**КУРСОВАЯ РАБОТА**

**Тема: «Информационная защищенность волоконно-оптических линий связи»**

2008 г.

# Содержание

Введение

1. Особенности оптических систем связи

2. Физические принципы формирования каналов утечки информации в волоконно-оптических линиях связи

3. Доказательства уязвимости ВОЛС

4. Методы защиты информации, передаваемой по ВОЛС

4.1. Физические методы защиты

4.2. Криптографические методы защиты

Заключение

Список использованной литературы

Введение

В информационном обществе главным ресурсом является информация. Именно на основе владения информацией о самых различных процессах и явлениях можно эффективно и оптимально строить любую деятельность.
Важно не только произвести большое количество продукции, но произвести нужную продукцию в определённое время. С определёнными затратами и так далее. Поэтому в информационном обществе повышается не только качество потребления, но и качество производства; человек, использующий информационные технологии, имеет лучшие условия труда, труд становится творческим, интеллектуальным и так далее.

Информация сегодня стоит дорого и её необходимо охранять. Массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Информацией владеют и используют её все люди без исключения. Каждый человек решает для себя, какую информацию ему необходимо получить, какая информация не должна быть доступна другим и т.д. Человеку легко, хранить информацию, которая у него в голове, а как быть, если информация занесена в «мозг машины», к которой имеют доступ многие люди.

Для предотвращения потери информации разрабатываются различные механизмы её защиты, которые используются на всех этапах работы с ней. Защищать от повреждений и внешних воздействий надо и устройства, на которых хранится секретная и важная информация, и каналы связи.

Повреждения могут быть вызваны поломкой оборудования или канала связи, подделкой или разглашением секретной информации. Внешние воздействия возникают как в результате стихийных бедствий, так и в результате сбоев оборудования или кражи.

Для сохранения информации используют различные способы защиты:

– безопасность зданий, где хранится секретная информация;

– контроль доступа к секретной информации;

– разграничение доступа;

– дублирование каналов связи и подключение резервных устройств;

– криптографические преобразования информации;

В настоящее время самой совершенной физической средой для передачи информации, а также самой перспективной средой для передачи больших потоков информации на значительные расстояния считается оптическое волокно.

В связи с чрезвычайно широким распространением оптоволокна в качестве среды передачи довольно актуальной является проблема его защищенности от несанкционированного съема информации.

Целью данной работы является описание основных методов скрытого съема информации и основных способов защиты передаваемой по ВОЛС информации.

# 1. Особенности оптических систем связи

Волоконно-оптические линии связи – это вид связи, при котором информация передается по оптическим диэлектрическим волноводам, известным под названием "оптическое волокно".

В последнее время одним из наиболее перспективных и развивающихся направлений построения сетей связи в мире являются волоконно-оптические линии связи (далее – ВОЛС). В области систем передачи информации с большой информационной емкостью и высокой надежностью работы ВОЛС не имеют конкурентов. Это объясняется тем, что они значительно превосходят проводные по таким показателям, как пропускная способность, длина регенерационного участка, а также помехозащищенность.

Считается, что ВОЛС, в силу особенностей распространения электромагнитной энергии в оптическом волокне (далее – ОВ), обладают повышенной скрытностью [3]. Это объясняется тем, что оптическое излучение, являющее носителем информации, распространяется в ОВ согласно закону полного внутреннего отражения, а за ОВ электромагнитное излучение экспоненциально спадает.

Понятие ВОЛС является собирательным [4]. Оно включает приемники, передатчики оптического сигнала, оптический тракт, регенераторы и иное оборудование. В связи с этим волоконно-оптическую линию можно разделить на локальные и распределенные участки. *Локальные участки*, включающие в себя модуляторы, оптические передатчики и приемники, регенераторы, наиболее защищены от несанкционированного съема в виду локализованной области их расположения. *Распределенные участки* (волоконно-оптические тракты) обладают наибольшей протяженностью и, соответственно, наименьшей защищенностью от несанкционированного съема. В отличие от всех других сред передачи информации, для формирования каналов утечки на участках оптического тракта, как правило, требуют прямого доступа к оптоволокну и специальных мер отвода части излучения из оптоволокна или регистрации прохождения излучения.

