Учебный курс
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЙ»

Тема :
Волоконно-оптические (технические) каналы утечки информации

5 курс, осенний семестр

Состав:
26 акд. час – лекции; 20 акд. час – практика; отчетность - зачет

Лектор:
кфмн, доцент Гришачев Владимир Васильевич

Программа курса

Вводная лекция
«Проблема информационной защищенности волоконно-оптических технологий»

I. Перехват трафика в волоконно-оптических коммуникациях
   - 12 акд. час - лекции; 4 акд. час - коллоквиум

II. Сбор информации (НСИ) через штатные волоконно-оптические коммуникации
   - 12 акд. час - лекции; 4 акд. час - коллоквиум

III. Волоконно-оптические технические средства разведки
   - 8 акд. час - лекции; 2 акд. час – коллоквиум

Лекция 1-2

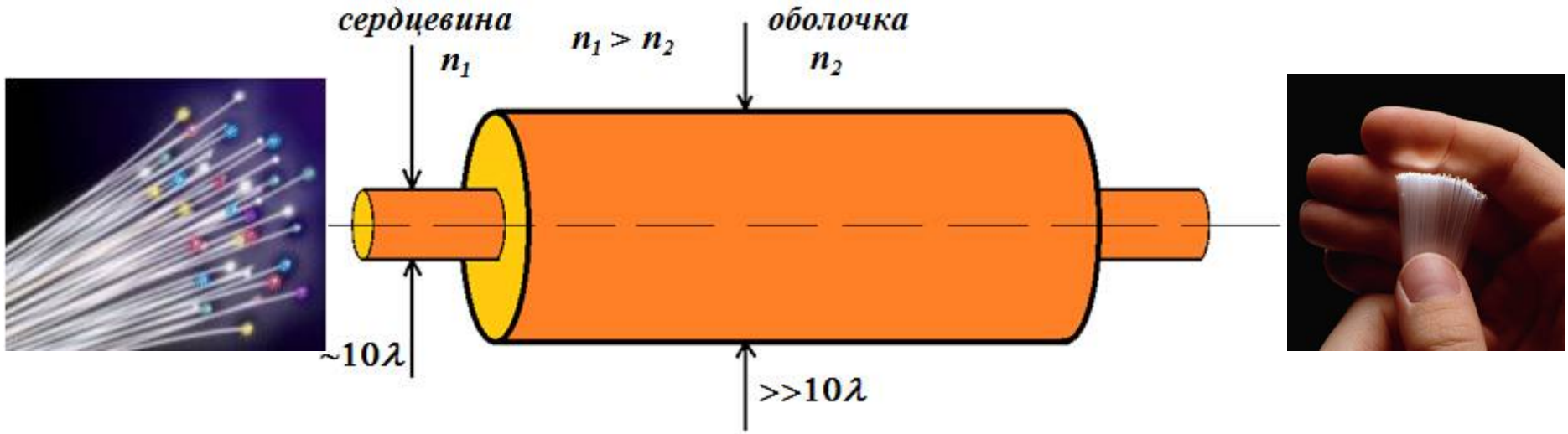
«Проблема информационной защищенности волоконно-оптических технологий»

1. Преимущества волоконно-оптических технологий в системах защиты информации;
2. Объект информатизации без ПЭМИНа, возможности замены электронных технологий на фотонные и волоконно-оптические технологии;
3. Основные понятия информационной безопасности;
4. Модель угроз безопасности информации на объекте информатизации и их характеристика;
5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации;
6. Понятие сценария утечки информации в структуре канала утечки информации;
7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации.

1. Преимущества волоконно-оптических технологий в системах защиты информации: понятие

- Волоконно-оптические технологии – применение совокупности методов, процессов и материалов волоконной оптики и техники на её основе для реализации передачи информации и энергии, для проведения измерения физических величин и для преобразования светового излучения.

- Основа волоконно-оптических технологий – оптоволокно, цилиндрическая диэлектрическая оптическая направляющая на основе полного внутреннего отражения.



1. Преимущества волоконно-оптических технологий в системах защиты информации: применение волоконной оптики

Связь

оптические телекоммуникации, локальные сети, кабельное телевидения, структурированные кабельные системы (СКС) и др.

Измерения

волоконно-оптические системы контроля температуры, деформаций, вибрационный контроль, электромагнитного поля и др.

Безопасность

волоконно-оптические системы охраны периметра, системы пожарной безопасности, системы контроля доступа, системы передачи в видеонаблюдении и др.

Интерфейсы

волоконно-оптические удлинители интерфейсов RS232, USB, DVI, HDMI, FireWire и др.

1. Преимущества волоконно-оптических технологий в системах защиты информации

- практически полное отсутствие ПЭМИН – нет влияния внешних электромагнитных излучений и нет собственных значительных излучений в не оптической области спектра;
- незначительные шумы оптического канала
  - мультипликативные шумы связаны с влиянием собственного излучения на свойства волокна или сетевого устройства,
  - аддитивные шумы имеют внешнее происхождение и не оказывают значительного влияния, так как оптическое излучение не проникает в кабель.
- обеспечивается высокая информационная емкость канала (для одной длины волны достигается 100 Гб/с) с малыми ошибками (появление ошибочного бита меньше 10E-10);
- малые потери (до 0.16 дБ/км на 1550 нм) обеспечивают большую дальность передачи информации без промежуточного регенеративного участка (более 500 км с скоростью 800 Гб/с , с одним оптическим усилителем при удаленной накачке по волокну, http://t8.ru/);
- размеры оптического канала малы и не превышают размеров самого волокна (менее 1 мм в диаметре);
- оптический кабель может быть выполнен только из диэлектрических материалов, поэтому трудно обнаруживаем, пожаро- и электро- безопасен, долговечен (25 лет гарантии);
- межволоконные наводки незначительны, что позволяет плотно упаковывать волокна (∅ 0,9 мм) в кабеле диаметром несколько мм;

1. Преимущества волоконно-оптических технологий в системах защиты информации: высокая пропускная способность

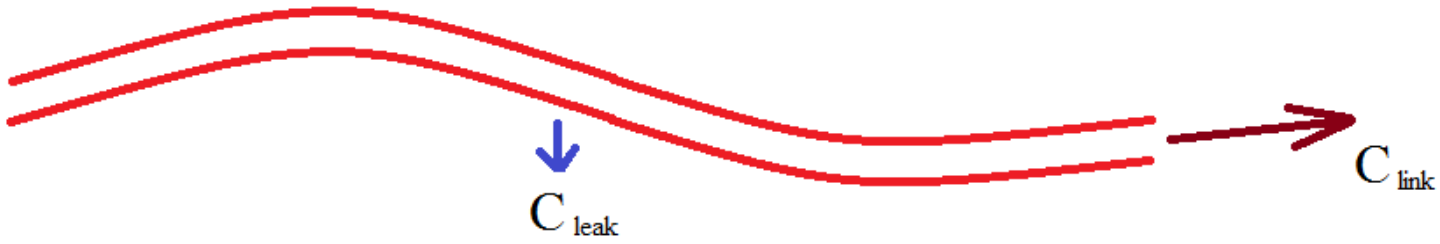
- Высокая скорость передачи информации в волоконно-оптическом канале связана с низкими потерями и шумами, отсутствием паразитных электромагнитных модуляций и наводок, возможностью волнового уплотнения каналов, что накладывает сильные ограничения на канал утечки информации при перехвате

требование для пропускной способности канала утечки формируемого нарушителем

$$C_{leak} \geq C_{link}$$

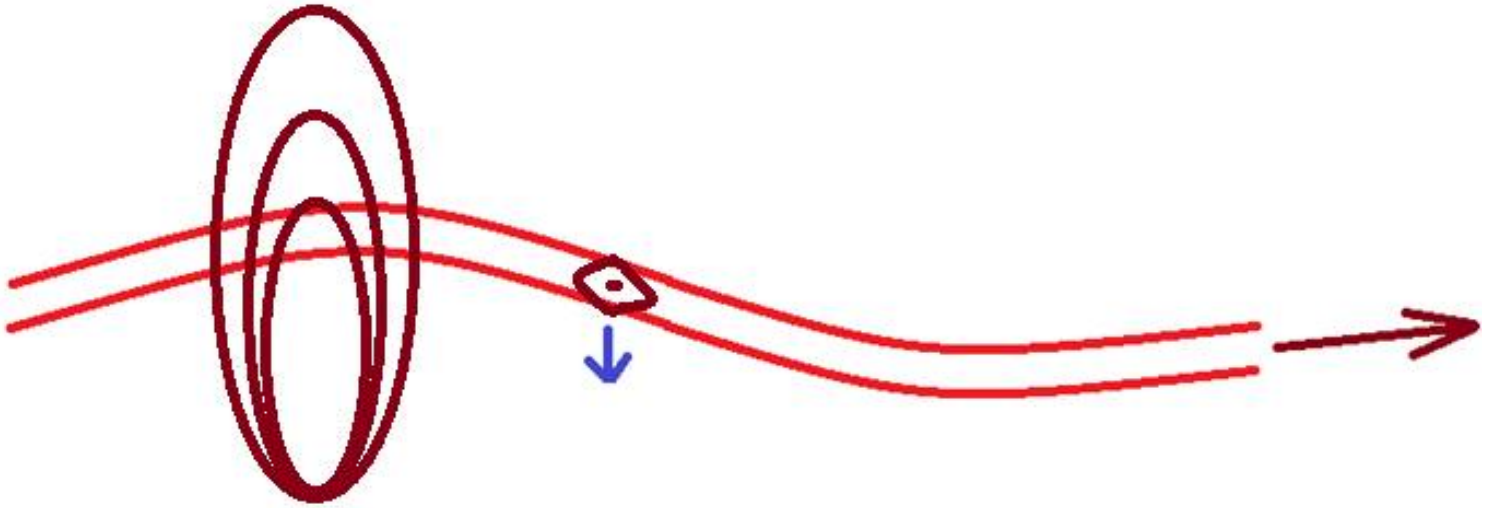
фактически реализуемое соотношение вследствие названных технических характеристик волоконно-оптического канала

$$C_{leak} << C_{link}$$



1. Преимущества волоконно-оптических технологий в системах защиты информации: низкие потери и шумы

- Низкие потери и шумы, отсутствие значительных побочных электромагнитных излучений и наводок (ПЭМИН), что позволяет эффективно обнаруживать изменения, вызванные появлением технического канала утечки информации.



1. Преимущества волоконно-оптических технологий в системах защиты информации: скрытность канала

- Волоконно-оптическое волокно и кабель
  - обладают малыми размерами и имеют незначительные межволоконные наводки, что позволяет создавать кабель малых поперечных размеров с высокой упаковкой волокон (например, кабель для внутреннего монтажа Hyperline FO-D-IN-XX-YY-FRPVC, XX=тип, YY=число волокон имеет 2-24 волокон в кабеле диаметром 5 мм);
  - обладает высокой скрытность от обнаружения техническими средствами, так как существует кабель выполненный полностью из диэлектрических материалов

1. Преимущества волоконно-оптических технологий в системах защиты информации: выводы

- фотонные технологии, включая волоконно-оптические технологии, позволяют удовлетворить все основные технические потребности объекта информатизации, такие как связь, измерения и безопасность, на более высоком уровне, чем радиоэлектронные технологии;

- оптическое волокно и кабель замещают электрический провод и кабель и создают новую техническую среду вокруг человека;

- новая техническая среда с одной стороны повышает информационную защищенность объекта, а с другой создает новые угрозы информационной безопасности;

2. Объект информатизации без ПЭМИНа: проблема ПЭМИН

- Побочные ЭлектроМагнитные Излучения и Наводки (ПЭМИН) радио и СВЧ диапазона сопровождают работу любой электронной аппаратуры объекта информатизации и являются основным каналом утечки информации:
  - электромагнитные волны радио и СВЧ диапазона имеют высокую проникающую способность и выходят за пределы помещений;
  - электрический кабель является излучателем электромагнитных волн с резонансными свойствами, что повышает опасность ПЭМИН;
  - экранировка ЭМИ в любой электронной аппаратуре всегда связана с непрерывным контролем за её состоянием и эффективностью;

Мощность электромагнитного излучения бытовых приборов (сравнение):

Устройство	Плотность потока энергии
Вытяжка	5 мВт/м2 – 400 мВт/м2
Электроплита	5 мВт/м2 – 100 мВт/м2
Холодильник	9 мВт/м2 – 20 мВт/м2
Электрочайник	1 мВт/м2 – 100 мВт/м2
Телевизор	18 мВт/м2 – 90 мВ/м2
Ноутбук	2 мВт/м2 – 16 мВт/м2
Мобильный телефон (GSM)	40 мВт/м2 – 800 мВт/м2
Мобильный телефон (CDMA)	35 мВт/м2 – 150 мВт/м2

2. Объект информатизации без ПЭМИНа: возможности фотонных технологий

Современные фотонные технологии позволяют свести ПЭМИН оборудования объекта информатизации до уровня фона

достигается путем:

