МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине

ЗАЩИТА ИНФОРМАЦИИ В ОПТОВОЛОКОННЫХ ЛОКАЛЬНЫХ СЕТЯХ

Направление подготовки	**10.03.01 Информационная безопасность**
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск, 2020 г.

ВВЕДЕНИЕ

Методические указания предназначены для студентов специальности 090900.62 «Комплексная защита объектов информатизации» очной формы обучения и содержат материалы и задания для выполнения лабораторных работ по дисциплине «Защита информации в оптоволоконных локальных сетях»

СОДЕРЖАНИЕ

1. Оптические системы связи. Параметры ВОЛС.

1.1*Волоконно-оптический кабель*

Самой высокой пропускной способностью среди всех существующих средств связи обладает оптическое волокно (диэлектрические волноводы).

Волоконно-оптические кабели применяются для создания **ВОЛС** – волоконно-оптических линий связи, способных обеспечить самую высокую скорость передачи информации (в зависимости от типа используемого активного оборудования скорость передачи может составлять десятки гигабайт и даже терабайт в секунду).

Кварцевое стекло, являющееся несущей средой ВОЛС, помимо уникальных пропускных характеристик, обладает ещё одним ценным свойством – малыми потерями и нечувствительностью к электромагнитным полям. Это выгодно отличает его от обычных медных кабельных систем.

Данная система передачи информации, как правило, используется при постройке рабочих объектов в качестве внешних магистралей, объединяющих разрозненные сооружения или корпуса, а также многоэтажные здания.

Она может использоваться и в качестве внутреннего носителя структурированной кабельной системы (СКС), однако законченные СКС полностью из волокна встречаются реже – в силу высокой стоимости строительства оптических линий связи.

Применение ВОЛС позволяет локально объединить рабочие места, обеспечить высокую скорость загрузки Интернета одновременно на всех машинах, качественную телефонную связь и телевизионный приём.

Профессиональное проектированиеи профессиональный монтаж ВОЛС обеспечивает целый ряд существенных преимуществ:

- *Высокая пропускная способность* за счёт высокой несущей частоты. (потенциальная возможность оптического волокна – несколько терабит информации за 1 секунду).

- *Низкий уровень шума.* Волоконно-оптический кабель отличается низким уровнем шума, что положительно сказывается на его пропускной способности и возможности передавать сигналы различной модуляции.

- *Пожаробезопасность*. В отличие от других систем связи, ВОЛС может использоваться безо всяких ограничений на предприятиях повышенной опасности, в частности на нефтехимических производствах, благодаря отсутствию искрообразования.

- *Низкий уровень затухания светового сигнала.* Благодаря малому затуханию светового сигнала оптические системы могут объединять рабочие участки на значительных расстояниях (более 100 км) без использования дополнительных ретрансляторов (усилителей).

- *Информационная безопасность.* Волоконно-оптическая связь обеспечивает надёжную защиту от несанкционированного доступа и перехвата конфиденциальной информации. Такая способность оптики

объясняется отсутствием излучений в радиодиапазоне, а также высокой чувствительностью к колебаниям. В случае попыток прослушки встроенная система контроля может отключить канал и предупредить о подозреваемом взломе. Именно поэтому ВОЛС активно используют современные банки, научные центры, правоохранительные организации и прочие структуры, работающие с секретной информацией.

- *Высокая надёжность и помехоустойчивость системы.* Волокно, будучи диэлектрическим проводником, не чувствительно к электромагнитным излучениям, не боится окисления и влаги.

- *Экономичность.* Несмотря на то, что создание оптических систем в силу своей сложности дороже, чем традиционных СКС, в общем итоге их владелец получает реальную экономическую выгоду. Оптическое волокно, которое изготавливается из кварца, стоит примерно в 2 раза дешевле медного кабеля, кроме того дополнительно при строительстве обширных систем можно сэкономить на усилителях. Если при использовании медной пары ретрансляторы нужно ставить через каждые несколько километров, то в ВОЛС это расстояние составляет не менее 100 км. При этом скорость, надёжность и долговечность традиционных СКС значительно уступают оптике.

- *Срок службы.*Срок службы ВОЛС составляет полрядка четверти века. Через 25 лет непрерывного использования в несущей системе увеличивается затухание сигналов.

- *Вес и габариты.* Если сравнивать медный и оптический кабель, то при одной и той же пропускной способности второй будет весить примерно в 4 раза меньше, а его объём даже при использовании защитных оболочек будет меньше, чем у медного, в несколько раз.

- *Перспективы.* Использование волоконно-оптических линий связи позволяет легко наращивать вычислительные возможности локальных сетей благодаря установке более быстродействующего активного оборудования, причем без замены коммуникаций.

Как уже было сказано выше, волоконно-оптические кабели (ВОК) используются для передачи сигналов вокруг или между зданий, а также внутри объектов.

При построении вешних коммуникационных магистралей предпочтение отдаётся оптическим кабелям, а внутри зданий (внутренние подсистемы) наравне с ними используется традиционная витая пара. Таким образом, различают ВОК для внешней (outdoor cables) и внутренней (indoor cables) прокладки.

К отдельному виду относятся соединительные кабели: внутри помещений они используются в качестве соединительных шнуров и коммуникаций горизонтальной разводки – для оснащения отдельных рабочих мест, а снаружи – для объединения зданий.

Монтаж волоконно-оптического кабеля осуществляется с помощью специальных инструментов и приборов.

1.2 *Оптические соединители. Электронные компоненты систем оптической связи*

ВОЛС - это вид связи, при котором информация передается по оптическим диэлектрическим волноводам, известным под названием «оптическое волокно».

Оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, а также самой перспективной средой для передачи больших потоков информации на значительные расстояния. Основания так считать вытекают из ряда особенностей, присущих оптическим волноводам.

Физические особенности:

- *Широкополосность.* Широкополосность оптических сигналов, обусловлена чрезвычайно высокой частотой несущей ($F_o=10^{14}$ Гц). Это означает, что по оптической линии связи можно передавать информацию со скоростью порядка 10^{12} бит/с или Терабит/с. Говоря другими словами, по одному волокну можно передать одновременно 10 миллионов телефонных разговоров и миллион видеосигналов. Скорость передачи данных может быть увеличена за счет передачи информации сразу в двух направлениях, так как световые волны могут распространяться в одном волокне независимо друг от друга. Кроме того, в оптическом волокне могут распространяться световые сигналы двух разных поляризаций, что позволяет удвоить пропускную способность оптического канала связи. На сегодняшний день предел по плотности передаваемой информации по оптическому волокну не достигнут.

- *Скорость затухания.* Очень малое (по сравнению с другими средами) затухание светового сигнала в волокне. Лучшие образцы российского волокна имеют затухание 0.22 дБ/км на длине волны 1.55 мкм, что позволяет строить линии связи длиной до 100 км без регенерации сигналов. Для сравнения, лучшее волокно Sumitomo на длине волны 1.55 мкм имеет затухание 0.154 дБ/км. В оптических лабораториях США разрабатываются еще более «прозрачные», так называемые фтороцирконатные волокна с теоретическим пределом порядка 0,02 дБ/км на

длине волны 2.5 мкм. Лабораторные исследования показали, что на основе таких волокон могут быть созданы линии связи с регенерационными участками через 4600 км при скорости передачи порядка 1 Гбит/с.

*Технические особенности***:**

1. Волокно изготовлено из кварца, основу которого составляет двуокись кремния, широко распространенного, а потому недорогого материала, в отличие от меди.

2. Оптические волокна имеют диаметр около 100 мкм, то есть очень компактны и легки, что делает их перспективными для использования в авиации, приборостроении, в кабельной технике.

3. Стеклянные волокна - не металл, при строительстве систем связи автоматически достигается гальваническая развязка сегментов. Применяя особо прочный пластик, на кабельных заводах изготавливают самонесущие подвесные кабели, не содержащие металла и тем самым безопасные в электрическом отношении. Такие кабели можно монтировать на мачтах существующих линий электропередач, как отдельно, так и встроенные в фазовый провод, экономя значительные средства на прокладку кабеля через реки и другие преграды.

4. Системы связи на основе оптических волокон устойчивы к электромагнитным помехам, а передаваемая по световодам информация защищена от несанкционированного доступа. Волоконно-оптические линии связи нельзя подслушать неразрушающим способом. Всякие воздействия на волокно могут быть зарегистрированы методом мониторинга (непрерывного контроля) целостности линии. Теоретически существуют способы обойти защиту путем мониторинга, но затраты на реализацию этих способов будут столь велики, что превзойдут стоимость перехваченной информации.

Существует способ скрытой передачи информации по оптическим линиям связи. При скрытой передаче сигнал от источника излучения модулируется не по амплитуде, как в обычных системах, а по фазе. Затем сигнал смешивается с самим собой, задержанным на некоторое время, большее, чем время когерентности источника излучения.

При таком способе передачи информация не может быть перехвачена амплитудным приемником излучения, так как он зарегистрирует лишь сигнал постоянной интенсивности.