Таблица 1.1

Основные преимущества и недостатки волоконно-оптических линий связи

|  |  |
| --- | --- |
| **Преимущества волоконной оптики** | **Недостатки волоконной оптики** |
| **Широкополосность ВОЛС** оптических сигналов, обусловленная чрезвычайно высокой частотой несущей (F0 = 1014 Гц). Это означает, что по ВОЛС можно передавать информацию со скоростью порядка 1012 бит/с.**Очень малое затухание ВОЛС** светового сигнала в волокне, что позволяет строить ВОЛС длиной до 100 км и более без регенерации сигналов. **Устойчивость ВОЛС к электромагнитным помехам** со стороны окружающих медных кабельных систем, электрического оборудования (линии электропередачи, электродвигательные установки и т.д.) и погодных условий. **Высокая** з**ащищенность ВОЛС от несанкционированного доступа** – информацию, передающуюся по волоконно-оптическим линиям связи, практически нельзя перехватить неразрушающим способом. **Электробезопасность ВОЛС**Из-за отсутствия искрообразования оптическое волокно повышает взрыво- и пожаробезопасность сети, что особенно актуально на химических, нефтеперерабатывающих предприятиях, при обслуживании технологических процессов повышенного риска. **Невысокая стоимость ВОЛС** – волокно изготовлено из кварца, основу которого составляет двуокись кремния, широко распространенного, а потому недорогого материала, в отличие от меди. **Долговечность ВОЛС** – срок службы составляет не менее 25 лет. | **Относительно высокая стоимость активных элементов ВОЛС**, преобразующих электрические сигналы в свет и свет в электрические сигналы. **Относительно высокая стоимость сварки оптических волокон** – для этого требуется прецизионное, а потому дорогое, технологическое оборудование. Как следствие, при обрыве оптического кабеля затраты на восстановление ВОЛС выше, чем при работе с медными кабелями. |

Преимущества от применения волоконно-оптических линий связи (ВОЛС) настолько значительны, что, несмотря на перечисленные недостатки оптического волокна, эти линии связи все шире используются для передачи информации.

Основные электронные компоненты системы оптической связи изображены на табл. 1.1.

 Табл. 1.1.

|  |  |  |
| --- | --- | --- |
| *Электрический сигнал* | *Оптический интерфейс* | *Электрический сигнал* |
|  транcивер **=>** E/0  | **Х---*х*---*х*---*х*---Х**Х - оптический соединитель--- - синтетический кабель***х*** - места сварки | Трансивер0/E **=>** |

# 2. Физические принципы формирования каналов

# утечки информации в волоконно-оптических

# линиях связи

Изначально ВОЛС имеют более высокую степень защищенности информации от несанкционированного доступа, чем какие-либо другие линии связи [4]. Это связано с физическими принципами передачи информации, которые основываются на модуляции света, распространяющегося в оптическом волноводе. Электромагнитное излучение оптического диапазона выходит за пределы волокна на расстояния не более длины волны (менее 2 мкм) при ненарушенном канале связи, поэтому в окружающем волновод пространстве отсутствуют поля на оптических частотах несущие информацию.

В современных ВОЛС основной способ передачи информации основан на модуляции интенсивности света. Это наиболее простой способ передачи информации по ВОЛС, поэтому каналы утечки информации напрямую связаны с интенсивностью светового потока. Волоконно-оптический кабель представляет собой сложную конструкцию с несколькими слоями покрытия оптического волновода. Параметры его таковы, что в окружающем кабель пространстве информативное оптическое излучение практически не создает каких-либо электромагнитных полей диапазона близкого к частоте модуляции. Вследствие этого для формирования канала утечки информации требуется *физический контакт* с оптическим каналом передачи информации – оптоволокном. Это требование является одним из главных факторов защищенности информации в волоконно-оптических системах передачи. В дальнейшем мы будем обсуждать только формирование каналов утечки информации, основанное на оптическом контакте с оптоволокном без нарушения канала связи. Также не обсуждаются возможности утечки информации на элементах волоконно-оптической линии связи в местах соединения, разветвления, ретрансляции и других, которые находятся под контролем специальных средств.

Формирование каналов утечки информации из ВОЛС можно разделить на три типа, которые связанны с возможными особенностями распространения света в волоконно-оптических линиях связи [4].

