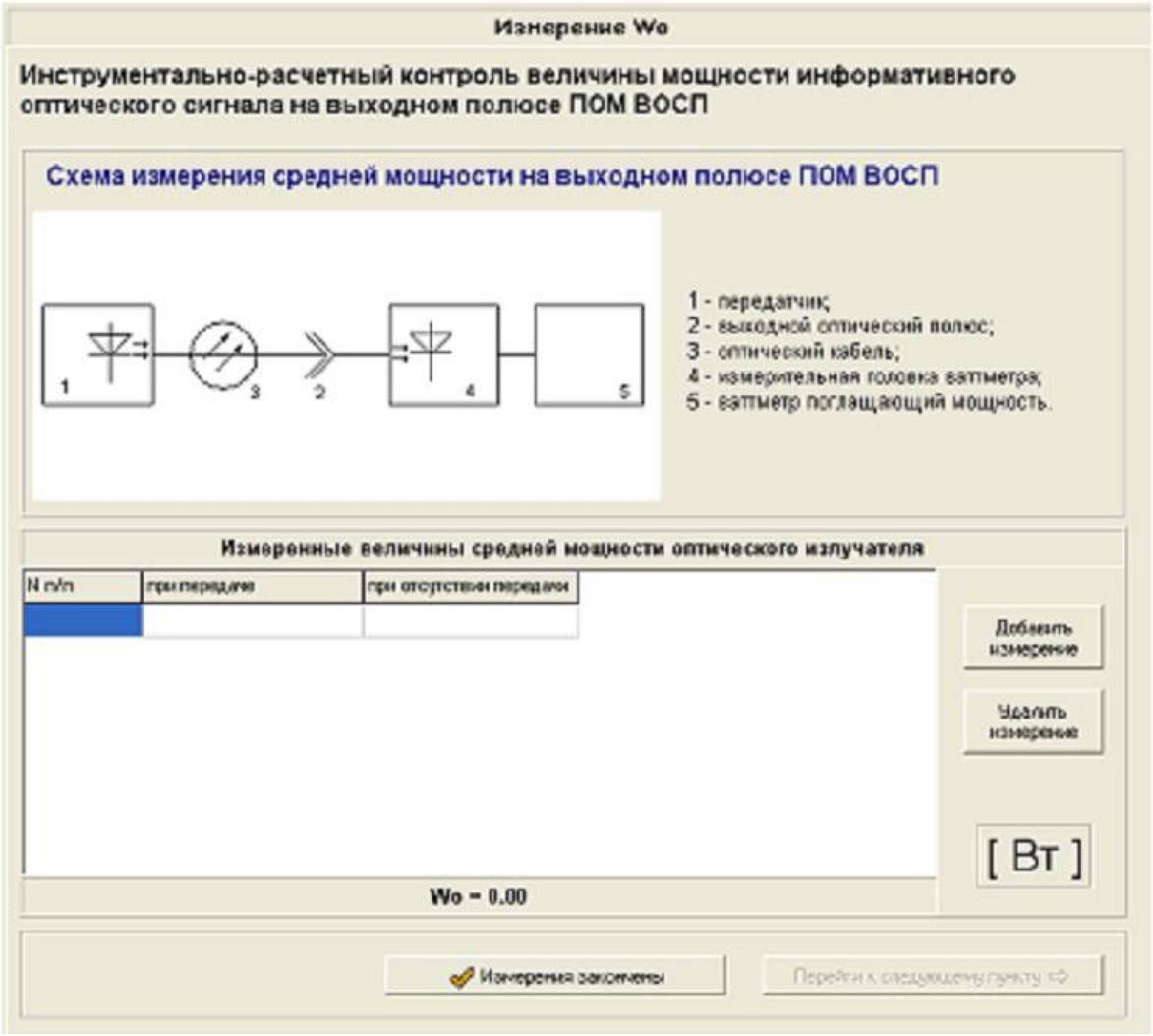
Главное окно



3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: ПАК «Сапфир»**

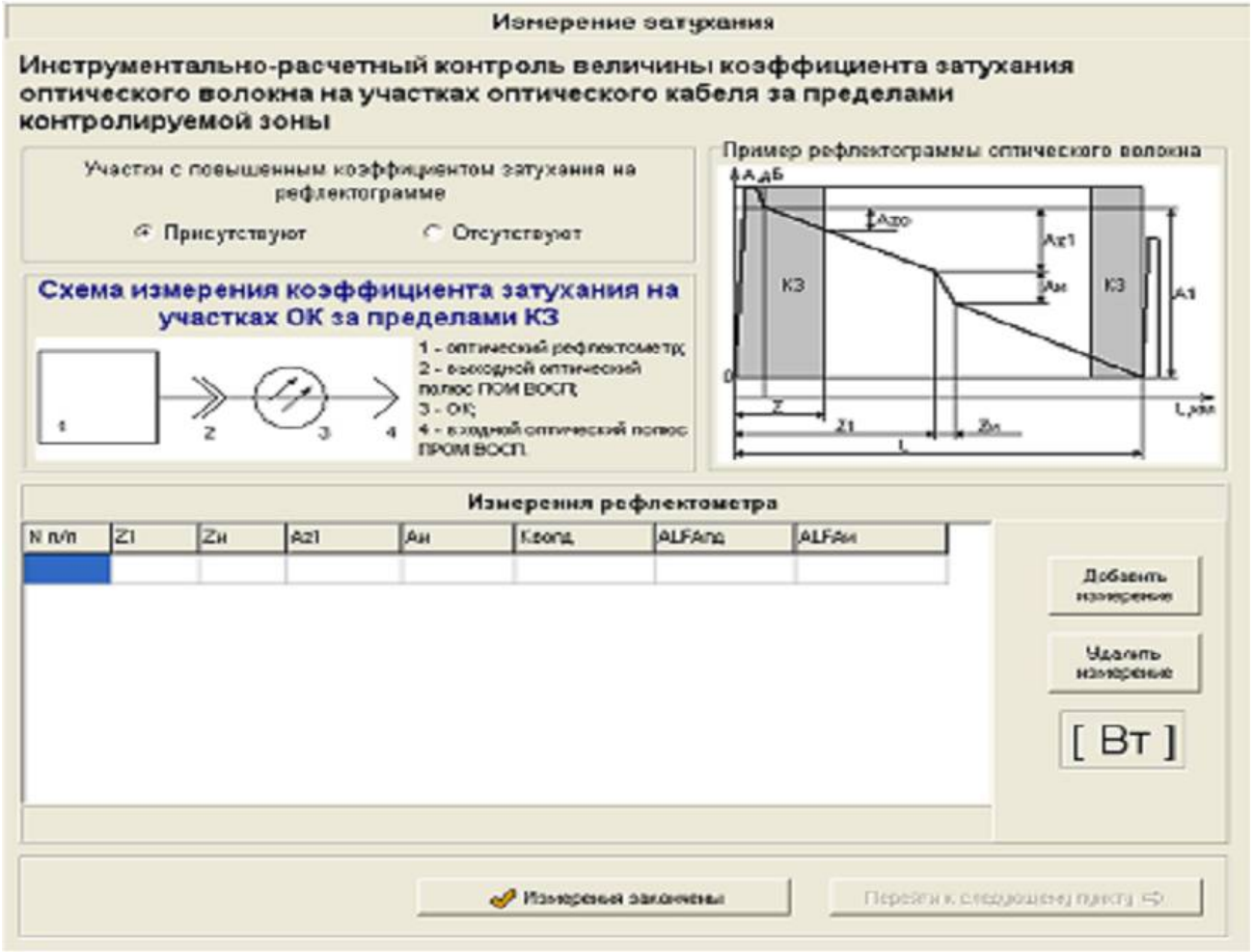
Измерение величины мощности оптического информативного сигнала на выходном полюсе передающего оптического модуля волоконно-оптической системы передачи



3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: ПАК «Сапфир»**

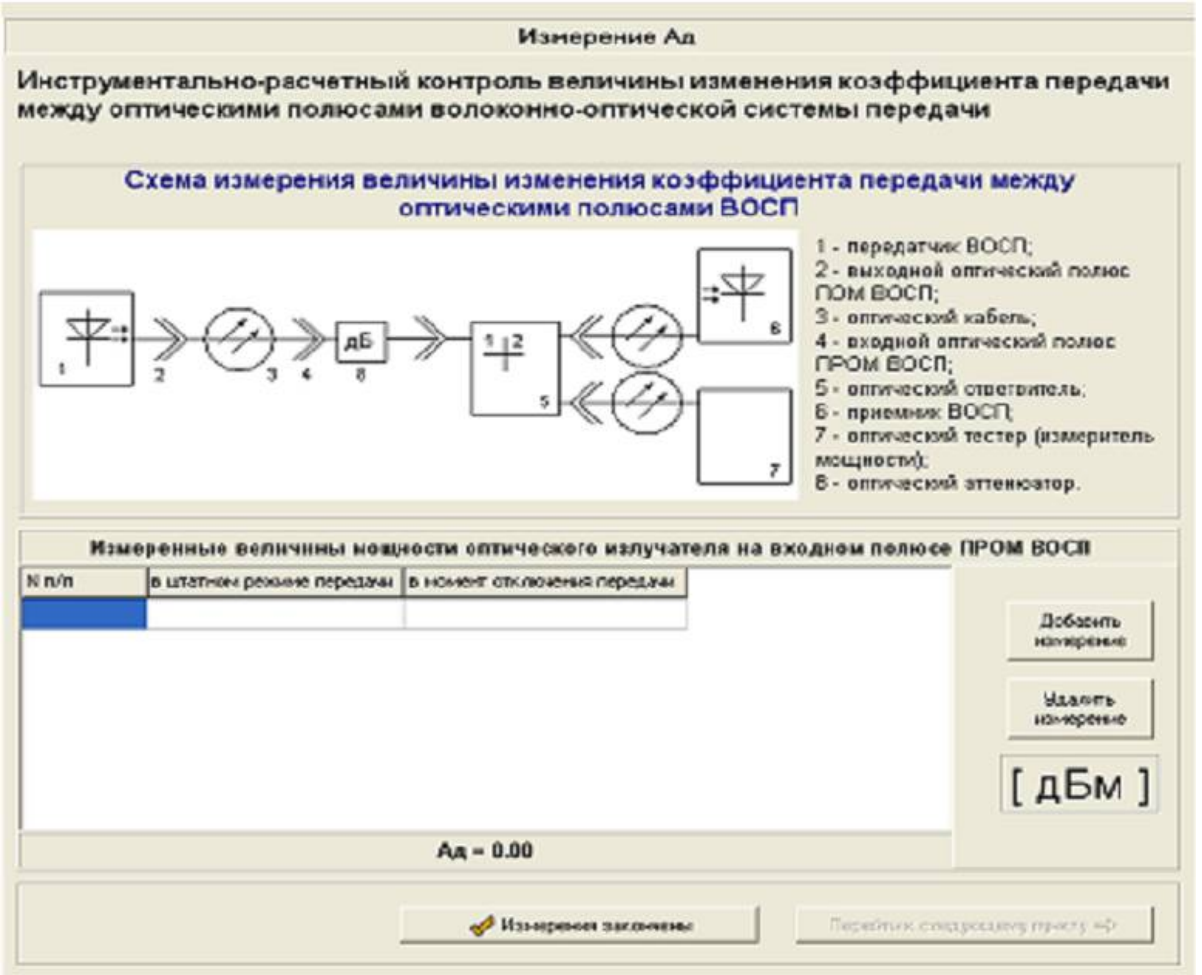
Измерение величины коэффициента затухания оптического волокна на участках оптического кабеля за пределами контролируемой зоны