Для обнаружения перехватываемого сигнала понадобится перестраиваемый интерферометр Майкельсона специальной конструкции. При этом интерференционная картина может быть ослаблена как 1/2N, где N - количество сигналов, одновременно передаваемых по оптической системе связи. Кроме того, можно распределить передаваемую информацию по множеству сигналов или передавать несколько шумовых сигналов, ухудшая этим условия перехвата информации. В этом случае потребуется значительный отбор мощности из волокна, чтобы несанкционированно принять оптический сигнал, а это вмешательство легко зарегистрировать системами мониторинга.

5. Другое важное свойство оптического волокна –его долговечность. Время жизни волокна, то есть сохранение им своих свойств в определенных пределах, превышает 25 лет, что позволяет проложить оптико-волоконный кабель один раз и, по мере необходимости, наращивать пропускную

способность канала путем замены приемников и передатчиков на более быстродействующие.

В волоконной технологии имеются и свои недостатки:

1. При создании линии связи требуются высоконадежные активные элементы, преобразующие электрические сигналы в свет и свет в электрические сигналы. Необходимы также оптические коннекторы (соединители) с малыми оптическими потерями и большим ресурсом на подключение-отключение. Точность изготовления таких элементов линии связи должна соответствовать длине волны излучения, то есть погрешности должны быть порядка доли микрона. Поэтому производство таких компонентов оптических линий связи очень дорогостоящее.

2. Другой недостаток заключается в том, что для монтажа оптических волокон требуется прецизионное, а потому дорогое, технологическое оборудование.

3. Как следствие, при аварии (обрыве) оптического кабеля затраты на восстановление выше, чем при работе с медными кабелями.

Однако преимущества от применения ВОЛС настолько значительны, что несмотря на перечисленные недостатки оптического волокна, эти линии связи все шире используются для передачи информации.

Промышленность многих стран освоила выпуск широкой номенклатуры изделий и компонентов ВОЛС. Следует заметить, что производство компонентов ВОЛС, в первую очередь оптического волокна, отличает высокая степень концентрации. Большинство предприятий сосредоточено в США. Обладая главными патентами, американские фирмы (в первую очередь это относится к фирме "CORNING") оказывают влияние на производство и рынок компонентов ВОЛС во всем мире, благодаря заключению лицензионных соглашений с другими фирмами и созданию совместных предприятий.

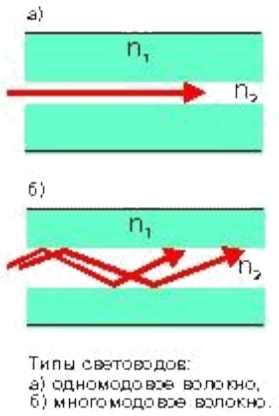
Оптическое волокно.

Важнейший из компонентов ВОЛС - оптическое волокно. Для передачи сигналов применяются два вида волокна: *одномодовое* и *многомодовое*. Свое название волокна получили от способа распространения излучения в них. Волокно состоит из сердцевины и оболочки с разными показателями преломления n1 и n2.

В одномодовом волокне диаметр световодной жилы порядка 8-10 мкм, то есть сравним с длиной световой волны. При такой геометрии в волокне может распространяться только один луч (одна мода).

В многомодовом волокне размер световодной жилы порядка 50-60 мкм, что делает возможным распространение большого числа лучей (много мод).

Оба типа волокна характеризуются двумя важнейшими параметрами: затуханием и дисперсией.



Типы световодов:
а) одномодовое волокно,
б) многомодовое волокно.

Рис. 1.

Затухание обычно измеряется в дБ/км и определяется потерями на поглощение и на рассеяние излучения в оптическом волокне.

Потери на поглощение зависят от чистоты материала, потери на рассеяние зависят от неоднородностей показателя преломления материала.

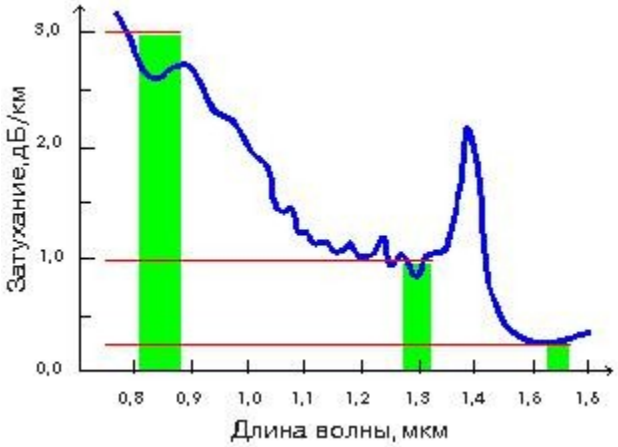


Рис. 2.

Затухание зависит от длины волны излучения, вводимого в волокно. В настоящее время передачу сигналов по волокну осуществляют в трех диапазонах: 0.85 мкм, 1.3 мкм, 1.55 мкм, так как именно в этих диапазонах кварц имеет повышенную прозрачность.

Другой важнейший параметр оптического волокна - дисперсия. Дисперсия - это рассеяние во времени спектральных и модовых составляющих оптического сигнала. Существуют три типа дисперсии: *модовая*, *материальная* и *волноводная*.

Модовая дисперсия присуща многомодовому волокну и обусловлена наличием большого числа мод, время распространения которых различно.

Материальная дисперсия обусловлена зависимостью показателя преломления от длины волны.

Волноводная дисперсия обусловлена процессами внутри моды и характеризуется зависимостью скорости распространения моды от длины волны.

Поскольку светодиод или лазер излучает некоторый спектр длин волн, дисперсия приводит к уширению импульсов при распространении по волокну и тем самым порождает искажения сигналов. При оценке

пользуются термином «полоса пропускания» - это величина, обратная к величине уширения импульса при прохождении им по оптическому волокну расстояния в 1 км. Измеряется полоса пропускания в МГц/км. Из определения полосы пропускания видно, что дисперсия накладывает ограничение на дальность передачи и на верхнюю частоту передаваемых сигналов.

Если при распространении света по многомодовому волокну, как правило, преобладает модовая дисперсия, то одномодовому волокну присущи только два последних типа дисперсии. На длине волны 1.3 мкм материальная и волноводная дисперсии в одномодовом волокне компенсируют друг друга, что обеспечивает наивысшую пропускную способность.

Затухание и дисперсия у разных типов оптических волокон различны. Одномодовые волокна обладают лучшими характеристиками по затуханию и по полосе пропускания, так как в них распространяется только один луч. Однако, одномодовые источники излучения в несколько раз дороже многомодовых. В одномодовое волокно труднее ввести излучение из-за малых размеров световодной жилы, по этой же причине одномодовые волокна сложно сращивать с малыми потерями. Оконцевание одномодовых кабелей оптическими разъемами также обходится дороже.

Многомодовые волокна более удобны при монтаже, так как в них размер световодной жилы в несколько раз больше, чем в одномодовых волокнах. Многомодовый кабель проще оконцевать оптическими разъемами с малыми потерями (до 0.3 dB) в стыке. На многомодовое волокно рассчитаны излучатели на длину волны 0.85 мкм - самые доступные и дешевые излучатели, выпускаемые в очень широком ассортименте.

Но затухание на этой длине волны у многомодовых волокон находится в пределах 3-4 dB/км и не может быть существенно улучшено. Полоса пропускания у многомодовых волокон достигает 800 МГц/км, что приемлемо для локальных сетей связи, но не достаточно для магистральных линий.

Волоконно-оптический кабель.

Вторым важнейшим компонентом, определяющим надежность и долговечность ВОЛС, является волоконно-оптический кабель (ВОК). На сегодня в мире несколько десятков фирм, производящих оптические кабели различного назначения. Наиболее известные из них: AT&T, General Cable Company (США); Siecor (ФРГ); BICC Cable (Великобритания); Les cables de Lion (Франция); Nokia (Финляндия); NTT, Sumitomo (Япония), Pirelli(Италия).

Рассмотрим структуру и основные параметры оптоволоконного кабеля, что позволит нам указать некоторые решения по защите целостности соответствующих сетей передачи данных.Волоконно-оптические кабели дифференцируются по размеру несущего волокна и оболочки – слоя стекла, отражающего свет.

Центральным элементом оптоволоконного кабеля является внутренний

сердечник из стекла или пластика (рис. 1, позиция 1). Диаметр и чистота стекловолокна определяют количество передаваемого им света.Если современным стеклом, используемым для оптоволокна, заполнить океан, то в любой его точке мы смогли бы видеть дно, как мы видим землю с борта самолета.

Волоконно-оптические кабели толщиной в 8,3 микрона очень трудно соединить точно. Поэтому возможны монтажные ошибки, в том числе и трудно выявляемые при тестировании кабельной проводки. Подобные ошибки часто устраняются установкой дополнительных оптоволоконных повторителей (концентраторов), что увеличивает уровень электромагнитных излучений кабельной системы в целом. Однако в последнее время на рынке появились так называемые заказные кабельные комплекты, то есть кабели с уже смонтированными и проверенными в заводских условиях коннекторами. Они полностью избавляют инсталляторов от утомительных процедур монтажа и тестирования проводки в полевых условиях.