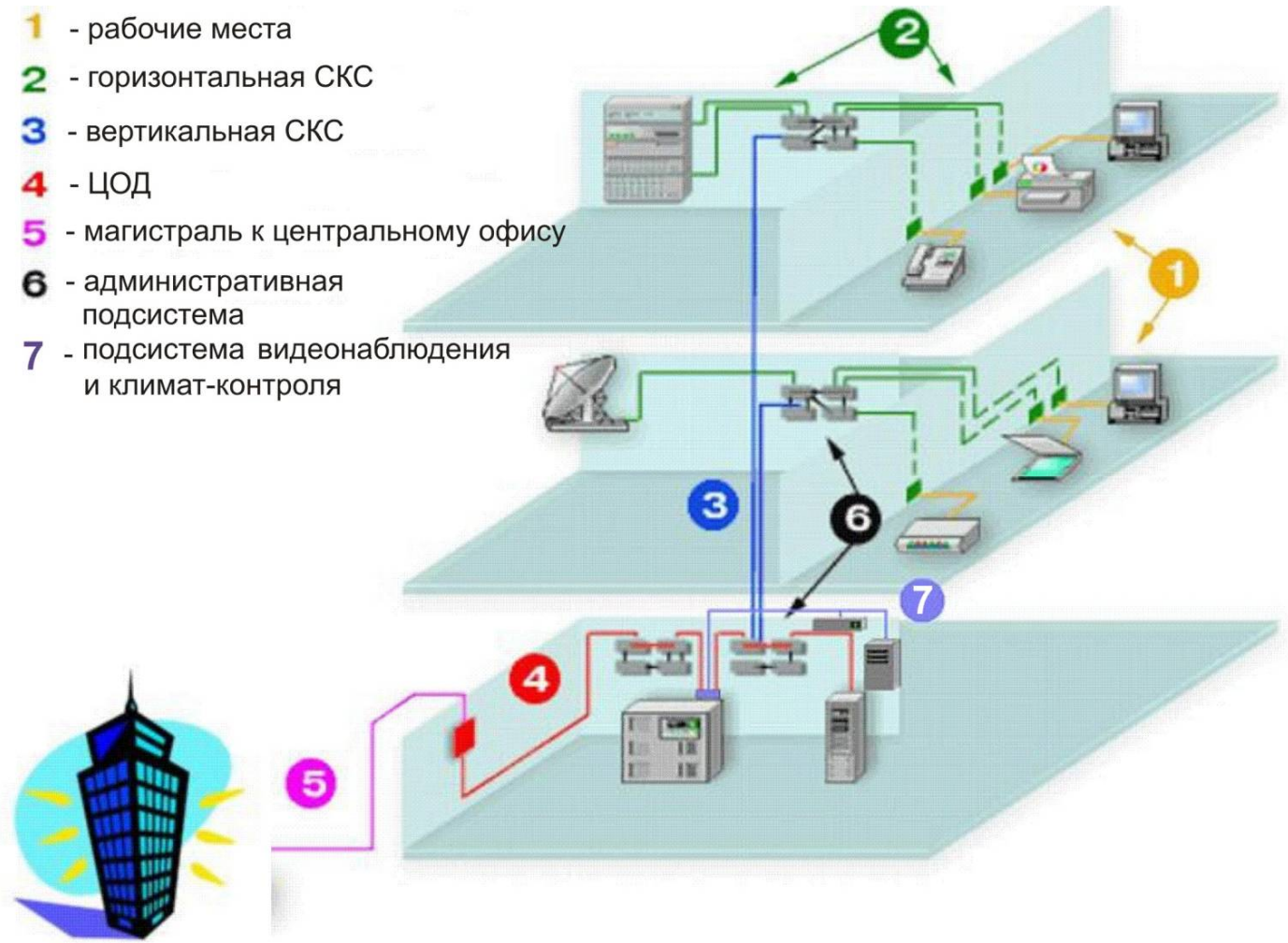
- замены медного кабеля на оптический кабель в стационарных системах передачи информации и связи с периферийными устройствами;
- замены мобильной связи радиодиапазона на беспроводную оптическую связь внутри помещений (технологии IrDA, TOSLINK, Visible Light Communication (VLC, Li-Fi));
- замена систем контроля и мониторинга на волоконно-оптические измерительные системы и датчики;
- замена систем освещения на световодные и волоконно-оптические и тд;

ЗАМЕЧАНИЕ:

большинство систем имеют свои оптические аналоги, а не имеющие позволяют локализовать электронные устройства в минимальном объеме

2. Объект информатизации без ПЭМИНа: ВО техника на ОИ

Системы связи объекта информатизации на базе PON



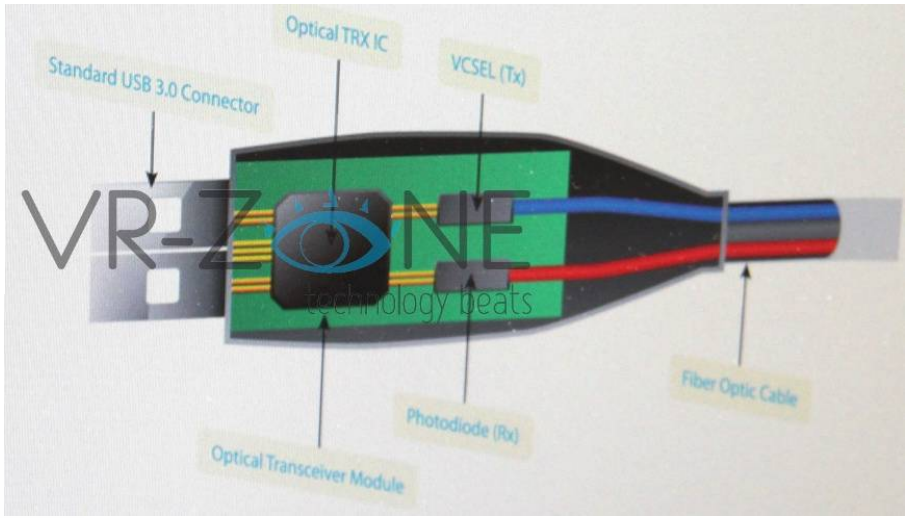
2. Объект информатизации без ПЭМИНа: ВО техника на ОИ

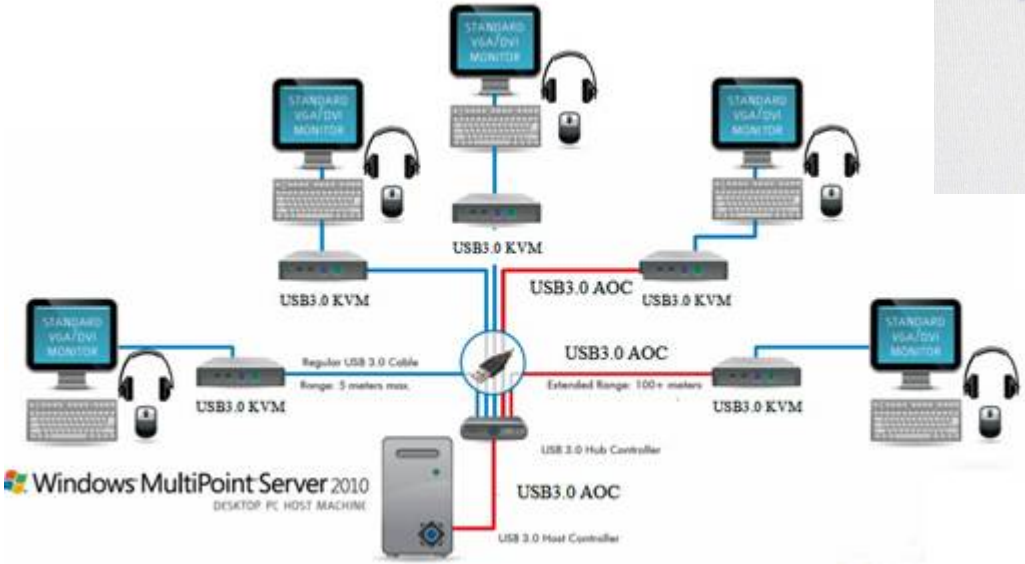
Волоконно-оптические удлинители интерфейсов
USB, FireWire, Ethernet, HDMI, DVI, RS-232 и другие

Например: USB3.0 Active Optical Cable (AOC) от VIA Labs
скорость передачи до 5 Gbps на дальности до 100 m (**выставка CES 2012**)

Feature:
- 5Gbps Dual Data Rate Transmission over 100 meters
- Daisy Chain Support
- Compliant to USB1.1/2.0 path through USB3.0 hub

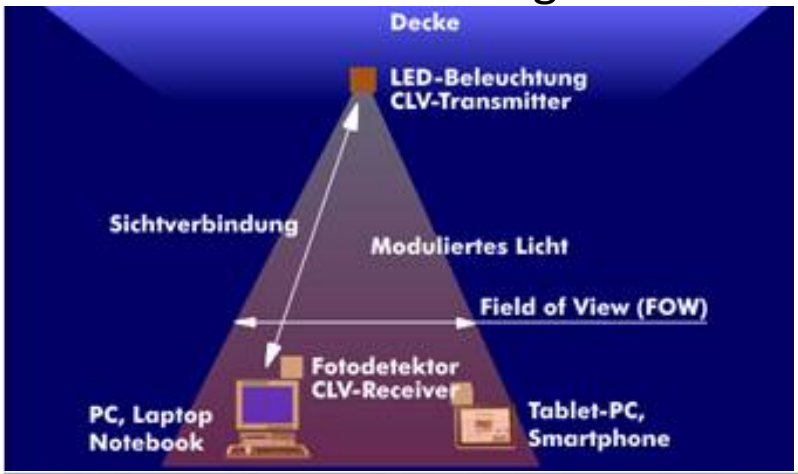
Application:
- Home/Office/SOHO Clouding Network
- w/ High Security Protection
- USB 3.0 KVM, USB3.0 hub
- High Speed Super Computer in Data Center Communication
- Digital FPD, PDP and Projector installation in Conference rooms, Auditoriums and for Kiosk system.
- Home theater system, Surveillance System, Digital Signage, and Campus training

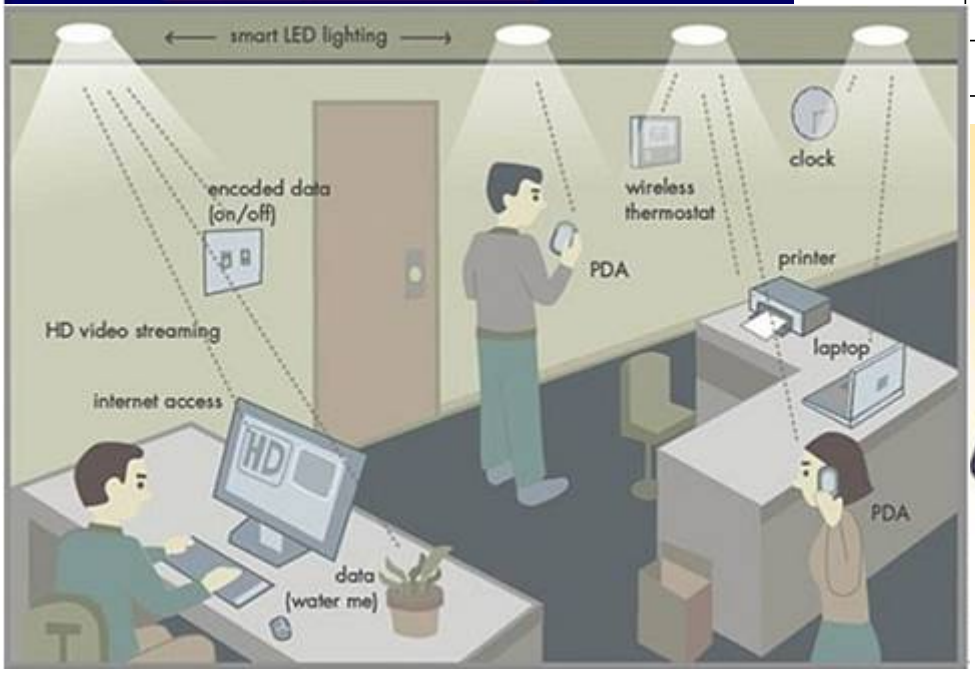




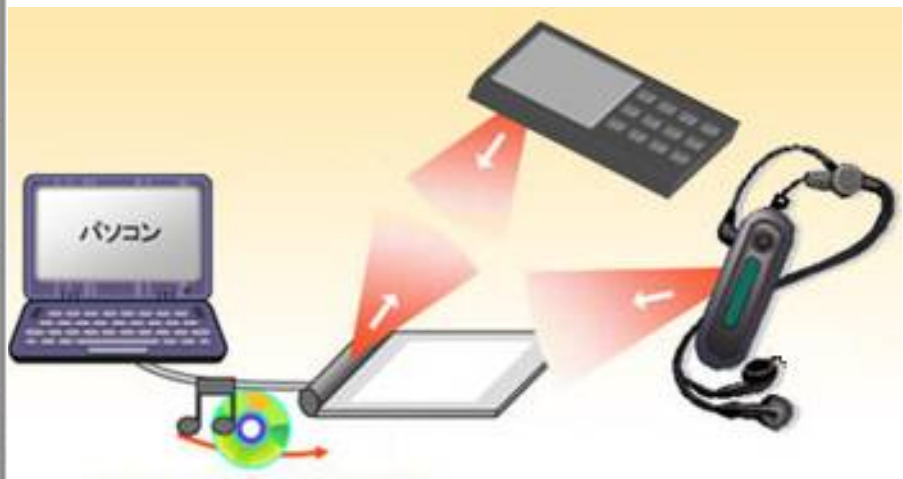
2. Объект информатизации без ПЭМИНа: ВО техника на ОИ