3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: ПАК «Сапфир»**

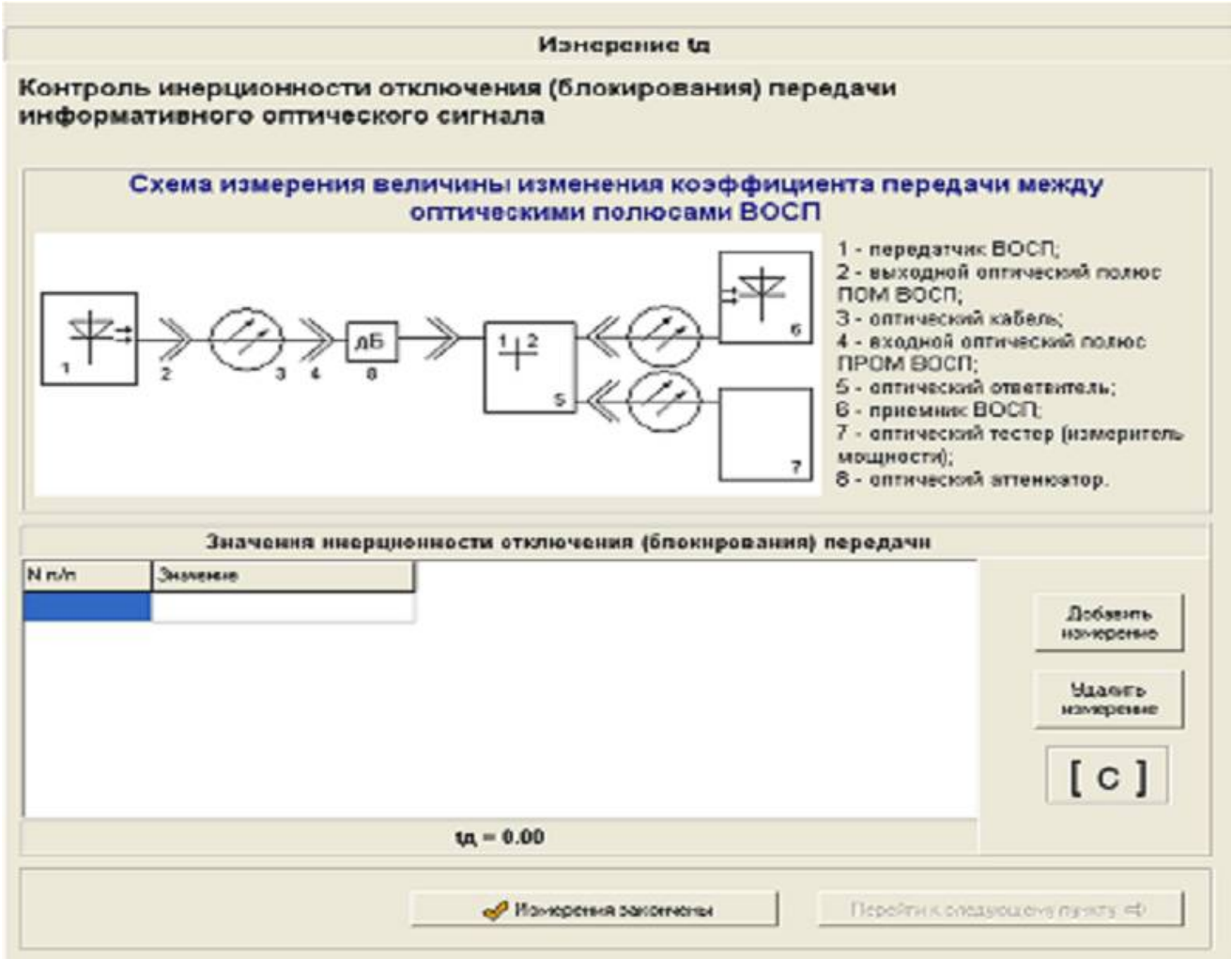
Измерение величины изменения коэффициента передачи между оптическими полюсами волоконно-оптической системы передачи



3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: ПАК «Сапфир»**

Измерение инерционности отключения (блокирования) передачи информативного оптического сигнала



3. Мониторинг состояния оптического тракта

○ Рефлектометрия оптических волокон

❖система мониторинга оптических волокон FIBERTEST
«Институт информационных технологий», Минск, Р. Беларусь, www.beliit.com

Функциональные характеристики системы FIBERTEST

- мониторинг резервных и рабочих волокон
- тестирование в автоматическом и ручном режимах
- удаленный и локальный доступ к серверу и RTU
- представление информации на электронной карте
- посылка отчетов по служебным каналам связи

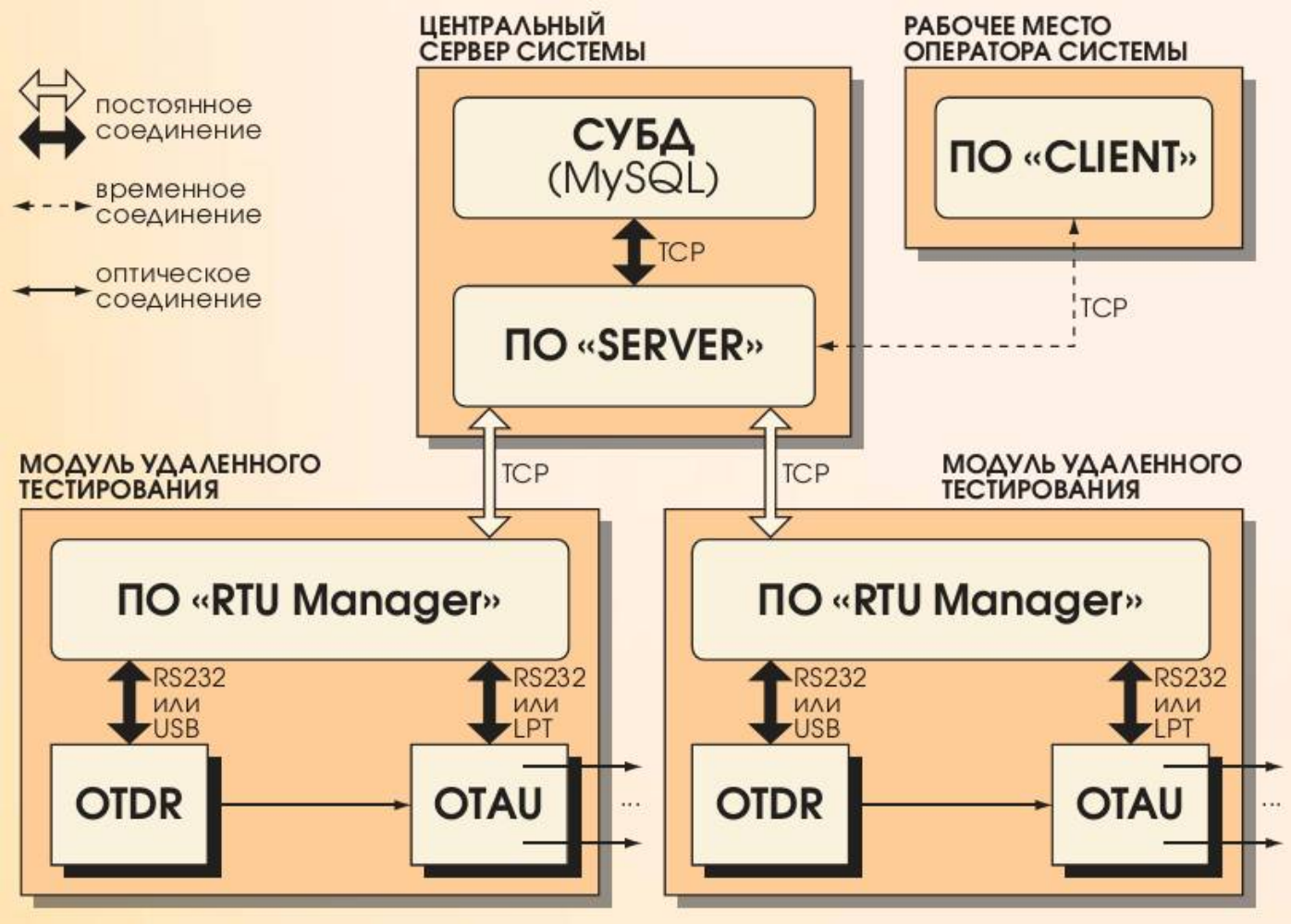
Состав системы FIBERTEST

- Аппаратная часть:
  - центральный сервер системы;
  - RTU
- Программная часть:
  - Data Center (включает СУБД);
  - RTU Manager;
  - Client (включает ГИС)

Система FIBERTEST значительно повышает безопасность сетей, любое несанкционированное подключение к волокну неизбежно приводит к дополнительным потерям в оптическом канале, а значит, будет обнаружено и зафиксировано системой в реальном масштабе времени.