*1.* ***Нарушение полного внутреннего отражения***

Первый способ несанкционированного доступа связан с отводом части светового потока из оптического волновода при нарушении полного внутреннего отражения. В идеальном случае свет не выходит из оптического волокна вследствие полного внутреннего отражения на его границах. Любые отклонения в распространении света приводят к выходу части излучения из волновода, которое образует канал утечки информации. Варианты формирования каналов утечки информации из ВОЛС при нарушении полного внутреннего отражения можно разделить по виду воздействия на оптоволокно:

– механическое воздействие;

Простейший пример механического воздействия на волокно – *изгиб*.

При изгибе волокна локальная концентрация механических напряжений вызывает уменьшение угла падения света на границе, который может оказаться меньше предельного угла, и как следствие – нарушение полного внутреннего отражения, то есть часть светового потока выходит из оптоволокна.

Максимальный радиус изгиба *R*, при котором наблюдается побочное излучение в точке изгиба световода с диаметром сердцевины *d*, связанное с нарушением полнового внутреннего отражения, определяется выражением:

*R ≤ d n2 , (2.1)*

 *n1 – n2*

здесь *n*1, *n*2 – показатели преломления сердцевины и оболочки световода.

Оценка радиуса изгиба для многомодового волокна с диаметром сердцевины *d* = 50 мкм и оптической оболочки *D* = 125 мкм (*n1* =1,481, *n2* = 1,476) показывает, что при *R* ≤ 3,5 см начинает наблюдаться сильное прохождение излучения в точке изгиба (до 80% значения интенсивности основного светового потока в оптоволокне). Надо отметить, что при оценке изгиба не учитывалось форма светового потока, цилиндрическая форма преломляющей поверхности и другие эффекты, изменяющие показатель преломления оптоволокна, например, фотоупругий эффект. Их вклад значительно меньше.

Кроме рассмотренного случая изгиба волокна, нарушение полного внутреннего отражения при механическом воздействии возможно и при локальном давлении на оптоволокно, что вызывает неконтролируемое рассеяние (в отличие от изгиба) в точке деформации.

*–* акустическоевоздействие;

*Акустическое воздействие* на оптическое волокно также изменяет угол падения. При этом в сердцевине оптоволокна создается дифракционная решетка периодического изменения показателя преломления, которая вызвана воздействием звуковой волны. Электромагнитная волна отклоняется от своего первоначального направления, и часть её выходит за пределы канала распространения. Физическое явление, с помощью которого возможно решить поставленную задачу, является дифракция Брэгга на высокочастотном звуке (*f* > 10 МГц), длина волны *L* которого удовлетворяет условию:

λL

\_\_\_\_> 1, (2.2)

Λ2

где *l* – длина волны электромагнитного излучения, *L* – ширина области распространения звуковой волны, *Λ* – длина волны действующего звукового излучения. Деформации, создаваемые упругой волной, формируют периодическое изменение показателя преломления внутри оптоволокна, которое для света является дифракционной решеткой .

Максимальный угол отклонения единственного наблюдаемого дифракционного максимума равен двум углам Брэгга (2*QB*). Частота отклоненной электромагнитной волны приблизительно равна частоте основного информационного потока. Вычисления показывают, что для многомодового оптоволокна с параметрами (*d*/*D*)=(50/125) при акустическом воздействии с длиной волны звука *Λ* = 10 мкм и длине взаимодействия *L* = 10-3 м максимальный угол отклонения от первоначального направления распространения составляет 5 градусов.

Даже при невысоких интенсивностях звуковой волны выводимое электромагнитное излучение достаточно велико для регистрации его современными фотоприемниками. При фиксированной интенсивности звука, путем изменения области озвучивания *L* можно добиться максимального значения интенсивности в дифракционном максимуме, тем самым увеличить интенсивность света отводимого в канал утечки.

– оптическое туннелирование света, т.е. приведение в оптический контакт с волокном другого оптического волокна с показателем преломления равным или большим основного, что приводит к “захвату” части информационного светового потока без обратного рассеянного излучения;

Явление оптического туннелирования состоит в прохождении оптического излучения из среды показателем преломления *n1* через слой с показателем преломления *n2* меньшим *n1* в среду с показателем преломления *n3* при углах падения больших угла полного внутреннего отражения. На принципах оптического теннелирования в интегральной и волоконной оптике создаются такие устройства как оптический ответвитель, оптофоны, волоконно-оптические датчики физических величин.