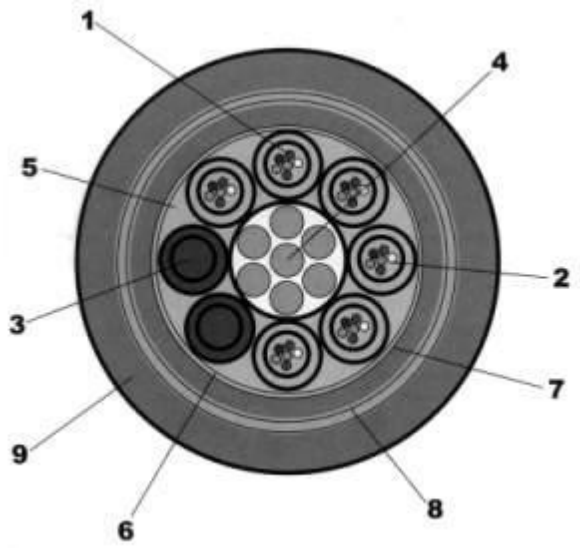


Рис. 3.

1 – оптическое волокно;2 – внутримодульный гидрофобный заполнитель;3 – кордель;4 – центральныйсиловой элемент – стальнойтрос;5 – гидрофобный заполнитель;6 – скрепляющая лента;7 – промежуточнаяоболочка из полиэтилена;8 – броняиз стальной гофрированной ленты;9 – защитная оболочка из полиэтилена.

Типовой профиль оптоволоконного кабеля имеет ряд характерных особенностей:

- количество оптических волокон в одном модуле – от 1 до 12;
- заполнение пространства между модулями упрочняющими элементами – корделями из стеклонитей или нитей из кевлара и гидрофобным гелем;
- наличие центрального силового элемента;
- размещение в полимерной трубке – модуле;

- покрытие всех этих элементов и модулей промежуточной полимерной оболочкой;
- внешняя защита оболочки из полиэтилена или металла;
- возможно наличие двух защитных оболочек – металлическойи полиэтиленовой.

Наряду с этими общими чертами оптические кабели различных фирм могут иметь дополнительные скрепляющие ленты, антикоррозийные и водозащитные обмотки, гофрированные металлические оболочки и т. д.

Определяющими параметрами при производстве ВОК являются условия эксплуатации и пропускная способность линии связи.

По условиям эксплуатации кабели подразделяют на:

- *монтажные;*
- *станционные;*
- *зоновые;*
- *магистральные;*

Первые два типа кабелей предназначены для прокладки внутри зданий и сооружений. Они компактны, легки и, как правило, имеют небольшую строительную длину.

Кабели последних двух типов предназначены для прокладки в колодцах кабельных коммуникаций, в грунте, на опорах вдоль ЛЭП, под водой. Эти кабели имеют защиту от внешних воздействий и строительную длину более двух километров.

Для обеспечения большой пропускной способности линии связи производятся ВОК, содержащие небольшое число (до 8) одномодовых волокон с малым затуханием, а кабели для распределительных сетей могут содержать до 144 волокон как одномодовых, так и многомодовых, в зависимости от расстояний между сегментами сети.

При изготовлении ВОК в основном используются два подхода:

- конструкции со свободным перемещением элементов;
- конструкции с жесткой связью между элементами.

По видам конструкций различают кабели повивной скрутки, пучковой скрутки, кабели с профильным сердечником, а также ленточные кабели. Существуют многочисленные комбинации конструкций ВОК, которые в сочетании большим ассортиментом применяемых материалов позволяют выбрать исполнение кабеля, наилучшим образом удовлетворяющее всем условиям проекта, в том числе – стоимостным.Особый класс образуют кабели, встроенные в грозотрос.

Оптические соединители.

Отдельно рассмотрим способы сращивания строительных длин кабелей.

Сращивание строительных длин оптических кабелей производится с использованием кабельных муфт специальной конструкции. Эти муфты имеют два или более кабельных ввода, приспособления для крепления

силовых элементов кабелей и одну или несколько сплайс-пластин. Сплайс-пластина - это конструкция для укладки и закрепления сращиваемых волокон разных кабелей.После того, как оптический кабель проложен, необходимо соединить его с приемо-передающей аппаратурой.

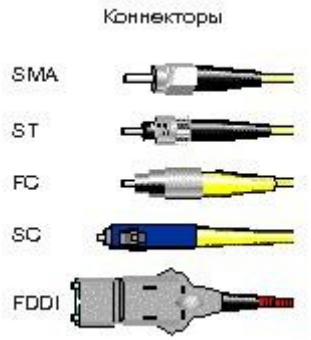


Рис. 4.

Сделать это можно с помощью оптических коннекторов (соединителей). В системах связи используются коннекторы многих видов. Сегодня мы рассмотрим лишь основные виды, получившие наибольшее распространение в мире. Внешний вид разъемов показан на рисунке.

Характеристики коннекторов представлены в таблице 1. Когда мы говорим, что данные виды коннекторов имеют наибольшее распространение, то это означает, что большинство приборов ВОЛС имеют розетки (адаптеры) под один из перечисленных видов коннекторов. Хотелось бы сказать несколько слов о последнем разделе таблицы 1. В нем упомянут новый тип фиксации: «Push-Pull».

Таблица 1:

Тип разъема	ВС	Телекоммуникации	Кабельное ТВ	Измерительная аппаратура	Дуплексные системы связи	Фиксация
FC/PC		+	+			резьба
ST		+				BNC
SMA				+		резьба
SC		+	+	+		Push-Pull
FDDI(MIC)					+	Push-Pull

Фиксация "Push-Pull" обеспечивает подключение коннектора к розетке наиболее простым образом - на защелке. Защелка-фиксатор обеспечивает надежное соединение, при этом не нужно вращать накидную гайку. Важное преимущество разъемов с фиксацией Push-Pull - это высокая плотность

монтажа оптических соединителей на распределительных и кроссовых панелях и удобство подключения.

2. Проблемы безопасности в ОКС. Типы угроз ВОЛС

2.1. Постановка задачи анализа потенциальных угроз. Наличие и применение стандартов, регламентирующих разработку и функционирование различных аппаратных или программных средств для ОКС.

Оптоволокно – это обычное стекло, передающее электромагнитную энергию в виде света инфракрасного диапазона. Излучение наружу практически отсутствует. Перехватить сообщение можно, только физически подключившись к волокну. Поэтому, на первый взгляд, проблема информационной безопасности окончательно решена.

Однако не все так просто. Оптоэлектроника (особенно для поддержки высокоскоростных приложений, систем видеонаблюдения и видеоприложений) стоит дорого и во многих случаях не снимает проблемы излучения электромагнитной энергии в окружающее пространство, поскольку рабочие станции, серверы, интерфейсные карты, концентраторы и другие сетевые устройства также являются активным оборудованием и задают собственный уровень излучений. Поэтому, принимая решения об использовании оптоволоконных кабельных систем (ОКС), важно представлять фактическое состояние дел по вопросам безопасности.

Понятно, что подключиться к оптоволоконному кабелю в полевых условиях трудно. Это является одним из аргументов сторонников мнения о полной безопасности ОКС. Но известный принцип противодействия брони и снаряда предопределил разработку и доведение до коммерческого использования многочисленных инноваций в технике монтажа. Это улучшенные инструменты и приспособления для сплавления волокон, быстрозатвердевающие эпоксидные смолы, специальные коннекторы и т. п. Появилась информация о создании специальных роботов, которые управляются дистанционно, могут самостоятельно передвигаться по кабельным канализациям и без непосредственного участия человека подключаться к оптоволоконному кабелю для последующей трансляции циркулирующих в ОКС данных.

Для противодействия злоумышленникам, вооруженным специальной техникой, предложено использовать в качестве сигнальных проводов внутренние силовые металлические конструкции оптоволоконных кабелей. Чтобы получить доступ к оптоволокну, необходимо нарушить целостность указанных конструкций. Это приводит к немедленному срабатыванию сигнализации в центре контроля за ОКС.

Дополнительного оборудования для реализации подобной охранной системы практически не требуется. Например, нет необходимости, как это