3. Мониторинг состояния оптического тракта

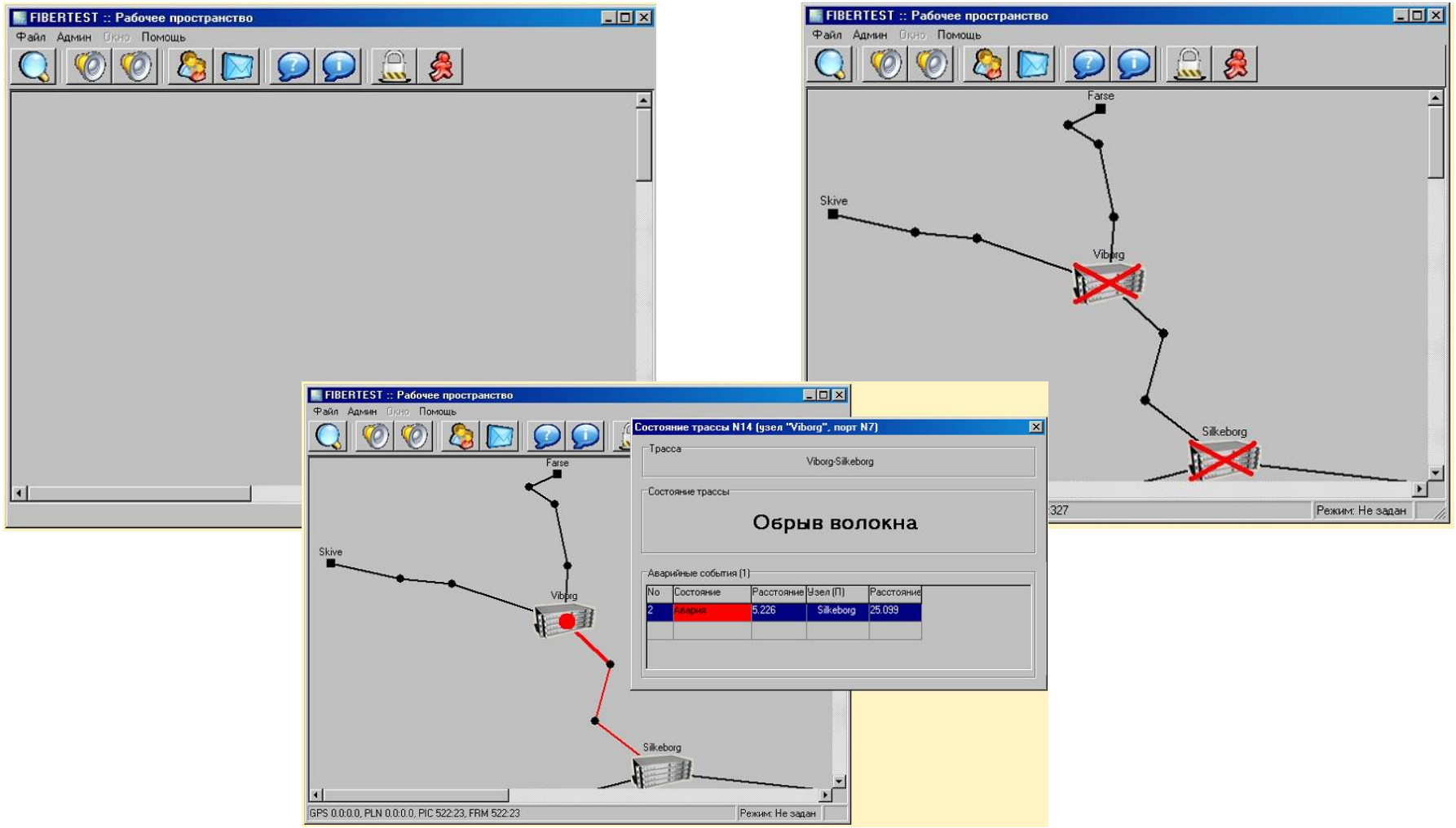
- **Рефлектометрия оптических волокон: FIBERTEST - АРХИТЕКТУРА**



OTDR
-оптический рефлектометр;
OTAU
-оптический коммутатор;
TCP
-используемый протокол передачи данных;
LPT, RS232, USB
-основные интерфейсы взаимодействия;

3. Мониторинг состояния оптического тракта

- **Рефлектометрия оптических волокон: FIBERTEST - ИНТЕРФЕЙС**



3. Мониторинг состояния оптического тракта

○ Рефлектометрия оптических волокон: FIBERTEST - ПРЕИМУЩЕСТВА

- возможность построения иерархической структуры системы
- возможность построения систем двух видов архитектур:
  - распределенная (в состав блоков дистанционного тестирования RTU входит PC)
  - арбитражная (в состав RTU входит контроллер)
- возможность организации служебной связи системы по ETHERNET и по SDH (G.703)
- возможность управления системой посредством удаленного клиента
- возможность присоединения к одному узлу системы нескольких клиентов в режиме обозревателя
- две группы критериев обнаружения повреждений:
  - отклонение любой точки измеренной рефлектограммы от контрольной на величину, превышающую порог
  - отклонение величины затухания в линии, в соединениях и коэффициента отражения от нормы
- прогнозирование возможных отказов

3. Мониторинг состояния оптического тракта

○ Рефлектометрия оптических волокон: FIBERTEST - ДОСТОИНСТВА

•повышение надежности ВОЛС за счет выявления предаварийного состояния и прогнозирования деградации ОВ

•усиление безопасности передачи данных за счет возможности обнаружения несанкционированного доступа к ВОЛС

•открытость архитектуры (универсальность, масштабируемость, документированность)

•технология “клиент-сервер”, позволяющая системе работать в режиме реального времени

•автономная работа удаленных модулей тестирования и их локальная настройка

•безопасность системы (доменная организация и санкционированный доступ к ресурсам системы)

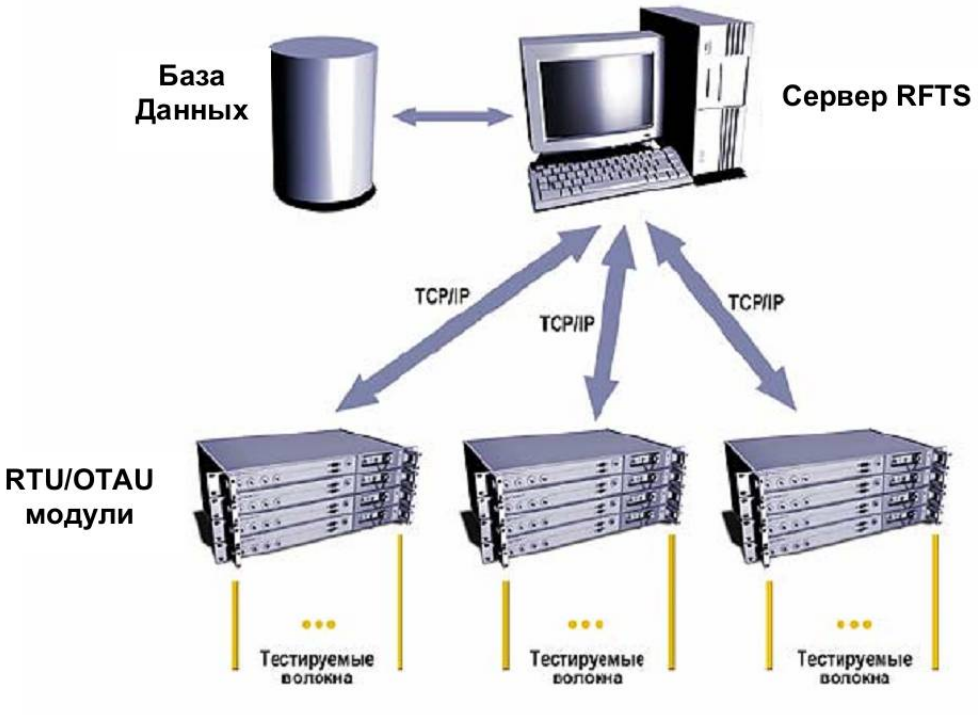
•улучшение динамики и качества развития сети передачи данных за счет облегчения управления ее ресурсами, планирования ее развития и проведения контрольных испытаний

•уменьшение затрат на эксплуатацию оптических линий за счет сокращения обслуживающего персонала и парка измерительного оборудования, автоматизации процессов контроля и диагностики ВОЛС, а также ведения статистики измерений параметров ОВ

3. Мониторинг состояния оптического тракта

○ Рефлектометрия оптических волокон: RTFS

❖архитектура системы RFTS



Система дистанционного тестирования волокон предназначена для непрерывного автоматического мониторинга состояния оптических волокон в ВОЛС и состоит из блоков дистанционного тестирования (**R**emote **T**est **U**nit , **RTU**), дистанционно управляемых оптических коммутаторов (**O**ptical **T**est **A**ccess **U**nit, **OTAU**) и сервера управления системой. **RTU** предназначены для удаленного тестирования оптических волокон рефлектометрическим методом и передачи полученной информации на сервер, где осуществляется управление системой и накапливаются данные о состоянии всех контролируемых оптических волокон, **OTAU** предназначены для тестирования различных ветвей сети и позволяют минимизировать количество **RTU** использующихся в системе, снижая таким образом стоимость решения, сервер осуществляет общее управление системой.

3. Мониторинг состояния оптического тракта

○ Рефлектометрия оптических волокон: RFTS

Принципы работы RFTS

оптический рефлектометр непрерывно снимает данные по затуханию в волокне и сравнивает их с эталонной рефлектограммой, и при обнаружении отклонений превышающих заданные пороговые значения, начинает передавать сигнал тревоги. Поскольку система позволяет не только выявить сам факт появления аномалии в волокне, но и определить ее на местности, это дает возможность оперативно реагировать на возникающие проблемы. Порядок, временные интервалы опроса и допустимые отклонения от эталонной рефлектограммы задаются в центральном офисе.