Системы мобильной оптической связи в помещении технологии IrDA, TOSLINK, Visible Light Communication (VLC), Light Fidelity (Li-Fi)





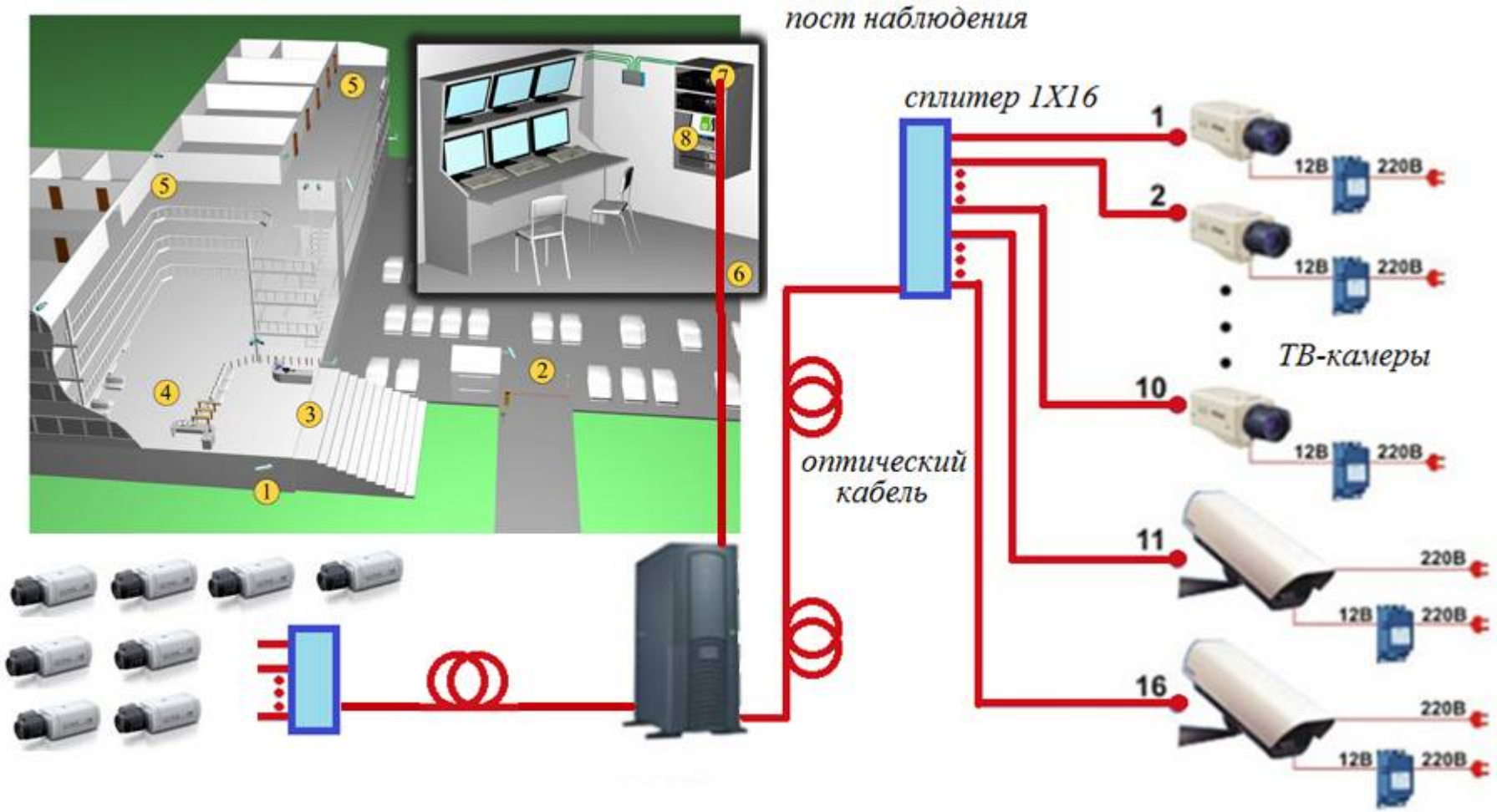
	Visible light communication	Infrared communication
Data rate	>100Mb/s possible (LED dependent)	4 Mb/s (FIR), 16 Mb/s (VFIR)
Status	Research and standardization in IEEE	Standardization (IrDA)
Distance	~meters	~3 meters
Regulation	No	No
Security	Good	Good
Carrier wavelength (frequency)	380~780 nm visible light (multiple wavelengths)	850 nm infrared
Services	Communication, illumination	Communication
Noise source	Sun light, Other illumination	Ambient light
Environmental	Daily usage Eye safe (visible)	Eye safe for low power (invisible)
Applications	Indoor & vehicular communication, Optical ID	Remote control, Point-to-point connection



2. Объект информатизации без ПЭМИНа: ВО техника на ОИ

Волоконно-оптические удлинители интерфейсов

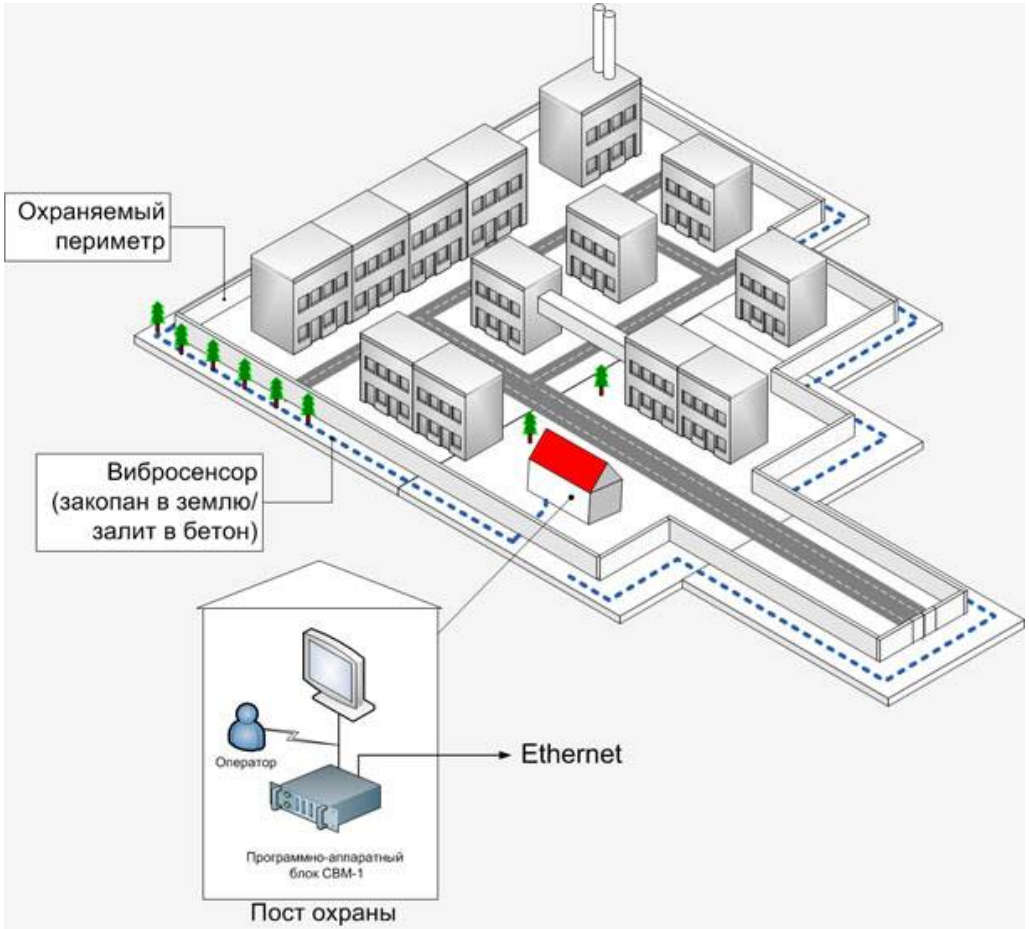
Волоконно-оптический интерфейс системы охранного видеонаблюдения позволяет соединять по оптическому кабелю с одним одномодовым волокном 16 ТВ-камер на расстоянии 100 км с передачей видео и аудио сигналов в реальном времени.



2. Объект информатизации без ПЭМИНа: ВО техника на ОИ

Системы мониторинга объекта информатизации на базе FOT

Оптоволоконная распределенная система вибромониторинга и охраны периметра (периметральная система охраны) предназначена для непрерывного контроля, регистрации и визуального отображения в реальном времени вибросостояния и целостности контролируемого объекта (объектов).

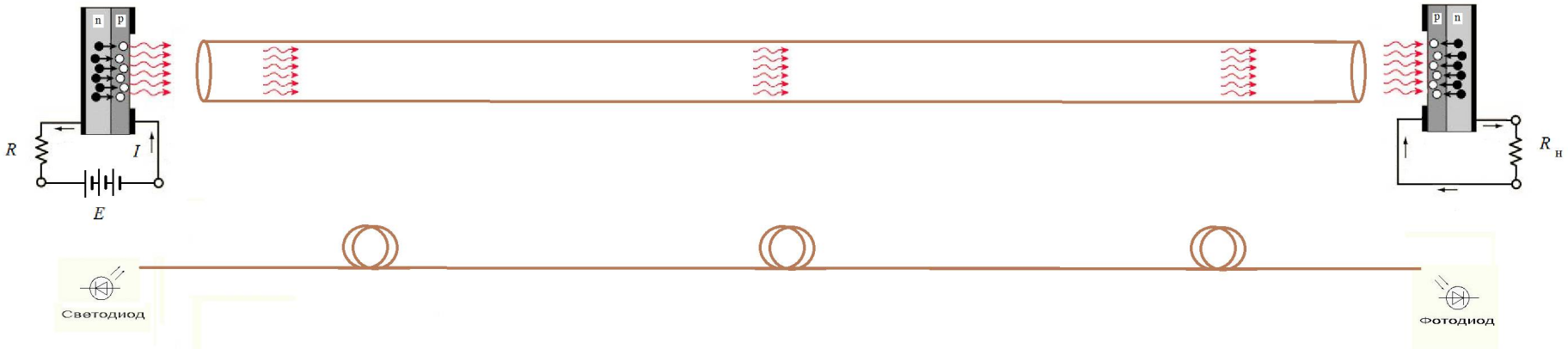


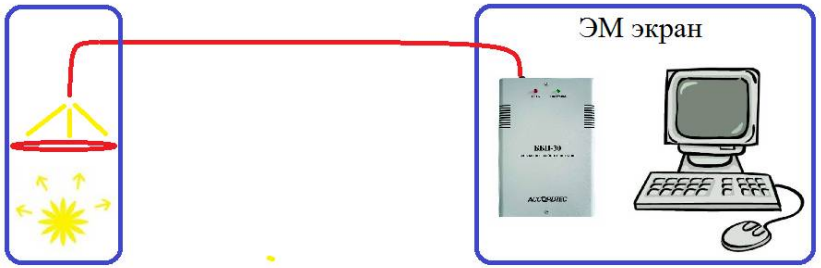
2. Объект информатизации без ПЭМИНа: ВО техника на ОИ

Волоконно-оптические линии передачи энергии для систем безопасности

обладают особенностями:

- ✓высокая скрытность – отсутствует ПЭМИН, так как создается полностью из диэлектрических материалов;
- ✓низкие потери, высокий кпд передачи энергии (более 25%);
- ✓электропитание маломощных датчиков,
- ✓электропитание управляющих элементов

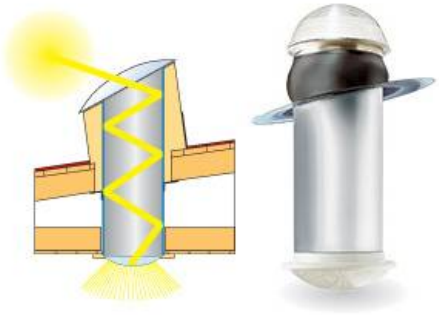




2. Объект информатизации без ПЭМИНа: ВО техника на ОИ

Волоконно-оптическое освещение

свет из проектора поступает в один из концов оптоволоконного световода, доставляется в нужную точку пространства, распространяясь внутри волокна благодаря явлению полного внутреннего отражения, и свободно излучается другим концом световода. Эффективность оптоволоконной системы освещения обычно не превышает 15-20%.