Формирование канала утечки оптическим туннелированием; *n1*, *n2* – показатели преломления сердцевины и оболочки оптоволокна, *n3* – показатель преломления дополнительного оптоволокна.

Интенсивность излучения переходящего в дополнительный волновод определяется выражением:

*I = I0  sin 2 (k . S),* (2.3)

где *k* – коэффициент связи оптических волокон, *S* – длина оптического контакта двух волокон. Максимум значения коэффициента связи достигается при нулевом расстоянии между оболочкой и дополнительным оптоволокном (*l*=0) и показателе преломления дополнительного волокна *n3* = *n1*.

Излучение периодически переходит из одного волновода в другой.

Отличительной особенностью оптического туннелирования является отсутствие обратно рассеянного излучения, что затрудняет детектирование несанкционированного доступа к каналу связи. Этот способ съема информации наиболее скрытный.

– специальные напыляемые покрытия и оптические смазки основного оптоволокна, которые приводят к эффекту интерференции света в тонких пленках, что позволяет выводить часть излучения также без обратного рассеяния;

– воздействие стационарных электромагнитных полей, что вызывает изменение оптических свойств на границе сердцевина – оболочка оптоволокна, которое приводит к нарушению полного внутреннего отражения.

Надо отметить, несмотря на то, что изменения значения предельного угла, вызываемое как механически напряжениями, так и электрическим полем малы, но комплексное воздействие с другими способами может привести к эффективному способу формирования канала утечки. Рассмотренные выше методы обладают одним недостатком, который позволяет легко фиксировать каналы утечки, созданные на их основе. Это определяется значительным обратным рассеянием света в местах каналов утечки. С помощью рефлектометрии обратно рассеянного света такие подключения легко детектируются с высоким пространственным и временным разрешением.

*2.* ***Нарушение отношения показателей преломления***

Растяжение представляет собой механическое воздействие без изменения формы волокна.

Растяжение волокна вызывает изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптоволокна.

С учетом того, что плавленый кварц выдерживает большие напряжения (до 106 Па в идеальном состоянии), то, прикладывая большие механические напряжения к оптоволокну, можно добиться изменения предельного угла на величину, достаточную для вывода части интенсивности основного информационного потока за пределы оптического волокна.

К способам, вызывающим изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптоволокна путем механического напряжения, также относится и скручивание оптоволокна.

*3.* ***Регистрация рассеянного излучения***

Современные оптические волноводы обладают очень маленькими потерями (вплоть до 0,2 дБ/км и менее на длине волны 1,55 мкм) – это позволяет передавать информацию на значительные расстояния без необходимости усиления сигнала. Расстояния между участками ретрансляции составляет более 100 км, что требует генерации световых импульсов значительной мощности. Высокие мощности входного светового потока создают значительное по величине рассеяние на ближайших к ретрансляторам участках, которые можно использовать для формирования каналов утечки информации. Современные приемники оптического излучения позволяют регистрировать световые потоки состоящие практически из одного фотона с временным разрешением менее 1 нс, что соответствует регистрации оптической мощности излучения менее 10-10 Вт.

Рассеянное излучение позволяет сформировать каналы утечки информации, основанные на следующих физических принципах:

– прямое измерение рассеянного излучения на длинах волн носителя информации ;

– регистрация рассеянного излучения на комбинационных частотах;

– специальная “обработка” оптоволокна внешними полями (тепловым, электромагнитным, радиационным), с целью увеличения интенсивности рассеянного излучения.

С помощью внешнего воздействия можно усилить потери в световоде на локальных участках формирования каналов утечки, что вызовет увеличение сигнала утечки.

*4.* ***Параметрические методы регистрации проходящего излучения***

Оптическое излучение, являющееся носителем информации, при распространении по оптоволокну вызывает изменение его физических свойств. Модуляцию свойств оптоволокна в зависимости от интенсивности световых импульсов можно регистрировать специальными высокочувствительными устройствами. Изменение свойств оптоволокна является основой для формирования канала утечки информации. Среди них можно выделить следующие параметры оптоволокна, модулируемые световым потоком:

-     показатель преломления;

-     показатель поглощения при прохождении света;

-     малые изменения геометрических размеров (фотоупругий эффект);

-     регистрация модуляции свойств поверхности волокна.

Существующая техника измерений позволяет регистрировать очень малые изменения свойств волокна. В частности, применение спектроскопии потерь позволяет регистрировать незначительное изменение показателя поглощения, которое вызывается информационным потоком света.