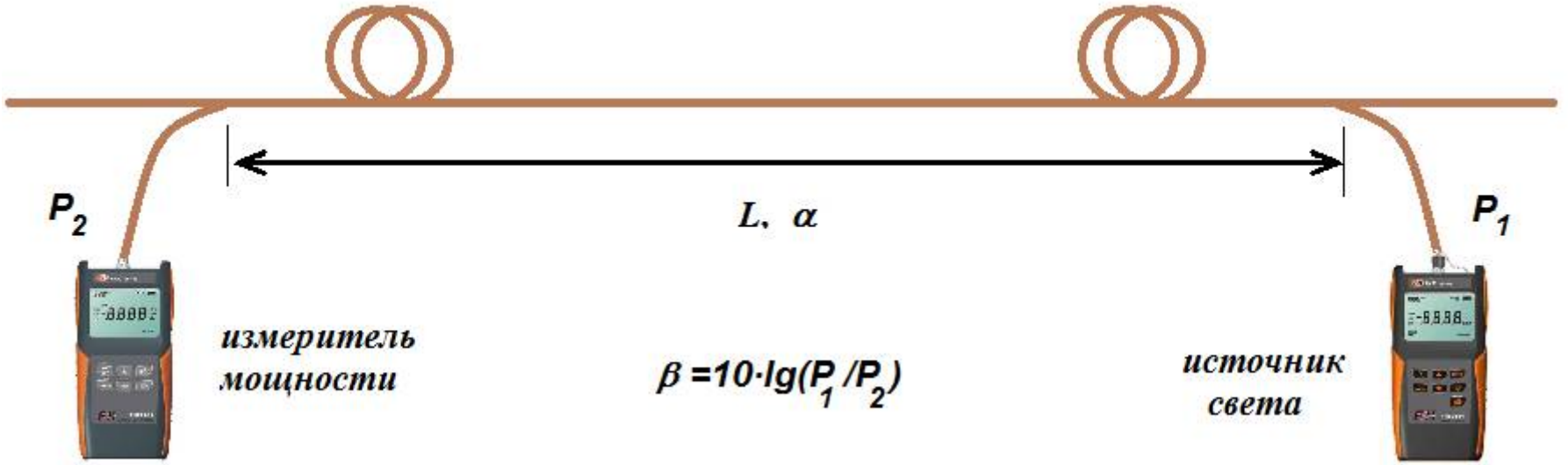
Возможности RFTS

Непрерывный контроль ВОСП - Сокращение времени поиска и устранения аварий - Своевременный профилактический ремонт - Меньший обслуживающий персонал - Анализ состояния и динамики развития системы

Обнаружение несанкционированного доступа – несанкционированное подключение происходит путем разделки оптического кабеля, получении доступа к волокну и последующего съема передаваемой по волокну информации через оптическую клипсу, так как подобное воздействие на волоконно-оптический кабель всегда приводит к приросту потерь, фиксируемых рефлектометром, мы получаем информацию об аномалии в передаче данных по волокну в реальном масштабе времени. Система позволяет не только выявить сам факт подключения, но и определить точку подключения, что дает возможность оперативно реагировать на такого рода действия. Будет подан сигнал тревоги, волокно немедленно отключено от сети, а данные о точке и времени подключения сохранены для дальнейшего анализа.

3. Мониторинг состояния оптического тракта

- **Контроль оптического бюджета в оптическом канале**



варианты

- ✓ проводится измерение потерь в канале связи в реальном времени
- ✓ выбирается мощность сигнала таковой, что при любом воздействии он перестает регистрироваться на уровне шумов канала связи

3. Мониторинг состояния оптического тракта

- **Контроль временных параметров прохождения сигнала**

❖Контроль прохождения сигнала (целостности линии)

регистрируется время прохождения сигнала по пути A → B → A

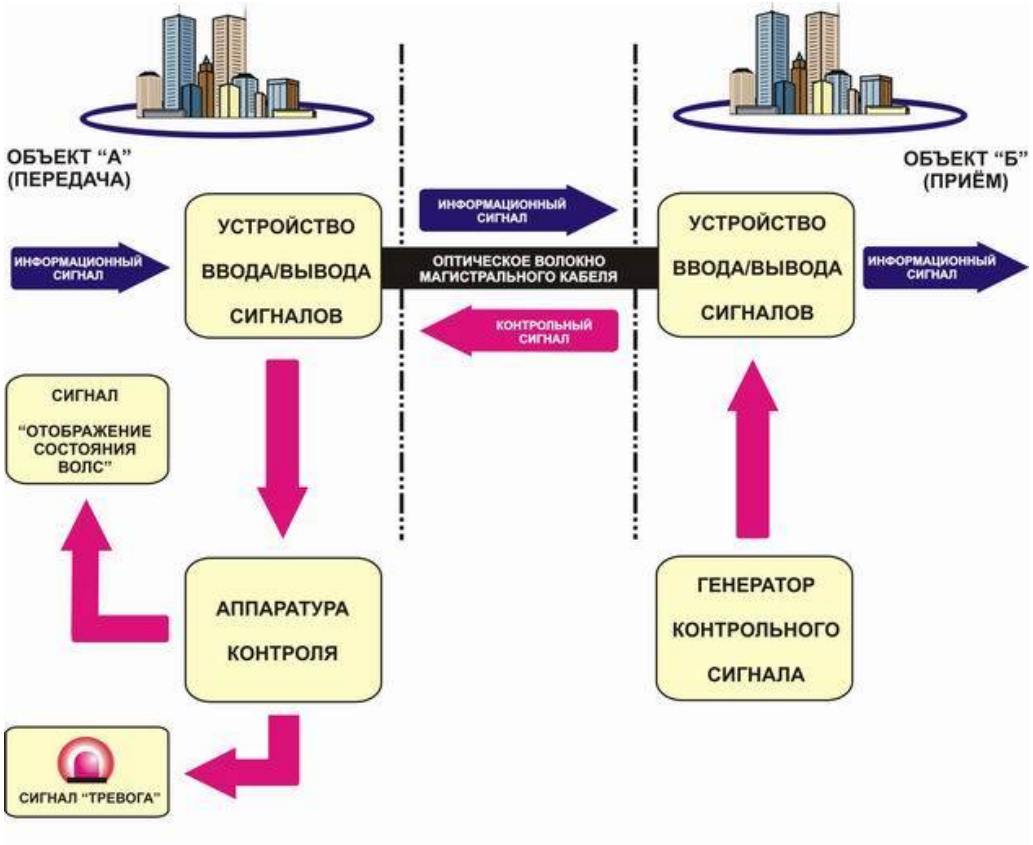
контролируется непрерывность прохождения оптического сигнала

контролируются изменения параметров оптического излучения (фаза, поляризация, частота)

3. Мониторинг состояния оптического тракта

- **Комплексный мониторинг оптических волокон**

СИСТЕМА МОНИТОРИНГА ВОЛС КБПМ (Москва) www.kbpm-ib.ru



Комплекс технических средств мониторинга ВОЛС предназначен для контроля целостности волоконно-оптических линий связи, сигнализации о несанкционированном доступе к ним.

Комплекс состоит из двух идентичных оптоэлектронных устройств, включаемых в разрез между входом/выходом оптических волокон и оконечным оборудованием дуплексной ВОЛС так, что информационные и контрольные оптические сигналы распространяются по оптическим волокнам навстречу друг другу.

Комплекс обеспечивает пассивную передачу по одномодовым оптическим волокнам оптического информационного сигнала и обнаруживает попытку несанкционированного доступа к передаваемой информации по изменению потерь в оптическом волокне с выводом сигнала «Блокировка (или «Переключение на резервный тракт»)» на передающую аппаратуру информационного тракта.

3. Мониторинг состояния оптического тракта

○ Комплексный мониторинг оптических волокон

комплекс технических средств контроля несанкционированного доступа к оптическим волокнам (КТС ОВ) *ООО «КБПМ - ИБ»* www.kbpm-ib.ru предназначен для обнаружения попыток несанкционированного подключения к контролируемым оптическим волокнам.

Наименование параметра	Значение
Длина волны информационного оптического сигнала, мкм	1,3
Длина волны контрольного оптического сигнала, мкм	1,55
Динамический диапазон контрольного сигнала, дБ	15
Разрешающая способность, дБ	0,04
Режим работы	круглосуточный

Диагностика оптических волокон осуществляется сравнением текущего и исходного значения потерь в оптическом волокне и сопоставлением найденных отклонений с заданным пороговым значением.

Контроль осуществляется в рабочих волокнах, передача информации и измерения производятся на разных длинах волн.

При изменениях величины потерь в информационном канале появляются предупредительные сигналы:

«Тревога» - при приближении уровня потерь к пороговому значению;

«Блокировка» - при превышении значений уровня установленного порога, при этом КТС ОВ обеспечивает переключение информационного сигнала на резервный канал.

КТС ОВ обеспечивает возможность установки уровня мощности передаваемого оптического информационного сигнала ниже уровня, при котором возможен перехват информации.

КТС ОВ состоит из двух идентичных оптоэлектронных приёмо-передающих устройств (ОУ).

ОУ включаются в разрыв оптических линий связи таким образом, чтобы информационный и контрольный оптические сигналы распространялись по ОВ навстречу друг другу.

3. Мониторинг состояния оптического тракта

- **Выводы**

1. Мониторинг состояния оптических волокон на предмет возможных изменений в сети действует только между активными элементами оптической сети, что ограничивает применение локальными сетями;

2. В некоторых случаях возможно использование методов мониторинга сети для телекоммуникаций, но с ростом протяженности их эффективность падает, так как растет неопределенность параметров сети;

3. Основные контролируемые параметры: непрерывность, потери, время прохождения сигнала, контроль состояния сети (число и тип неоднородностей, их расположение);

4. Программно-аппаратная защита трафика

○ Характеристика методов защиты трафика

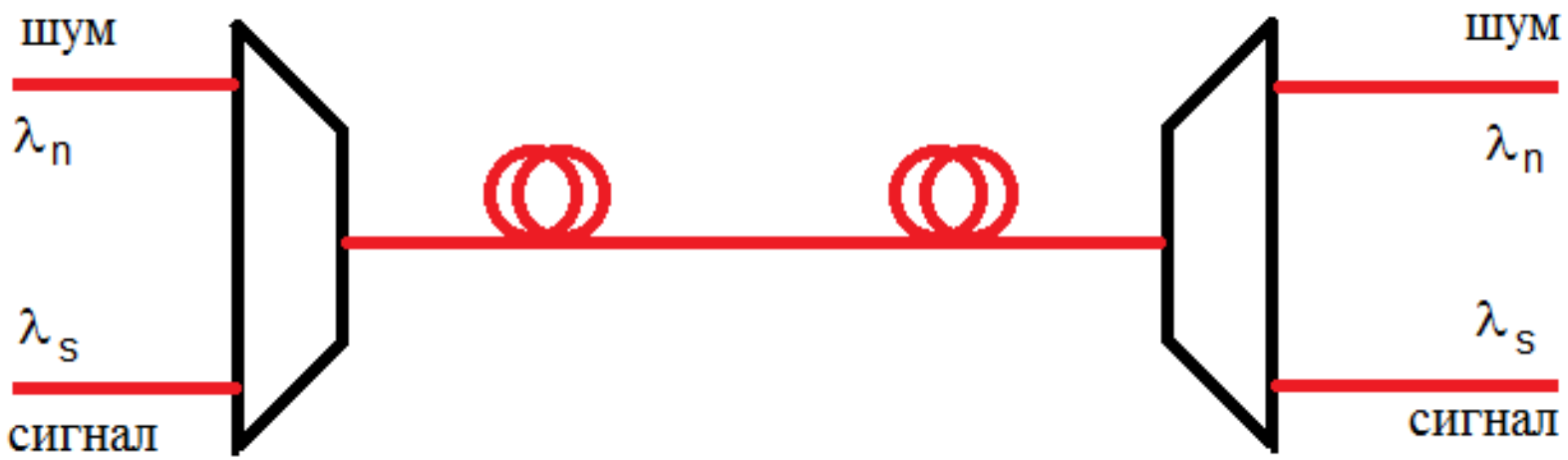
этап работы с информационным и информативным сигналами