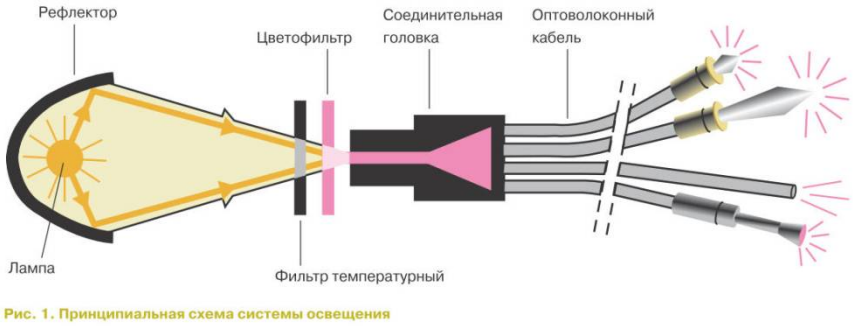
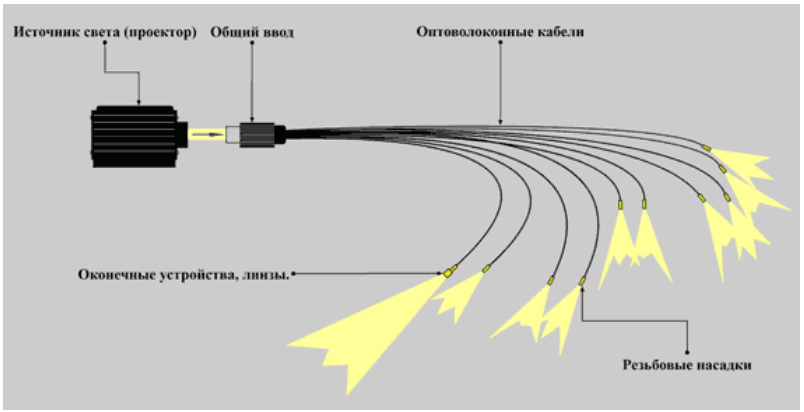
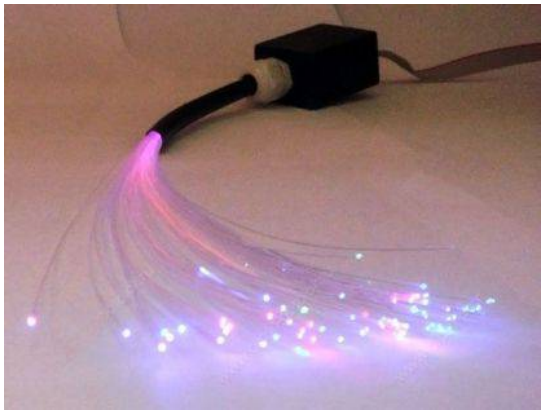


Рис. 1. Принципиальная схема системы освещения





2. Объект информатизации без ПЭМИНа: выводы

Объекта информатизации на базе фотонных технологий

3. Основные понятия информационной безопасности

- **по документами ФСТЭК России** http://www.fstec.ru

✓*объект информатизации:*

совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

✓*выделенное помещение:*

специальное помещение, предназначенное для проведения собраний, совещаний, бесед и других мероприятий речевого характера по секретным или конфиденциальным вопросам; мероприятия речевого характера могут проводиться в выделенных помещениях как с использованием технических средств обработки речевой информации (ТСОИ), так и без них.

✓*контролируемая зона:*

пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств, технических и иных материальных средств.

3. Основные понятия информационной безопасности

- **по документами ФСТЭК России** http://www.fstec.ru

✓*утечка информации:*

бесконтрольный выход защищаемой информации за пределы организации или крута лиц, которым она были доверена по службе или стала известна в процессе работы;

которая реализуется, в том числе, следующими методами

✓*НСД (несанкционированный доступ):*

доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

✓*НСИ (несанкционированный съем информации) или перехват:*

неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

3. Основные понятия информационной безопасности

- **по документами ФСТЭК России** http://www.fstec.ru

✓*под техническим каналом утечки информации (ТКУИ)*

понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте.

✓*ТСР (технические средства разведки):*

совокупность разведывательной аппаратуры, предназначенной для обнаружения демаскирующих признаков, предварительной обработки, регистрации перехваченной информации и ее передачи через каналы передачи информации в центры сбора и обработки информации.

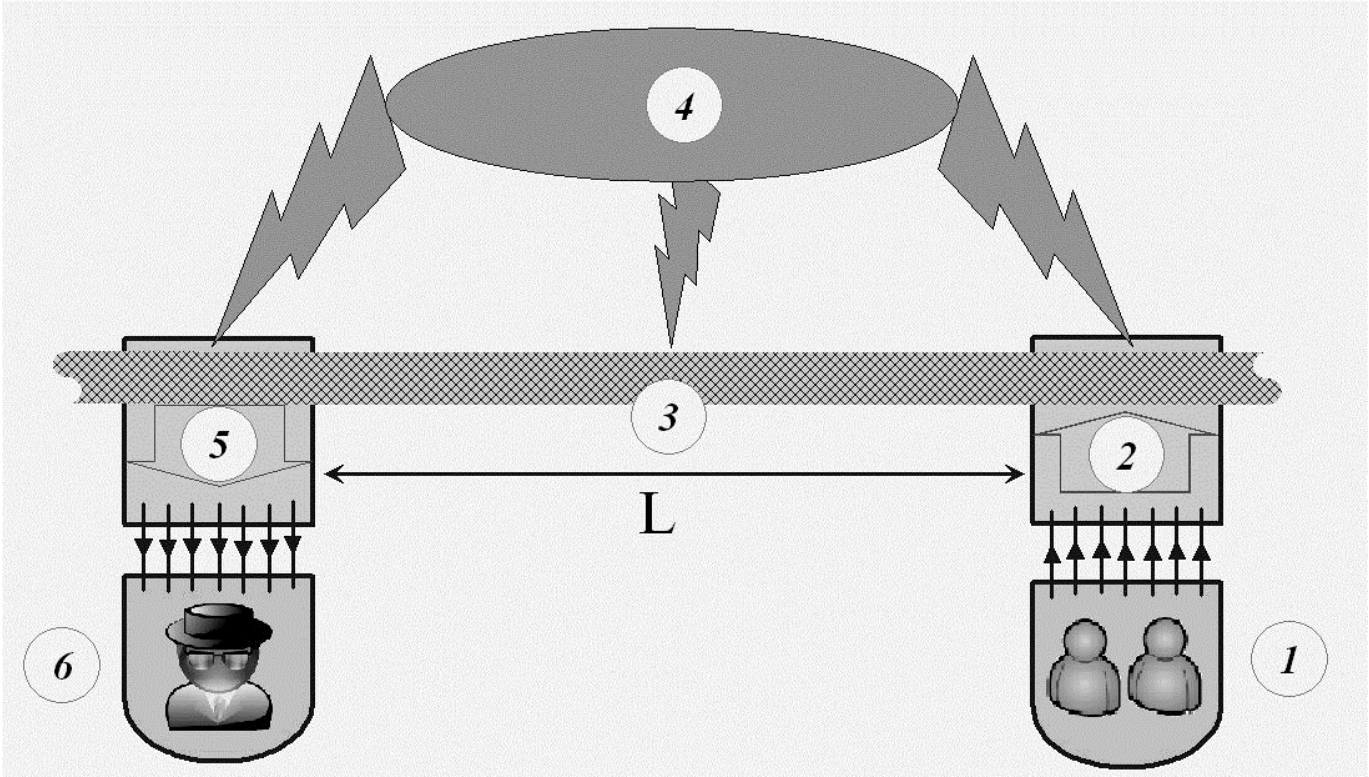
✓*информативный сигнал:*

электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

дополнительно: сигнал утечки информации - информативный сигнал в ТКУИ

- **НСИ с помощью ТКУИ (сбор информации)**

обобщенная структура

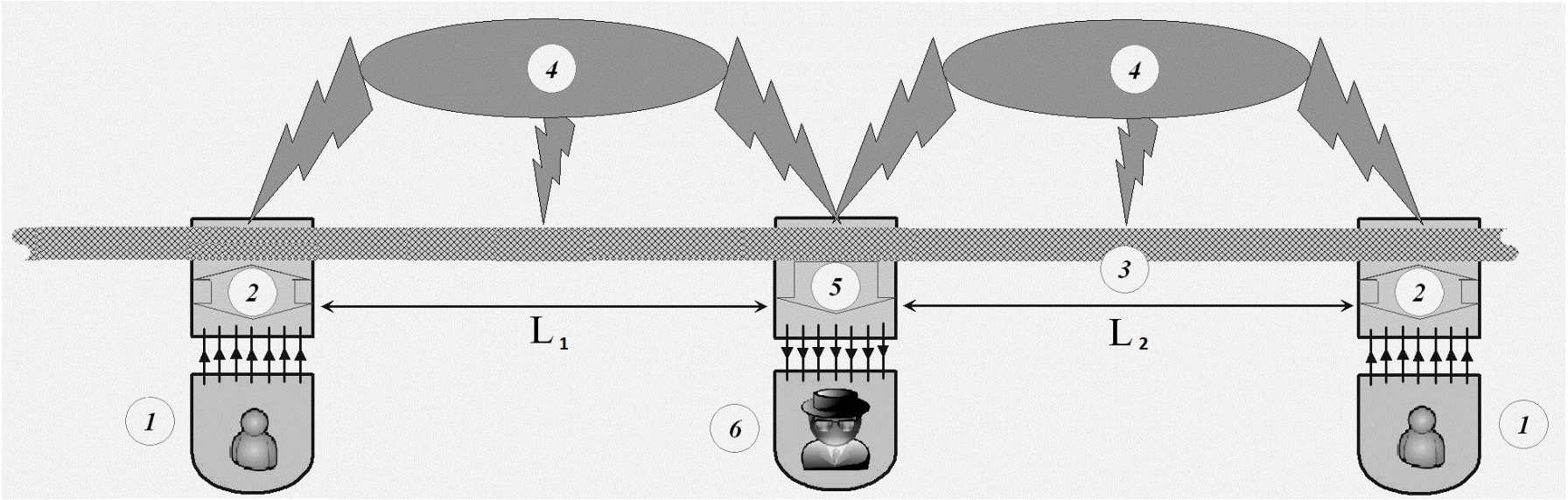


(1) источники, (2) нештатный преобразователь, (3) канал утечки длинной L, (4) помехи, (5) приемник ТСР, (6) злоумышленник.

3. Основные понятия информационной безопасности

- **НСИ с помощью ТКУИ (перехват информации)**

обобщенная структура



(1) источники-абоненты, (2) штатный приемопередатчик, (3) канал связи длинной L_1+L_2, (4) помехи, (5) приемник ТСР, (6) злоумышленник.

3. Основные понятия информационной безопасности

- **по документами ФСТЭК России** http://www.fstec.ru

✓*модель угроз информации (техническими средствами)*

формализованное описание технических каналов утечки, сведения о методах и средствах осуществления угроз информации.

ВВЕДЕМ ПОНЯТИЕ

сценарий угрозы информации

последовательность действий нарушителя, направленная на получение, искажение, уничтожение конфиденциальной (защищаемой) информации с применением специальных технических средств.

ОБОБЩЕННЫЙ СЦЕНАРИЙ УГРОЗЫ ИНФОРМАЦИИ

I. выявление возможного канала утечки информации, определение его характеристик и параметров;
II. выбор специальных технических средств и реализация подключения к каналу утечки;
III. мероприятия по повышению эффективности канала утечки информации;
IV. регистрация сигнала утечки информации

3. Основные понятия информационной безопасности

- **по документами ФСТЭК России** http://www.fstec.ru

✓*модель нарушителя*

предположение о возможностях нарушителя, которые он может использовать для разработки и проведения мероприятий по реализации угроз безопасности информации, а также об ограничениях на эти возможности

Модель нарушителя

- ***цели:*** *утечка, ограничение доступа, фальсификация, уничтожение конфиденциальной информации, циркулирующей на объекте информатизации;*
- ***тип:*** *внутренний или внешний тип нарушителя определяет его возможности и требования к техническим средствам разведки;*
- ***возможности:*** *рассматриваются только технические возможности нарушителя и они ограничиваются исключительно физическими законами и современным состоянием техники;*

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Модель угроз – перечень возможных угроз безопасности информации на объекте информатизации и их описание (на физическом уровне)**

Основные угрозы ИБ состоят в нарушении

- ✓ **<u>конфиденциальности</u>** – угроза неправомочного получения доступа к защищаемой информации
- ✓ целостности – угроза преднамеренного преобразования защищаемой информации
- ✓ доступности - угроза полной или временной невозможности получения доступа к информации

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Модель угроз – перечень возможных угроз безопасности информации на объекте информатизации и их описание (на физическом уровне)**

❖ *Модель угроз ИБ на объекте информатизации от использования волоконно-оптических коммуникаций и техники включает следующие угрозы защищаемой информации по техническим каналам*

I. угроза трафику в штатных оптических сетях связи на объекте информатизации и вне его пределов, главным образом перехват трафика;