# В заключение надо отметить, что существует много других способов несанкционированного доступа и способов съема информации с оптоволокна. Это опровергает утверждение о невозможности формирования канала утечки из оптического волновода, которое прослеживается в повседневной жизни и в российских нормативных документах. В документе закреплено, что при использовании волоконно-оптических линий связи не требуется шифрование конфиденциальной информации,  в отличии от других каналов передачи информации. Особенностью волоконно-оптических телекоммуникаций является необходимость физического контакта с линией связи для формирования канала утечки.

# 3. Доказательства уязвимости ВОЛС

Почти все преимущества ВОЛС не вызывают сомнений, но тезис о хорошей защищенности волоконно-оптической линии связи требует разъяснений [2]. Определимся, что применительно к  ВОЛС это означает невозможность перехвата информации без физического нарушения целостности волоконно-оптической линии и отсутствие паразитных наводок.

В Центре компетенций компании «ОТ» был собран стенд для исследования возможной уязвимости ВОЛС, представляющий собой модель распределенного центра обработки данных. Оптическая магистраль имитировалась кросс-панелью с петлей из разделанного многожильного оптического кабеля для внешней проводки. В качестве перехватчика использовалось пассивное устройство типа «ответвитель-прищепка» FOD 5503. Такое устройство создает микроизгиб в волокне и ответвляет сигнал, который может быть получен через имеющийся патч-корд. В процессе тестирования удалось перехватить сигнал, передаваемый в одном направлении.

Следует отметить, что описанные действия можно выполнить без применения специализированного дорогостоящего инструмента (приемлемая стоимость средств перехвата позволяет их использовать не только организациям, но и частным лицам) и за сравнительно небольшое время. Линии связи остались без разрывов: в процессе подготовки стенда кабель был освобожден лишь от внешних защитных оболочек, а волокна находились в защитном цветном буфере толщиной 250 мкм.

Из результатов эксперимента следует такой вывод: уязвимость ВОЛС доказана на практике. А потому в связи с возможностью компрометации передаваемых данных или их модификации необходимо использовать средства криптографической защиты информации, передаваемой по ВОЛС.

# 4. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО

# ВОЛС

#

# **4.1. ФИЗИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ**

1. Разработка технических средств защиты от НД к информационным сигналам, передаваемым по ОВ.

Данная группа работ связана с разработкой конструкционных, механических и электрических средств защиты от НД к оптическим кабелям (ОК), муфтам и ОВ [3]. Одни из видов средств защиты этой группы построены так, чтобы затруднить механическую разделку кабеля и воспрепятствовать доступу к ОВ. Подобные средства защиты широко используются и в традиционных проводных сетях специальной связи. Также перспективным представляется использование пары продольных силовых элементов ОК, которые представляют собой две стальные проволоки, размещенные симметрично в полиэтиленовой оболочке, и используемые для дистанционного питания и контроля датчиков, установленных в муфтах, и контроля НД. Целесообразно также применение комплекта для защиты места сварки, который заполняет место сварки непрозрачным затвердевающим гелем. Одним из предложенных методов защиты является использование многослойного оптического волокна со специальной структурой отражающих и защитных оболочек. Конструкция такого волокна представляет собой многослойную структуру с одномодовой сердцевиной. Подобранное соотношение коэффициентов преломления слоев позволяет передавать по кольцевому направляющему слою многомодовый контрольный шумовой оптический сигнал. Связь между контрольным и информационным оптическими сигналами в нормальном состоянии отсутствует. Кольцевая защита позволяет также снизить уровень излучения информационного оптического сигнала через боковую поверхность ОВ (посредством мод утечки, возникающих на изгибах волокна различных участков линии связи). Попытки проникнуть к сердцевине обнаруживаются по изменению уровня контрольного (шумового) сигнала или по смешению его с информационным сигналом. Место НД определяется с высокой точностью с помощью рефлектометра.

2. Разработка технических средств контроля НД к информационному сигналу, передаваемому по ОВ.

Вторая группа работ в этом направлении связана с мониторингом "горячих" волокон и разработкой различных устройств контроля параметров оптических сигналов на выходе ОВ и отраженных оптических сигналов на входе ОВ.