❖ маскировка, сокрытие информационного сигнала от перехвата путем

1. Мультиплексирования сигнала и шума;
2. Распространение информационного сигнала по случайно выбранным каналам;
3. Искажение информационного сигнала в канале связи и последующее восстановление;
4. Сокрытие (стеганография) передачи информационного сигнала;

4. Программно-аппаратная защита трафика

- **Мультиплексирование сигнала и шума**

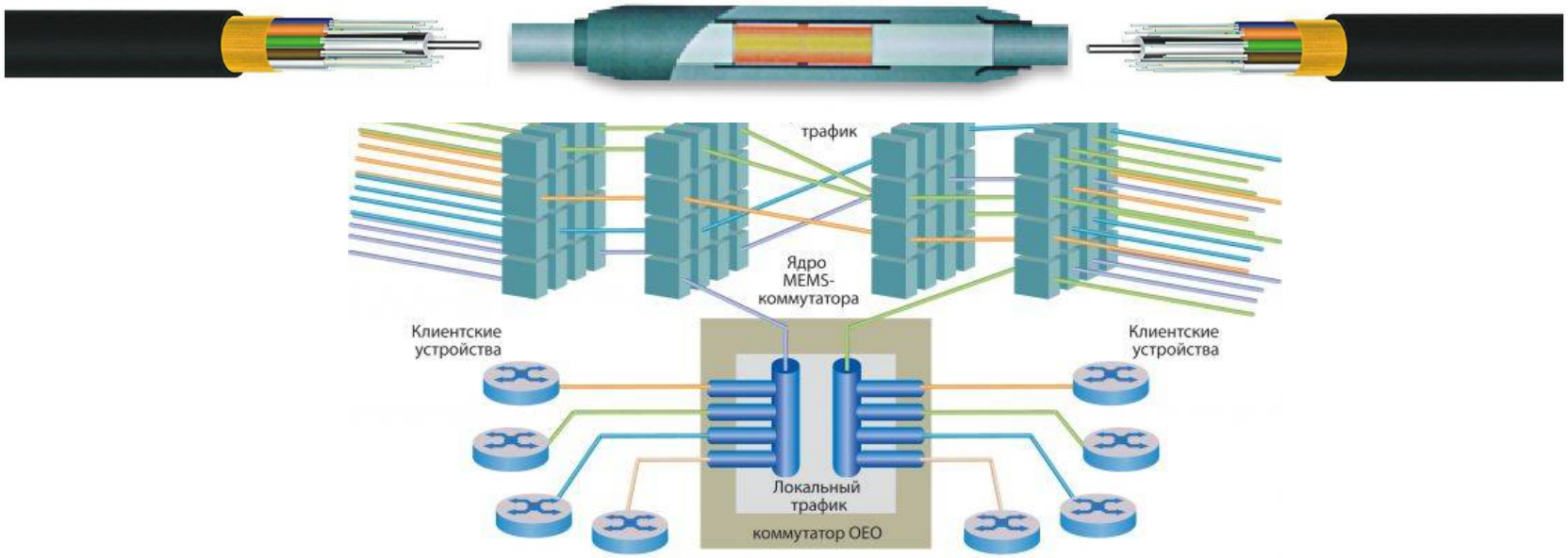


в оптический канал связи на входе, вместе с информативным сигналом на длине волны λ_s, вводится оптическое излучение на длинах волн λ_n отличных от длин волн информационного сигнала с помощью мультиплексора, а на выходе информативный сигнал отделяется от шума с помощью демультиплексора;

защита связана с неизвестностью длины волны носителя, которая может меняться при функционировании системы связи

4. Программно-аппаратная защита трафика

- **Метод случайной коммутации каналов**



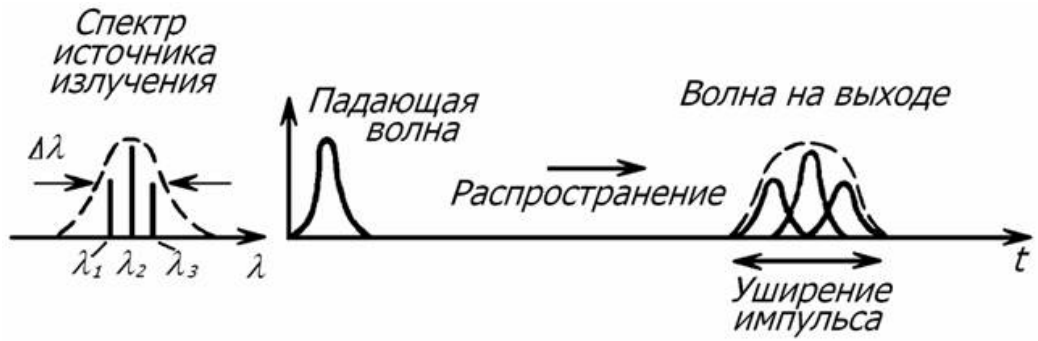
Коммутаторы на базе MEMS

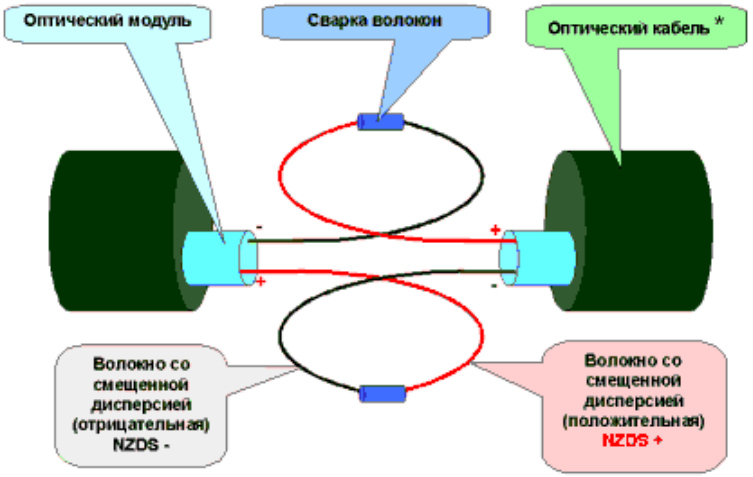
непрерывная коммутация трафика от одного волокна к другому, не влияя на передачу информации, требует от нарушителя одновременно перехватывать трафик следующий по всем каналам и волокнам оптической системы связи

4. Программно-аппаратная защита трафика

- **Искажение и восстановление информационного сигнала**

применение разно-знаковых компенсаторов дисперсии вызывает искажение формы сигналов до степени не различимости

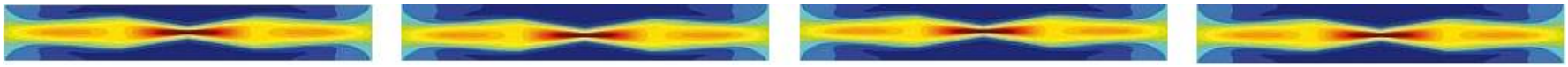




4. Программно-аппаратная защита трафика

- **Стенография – сокрытие факта передачи информационного сигнала**

- стеганографические методы защиты информации могут быть применены в оптических телекоммуникациях, в виде пространственного сокрытия (spatial cloaking), где контейнер несекретный файл с фотографией т.д.
- другой способ сокрытия в виде временного сокрытия (temporal cloaking) применимого только в волоконно-оптических системах связи



последовательность световых импульсов пропускают через материал с заранее известными и рассчитанными оптическими свойствами. Относительно друг друга эти импульсы сдвигаются так, что определенный кусок из всей последовательности в конечном результате исчезает. За счет этого появляется интервал, в который можно передать что угодно, и эта информация будет недоступна для стороннего наблюдателя, но, используя специальную оптическую приставку, через которую вновь пропускается последовательность импульсов (обратное преобразование), необходимую информацию можно будет извлечь из «временной дыры».
http://www.physics-online.ru/php/paper.phtml?jrnid=null&paperid=14751&option_lang=rus

Joseph M. Lukens, Daniel E. Leaird & Andrew M. Weiner A temporal cloak at telecommunication data rate // Nature, v. 498, pp. 205–208 (13 June 2013) doi:10.1038/nature12224

4. Программно-аппаратная защита трафика

- **Выводы**

1. Данные методы защиты применимы как в локальных линиях связи, так и телекоммуникациях;
2. Надежность защиты определяется сложностью и точностью реализации метода защиты;
3. В перспективе возможно создания простых и эффективных методов защиты трафика;

5. Адаптированные методы кодировки для защиты информации

- **Характеристика методов защиты информации в сетях связи**

этап работы с информационным и информативным сигналами

- защита трафика от перехвата путем использования специальных методов кодирования, которые затрудняют или делают невозможным перехват, таких как

1. Технология оптической связи множественного доступа с кодовым разделением;
2. Кодовое зашумление информационного сигнала (использование метода случайного кодирования);
3. Использование режима динамического хаоса для сокрытия сигнала;

5. Адаптированные методы кодировки для защиты информации

○ Технология связи O-CDMA

❖ Технология оптической связи множественного доступа с кодовым разделением (optical code division multiple access, O-CDMA) –

при которой каналы передачи имеют общую полосу частот, но разную кодовую модуляцию. В отличие от других методов доступа абонентов к сети, где энергия сигнала концентрируется на выбранных частотах (Frequency Division Multiple Access, FDMA) или временных интервалах (Time Division Multiple Access, TDMA), сигналы CDMA распределены в непрерывном частотно-временном пространстве. Фактически метод манипулирует и частотой, и временем, и энергией.

Преимущества

Высокая спектральная эффективность. Кодовое разделение позволяет обслуживать больше абонентов на той же полосе частот, чем другие виды разделения (TDMA, FDMA).