II. сбор информации (несанкционированный съем информации) через штатные кабельные системы объекта информатизации;

III. сбор информации (несанкционированный съем информации) с помощью волоконно-оптических технических средств разведки;

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

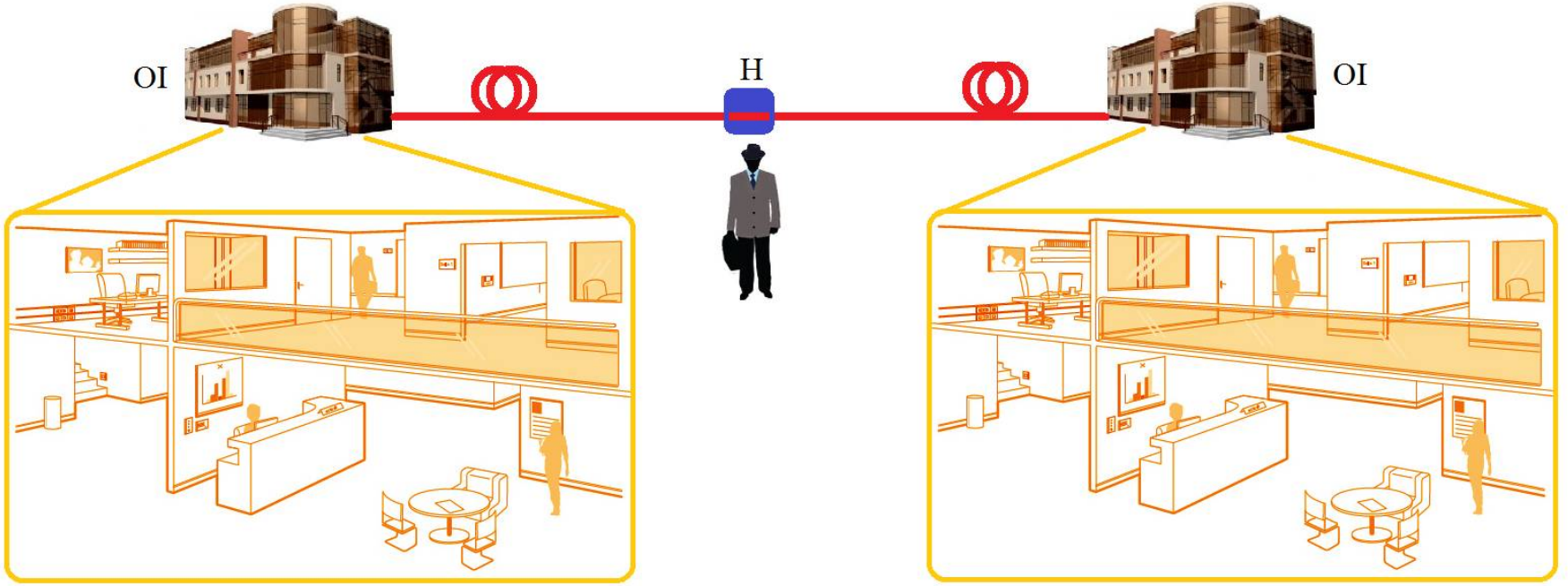
- **Информативный сигнал – оптическое излучение, распространяющееся в оптических волокнах кабельной системы объекта информатизации**

Оптические излучение в волоконно-оптических системах и устройствах

- длина волны излучения от 100 нм до 5000 нм;
- мощность излучения от энергии одного фотона в системах счета фотонов до десятков кВт в технологических лазерах;
- длительность импульса от непрерывного до фемтосекунд (10E-15 сек);
- когерентность до сотен метров (длина когерентности);
- спектральную полосу от 400 нм до 2500 нм (например, волоконные лазерные источники белого света перекрывают всю видимую область);

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Перехват трафика – получение доступа к трафику информации между субъектами объекта информатизации, идущему через ВОК**



- нарушитель (Н) получая доступ к оптической кабельной системе, например, линии связи между объектами информатизации (OI) может перехватить трафик сети, в котором может содержаться конфиденциальная информация, и остаться незамеченным.

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Информативный сигнал – оптическое излучение, распространяющееся в оптических волокнах кабельной системы объекта информатизации**

Информативный сигнал при перехвате – это оптические излучение

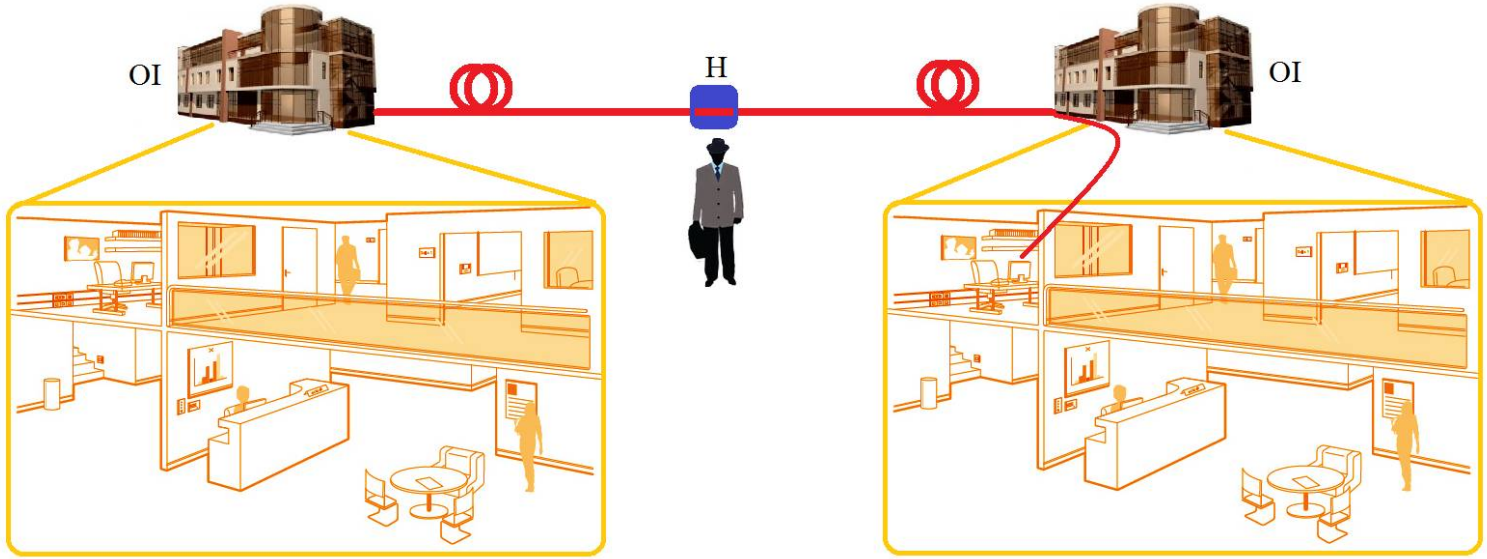
- в волоконно-оптических системах передачи информации
  - ✓ длина волны вблизи окон прозрачности кварцевого волокна – 1550 нм, 1310 нм, 850 нм
  - ✓ типичная мощность от +20 дБм до -40 дБм
  - ✓ имеет цифровую модуляцию по амплитуде/фазе с частотой с 100 МГц, 1 ГГц, 10 ГГц, 100 ГГц и другое

и

- в волоконно-оптических системах измерения
  - ✓ длина волны любая от 100 нм до 3000 нм и вне данного диапазона в зависимости требований измерений
  - ✓ имеет аналоговую модуляцию по любому параметру волны

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Сбор информации (НСИ) через штатные оптические кабельные системы – получение доступа к информации циркулирующей на объекта информатизации через штатные ВОК**



- нарушитель (Н) получая доступ к оптической кабельной системе, например, линии связи между объектами информатизации (OI) может воспользоваться волноводными свойствами штатной оптической сети, путем зондирования сети получить доступ к конфиденциальная информация циркулирующей на объекте информатизации.

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

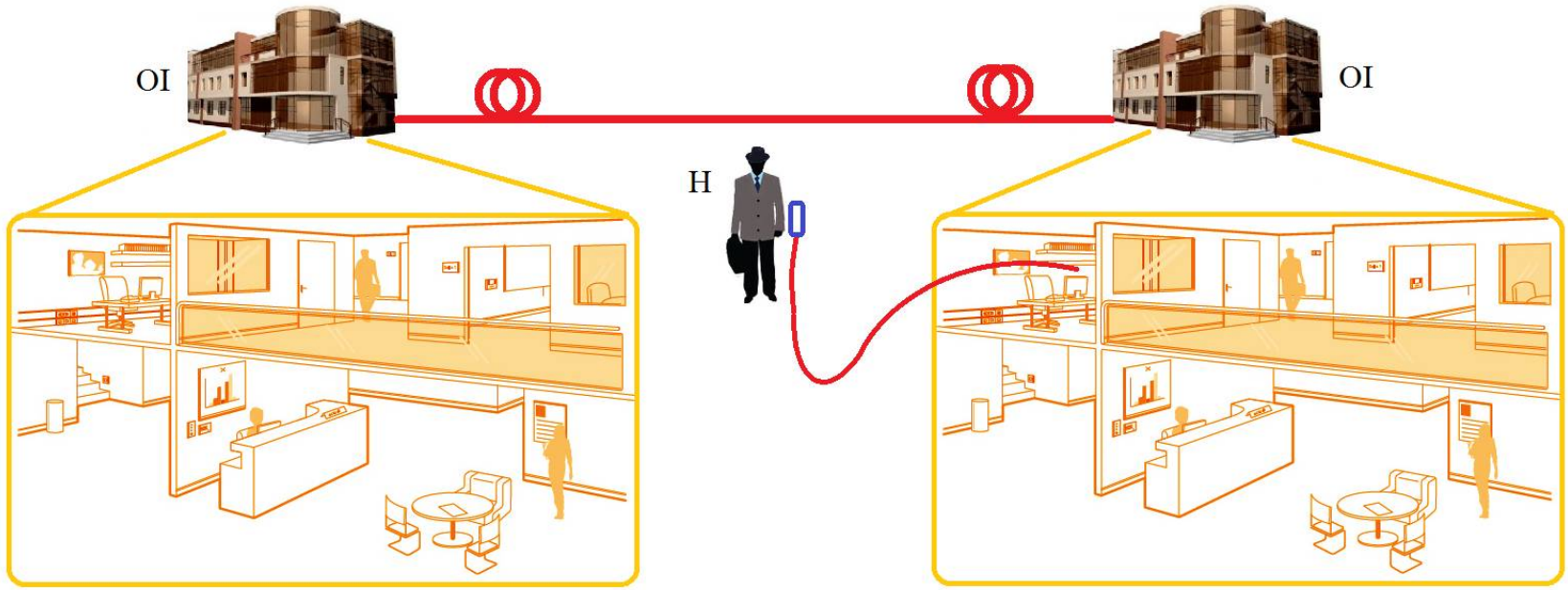
- **Информативный сигнал – оптическое излучение, распространяющееся в оптических волокнах кабельной системы объекта информатизации**

Информативный сигнал при НСИ через штатные оптические сети – это оптические излучение используемое для зондирования, параметры которого определяются задачами зондирования и свойствами оптического канала

- ✓ длина волны любая от 100 нм до 3000 нм и вне данного диапазона в зависимости требований измерений;
- ✓ имеет аналоговую модуляцию по любому параметру волны;
- ✓ возможно использования штатного излучения или излучения с параметрами штатного;

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Сбор информации (НСИ) с помощью волоконно-оптических ТСР – получение доступа к информации циркулирующей на объекта информатизации с помощью ТСР на основе волоконной оптики**



- нарушитель (Н) может получить доступ к конфиденциальная информация циркулирующей на объекте информатизации (OI) через оптическое волокно или кабель, которое скрытно размещается на объекте, используя его измерительные возможности.

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Информативный сигнал – оптическое излучение, распространяющееся в оптических волокнах кабельной системы объекта информатизации**

Информативный сигнал при НСИ – это оптические излучение используемое для зондирования

- ✓ длина волны любая от 100 нм до 3000 нм и вне данного диапазона в зависимости требований измерений;
- ✓ имеет аналоговую модуляцию по любому параметру волны: амплитуде, фазе, частоте или поляризации;

параметры выбираются в зависимости от решаемых задач и свойств волоконно-оптических элементов канала утечки

- ❖ данная система НСИ является волоконно-оптической локальной или распределенной измерительной системой, скрытно используемой для регистрации информационного сигнала.

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Характеристика ТКУИ – основные параметры технического канала утечки информации на основе волоконно-оптических технологий**

Эффективность канала утечки

$$CEL=(I_{leak}/I_{link}) \quad \text{(измеряется в в отн. ед. от 0 до 1 или в \%)}$$

I_{leak} - объем информации переносимый сигналом утечки на выходе ТКУИ

I_{link} – объем информации переносимый информативным сигналом на входе технического канала утечки информации

Защищенность от утечки по данному каналу утечки

$$CPL=1-CEL \quad \text{(измеряется в отн. ед. от 0 до 1 или в \%)}$$

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Характеристика ТКУИ – основные параметры технического канала утечки информации на основе волоконно-оптических технологий**

В ТКУИ по перехвату трафика

$$CEL \rightarrow (C_{leak} / C_{link})$$

C_{leak} - пропускная способность канала утечки информации по перехвату

C_{link} - пропускная способность штатного канала связи, подверженного перехвату

например: в речевом ТКУИ эффективность канала утечки стремиться к оценки разборчивости речи W, определяемой методом артикуляционных измерений (ГОСТ 16600-72)

$$CEL \rightarrow W=(N_{leak} / N_{link})$$

N_{leak} - количество правильно принятых оператором слов на выходе ТКУИ

N_{link} - количество преданных слов по данному ТКУИ

4. Модель угроз безопасности информации на объекте информатизации и их характеристика

- **Характеристика ТКУИ – основные параметры технического канала утечки информации на основе волоконно-оптических технологий**

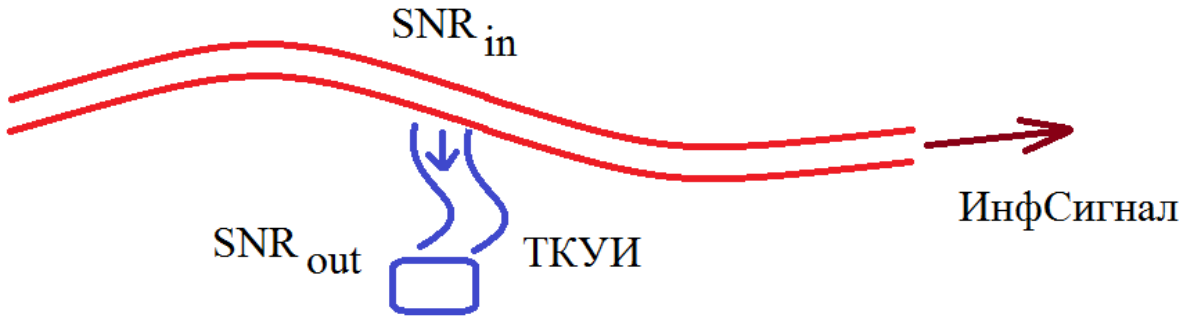
Коэффициент шума канала утечки $CNL=(SNR_{in} /SNR_{out})$

