Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 621.391.7:004.056.53

Дудак
Максим Николаевич

# Методы несанкционированного доступа к оптическим каналам «многоволновых ВОСП»

**АВТОРЕФЕРАТ**

на соискание степени магистра технических наук
по специальности 1-45 80 01 «Системы, сети и устройства телекоммуникаций»

Научный руководитель
Урядов Владимир Николаевич
кандидат технических наук, доцент

Минск 2020

## КРАТКОЕ ВВЕДЕНИЕ

В настоящее время самым современным, быстрым и помехозащищенным видом связи является связь, где в качестве переносчика информационного сигнала используется волоконно-оптический кабель. Благодаря своим пропускным способностям, возможности использовать высокую несущую частоту, а также большим возможностям мультиплексирования, работа ВОЛС на порядки превосходят возможности пропускной способности других систем связи и измеряются терабитами в секунду, то есть имеют огромную скорость передачи данных.

В последнее время можно встретить оптическое волокно не только в больших магистральных линиях передачи, но и в локальной компьютерной сети, расположенной в пределах одного здания или кампуса, а также при организации «последней мили».

Долгое время считалось, что по причине отсутствия излучения организовать несанкционированный доступ (НСД) в оптическом кабеле вообще не представляется возможным. Но позже, после проведения некоторых исследований, стало ясно, что съем информации в ВОЛС возможен, хотя и более трудно осуществим технически, нежели в случае с медным кабелем. Одна из сложностей состоит в том, что злоумышленник, осуществляющий съем информации с оптического кабеля, может сделать это, только имея физический доступ к кабелю. Тогда он может каким-либо способом отвести часть оптической мощности из световода, а затем направить ее в свое приемное устройство. Тут встречается вторая сложность: величины оптической мощности, которую обычно удается отвести, очень малы. Они могут составлять 0,01÷0,1% от мощности сигнала. Чтобы из отведенного сигнала извлечь затем полезную информацию, злоумышленник вынужден применять приемные устройства и фотодетекторы особой конструкции.

Поскольку доступ к информации возможен, для пользователя линии могут представлять интерес меры по выявлению и пресечению несанкционированного подключения. Аппаратура контроля НСД, устанавливаемая для этого на приемной стороне линии, производит слежение за уровнем принимаемого сигнала. Если она выявляет его уменьшение, то это может являться признаком нелегального подключения: ведь злоумышленник отбирает мощность из линии. Поскольку отбираемая мощность мала, то обнаружить подключение достаточно сложно. Вот еще одна причина, почему злоумышленник не может отвести большие объемы мощности: достоверность перехваченной информации это бы повысило, но на приемной стороне это вызвало бы большое падение мощности, и для аппаратуры контроля такое подключение было бы проще обнаружить.

Таким образом, чтобы обезопасить пользователей от утечки информации был принят Закон на территории РБ "Об информации, информатизации и защите информации" от 10 ноября 2008 года, где провайдеры связи должны обеспечивать соблюдение неразглашение тайны связи и защиту личных файлов, а также сооружений связи от незапланированного или незаконного доступа к ним. Незаконный доступ к личным данным связи и передаваемой по ним информации влечет за собой административную, гражданско-правовую, дисциплинарную или уголовную ответственность в соответствии с законодательством РБ.

Настоящая магистерская работа посвящена исследованию методов несанкционированного доступа к каналам многоволновых ВОСП. Предложены два решения обеспечивающие эту возможность: использование стандартного мультиплексора и акустооптической фильтрации.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы**

В современном мире эффективная работа с информацией является одним из факторов успеха. Защита информации получила свою актуальность в связи с большим количество атак, как на линии связи, так и на средства хранения информации.

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

**Цель работы**

Целью работы является исследование, а также оценка эффективности и определения методов несанкционированного доступа к оптическим каналам многоволновых волоконно-оптических систем передач (ВОСП).

**Задачи исследования**

Для достижения поставленной цели решались следующие задачи:

1. Анализ многоволновых ВОСП.
2. Разработка модели несанкционированного доступа к многоволновым ВОСП.
3. Разработка методики оценки эффективности многоволновых ВОСП.