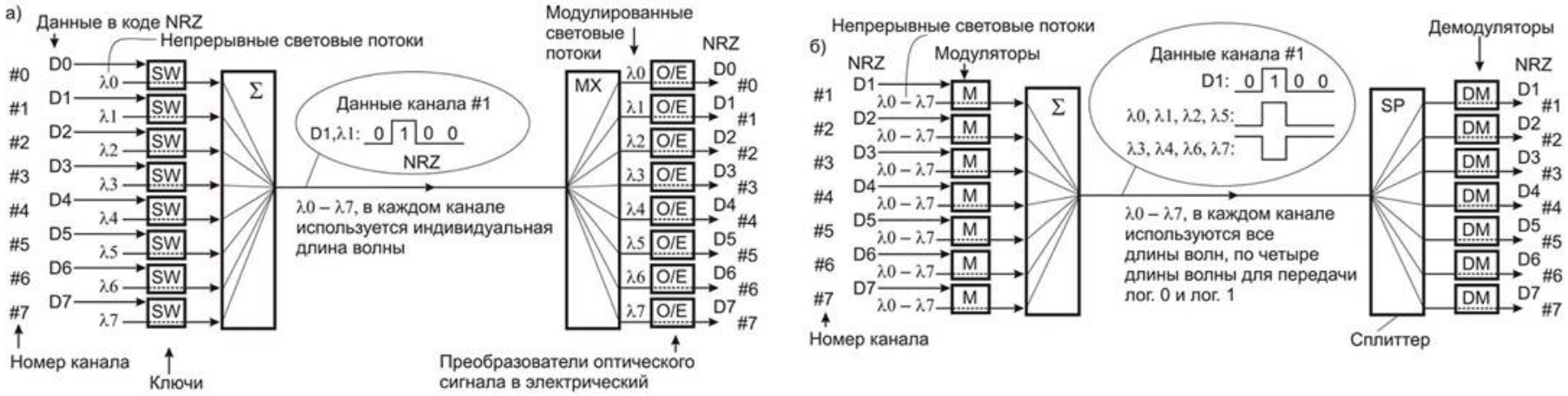
Гибкое распределение ресурсов. При кодовом разделении нет строгого ограничения на число каналов. С увеличением числа абонентов постепенно возрастает вероятность ошибок декодирования, что ведёт к снижению качества канала, но не к отказу обслуживания.

Более высокая защищённость каналов. Выделить нужный канал без знания его кода весьма трудно. Вся полоса частот равномерно заполнена шумоподобным сигналом.

Технология активно применяется в военной радиосвязи, в мобильных системах связи.

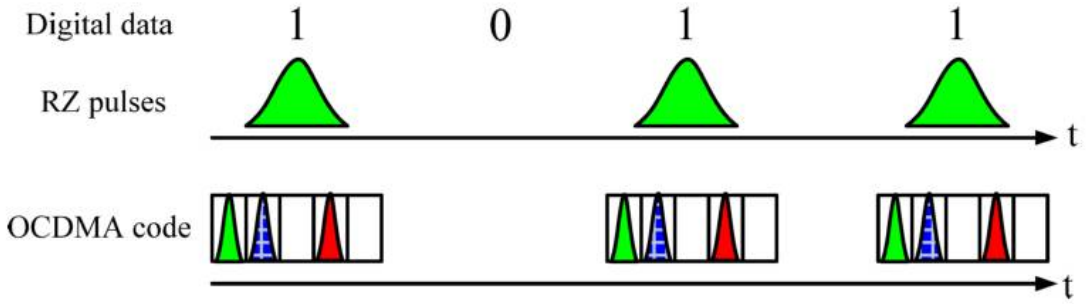
5. Адаптированные методы кодировки для защиты информации

- **Технология защиты трафика на основе O-CDMA**



а) — WDM б) — CDM

структурные схемы систем передачи данных с использованием технологий



Schematics of OOK modulation on RZ optical pulses and OCDMA codes to transmit a binary data stream.

5. Адаптированные методы кодировки для защиты информации

○ Защита трафика путем кодового зашумления

❖ Кодовое зашумление информационного сигнала (использование метода случайного кодирования)

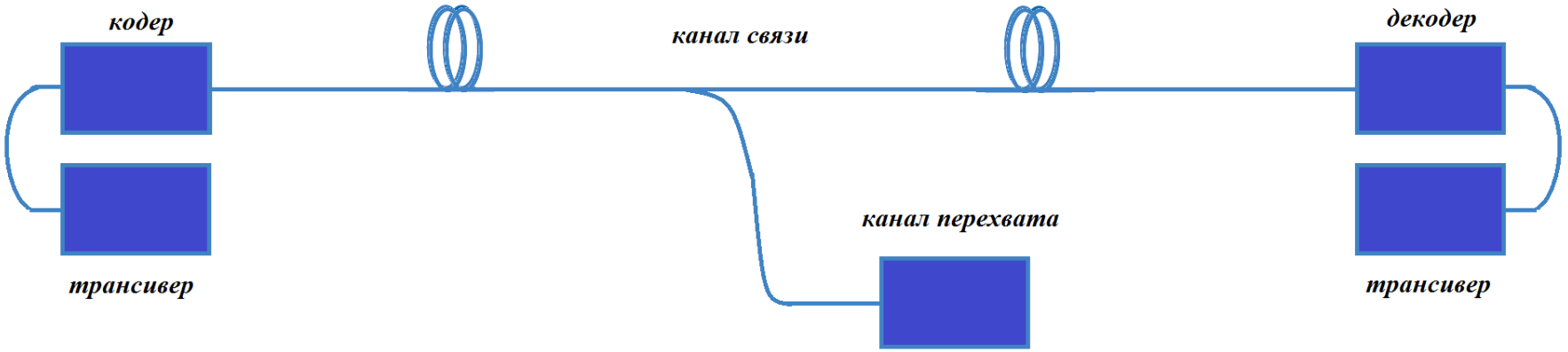
Один из алгоритмических методов, состоящий в применении специально подобранных преобразований передаваемой информации, которые гарантируют уменьшение вероятности правильного приема сообщений при оптимальном декодировании сигналов, получаемых из канала утечки информации.

Защита информации обеспечивается не за счет воздействия на параметры каналов утечки, а за счет вероятностного преобразования информации перед передачей по каналу связи. Невозможность восстановления информации злоумышленником основана на том свойстве, что канал утечки имеет меньшую пропускную способность, чем штатный канал пользователя. Способ кодирования выбирается так, чтобы в канале утечки количество возникающих ошибок сильно возрастало, обеспечивая эффект зашумления передаваемого сигнала, в то время как в основном канале обеспечивалась надежная связь.

5. Адаптированные методы кодировки для защиты информации

○ Защита трафика путем кодового зашумления

❖ Кодовое зашумление информационного сигнала (использование метода случайного кодирования)



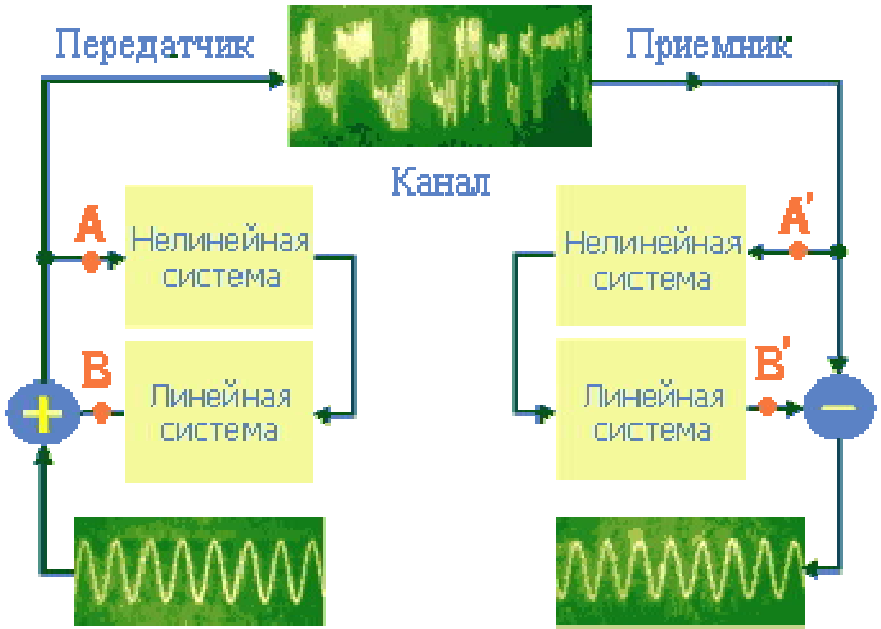
канал перехвата имеет пропускную способность меньшую, чем в линии связи $C_{leak} < C_{link}$, что позволяет использовать специальное кодирование, в котором малые ошибки ведут к невозможности декодирования информационного сигнала

5. Адаптированные методы кодировки для защиты информации

○ Защита трафика в режиме динамического хаоса

❖Режим динамического хаоса

Передатчик и приемник включают в себя такие же нелинейные и линейные системы, как источник. Дополнительно в передатчик включен сумматор, а в приемник - вычитатель. В сумматоре производится сложение хаотического сигнала источника и информационного сигнала, а вычитатель приемника предназначен для выделения информационного сигнала. Сигнал в канале хаосоподобный и не содержит видимых признаков передаваемой информации, что позволяет передавать конфиденциальную информацию. Сигналы в точках *A* и *A'*, *B* и *B'* попарно равны. Поэтому при наличии входного информационного сигнала *S* на входе сумматора передатчика такой же сигнал будет выделяться на выходе вычитателя приемника.



5. Адаптированные методы кодировки для защиты информации

- **Выводы**

---

1. Данные методы защиты являясь адаптированным развитием известным методов путем использования особенностей оптической сети позволяют создать эффективную систему защиты трафика как в локальных сетях, так и в телекоммуникациях;

2. Также, они являются и наиболее эффективным применением методов на новых принципах трудно реализуемых в других системах связи;

3. Наиболее эффективные методы защиты трафика могут строиться на специальных способах кодирования информации в оптических сигналах, например, на основе оптических вихрей (optical vortices) несущих ненулевой орбитальный момент;

○ Характеристика методов защиты информации сетях связи

этап работы с информационным сигналом

❖ защита передаваемой информации путем использования стандартных криптографических методов и перспективных методов защиты

1. Программно-аппаратные системы криптографической защиты информации, адаптированные к оптическим сетям связи;
2. Квантовая криптография, как абсолютный метод защиты передаваемой информации от перехвата;