SNR_{in} – отношение мощности сигнала к мощности шума на входе канала утечки

SNR_{out} - отношение мощности сигнала к мощности шуму на выходе канала утечки

т.е. коэффициент шума показывает во сколько раз вырос вклад шума в сигнал при его прохождении в ТКУИ

эффективность канала утечки определяется коэффициентом его шума - CEL(CNL)



5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Модель нарушителя – формализованное описание типа, целей, возможностей злоумышленника, его общая характеристика**

❖ *Технические возможности нарушителя (основное предположение)*

A. нарушитель обладает всеми физическими знаниями о процессах формирования технического канала утечки информации (ТКУИ);

B. нарушитель имеет возможность использовать любое производимое волоконно-оптическое оборудование, в том числе и экспериментальное, для реализации своих планов;

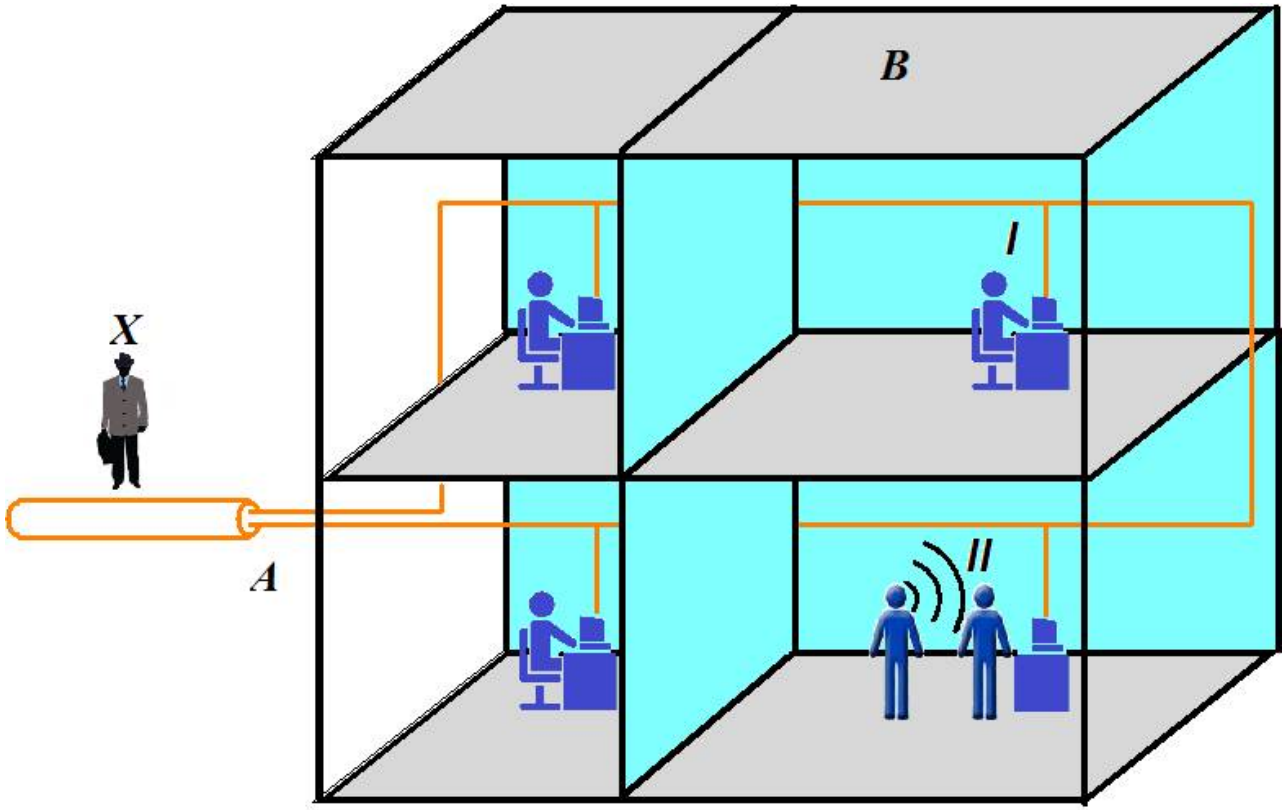
C. возможности нарушителя ограничиваются только физическими законами, которые позволяют или не позволяют создать ТКУИ;

D. возможности нарушителя, также, ограничиваются техническими характеристиками серийного и экспериментального оборудования.

5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Внутренний и внешний нарушитель: внешний нарушитель**

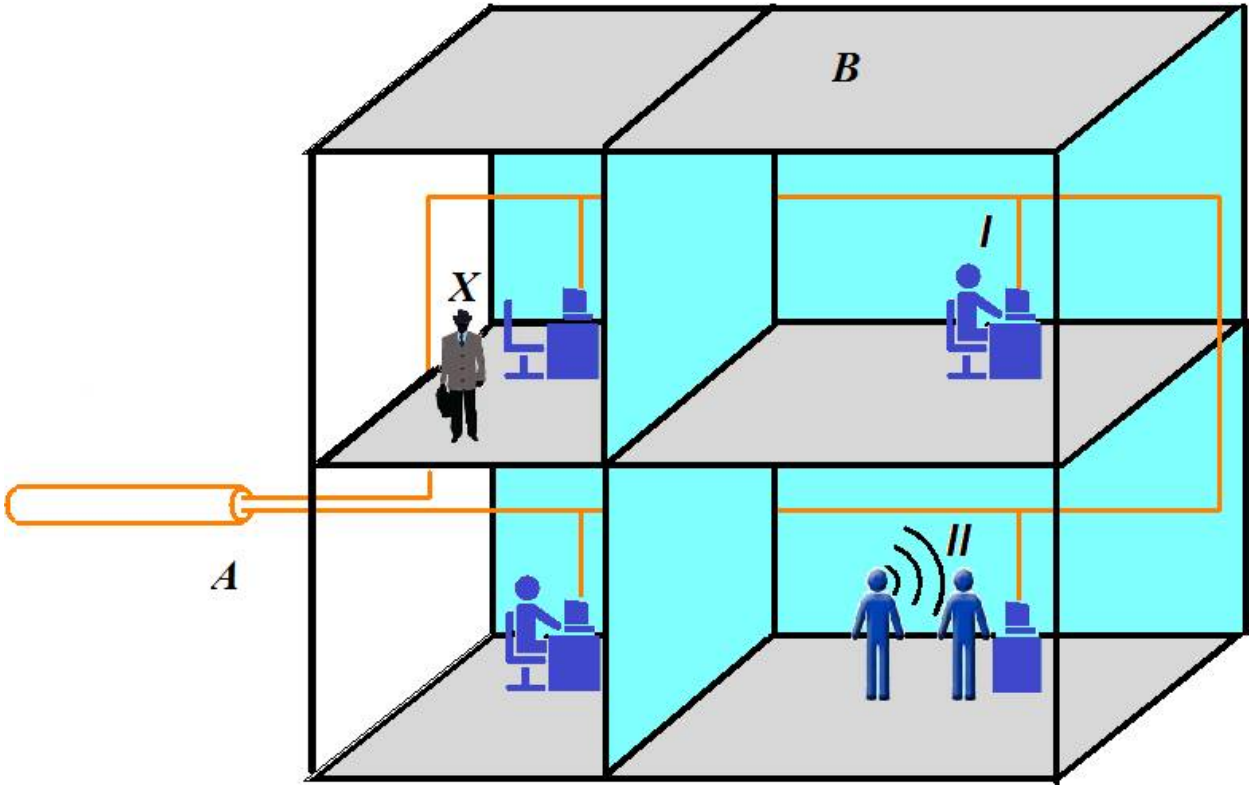
❖ Условная схема (перехвата) несанкционированного съема информации (НСИ) с волоконно-оптических коммуникаций (*A*) на основе технологии *PON* вне контролируемой зоны (*B*) внешним нарушителем *X*.



5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Внутренний и внешний нарушитель: внутренний нарушитель**

❖ Условная схема (перехвата) несанкционированного съема информации (НСИ) с волоконно-оптических коммуникаций (*A*) на основе технологии *PON* внутри контролируемой зоны (*B*) внутренним нарушителем *X*.

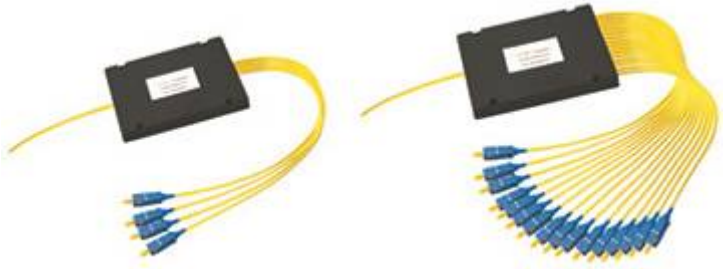


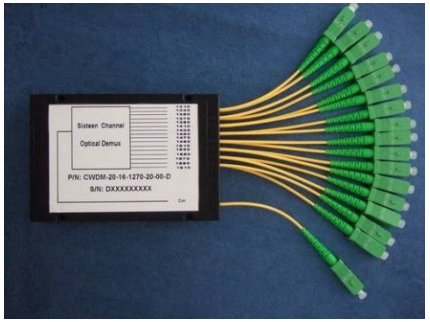
5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Технические возможности нарушителя**

Основные ТСР используемы для проведения НСИ через ВОК:

- ✓ пассивные волоконно-оптические элементы по управлению оптическими потоками в волокне – оптический кабель, соединители разъемные, ответвители, делители/объединители, аттенюаторы, циркуляторы, поляризаторы, изоляторы, мультиплексоры/демультиплексоры;





5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Технические возможности нарушителя**

Основные ТСР используемы для проведения НСИ через ВОК:

- ✓ активные волоконно-оптические элементы по управлению оптическим излучением в волокне – сварочные аппараты, переключатели/ коммутаторы, усилители, регенераторы, модуляторы, источники/лазеры, приемники;

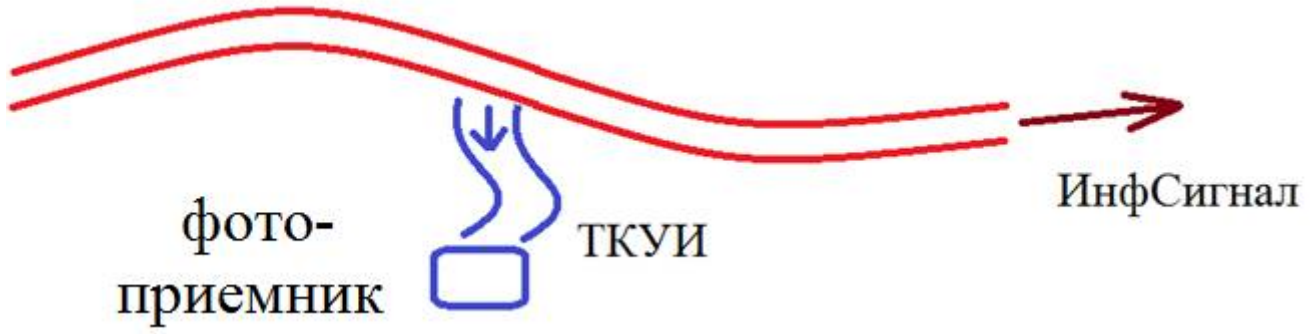
- ❖ пассивные и активные волоконно-оптические элементы позволяют создавать требуемые для нарушителя структуру ТКУИ на основе волоконно-оптических каналов.

5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Технические возможности нарушителя**

Регистрация оптического излучения, технические характеристики:

- ✓ точность измерения – характеризует близость измеренного значения к его действительному , обычно оценивается погрешностью;
- ✓ разрешающая способность – соответствует наибольшей точности измерительной системы;
- ✓ чувствительность – определяется отношением изменения измеряемой величины к изменению величины на выходе измерительной системы;
- ✓ динамический диапазон, время отклика, линейность



5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Технические возможности нарушителя**

Регистрация оптического излучения, технические характеристики:

PCU-100 - компактный счетчик фотонов, предназначенный для использования в качестве самостоятельного фотометрического блока в люминесцентной и другой светочувствительной аппаратуре:

тип детектора: ФЭУ (Hamamatsu, Япония)	
режим детектирования:	счет фотонов
спектральная чувствительность:	400-700 нм.
динамический диапазон измерений:	7 порядков
темновой счет:	10-30 имп/сек
частота измерений:	до 100 Гц
интерфейс связи с компьютером:	USB
питание:	5 Вольт от USB
размеры (Д х Ш х В):	13 х 8 х 8 $см^3$
вес:	700 г

5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- **Технические возможности нарушителя**

Регистрация оптического излучения, технические характеристики:

Фотоприемные модули

Модули для спектрального диапазона 1100-1650 нм на основе высокочувствительных InGaAs PIN фотодиодов.

Предназначены для цифровой и аналоговой аппаратуры ВОЛС.