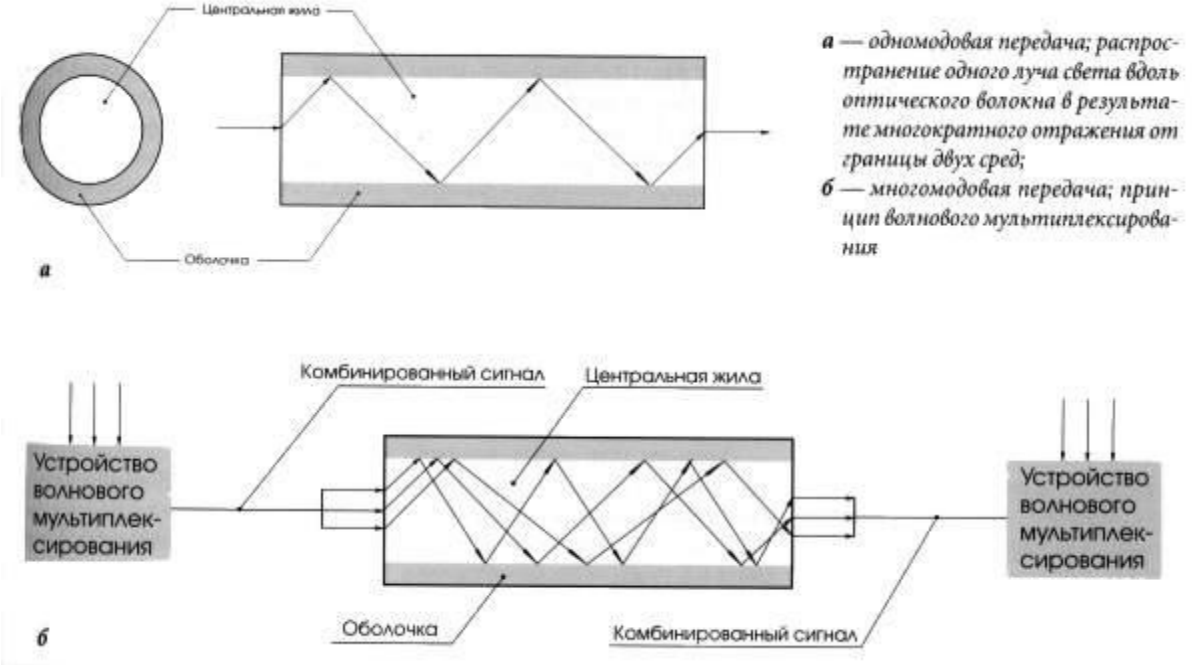
часто делают с медными кабелями, прокладывать оптоволоконный кабель в трубопроводах, где поддерживается высокое давление (в этом случае сигнал тревоги срабатывает при разгерметизации защитного трубопровода).

Параметры ОКС косвенно влияют на безопасность системы передачи данных в целом. Рассмотрим одномодовый и многомодовый режимы передачи (рис. 2). По одномодовым волокнам передаются оптические сигналы с одной длиной волны.

В многомодовых волокнах могут передаваться сигналы с различной длиной волны. Для совмещения нескольких оптических сигналов применяется так называемый волновой мультиплексор Wave Division Multiplexer – WDM, который работает как призма.

Сигналы с различной длиной волны комбинируются в нем, а затем пересылаются по одному из оптических волокон. Призма на приемном конце разлагает сигнал на волны исходной длины и направляет их на вход соответствующего оптического приемника.

Применение мультиплексирования позволяет увеличить число возможных каналов передачи данных. Однако в многомодовых кабелях сигналы затухают сильнее, следовательно, расстояния между узлами регенерации должны быть значительно уменьшены, что, конечно, сделает систему более дорогой, более «излучающей» и, соответственно, менее защищенной.



а — одномодовая передача; распространение одного луча света вдоль оптического волокна в результате многократного отражения от границы двух сред;
б — многомодовая передача; принцип волнового мультиплексирования

Рис. 6. Одномодовый и многомодовый режимы передачи

В целом же затухание сигналов в оптоволоконном кабеле (до 5 дБ/км) примерно соответствует показателям электрического коаксиального кабеля, но все-таки меньше. Это объясняется тем, что свет не излучается вне кабеля, как электрический сигнал в медных проводах. Очень важно то, что с ростом

частоты более 200 МГц оптоволоконные кабели имеют несомненное преимущество перед любыми электрическими кабелями. Поэтому для обеспечения безопасности информации целесообразна высокочастотная передача.

Затухание сигнала существенно увеличивается при разветвлении и ответвлении кабеля, хотя оптоволокно допускает это. Соответственно, предпочтительнее использовать однонаправленные кабели, что сразу определяет возможные топологии сети: «звезда» (с двумя разнонаправленными кабелями между центральным абонентом и каждым из периферийных) или кольцо (с одним однонаправленным кабелем). Особенности защиты в сетях с указанными топологиями приведены в таблице.

Таблица. Особенности защиты в сетях с различными топологиями

Топология	Достоинства	Недостатки	Комментарий
Звезда	Легкость подключения новых устройств без реконфигурации сети. Центральный узел может осуществлять коммутацию каналов, сообщений и пакетов	В случае сбоя на центральном узле вся сеть выходит из строя. Центральный узел требует жесткой физической и логической защиты. Установленное соответствие «точка-точка», широковещательные передачи невозможны	Основная информация содержится на центральном узле, периферийные узлы играют роль терминалов
Кольцо - узлы сети равноправ-ны	Нет центрального узла, с которым ассоциируются проблемы безопасности. Каждый узел имеет равноправные возможности для передачи сообщения	Разрыв кольца выводит систему из строя. При добавлении нового узла требуется реконфигурация сети. Передача сообщения через другие узлы снижает безопасность сети	Каждый узел должен быть достаточно производительным. Передача сообщения через промежуточный узел позволяет производить с ним любые манипуляции, криптозащита приведет к потере производительности

Несмотря на малое затухание, волоконной оптике присуща другая проблема – хроматическаядисперсия. Волны света различной длины стекло пропускает по-разному, поэтому импульс света, проходя через кабель, «размывается».

Получается эффект радуги – световойсигнал разделяется на цветовые компоненты. На расстоянии в несколько километров он может «залезть» в следующий бит, что приведет к потерям данных. Это нарушит их целостность, которая является наряду с конфиденциальностью и доступностью важнейшим аспектом информационной безопасности. В

одномодовых кабелях передается свет одной частоты, поэтому здесь нет эффекта хроматической дисперсии.

Одно из возможных решений указанной проблемы – увеличитьрасстояние между соседними сигналами, но это понижает скорость передачи. К счастью, исследования показали, что если генерировать сигнал в некоторой специальной форме, то дисперсионные эффекты почти исчезают, и сигнал можно передавать на тысячи километров. Сигналы в этой специальной форме называются *силитонами*.

К недостаткам оптоволоконного кабеля, влияющим на безопасность ОКС, следует отнести меньшую механическую прочность и меньшую долговечность, чем у электрического кабеля, а также чувствительность к ионизирующим излучениям (снижение прозрачности оптоволокна).

Таким образом, конфигурация оптоволоконного кабеля влияет на политику безопасности при работе с ОКС. Однако обсуждение вопроса, связанного с электромагнитным излучением, видится не менее важным.

Как было отмечено выше, компьютерные сети, построенные на базе оптоволоконных каналов, излучают в окружающее пространство конфиденциальные данные; некоторые ведущие аналитики весьма язвительно называют их даже «широковещательными» сетями. Уточним суть проблемы.

Расстояние, на котором можно перехватить электромагнитное излучение кабеля, например неэкранированной витой пары, не превышает полуметра, а дальность излучения монитора компьютера составляет более двух километров.

Другой пример, иллюстрирующий обратный процесс – воздействиена вычислительную систему. При тестировании ЛВС, которая функционировала в режиме передачи со скоростью 155 Мбит/с на линиях с незащищенной витой парой, защищенной витой парой и с оптоволокном.

В качестве воздействия было определено влияние радиочастотного поля с интенсивностью 3 В/м (мобильный телефон стандарта GSM создает поле интенсивностью 4,7 В/м).

Система на базе незащищенной витой пары характеризовалась высоким уровнем появления сбоев и, в конце концов, вышла из строя. ЛВС на оптоволокне имела сбои, но работала.И только ЛВС на основе защищенной витой пары была совершенно не подвержена помехам.

Таким образом, безопасность ОКС определяется самим «узким» местом телекоммуникационных систем – сетевым активным оборудованием.

Одной из возможностей гарантированного обеспечения конфиденциальности и безопасности данных может стать электрическое экранирование всего здания с помощью, так называемой клетки Фарадея. Однако такой способ слишком дорог, он применяется только в организациях, занимающихся разведкой.

Вопросы обеспечения информационной безопасности тесно связаны с наличием и применением стандартов, регламентирующих разработку и функционирование различных аппаратных или программных средств.

Известно, что где хаос, там раздолье для злоумышленников.

Поэтому параметры передачи сигнала по оптическим линиям определены однозначно. Наряду с подробным техническим описанием ссылка на соответствующий стандарт оптической передачи данных может быть использована для определения полного набора требований к компьютерной системе в целом.

Наиболее популярный в США и Европе стандарт, регламентирующий параметры оптической передачи для коммуникаций в производственных помещениях, — это ANSI/ T1A/E1A-568A. Он определяет затухание и полосу пропускания для многомодового волокна и максимальное затухание для одномодового волокна.

Большинство разработчиков кабельных систем и другого оборудования продолжают полагаться на тексты стандартов и составляют кабельные системы из отдельных компонентов от различных производителей. В такой ситуации особенно важно, чтобы лица, отвечающие за безопасность и конфиденциальность информации, проверяли надежность системы в целом, а не отдельных ее частей.

Обсуждение особенностей обеспечения безопасности ОКС нельзя считать законченным без упоминания о безопасности работы с оптоволоконным кабелем. Стеклянные волокна настолько тонки, что их невозможно увидеть невооруженным глазом. Кусочек волокна может попасть в глаза прежде, чем вы успеете разглядеть его.

Потенциально опасен для человека и излучатель оптического сигнала. Это может быть очень мощный лазер, который в состоянии нанести непоправимый ущерб здоровью. Итак, работая с ОКС, возьмите себе за правило никогда не смотреть в торец волокна, а для обследования кабелей обязательно использовать соответствующее оборудование.