○ Системы криптографической защиты информации в оптических сетях

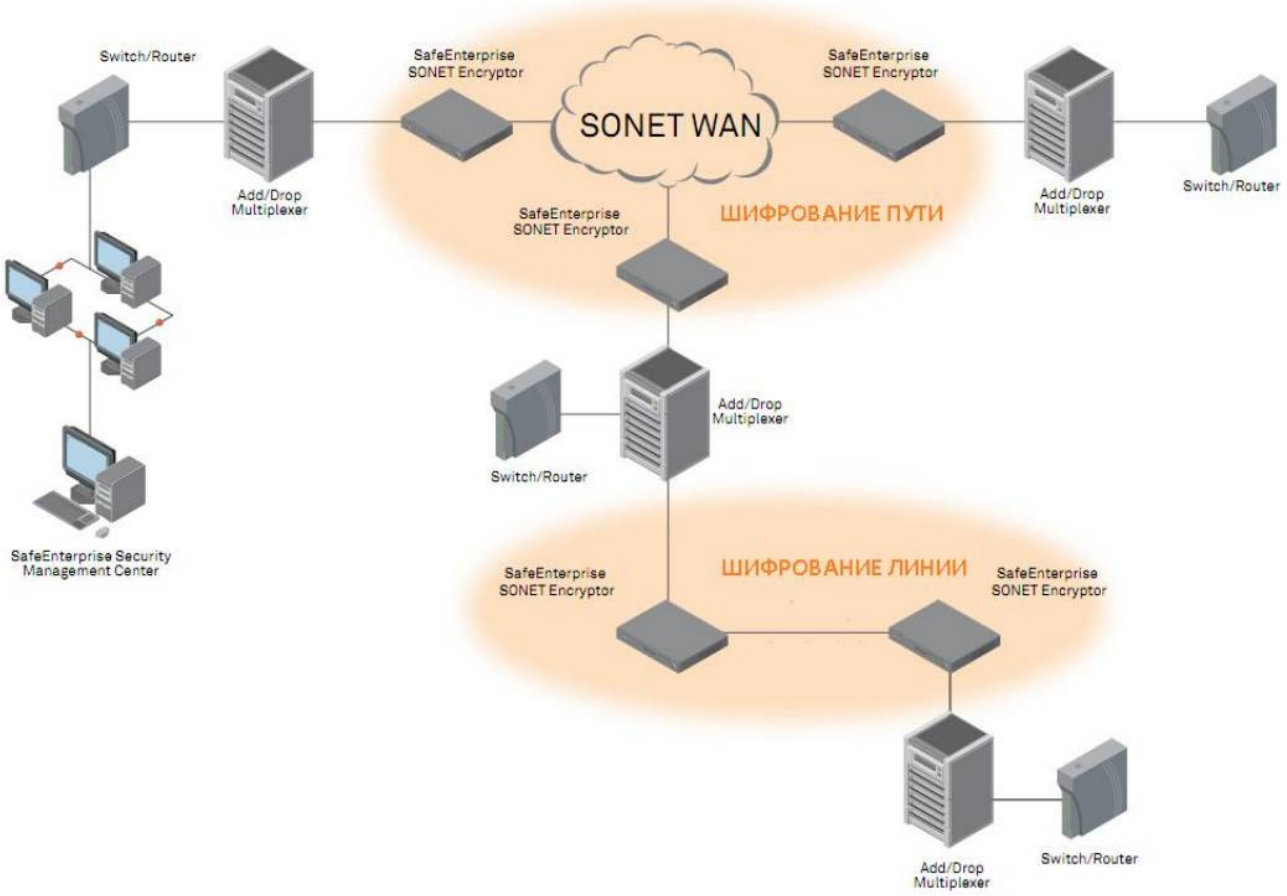
❖ SafeNet SONET Encryptor
адаптированная к оптическим сетям СКЗИ

Шифратор волоконно-оптических линий связи SafeNet SONET Encryptor является специализированным аппаратным решением для защиты коммуникаций по линиям связи стандартов SONET/SDH с пропускной способностью до 10 Гбит/с. Решение прозрачно для существующей сетевой инфраструктуры и легко в неё интегрируется, шифруя трафик алгоритмом AES-256 на номинальной скорости канала.

Предельно низкая задержка фреймов при шифровании делает шифраторы серии SafeNet SONET Encryptor идеальным решением для приложений, работающих в режиме реального времени и требующих моментальной передачи данных, например, при передаче голоса, видео, а также для обычного сетевого и Интернет-трафика.

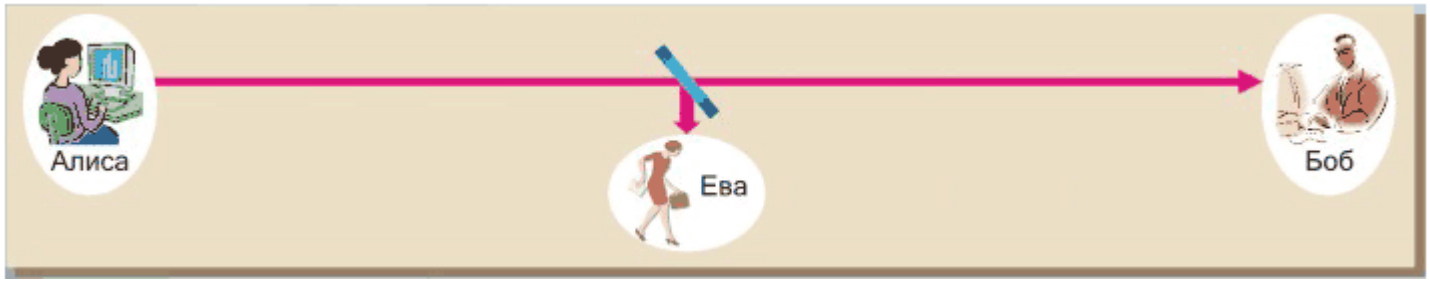
- **Системы криптографической защиты информации в оптических сетях**

- *SafeNet SONET Encryptor*



6. Классическая и квантовая криптография

○ Квантовая криптография



Передача информации от передатчика (Алиса) к приемнику (Боб) по оптической линии связи с абсолютной секретностью, перехват (Евой) невозможен.

Проблемы:

1. Классическая линия передачи с большим числом фотонов не защищена от перехвата.
2. Классическая криптография основана на отсутствии быстрого алгоритма факторизации больших чисел.

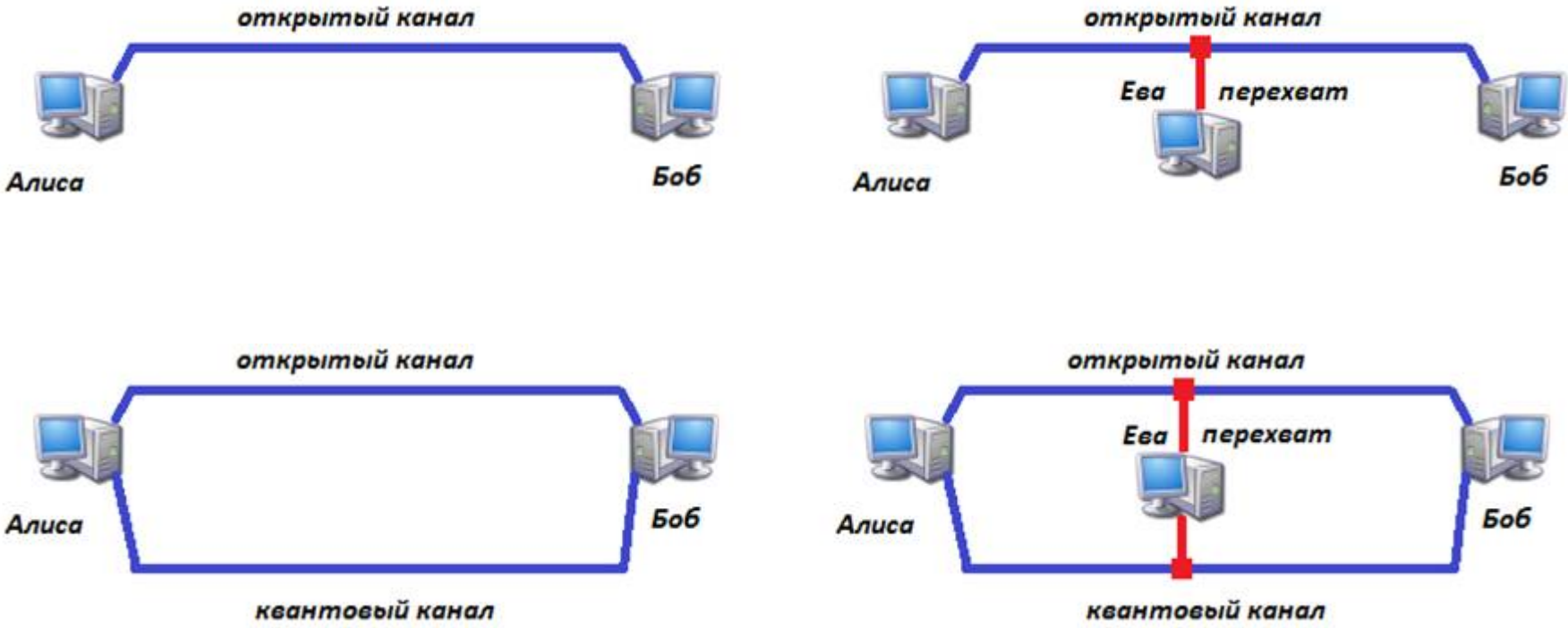
Метод: Носитель информации - одиночный поляризованный фотон.

Основание: Законы квантовой механики - всякое измерение изменяет квантовое состояние фотона. Перехват шпионом (Ева) связан с измерением и последующим воспроизведением (клонированием) состояния фотона.

Однако точное клонирование фотона невозможно!

- **Квантовая криптография**

Схема реализации перехвата трафика



- **Квантовая криптография**

ЗАДАЧА

современной квантовой криптографии сводится к безопасному (конфиденциальному) распределению криптографических ключей между двумя абонентами без предварительного обмена секретами. Несмотря на схожесть решаемых задач с задачами традиционных асимметричных протоколов распределения ключей, принципы квантовой криптографии в корне отличаются от основ традиционной.

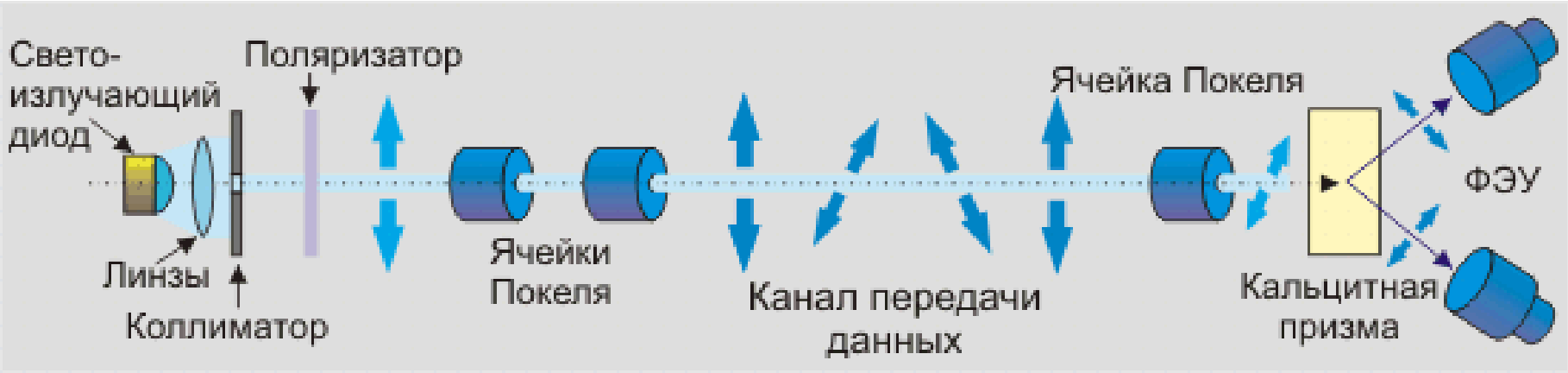
ПРИНЦИПЫ

квантовая криптография использует законы квантовой механики для гарантии безопасности распределения ключей. Это позволяет абонентам сгенерировать случайный ключ, известный только им. Он может быть использован в шифровании или аутентификации.