InGaAs PIN фотоприемные модули

Модель	Спектр. диапазон нм	Чувств., А/Вт	Тип волокна	Емкость, пФ	Полоса пропускания, ГГц
PD-1375-ip	1100-1650	0.9	SM/MM	1,5	>1,5
PD-1375-ir	1100-1650	0.9	SM/MM	1,5	>1,5
PD-1355-ip	1100-1650	0.8	SM/MM	0,7	>2,5
PD-1355-ir	1100-1650	0.8	SM/MM	0,7	>2,5

5. Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации

- Нормативно-методические рекомендации регуляторов:

- «Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, волоконно-оптических системах передачи», утвержден приказом ФСТЭК России от 15 марта 2012 г. №27дсп

- ✓ «Специальные и общие технические требования, предъявляемые к защищенным волоконно-оптическим системам передачи информации (СОТТ - ВОСП)», Нормативно-методический документ ФСТЭК России, введен в действие с 01.03.06 г.;
- ✓ «Сборник нормативно-методических документов по технической защите информации в волоконно-оптических системах передачи (НМД по ТЗИ ВОСП)», утвержден приказом ФСТЭК России от 15.11.2005 г. № 448;

6. Понятие сценария утечки информации в структуре канала утечки информации

- **Сценарий угрозы – наиболее вероятная последовательность (алгоритм) действий нарушителя, направленная на получения доступа к защищаемой информации с целью нарушения её безопасности**

---

a. *действия нарушителя во многом предопределены целями, которые он преследует, и его возможностями, все это позволяет однозначно определить наиболее вероятную последовательность его действий.*

b. *например, формирование ТКУИ связано с регистрацией информативных сигналов с целью нарушения конфиденциальности, целостности или доступности, что позволяет определить требуемые технические средства и способы их применения.*

c. *в нашем случае, информативными сигналами являются все физические поля связанные с прохождением света по оптоволокну и вызываемой ими модуляциями в оптоволокне.*

6. Понятие сценария утечки информации в структуре канала утечки информации

- **Обобщенный сценарий угрозы НСИ в оптических коммуникациях определяется этапами**

---

1. *Обнаружение возможного канала утечки, определение его характеристик, параметров информативного сигнала;*

2. *Выбор технических средств разведки и реализация подключения к техническому каналу утечки информации;*

3. *Мероприятия по повышению эффективности технического канала утечки информации;*

4. *Регистрация сигнала утечки информации;*

6. Понятие сценария утечки информации в структуре канала утечки информации

1. *Обнаружение возможного канала утечки, определение его характеристик, параметров информативного сигнала*

Решаемые проблемы

- *определение типа информации, подвергаемой угрозе нарушения её безопасности, определение типа ТКУИ, используемых ТСР;*

- *определение типа штатной оптической сети подвергаемой угрозе перехвата или НСИ, т.е. телекоммуникационная, локальная сеть, измерительная сеть, архитектура сети, её топология и другие параметры;*

- *определение типа носителя информативного сигнала: дискретный или аналоговый сигнал, модуляция по амплитуде, частоте, поляризации, фазе и другими характеристиками;*

6. Понятие сценария утечки информации в структуре канала утечки информации

2. *Выбор технических средств разведки и реализация подключения к техническому каналу утечки информации*

Решаемые проблемы

- *определение по параметрам информативного сигнала используемых ТСР: чувствительность, динамический диапазон, частотные характеристики;*

- *Определение типа подключения к оптическому каналу, шумовые характеристики подключения, возможен ли дистанционный съем информации и другое;*

- *в ТКУИ через штатные ВОК наиболее сложная проблема – подключение или отвод части излучения, что связано с физическими характеристиками волоконно-оптического канала.*

6. Понятие сценария утечки информации в структуре канала утечки информации

3. Мероприятия по повышению эффективности технического канала утечки информации

Решаемые проблемы:

- *выбор участка подключения к оптическому каналу с наилучшими параметрами;*
- *повышение эффективности ТКУИ на основе улучшения подключения к оптическому каналу;*
- *использование регистрирующей аппаратуры с улучшенными параметрами для данного конкретного случая;*
- *использование методов обработки информации с целью выделения сигнала;*

6. Понятие сценария утечки информации в структуре канала утечки информации

4. Регистрация сигнала утечки информации

Решаемые проблемы

Выбор регистрирующей аппаратуры на основе параметров сигнала утечки;

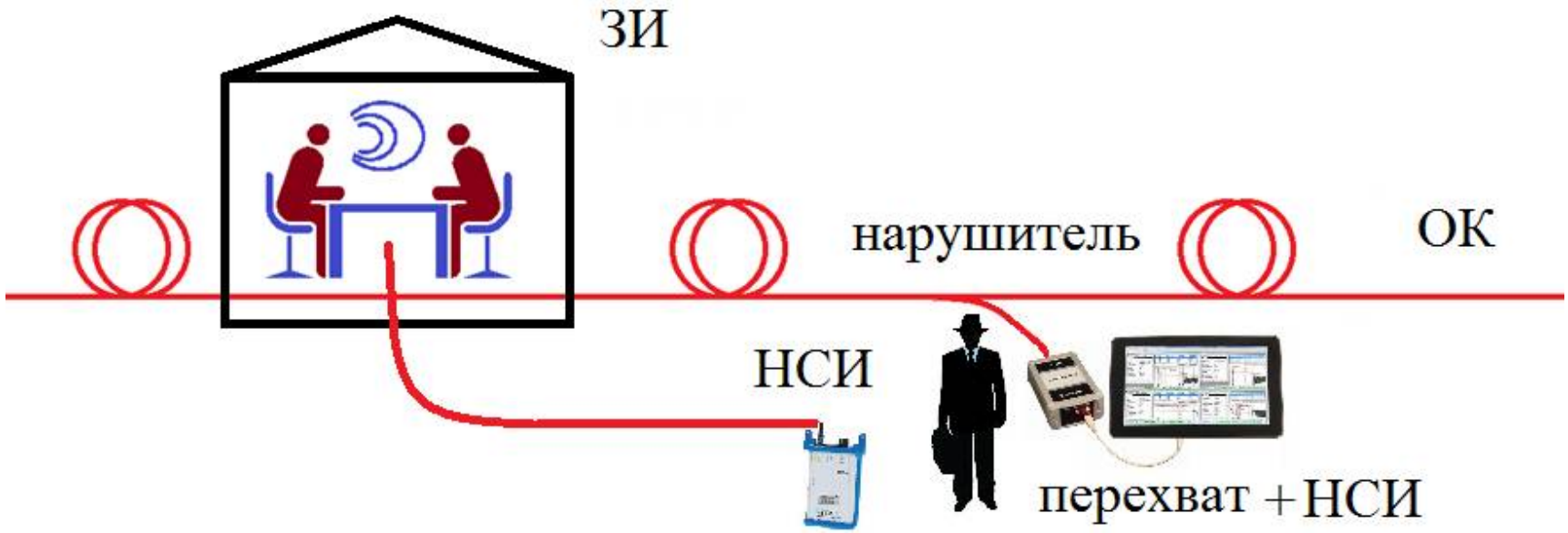
сигнал систем передачи информации

сигнал в измерительных системах

6. Понятие сценария утечки информации в структуре канала утечки информации

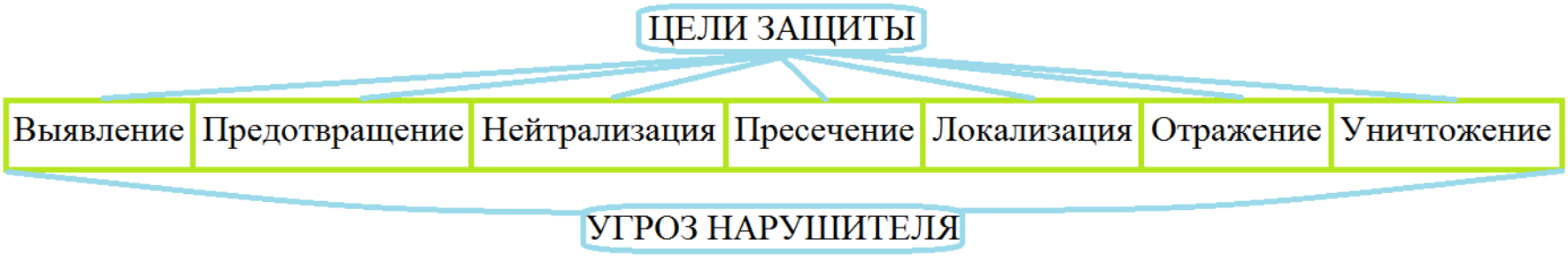
Выводы

- *Проведение анализа возможных сценариев по реализации ТКУИ позволяет выявить наиболее опасные участки системы защиты информации;*
- *Сценарии угроз и мероприятия по их нейтрализации определяются видом угрозы – перехват трафика из ВОК или НСИ через ВОК или НСИ с помощью ВО ТСР;*



7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- **Цели защиты информации и технические средства защиты информации**



- обсуждаются только методы защиты связанные с физическими и техническими способами достижения целей защиты, т.е. ТСЗИ.

- ТСЗИ связаны с воздействием на информативный сигнал или его проявлениями в виде других полей.

7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- *информативный сигнал в техническом канале утечки информации*

Основные параметры технического канала утечки информации:

мощность информативного сигнала P_{signal}

мощность шума в канале P_{noise}

разрешающая способность регистрирующей аппаратуры P_{sense}

общие требования к информативному сигналу и ТСР в ТКУИ для эффективной регистрации нарушителем

$P_{signal} + P_{noise} > P_{sense}$ - регистрирующая аппаратура фиксирует сигнал утечки

$SNR = P_{signal} / P_{noise} \geq 1$ (0 dB) – регистрирующая аппаратура выделяет сигнал на фоне шума

7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- **Методы защиты информации на основе ТСЗИ связаны с информативным сигналом и включают мероприятия/действия направленные на**

---

1. *зашумление информативного сигнала до уровня при котором невозможно его регистрация/обнаружение (зашумление, физическая маскировка);*

2. *ослабление информативного сигнала до уровня фона, т.е. естественных шумов (фильтрация, селекция, экранировка);*

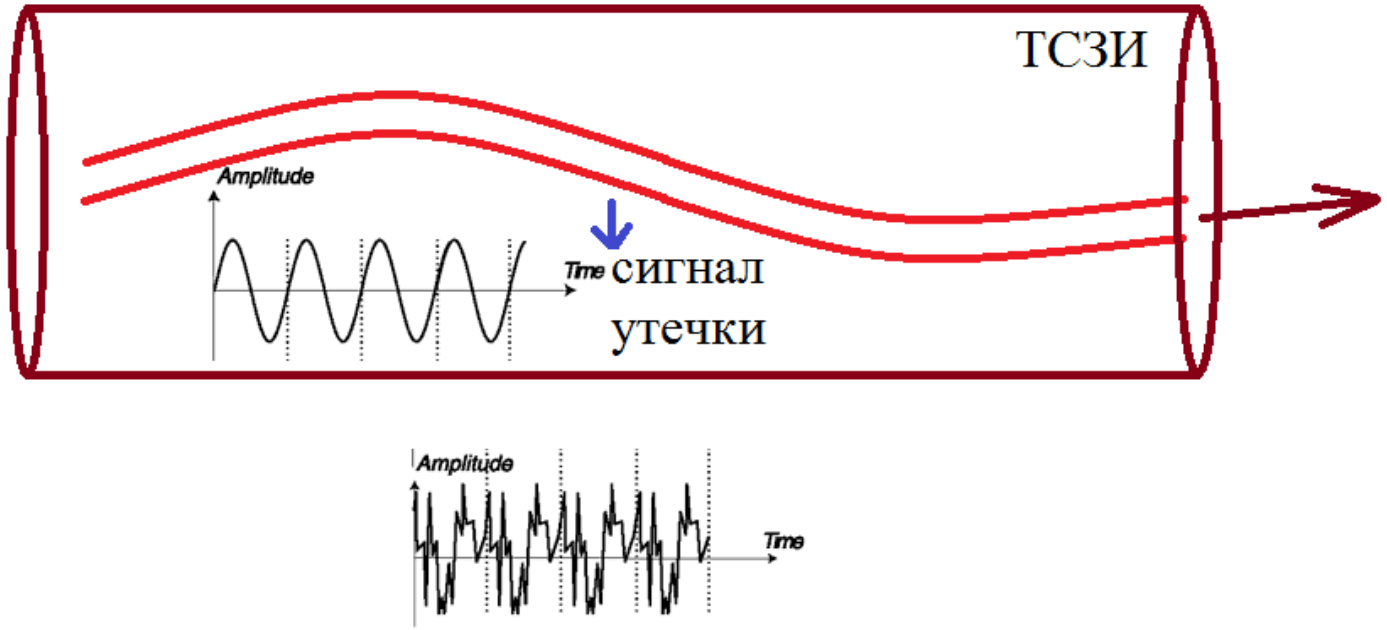
3. *ограничение доступа к информативному сигналу путем выявление угрозы/нарушителя (мониторинг, контроль, выявление);*

4. *сокрытие информационного сигнала от технических средств разведки нарушителя (стеганография, кодирование, шифрование);*

7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- **Методы защиты информации связаны с информативным сигналом и включают мероприятия/действия направленные на**

- *зашумление информативного сигнала до уровня при котором невозможно его регистрация/обнаружение (зашумление, физическая маскировка);*