ОКС может сформировать у пользователей ложное чувство полной Применение безопасности. Более корректен другой подход: выбор оптоволоконных кабельных систем является лишь частичным решением проблемы обеспечения безопасности данных. Он позволяет сделать нежелательный доступ к сети извне значительно более трудным, чем в случае использования системы со стандартными неэкранированными линиями, применяемыми в современных сетях.

2.2. Нарушение полного внутреннего отражения. Нарушение отношения показателей преломления. Регистрация рассеянного излучения

Разработка технических средств контроля НД к информационному сигналу, передаваемому по ОВ (система диагностики состояния (СДС) оптического тракта): СДС с анализом прошедшего сигнала; СДС с анализом отраженного сигнала.Высокие требования, предъявляемые к современным системам телекоммуникаций (высокая скорость передачи информации, надёжность, защищённость от несанкционированного доступа), приводят к осознанию неоспоримого преимущества волоконно-оптических линий связи.

В ближайшем будущем, можно ожидать, что ВОЛС заменят все существующие магистральные линии передачи информации. В связи с возможной широкой распространённостью возникает проблема защиты информации в ВОЛС. Анализ возможных каналов утечки информации в результате несанкционированного доступа уже сейчас имеет первостепенное значение.

Уже изначально ВОЛС имеют более высокую степень защищённости информации от несанкционированного доступа, чем какие-либо иные линии связи, что связано с физическими принципами распространения электромагнитной волны в световоде. В оптическом волноводе электромагнитное излучение выходит за пределы волокна на расстояние не более длины волны при отсутствии внешнего воздействия на оптоволокно.

Понятие волоконно-оптической линии связи является собирательным. Оно включает приёмники, передатчики оптического сигнала, волоконно-оптический тракт, регенераторы и иное оборудование. В связи с этим волоконно-оптическую линию можно разделить на локальные и распределённые участки.

Локальные участки, включающие в себя модуляторы, оптические передатчики и приёмники, регенераторы, наиболее защищены от несанкционированного съёма в виду локализованной области их расположения.

Распределённые участки (волоконно-оптические тракты) обладают наибольшей протяжённостью и, соответственно, наименьшей защищённостью от несанкционированного съёма. В отличие от всех других сред передачи информации, для формирования каналов утечки на участках волоконно-оптического тракта, как правило, требуют прямого доступа к оптоволокну и специальных мер отвода части излучения из оптоволокна или регистрации прохождения излучения.

Основные физические принципы формирования каналов утечки в ВОЛС можно разделить на следующие типы:

1. Нарушение полного внутреннего отражения.
2. Регистрация рассеянного излучения на длинах волн основного информационного потока и комбинационных частотах.
3. Параметрические методы регистрации проходящего излучения.

Нарушение полного внутреннего отражения

В первую очередь рассмотрим каналы утечки информации на распределённых участках способами, связанными с нарушением полного внутреннего отражения. К такого рода способам относятся:

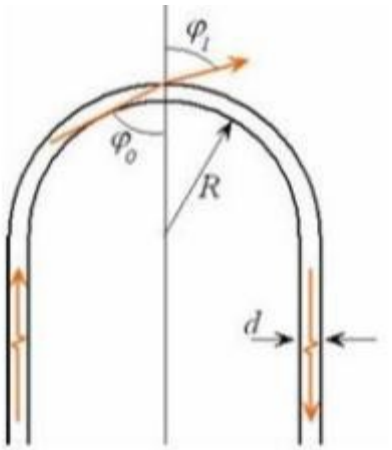
- *изменение угла падения*, путем использование внешнего воздействия для уменьшения угла падения до значения, меньшего значения предельного угла падения, при котором начинает наблюдаться полное внутреннее отражение;

- *изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптоволокна,* путем использование внешнего воздействия для увеличения угла полного внутреннего отражения до значений, больших характерных углов падения в световоде;

- *оптическое туннелирование,* которое состоит в прохождении излучения через оболочку оптоволокна с показателем преломления меньшим, чем у сердцевины, при углах падения больших угла полного внутреннего отражения.

Формирование каналов утечки при изменениях формы оптоволокна, путем физического воздействия

Изменение угла падения может достигаться путём механического воздействия на оптоволокно, например, его изгибом. При изгибе оптического волокна происходит изменение угла падения электромагнитной волны на границе сердцевина-оболочка. Угол падения становится меньше предельного угла, что означает выход части электромагнитного излучения из световода



(рис.9).

Рис. 9. Формирование канала утечки при изгибе радиусом ***R*** оптоволокна с диаметром сердцевины ***d***, где ϕ_0 - угол падения; ϕ_i - угол преломления

Изгиб оптического волокна приводит к сильному побочному излучению в месте изгиба, что создаёт возможность несанкционированного съёма информации в локализованной области.

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

$$R \le d \frac{n_2}{n_1 - n_2},$$

здесь n1, n2 – показатели преломления сердцевины и оболочки световода.

Интенсивность электромагнитной волны, выходящей из волокна в точке изгиба, определяется по формулам Френеля для p- и s-поляризаций, соответственно:

$$I_p = I_0 \frac{\sin 2\varphi_0 \sin 2\varphi_1}{\sin^2(\varphi_0 + \varphi_1)\cos^2(\varphi_0 - \varphi_1)},$$

$$I_s = I_0 \frac{\sin 2\varphi_0 \sin 2\varphi_1}{\sin^2(\varphi_0 + \varphi_1)},$$

где I_0 – интенсивность падающего излучения и I_p, I_s – интенсивности прошедшего излучения для p- is-поляризаций. Оценка радиуса изгиба для многомодового волокна с диаметром сердцевины ***d=50*** мкм и оптической оболочки – ***D***=125 мкм (n_1=1,481, n_2=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).

Необходимо помнить, что при оценке изгиба не учитывалась форма светового потока, цилиндрическая форма преломляющей поверхности и другие эффекты, изменяющие показатель преломления оптоволокна, например, фотоупругий эффект. Однако их воздействия на порядок меньше.

Нарушение полного внутреннего отражения при механическом воздействии возможно не только при изгибе волокна, но и при локальном давлении на оптоволокно, что вызывает неконтролируемое рассеяние (в отличие от изгиба) в точке деформации.

Формирование каналов утечки, вызывающим изменение отношения показателей преломления путем акустического воздействия

Изменения угла падения можно добиться не только изменением формы оптоволокна при механическом воздействии, но и акустическим воздействием на оптическое волокно.

В сердцевине оптоволокна создаётся дифракционная решётка периодического изменения показателя преломления, которая вызвана воздействием звуковой волны. Электромагнитная волна отклоняется от своего первоначального направления, и часть её выходит за пределы канала распространения.

Физическим явлением, с помощью которого возможно решить поставленную задачу, является дифракция Брэгга на высокочастотном звуке (>10 МГц), длина волны ***Λ*** которого удовлетворяет условию: ($\lambda L/\Lambda^2$), где λ - длина волны электромагнитного излучения, L - ширина области распространения звуковой волны.

Деформации, создаваемые упругой волной, формируют периодическое изменение показателя преломления внутри оптоволокна для света являющейся дифракционной решёткой (рис. 10).

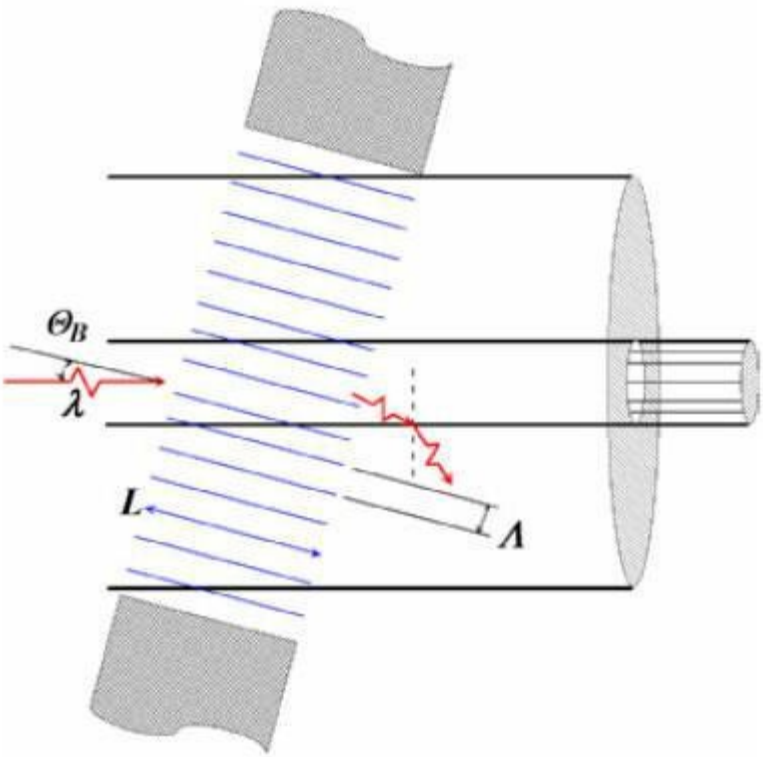


Рис. 10. Формирование дифракционной решетки в сердцевине оптоволокна звуковой волной