- **Квантовая криптография**

опирается на принципиальную неопределенность поведения квантовой системы - невозможно одновременно измерить взаимосвязанные параметры (принцип неопределенности Гейзенберга, 1927 г.), невозможно измерить один параметр фотона, не исказив другой, если пытаться что-то сделать с фотоном - измерить поляризацию (т. е. направление вращения) или длину волны (т. е. цвет), то его состояние изменится.

Практическая схема реализации квантовой криптографии



6. Классическая и квантовая криптография

○ Квантовая криптография

протокол BB84

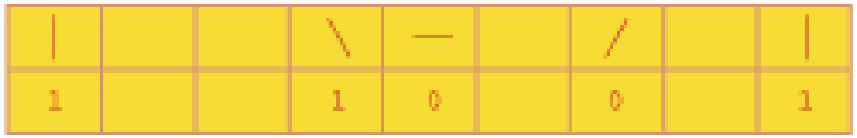
•Алиса посылает фотоны, имеющие одну из четырех возможных поляризаций, которую она выбирает случайным образом.

•Для каждого фотона Боб выбирает случайным образом тип измерения: он измеряет либо прямолинейную поляризацию (+) , либо диагональную (x).

•Боб записывает результаты изменения и сохраняет в тайне.

•Боб открыто объявляет, какого типа измерения он проводил, а Алиса сообщает ему, какие измерения были правильными.

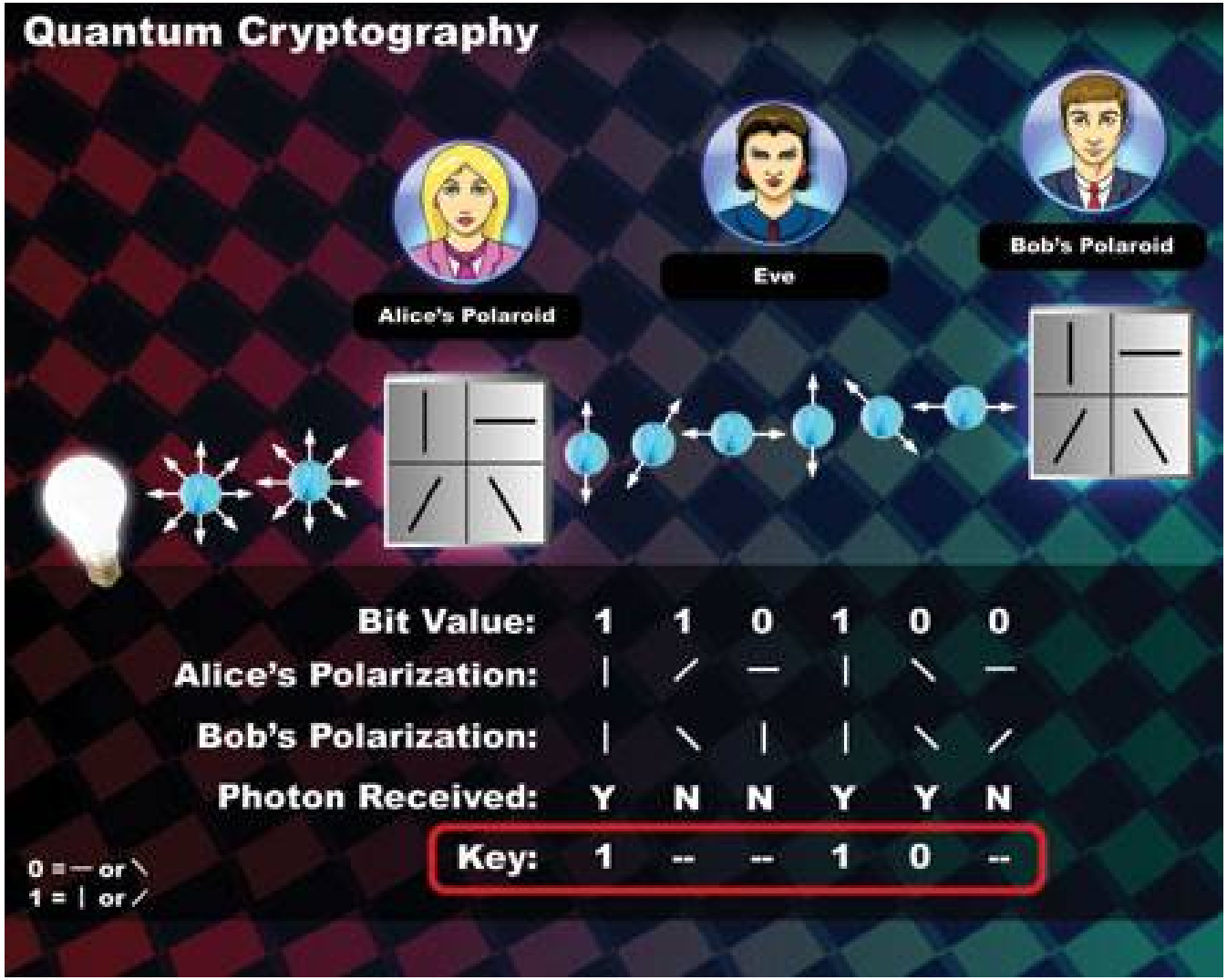
•Алиса и Боб сохраняют все данные, полученные в тех случаях, когда Боб применял правильное измерение. Эти данные затем переводятся в биты (0 и 1), последовательность которых и является результатом первичной квантовой передачи.



6. Классическая и квантовая криптография

- **Квантовая криптография**

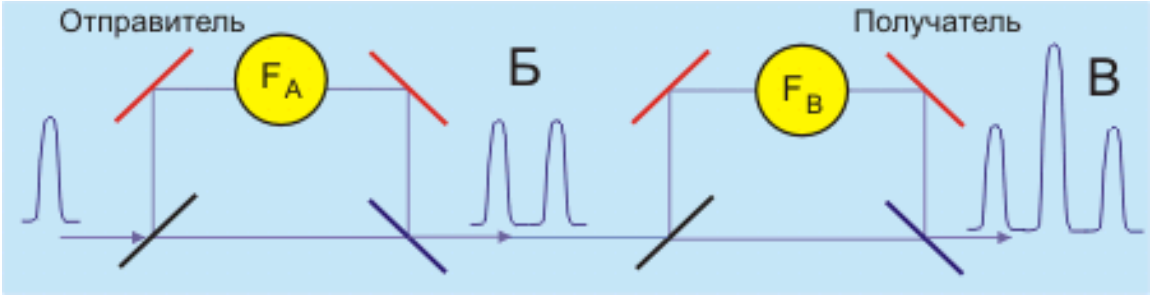
протокол BB84



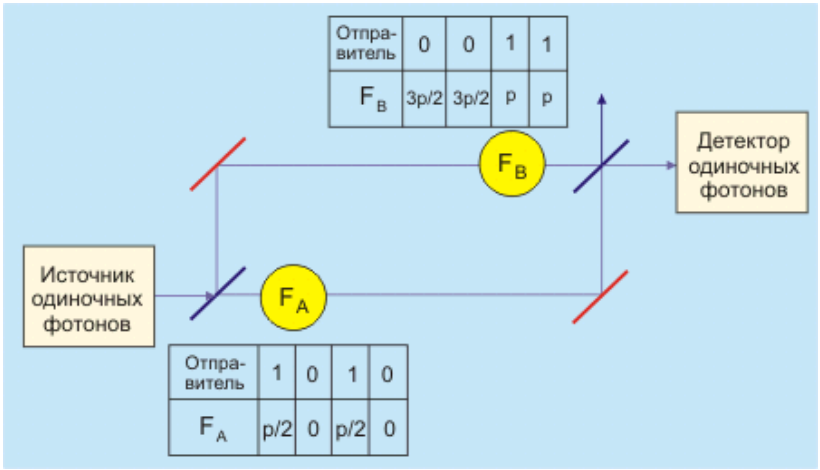
6. Классическая и квантовая криптография

○ Квантовая криптография

реализация алгоритма B92



•В алгоритме B92 приемник и передатчик создают систему, базирующуюся на интерферометрах Маха-Цендера. Отправитель определяет углы фазового сдвига, соответствующие логическому нулю и единице ($F_A=\pi/2$), а приемник задает свои фазовые сдвиги для логического нуля ($F_B=3\pi/2$) и единицы ($F_B=\pi$). В данном контексте изменение фазы 2π соответствует изменению длины пути на одну длину волны используемого излучения.



Интерферометр с одним транспортным волокном

- **Квантовая криптография**

❖*преимущества и недостатки:*

основным элементом системы передачи ключа по квантовому каналу является однофотонные передатчик и приемник, что формирует основные требования к параметрам оптической сети;

квантовый канал связи не должен содержать никаких активных элементов, что ограничивает максимальную длину (в настоящее время максимальная длина 200 км, скорость передачи кб/сек);

при передачи информации на большие расстояния требуется создание защищенных центров связи;

абсолютно защищенного протокола не разработано, существует вероятность незамеченного перехвата для основных протоколов.

7. Выводы

- **Защита трафика**

в настоящее время

– основные способы защиты от перехвата TCP связаны с мониторингом оптической сети методами рефлектометрии и др.;

– методы СКЗИ позволяют защитить трафик также как и в обычных линиях связи;

в ближайшее будущем

– существуют разработки, которые могут существенно повысить защищенность трафика от перехвата – квантовая криптография, OCDMA;

Темы для обсуждения по лекциям 7-8

«Методы защиты трафика»

Охрана периметра кабеля;
Мониторинг состояния оптического тракта;
Оптическая рефлектометрия в защите трафика;
Программно-аппаратная защита трафика;
Адаптированные методы кодировки для защиты информации при передаче по оптическим сетям: режим динамического хаоса, оптическая связь множественного доступа с кодовым разделением, особенности кодового зашумление сигнала;
Классическая и квантовая криптография.

http://www.analitika.info/

размещены дополнительные материалы по теме «ИБВОТ»