Основой системы фиксации НД является система диагностики состояния (далее – СДС) оптического тракта. СДС можно построить с анализом либо прошедшего через оптический тракт сигнала, либо отраженного сигнала (рефлектометрические СДС).

*СДС с анализом прошедшего сигнала* является наиболее простой диагностической системой. На приемной части ВОЛС анализируется прошедший сигнал. При НД происходит изменение сигнала, это изменение фиксируется и передается в блок управления ВОЛС.

При использовании анализатора коэффициента ошибок на приемном модуле ВОЛС СДС реализуется при минимальных изменениях аппаратуры ВОЛС, так как практически все необходимые модули имеются в составе аппаратуры ВОЛС. Недостатком является относительно низкая чувствительность к изменениям сигнала.

*Основным недостатком* СДС с анализом прошедшего сигнала является отсутствие информации о координате появившейся неоднородности, что не позволяет проводить более тонкий анализ изменений режимов работы ВОЛС (для снятия ложных срабатываний системы фиксации НСИ).

*СДС с анализом отраженного сигнала* (рефлектометрические СДС) позволяют в наибольшей степени повысить надежность ВОЛС.

Для контроля величины мощности сигнала обратного рассеяния в ОВ в настоящее время используется метод импульсного зондирования, применяемый во всех образцах отечественных и зарубежных рефлектометров.

Суть его состоит в том, что в исследуемое ОВ вводится мощный короткий импульс, и затем на этом же конце регистрируется излучение, рассеянное в обратном направлении на различных неоднородностях, по интенсивности которого можно судить о потерях в ОВ, распределенных по его длине на расстоянии до 100 - 120 км. Начальные рефлектограммы контролируемой линии фиксируются при разных динамических параметрах зондирующего сигнала в памяти компьютера и сравниваются с соответствующими текущими рефлектограммами. Локальное отклонение рефлектограммы более чем на 0,1 дБ свидетельствует о вероятности попытки несанкционированного доступа к ОВ в данной точке тракта.

*Основными недостатками* СДС с анализом отраженного сигнала на основе метода импульсной рефлектометрии являются следующие:

– при высоком разрешении по длине оптического тракта (что имеет важное значение для обнаружения локальных неоднородностей при фиксации НД) значительно снижается динамический диапазон рефлектометров и уменьшается контролируемый участок ВОЛТ ;

– мощные зондирующие импульсы затрудняют проведение контроля оптического тракта во время передачи информации, что снижает возможности СДС, либо усложняет и удорожает систему диагностики;

– источники мощных зондирующих импульсов имеют ресурс, недостаточный для длительного непрерывного контроля ВОЛС;

– специализированные источники зондирующего оптического излучения, широкополосная и быстродействующая аппаратура приемного блока рефлектометров значительно удорожает СДС.

4.2. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ

***Краткий обзор криптографических методов защиты***

1. Метод, основанный на использовании кодового зашумления передаваемых сигналов. При реализации этого метода применяются специально подобранные в соответствии с требуемой скоростью передачи коды, размножающие ошибки. Даже при небольшом понижении оптической мощности, вызванном подключением устройства съема информации к ОВ, в цифровом сигнале на выходе ВОЛС резко возрастает коэффициент ошибок, что достаточно просто зарегистрировать средствами контроля ВОЛС.

2. Метод, основанный на использовании пары разнознаковых компенсаторов дисперсии на ВОЛС. Первый компенсатор вводит в линию диспергированный сигнал, а на приемном конце второй компенсатор восстанавливает форму переданного сигнала.

3. Использование режима динамического (детерминированного) хаоса, который позволяет обеспечить передачу информации с псевдохаотически изменяющимися частотой и амплитудой несущей. В результате выходной сигнал внешне является шумоподобным, что затрудняет расшифровку.

4. Методы квантовой криптографии – соединяют достижения криптографической науки с квантовой механикой и квантовой статистикой. Они потенциально обеспечивают высокую степень защиты от перехвата информации на линии связи за счет передачи данных в виде отдельных фотонов, поскольку неразрушающее измерение их квантовых состояний в канале связи перехватчиком невозможно, а факт перехвата фотонов из канала может быть выявлен по изменению вероятностных характеристик последовательности фотонов.

***Пример использования криптографического метода защиты***

Для криптографической защиты следует выбрать средства, которые не вносят существенных временных задержек при криптографическом преобразовании передаваемой/принимаемой информации и обеспечивают шифрование/расшифровку для всего диапазона скоростей передачи данных, характерного для каналов SONET/SDH [2].