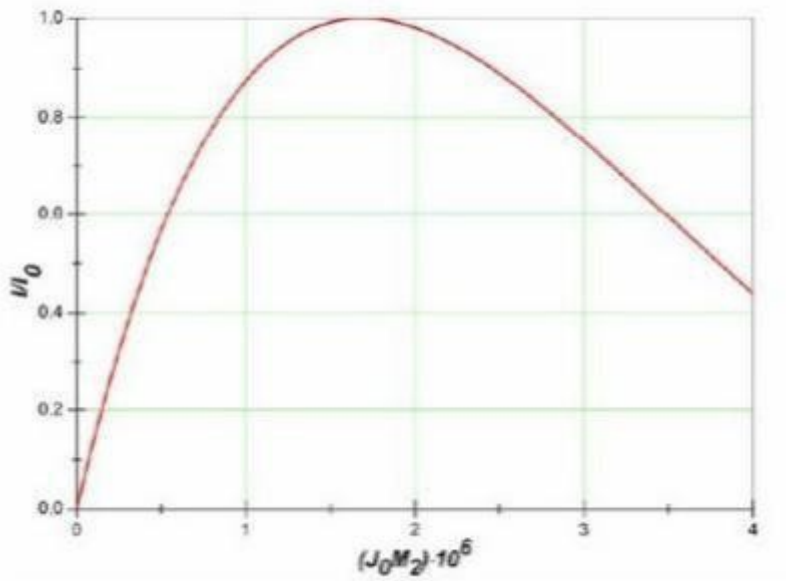
Максимальный угол отклонения единственного наблюдаемого дифракционного максимума равен двум углам Брэгга ($2\Theta_B$). Частота отклонённой электромагнитной волны приблизительно равна частоте основного информационного потока. Интенсивность дифракционного максимума может быть определена по формуле

$$I = I_0 \sin^2\left(\frac{\pi}{2}\sqrt{J_0 M_2}\,\frac{L}{\lambda}\right),$$

где J_0 – интенсивность звуковой волны, M_2=1,51×10-15 сек3/кг - акустооптическое качество кварца. 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.

График зависимости интенсивности первого дифракционного максимума от интенсивности звуковой волны представлен на рис.11.

Из графика видно, что даже при невысоких интенсивностях звуковой волны выводимое электромагнитное излучение достаточно велико для регистрации его современными фотоприёмниками. При фиксированной интенсивности звука, путём изменения области озвучивания L можно добиться максимального значения интенсивности в дифракционном максимуме, тем самым увеличить интенсивность света отводимого в канал



утечки.

Рис. 11. Зависимость интенсивности дифракционного максимумаот интенсивности звуковой волны

Другим внешним воздействием, изменяющим отношение показателя преломления оболочки к показателю преломления сердцевины оптоволокна (n_2/n_1), является механическое воздействие без изменения формы волокна, например, растяжение.

При растяжении оптического волокна происходит изменение показателей преломления сердцевины и оболочки оптического волокна на Δn_1 и Δn_2. При этом увеличивается значение угла полного внутреннего отражения от φ_r до φ'_r . Значения углов связаны выражением

$$\sin\varphi'_r \approx \left(1-\frac{\Delta n_1}{n_1}+\frac{\Delta n_2}{n_2}\right)\sin\varphi_r$$

Выражение для отношения ($\Delta n/n$) определяется фотоупругим эффектом так, что

$$\frac{\Delta n}{n}=-\frac{1}{2}n^2 p\varepsilon ,$$

где p, ε – эффективные составляющие тензоров фотоупругости и деформации, это связано с анизотропией оптического волокна возникающей при растяжении. С учётом того, что плавленый кварц выдерживает большие напряжения (до 106 Па в идеальном состоянии), то, прикладывая большие механические напряжения к оптоволокну, возможно добиться изменения предельного угла на величинуφ'$_r$ - φ$_r$ ≈ 10^{-6} sin φ$_r$, чего может оказаться достаточно для вывода части интенсивности основного информационного потока за пределы оптического волокна.

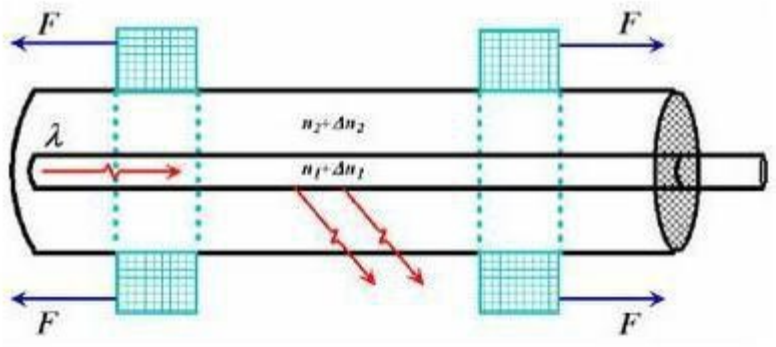


Рис. 12. Формирование канала утечки растяжением оптоволокна при воздействии внешнего усилия ***F***

К способам вызывающим изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптоволокна путём механического напряжения так же относится и скручивание оптоволокна.

К бесконтактным способам изменения отношения (n_2/n_1) можно отнести воздействие стационарных электрических полей, которые изменяют показатель преломления сердцевины и оболочки на Δn_1 и Δn_2 . Выражение для отношения ($\Delta n/n$) определяется из уравнения для обратного пьезоэлектрического эффекта и явления фотоупругости

$$\frac{\Delta n}{n} = -\frac{1}{2} n^2 pbE \quad ,$$

где b – модуль пьезоэлектрического эффекта, E – напряжённость электрического поля. Новый угол полного внутреннего отражения (при $\Delta n_1>0$ и $\Delta n_2>0$), если для оценки принять значение напряжённости электрического поля для пробоя идеального плавленого кварца (108 В/м), то воздействием стационарного электрического поля, можно добиться изменения предельного угла на величину φ'$_r$ - φ$_r$ ≈ $2\cdot10^{-6}$ sin φ $_r$

Надо отметить, несмотря на то, что изменения значения предельного угла, вызываемые как механическими 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.*

Формирование канала утечки методом оптического туннелирования

Способом, который позволяет захватывать часть электромагнитного излучения, выходящего за пределы сердцевины информационного оптического волокна дополнительным световодом, не внося дополнительных потерь и обратного рассеяния, является оптическое туннелирование.

Явление оптического туннелирования состоит в прохождении оптического излучения из среды с показателем преломления n_1 через слой с показателем преломления n_2 меньшим n_1 в среду с показателем преломления n_3 при углах падения больших угла полного внутреннего отражения. На принципах оптического туннелирования в интегральной и волоконной оптике создаются такие устройства как оптический ответвитель, оптофоны, волоконно-оптические датчики физических величин.

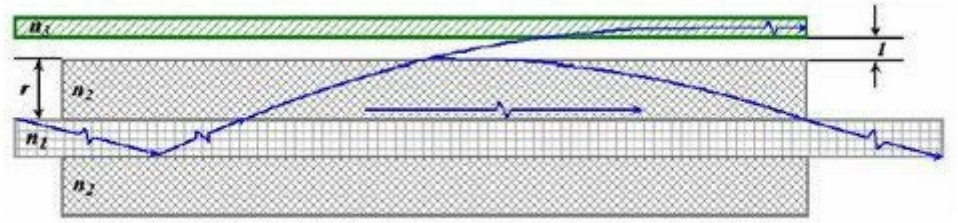


Рис. 13. Формирование каналаутечки оптическим туннелированием, где n_1,n_2 – показатели приломления и оболочки оптоволокна, n_3- показатель преломления дополнительного оптоволокна

При распространении света в оптическом волокне часть светового потока выходит за пределы сердцевины оптоволокна. Интенсивность излучения вышедшего из сердцевины в оболочку оптоволокна на расстояние r=(D-d)/2 в зависимости от угла падения на границе сердцевина-оболочка φ определяется выражением

$$I = I_0 \cdot \exp\left(-4\pi n_1 (r/\lambda)\sqrt{\sin^2\varphi - \sin^2\varphi_r}\right).$$

Это приводит к тому, что при изготовлении оптоволокна оболочка занимает значительную часть. Причём у одномодового волокна оболочка занимает гораздо больший объём, чем у многомодового.

Это следует из приведённой формулы проникновения света из сердцевины в оболочку. При приближении угла падения φ к углу полного отражения φ_r показатель степени экспоненты стремится к нулевому значению, свет распространяется по всей структуре волокна – сердцевине и оболочке.

Это приводит к тому, что часть интенсивности из основного оптоволокна может перейти в дополнительное оптоволокно (рис.13).

Интенсивность излучения переходящего в дополнительный волновод определяется выражением

$$I = I_0 \cdot \sin^2(k \cdot S),$$

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 $n_3=n_1$.

Как видно из выражения, излучение из основного оптического волновода переходит в дополнительный волновод полностью при некотором значении длины оптического контакта $S=\pi/2k$. При дальнейшем увеличении длины оптического контакта происходит обратный процесс. Таким образом, излучение периодически переходит из одного волновода в другой, если не учитывать потери на поглощение и рассеяние.

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

В заключение надо отметить, что существует много других способов несанкционированного доступа и способов съёма 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. Таким образом, особенностью волоконно-оптических телекоммуникаций является необходимость физического контакта с линией связи для формирования канала утечки.