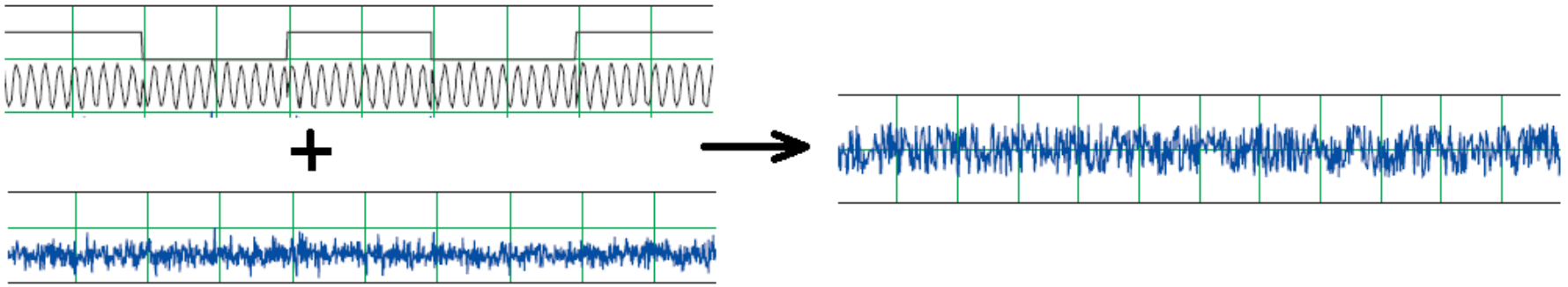


7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- *зашумление информативного сигнала до уровня при котором невозможно его регистрация/обнаружение (зашумление, физическая маскировка);*

общие требования к информативному сигналу при зашумлении

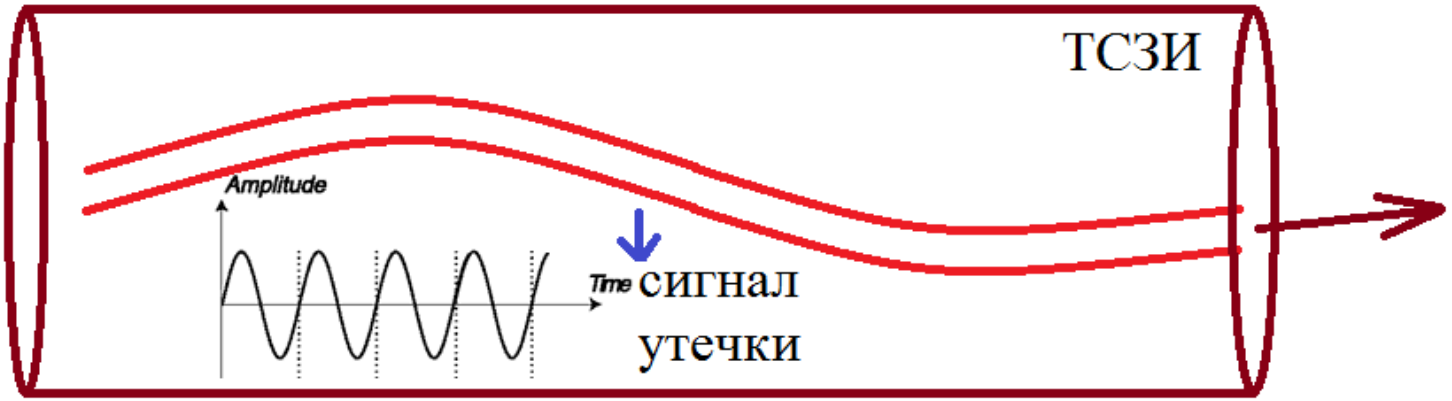
$$SNR = P_{signal} / P_{noise} < 1 \ (0 \text{ dB})$$

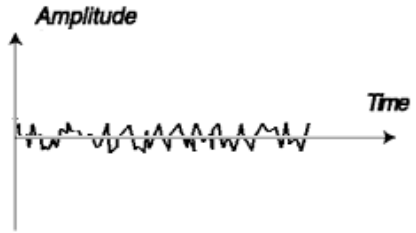


7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- **Методы защиты информации связаны с информативным сигналом и включают мероприятия/действия направленные на**

- *ослабление информативного сигнала до уровня фона (фильтрация, селекция, экранировка);*



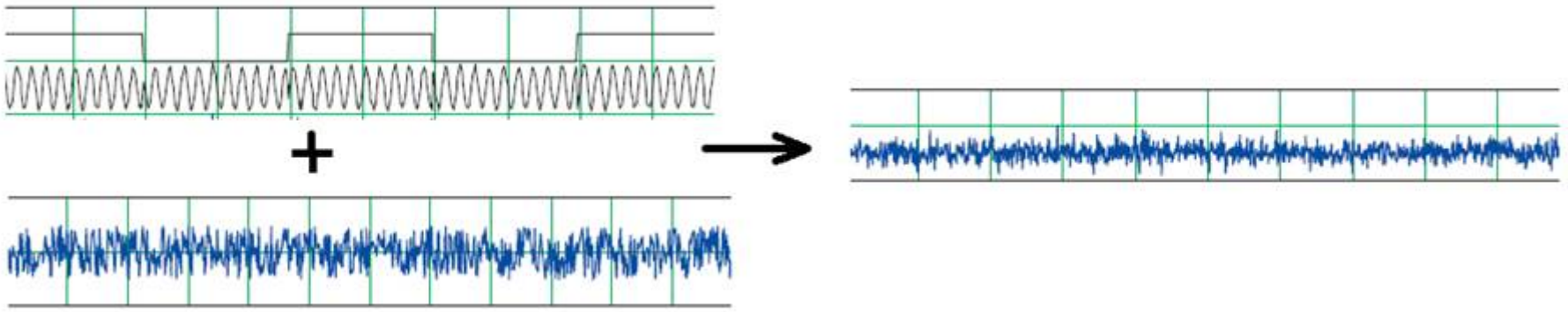


7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- *ослабление информативного сигнала до уровня фона (фильтрация, селекция, экранировка);*

общие требования к информативному сигналу при ослаблении

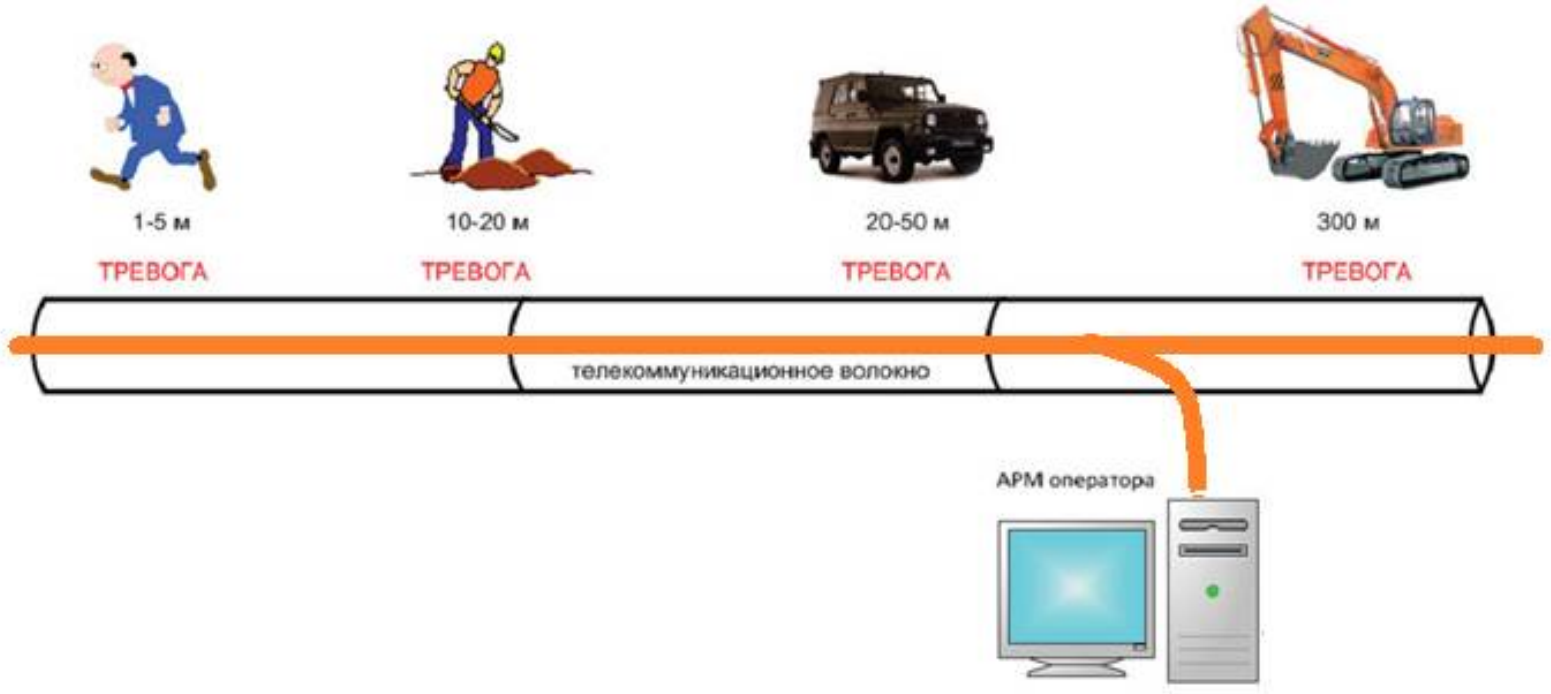
$$P_{signal} + P_{noise} < P_{sense} \quad \text{и/или} \quad SNR = P_{signal} / P_{noise} < 1 \ (0\ dB)$$



7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- **Методы защиты информации связаны с информативным сигналом и включают мероприятия/действия направленные на**

- *ограничение доступа к информативному сигналу путем выявление угрозы/нарушителя (мониторинг, контроль, выявление);*



7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- *ограничение доступа к информативному сигналу путем выявление угрозы/нарушителя (мониторинг, контроль, выявление)*

- *выявление угрозы на уровне воздействия на кабель, используя измерительные возможности кабеля;*

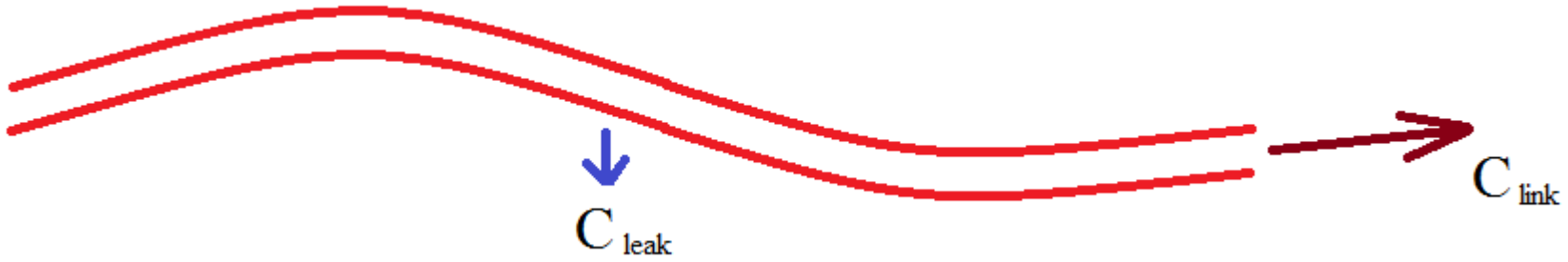
- *выявление угрозы на уровне воздействия на оптический канал, по изменению условий прохождения сигнала;*

- *выявление угрозы по изменению параметров штатных излучений;*

7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- сокрытие информационного сигнала от технических средств разведки нарушителя (стеганография, кодирование, шифрование)

- *методы связаны с представлением защищаемого сигнала в виде недоступном для нарушителя;*
- *данные методы применяются только для защиты от перехвата информационного сигнала в оптическом канале;*



❖ *будем обсуждать только физические методы сокрытия сигнала.*

7. Основные методы защиты информации от утечки через волоконно-оптические коммуникации

- сокрытие информационного сигнала от технических средств разведки нарушителя (стеганография, кодирование, шифрование);

Защита от перехвата в оптических сетях

- ✓ стеганография – сокрытие факта существования информационного сигнала;
- ✓ кодирование – представление сообщения в виде не доступном для выявления информационного сигнала без знания метода преобразования, т.е. скрывается метод кодирования;
- ✓ шифрование - обратимое преобразование информационного сообщения с помощью секретного ключа, который позволяет восстановить сообщение, т.е. скрывается ключ для восстановления сообщения;

Темы для обсуждения по лекциям 1-2

«Преимущества волоконно-оптических технологий в системах защиты информации»

Преимущества волоконно-оптических технологий в системах защиты информации;

Объект информатизации без ПЭМИНа, возможности замены электронных технологий на фотонные и волоконно-оптические технологии;

Модель угроз безопасности информации на объекте информатизации и их характеристика;

Характеристика информативного сигнала в волоконно-оптических технологиях;

Характеристика волоконно-оптических технических средств разведки;

Особенности модели нарушителя в утечке информации через волоконно-оптические коммуникации;

Понятие сценария утечки информации в структуре канала утечки информации;

Основные методы защиты информации от утечки через волоконно-оптические коммуникации.

http://www.analitika.info/

размещены дополнительные материалы по теме «ИБВОТ»