В качестве таких средств были выбраны устройства SafeEnterprise SONET Encryptor компании SafeNet. Они осуществляют шифрование всего трафика SDH на канальном уровне на скорости от ОС-3 (155,5 Мбит/с) до ОС-48 (2,4 Гбит/с). Их применение прозрачно для протоколов вышележащих уровней и, следовательно, не должно вносить существенной задержки в сигнал. Это предположение было решено проверить серией тестов.

Для проведения новой серии испытаний был собран стенд, имитирующий нагрузку на магистраль передачи данных между основным ЦОД и резервным. Оборудование шифрования трафика SafeEnterprise SONET Encryptor OC3/OC12 подключалось к магистрали SDH и обеспечивало прозрачное для конечных устройств шифрование трафика. Для тестирования использовались встроенные средства OS Sun Solaris, которые создавали нагрузку на дисковую подсистему и измеряли ее параметры. Параметры нагрузки варьировались как по видам нагрузки, так и размерам блока передаваемых данных (8 Kбайт и 1 Mбайт). Измерения последовательно проводились для двух конфигураций испытательного стенда: канал 100 Мбит/c с шифрованием и канал с той же пропускной способностью без шифрования.

Сравнение результатов тестов позволило сделать такой вывод: использование аппаратуры шифрования уменьшает пропускную способность канала на 2,46–4,32% при операциях чтения данных с диска и не более чем на 6,15% при операциях записи данных на диск. Таким образом, применение устройств канального шифрования SafeEnterprise SONET Encryptor OC3/OC12 незначительно уменьшает пропускную способность канала SDH (снижение производительности при шифровании по протоколу IPSec составляет, по разным оценкам, от 7 до 30%). Устройства шифрования компании SafeNet позволяют осуществлять криптографическую защиту передаваемых данных без изменения схемы IP-адресации и маршрутизации.

# Заключение

Все перечисленные выше методы защиты и их комбинации могут обеспечивать безопасность информации лишь в рамках известных моделей НД.

При этом эффективность систем защиты определяется как открытием новых, так и совершенствованием технологий НСИ, использующих уже известные физические явления.

С течением времени противник может освоить новые методы перехвата, потребуется дополнять защиту, что не свойственно криптографическим методам защиты, которые рассчитываются на достаточно длительный срок.

В заключение следует отметить, что необходимость практического внедрения и эффективного использования защищенных ВОЛС в сетях связи является задачей сегодняшнего дня.

# Список использованной литературы

### 1. Спирин А. А.. Введение в технику волоконно-оптических сетей.

#### http://www.citforum.ru/nets/optic/optic1.shtml

#### 2. Филатенков А.. Доказательства уязвимости ВОЛС.

#### http://www.osp.ru/nets/2008/09/5300705/

3. Манько А., Каток В., Задорожний М.. Защита информации на волоконно-оптических линиях связи от несанкционированного доступа.

http://bezpeka.com/files/lib\_ru/217\_zaschinfvolopt.zip

# 4. Гришачев В.В., Кабашкин В.Н., Фролов А.Д.. Физические принципы формирования каналов утечки информации в ВОЛС.

#### http://it4business.ru/itsec/FizicheskiePrincipyFormirovanijaKanalovUtechkiInformaciiVVolokonnoOpticheskixLinijaxSvjazi

#### 5. Убайдуллаев Р.Р. Волоконно-оптические сети. М., Эко-Трендз, 2000.

#### 6. Фриман Р. Волоконно-оптические системы связи. М., Техносфера; 2004 г.

#### 7. Иоргачев Д.В., Бондаренко О.В. Волоконно-оптические кабели и линии связи. М., 1998.

#### 8. Новиков Ю.В., Карпенко Д.Г. Волоконно-оптическая сеть. М, 1995.

#### 9. Семенов А. Б. Волоконно-оптические подсистемы современных СКС. М, 1994.

#### 10. Северин В.А. Средства защиты в сетях. Комплексная защита информации на предприятии. Учебник для вузов. М, 1999.

#### 11. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность .

#### 12. Домарев В. В. Защита информации и безопасность компьютерных систем 1999.

#### 13. Ярочкин В. И. Информационная безопасность. Учебник для вузов. М, 2003.