3. Физические методы защиты информации, передаваемой по ВОЛС

3.1. Разработка технических средств контроля НД к информационному сигналу, передаваемому по ОВ (система диагностики состояния (СДС) оптического тракта): СДС с анализом прошедшего сигнала; СДС с анализом отраженного сигнала

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. Принципы и методы криптографической защиты информации в ОКС

4.1. Квантовая криптография: природа секретности квантового канала; базовые принципы квантовой криптографии; простейший алгоритм генерации секретного ключа; протокол Беннета; современное состояние работ по созданию ККС

Квантовые компьютеры и связанные с ними технологии в последнее время становятся все актуальнее. Исследования в этой области не прекращаются вот уже десятилетия, и ряд революционных достижений налицо. Квантовая криптография - одно из них.

Технология квантовой криптографии крайне сложна, и, естественно, данная статья не претендует на широкое освещение темы. Мы также не будем начинать, что называется, "с места в карьер". Начнем с основ

шифрования. Это вполне уместно, тем более что нам понадобится рассмотреть, какими же преимуществами обладает квантовая криптография над распространенными ныне алгоритмами. Итак...

В современном мире передача конфиденциальных данных между несколькими абонентами в различных сетях связи может привести как к потере передаваемой информации, так и к ее компрометации. Компрометация означает превращение секретных данных в несекретные, т. е. разглашение информации, ставшей известной какому-либо лицу, не имеющему права доступа к ней.

Криптография - это наука о шифрах. Она представляет собой огромное количество методов изменения открытого сообщения для того, чтобы передаваемое сообщение стало бесполезным для криптоаналитика, специалиста по криптоанализу. Криптоанализ - наука о вскрытии шифров. Криптографические преобразования служат для достижения двух целей по защите информации. Во-первых, они обеспечивают недоступность ее для лиц, не имеющих ключа, и, во-вторых, поддерживают с требуемой надежностью обнаружение несанкционированных искажений. Важным понятием в криптографии является ключ - сменный элемент шифра, который применяется для шифрования конкретного сообщения.

Все криптографические системы основаны на использовании криптографических ключей. Практически все криптографические схемы делятся на симметричные и асимметричные криптосистемы.

Симметричные криптосистемы

В симметричной криптосистеме отправитель и получатель сообщения используют один и тот же секретный ключ.

Этот ключ должен быть известен всем пользователям и требует периодического обновления одновременно у отправителя и получателя.

Симметричная криптосистема генерирует общий секретный ключ и распределяет его между законными пользователями. С помощью этого ключа производится как шифрование, так и дешифрование сообщения.

Процесс распределения секретных ключей между абонентами обмена конфиденциальной информации в симметричных криптосистемах имеет весьма сложный характер. Имеется в виду, что передача секретного ключа нелегитимному пользователю может привести к вскрытию всей передаваемой информации. Наиболее известные симметричные криптосистемы - шифр Цезаря, шифр Вижинера, американский стандарт шифрования DES, шифр IDEA и отечественный стандарт шифрования данных ГОСТ 28147-89.

Асимметричные криптосистемы

Асимметричные криптосистемы предполагают использование двух ключей - открытого и секретного.

В таких системах для зашифрования сообщения используется один ключ, а для расшифрования - другой.

Асимметричные криптосистемы используют для работы два ключа. Первый, открытый, доступен любому пользователю, с помощью которого зашифровывается сообщение. Второй, секретный, должен быть известен только получателю сообщений.

Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование сообщения с помощью открытого ключа невозможно. Для расшифрования данных получатель зашифрованного сообщения применяет второй ключ, секретный. Ключ расшифрования не может быть определен из ключа зашифрования. Схему асимметрической криптографии в 1976 г. предложили два молодых американских математика Диффи и Хеллман. Наиболее известные асимметричные криптосистемы это шифр RSA и шифр Эль Гамаля. Данная схема является довольно-таки сложной для криптоанализа. Чем больше ключ, тем сложнее его подобрать обычным простым перебором. Для вскрытия современной криптосистемы со средней длиной ключа потребуется около 1050 машинных операций, что практически невозможно на современных компьютерных системах.

Безопасность любого криптографического алгоритма определяется используемым криптографическим ключом. Для получения ключей используются аппаратные и программные средства генерации случайных значений ключей. Как правило, применяют датчики псевдослучайных чисел. Однако степень случайности генерации чисел должна быть достаточно высокой. Идеальными генераторами являются устройства на основе натуральных случайных процессов, например на основе белого шума.

Важной задачей при работе с ключами является их распределение. В настоящее время известны два основных способа распределения ключей: с участием центра распределения ключей и прямой обмен ключами между пользователями.

Распределение ключей с участием центра распределения ключей

При распределении ключей между участниками предстоящего обмена информацией должна быть гарантирована подлинность сеанса связи, т. е. все участники должны пройти процедуру аутентификации. Центр распределения ключей осуществляет взаимодействие с одним или более участниками сеанса с целью распределения секретных или открытых ключей.

Прямой обмен ключами между пользователями

При использовании для обмена конфиденциальными данными криптосистемы с симметричным секретным ключом два пользователя должны обладать общим секретным ключом. Они должны обменяться им по каналу связи безопасным образом.

Однако современная наука произвела на свет новый алгоритм шифрования - генерацию секретного ключа при помощи квантовой криптографии.

Квантово-криптографические системы - это побочный продукт разрабатываемого в настоящее время так называемого квантового компьютера. Что это такое? Здесь самым лучшим для вас, дорогие читатели, будет освежить в памяти материал под названием "Квантовые компьютеры, нейрокомпьютеры и оптические компьютеры", который был опубликован в ПЛ №11 за 1999 г. Мы лишь вкратце перечислим базовые понятия.

Итак, основной строительной единицей квантового компьютера является кубит (qubit, Quantum Bit). Классический бит имеет, как известно, лишь два состояния - 0 и 1, тогда как множество состояний кубита значительно больше. Это означает, что кубит в одну единицу времени равен и 0, и 1, а классический бит в ту же единицу времени равен либо 0, либо 1. Основная причина бурных исследований в области квантовых компьютеров - это естественный параллелизм квантовых вычислений. Например, если квантовая память состоит из двух кубитов, то мы параллельно работаем со всеми ее возможными состояниями: 00, 01, 10, 11. За счет возможности параллельной работы с большим числом вариантов квантовому компьютеру необходимо гораздо меньше времени для решения задач определенного класса. К таким задачам, например, относятся задачи разложения числа на простые множители, поиск в большой базе данных и др.

Бурное развитие квантовых технологий и волоконно-оптических линий связи привело к появлению квантово-криптографических систем. Они являются предельным случаем защищенных ВОЛС. Использование квантовой механики для защиты информации позволяет получать результаты, недостижимые как техническими методами защиты ВОЛС, так и традиционными методами математической криптографии. Защита такого класса применяется в ограниченном количестве, в основном для защиты наиболее критичных с точки зрения обеспечения безопасности систем передачи информации в ВОЛС.

5. Квантовые компьютеры

5.1. Квантовые вычисления: квантовые биты – кубиты; принцип суперпозиции; квантовый параллелизм. Квантовая память.

Природа секретности квантового канала связи

При переходе от сигналов, где информация кодируется импульсами, содержащими тысячи фотонов, к сигналам, где среднее число фотонов, приходящихся на один импульс, много меньше единицы (порядка 0,1), вступают в действие законы квантовой физики. Именно на использовании этих законов в сочетании с процедурами классической криптографии основана природа секретности квантового канала связи (ККС).

В квантово-криптографическом аппарате применим принцип неопределенности Гейзенберга, согласно которому попытка произвести измерения в квантовой системе вносит в нее нарушения, и полученная в результате такого измерения информация определяется принимаемой

стороной как дезинформация. Процесс измерений в квантовой физике характеризуется тем, что он может активно вносить изменения в состояние квантового объекта, и ему присущи определенные стандартные квантовые ограничения.

Следует выделить ограничения, связанные с невозможностью одновременного измерения взаимодополняемых параметров этой системы, т. е. мы не можем одновременно измерить энергию и поляризацию фотона. Исследования показали, что попытка перехвата информации из квантового канала связи неизбежно приводит к внесению в него помех, обнаруживаемых законными пользователями этого канала. Квантовая криптография использует этот факт для обеспечения возможности двум сторонам, которые ранее не встречались и не обменивались никакой предварительной секретной информацией, осуществлять между собой связь в обстановке полной секретности без боязни быть подслушанными злоумышленником. Так в квантово-оптическом канале связи распространяются одиночные фотоны.

Немного истории

В 1984 г. Ч. Беннет (фирма IBM) и Ж. Брассард (Монреальский университет) предположили, что квантовые состояния (фотоны) могут быть использованы в криптографии для получения фундаментально защищенного канала. Они предложили простую схему квантового распределения ключей шифрования, названную ими BB84. Эта схема использует квантовый канал, по которому пользователи (пусть это будут Алиса и Боб) обмениваются сообщениями, передавая их в виде поляризованных фотонов.

Подслушивающий злоумышленник может попытаться производить измерение этих фотонов, но, как сказано выше, он не может сделать это, не внося в них искажений. Алиса и Боб используют открытый канал для обсуждения и сравнения сигналов, передаваемых по квантовому каналу, проверяя их на возможность перехвата. Если они при этом ничего не выявят, они могут извлечь из полученных данных информацию, которая надежно распределена, случайна и секретна, несмотря на все технические ухищрения и вычислительные возможности, которыми располагает злоумышленник.

Схема BB84

Схема BB84 работает следующим образом. Сначала Алиса генерирует и посылает Бобу последовательность фотонов, поляризация которых выбрана случайным образом и может составлять 0, 45, 90 и 135°. Боб принимает эти фотоны и для каждого из них случайным образом решает, замерять его поляризацию как перпендикулярную или диагональную. Затем по окрытому каналу Боб объявляет для каждого фотона, какой тип измерений им был сделан (перпендикулярный или диагональный), но не сообщает результат этих измерений, например 0, 45, 90 или 135°.

По этому же открытому каналу Алиса сообщает ему правильный ли вид измерений был выбран для каждого фотона. Затем Алиса и Боб отбрасывают все случаи, когда Боб сделал неправильные замеры. Если квантовый канал не

перехватывался, оставшиеся виды поляризации и будут поделенной между Алисой и Бобом секретной информацией, или ключом. Этот этап работы квантово-криптографической системы называется первичной квантовой передачей.

6. Порядок проектирования и создания оптоволоконных кабельных сетей (ОКС)

6.1. Основные требования к проектированию. Этапы проектирования ВОЛС

В настоящее время требования к передаче данных значительно выросли и постоянно растут. Отличным решением проблемы служит волоконно-оптический кабель (ВОК). Технологии высокоскоростной передачи данных, такие как Gigabit Ethernet и ATM, вкупе с высоким быстродействием современных микропроцессоров предъявляют повышенные требования к существующей инфраструктуре на основе медного кабеля.

Однако в настоящее время возможности передачи информации ограничены скоростью 100 Мбит/с и расстоянием порядка в сотни метров. В то же время волоконно-оптическая среда передачи данных поддерживает скорости от 9,6 Кбит/с до 40 Гбит/с и расстояния до 2 км. Вложения в такую кабельную систему надежно защищены - если она и устареет, то очень нескоро. Располагая сетью на основе ВОК, компания без труда перейдет на более скоростные технологии, соответствующие требованиям применяемых приложений.

Например, волоконно-оптическая линия может служить изначально в качестве канала SCADA, обеспечивающего передачу со скоростью 9,6 Кбит/с, а затем эксплуатироваться как линия SONET OC-12 на 622 Мбит/с. Для этого надо лишь сменить оконечное оборудование.

Естественно, ВОК система будет соответствовать требованиям высокоскоростных технологий только при правильном ее проектировании и инсталляции. В данном курсовом проекте рассматриваются распространенные ошибки при инсталляции ВОК, производится расчет ОВ и ВОК, и приводится экономическое обоснование выбора соответствующего кабеля.

ИНСТАЛЛЯЦИЯ ОПТИЧЕСКИХ СЕТЕЙ

Распространенные ошибки инсталляции

Приступая к реализации любого проекта, всегда полезно знать, чего именно следует избегать. Ниже перечислены некоторые наиболее распространенные ошибки, часто встречающиеся при инсталляции систем на основе ВОК.

Небрежное планирование. Данная ошибка наиболее типична при прокладке любого, а не только волоконно-оптического телекоммуникационного кабеля. Схему кабельной сети, поддерживающих ее

устройств и оконечных компонентов необходимо тщательно продумать и спланировать (в данном проекте главной целью стоит разработка схемы кабельной сети).

Если кабельная проводка должна инсталлироваться в строящемся или реконструируемом здании, то строительство или реконструкцию следует осуществлять с учетом последующей прокладки кабельной системы. Планирование телекоммуникационной системы не следует оставлять "на потом", тем самым вы увеличите стоимость работ и усложните их.

Приобретение волоконно-оптического кабеля без знания его рабочих спецификаций и характеристик. Прежде чем покупать кабель, следует разобраться в таких его характеристиках, как коэффициент отражения, диапазон рабочих частот кабеля, потери на километр длины при рабочей длине волны, физические размеры оптического волокна (ОВ) и оболочки, а также максимальное усилие, которое разрешается применять к кабелю, чтобы не повредить его внутренние волокна (нити стекловолокна).

Применение ВОК без результатов фабричного тестирования. Производитель кабеля после "сборки" продукции выполняет ее всесторонне тестирование, чтобы определить, отвечает ли она требованиям спецификаций, и защитить себя от возможных дополнительных расходов на возмещение ущерба покупателю. Каждая катушка ВОК должна поставляться с отчетом о результатах фабричного тестирования. Без такой информации нельзя быть уверенным, что полученная продукция соответствует предъявленным требованиям.

Невыполнение тестирования кабеля после его доставки. Это вторая по распространенности ошибка, встречающаяся в процессе инсталляции ВОК системы. Если вы не протестируете кабель перед инсталляцией, то определить, когда он был поврежден - при поставке или при прокладке, будет невозможно. Для этого необходимо использовать, как минимум, источник и измеритель мощности оптического сигнала, с целью проверки прохождения света по каждому волокну нового кабеля.

При получении (пока он еще находится в катушке) лучше всего проверить его с помощью оптического измерителя отраженного сигнала (Optical Time Domain Reflectometer, OTDR) - инструмента определения профиля каждого волокна кабеля.

Недостаточная протяженность кабеля в телекоммуникационном шкафу (для обеспечения правильной концевой заделки). Обычно рекомендуется оставлять от 3 до 3,5 м кабеля. Это облегчит внесение изменений в монтажном шкафу и уменьшит стоимость работ - при каких-либо модификациях (например, реорганизации монтажного шкафа) вам не придется наращивать кабель или заменять его на другой, более длинный.

Невыполнение контрольного тестирования и документирования проложенного волоконно-оптического кабеля (охватывающего одно здание или комплекс зданий) перед инсталляцией оконечного оборудования. Без тестирования проложенного кабеля нельзя быть уверенным в правильности

инсталляции. В случае неправильной инсталляции производительность может серьезно пострадать. Более того, отсутствие документации по кабельной проводке затруднит впоследствии диагностику и устранение неисправностей. Ниже будет рассказано о процедурах тестирования для проверки правильности инсталляции и соответствия кабельной системы требованиям производительности.

Невыполнение анализа оптических потерь до покупки и подключения оконечного оборудования. Бюджет оптических потерь - это разность между мощностью передаваемого по кабелю сигнала и оптической чувствительностью приемника, измеряемая в децибелах (дБ). Бюджет следует составить до прокладки кабеля и подключения оконечных устройств, а не предполагать заранее, что все будет работать, чтобы потом обнаружить проблемы.Отсутствие защиты магистрального ВОК путем его оконечного подключения к коммутационной панели. Для сохранения инвестиций каждый магистральный ВОК должен быть заделан в защищенный корпус, а каждое волокно кабеля иметь соединитель. После этого с помощью коротких перемычек кабель можно подключать к оконечному оборудованию.

Невыполнение тестирования оконечного волоконно-оптического оборудования перед его установкой. Во всех случаях аппаратное обеспечение нужно тестировать. Это позволит установить, будет ли данное оборудование взаимодействовать с другими оконечными устройствами. Во время такой контрольной установки полезно проверить мощность оптического выхода коммуникационного оборудования и определить долю ошибочных битов (Bit Error Rate, BER).

Комбинирование многомодовых и одномодовых волоконно-оптических компонентов. Такое сочетание компонентов создает избыточные оптические потери там, где их быть не должно. Основная разница между одномодовым и многомодовым оптическим волокном состоит в допусках на волоконно-оптические разъемы, соединительные муфты, стыки и другие компоненты. Для многомодовых компонентов размер допуска составляет +-3 микрона, а для одномодовых компонентов +-1 микрон.

Таким образом, одномодовые волоконно-оптические компоненты можно применять в многомодовых инсталляциях, но не наоборот. В первом случае подобная замена допустима лишь в экстренных случаях, поскольку одномодовые компоненты на порядок дороже многомодовых аналогичного назначения. Для отделения одномодовых участков от многомодовых каждое волокно должно заканчиваться в отдельном блоке. Такая концевая заделка защищает его и обычно предусматривает применение оптической панели переключений, при этом каждое волокно кабеля получает отдельный соединитель.

Рекомендуемая литература

1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие/ В. Ф. Шаньгин- М.: ИНФРА-М, 2010

2. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/ П. Б. Хорев- М.: ФОРУМ, 2009
3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : Питер, 2011
4. Алексеев Е.Б., Устинов С.А. Технологии оптических сетей доступа. Тенденции развития в мире и России//Технологии и средства связи: Отраслевой каталог. 2005.
5. Скляров О.К. Волоконно-оптические сети и системы связи: Учебное пособие. СПб.: Изд-во «Лань», 2010. 272 с.
6. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Учеб. пособ. – М.: ДМК Пресс, 2012. – 592 с.
7. Никоноров Н.В., Сидоров А.И. Материалы и технологии волоконной оптики: оптическое волокно для систем передачи информации: Учебное пособие. - СПб.: СПбГУ ИТМО, 2009. - 95 с.
8. Алексеев Е.Б. Оптические сети доступа. Учебное пособие - М: ИПК при МТУ СИ, 2005 г. - 140 с.