**Научная новизна результатов работы**

Научная новизна исследования состоит в том, что в ходе работы впервые проведен теоретический анализ работы приемника перехвата информации, а также работы аппаратуры контроля в многоволновых ВОСП.

**Достоверность полученных результатов**

Исходные данные для научных исследований были получены из работ отечественных и зарубежных авторов. Достоверность полученных научных и экспериментальных результатов обеспечивается использованием современных средств и методик проведения исследований, а также применением в исследованиях теоретических и экспериментальных общенаучных методов.

Достоверность также подтверждается теоретическим анализом работы приемника перехвата информации в многоволновых ВОСП.

**Практическая ценность результатов работы**

Практическая значимость полученных результатов состоит в том, что в ходе работы проведено экспериментальное исследование, посвященное изучению возможности обнаружения факта НСД к волоконному световоду.

Эти исследования могут быть использованы при нахождении места непосредственного съема информации в многоволновых ВОСП.

## КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении дается краткая характеристика работы, обоснована актуальность темы диссертации, сформулированы ее цель, практическая значимость, научная новизна и основные этапы исследований.

В 1-ой главе дано определение информационной безопасности, рассмотрены общие вопросы безопасности, угрозы и утечки информации.

Информационная безопасность – это «состояние» информации, характеризующее ее степень защищенности от влияния внешней (природы или человека) и внутренней среды. Ее сигнальная скрытность, конфиденциальность и целостность – это устойчивость к искажающим и разрушающим воздействиям.

С учетом определения «Информационная безопасность» дана классификация видов угроз на информацию (рисунок 1.1).

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).


Рисунок 1.1 - Классификация угроз

Концептуальная модель безопасности информации может содержать следующие компоненты (рисунок 1.2):

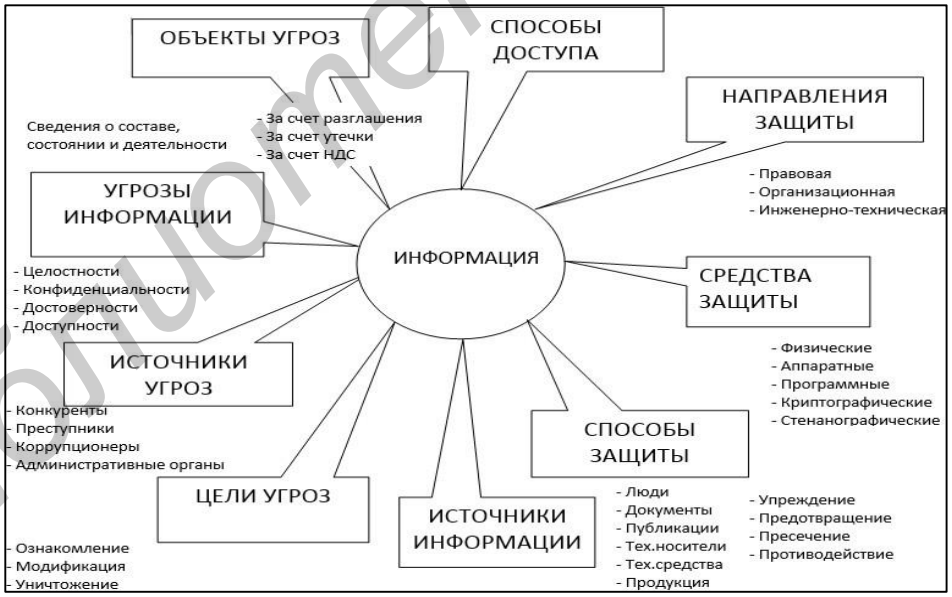


Рисунок 1.2 - Концептуальная модель безопасности информации

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности является несанкционированный доступ.

На рисунке 1.3 показано оптоволокно в разрезе, где видно, что точки 1,2,3, 7 являются наиболее защищенными от несанкционированного доступа, так как располагаются на режимных объектах (в телекоммуникационных центрах или на АТС). Пункты регенерации/усиления оптического сигнала на магистральных линиях обычно размещают в населенных пунктах, на объектах, обеспечивающих защиту от несанкционированного доступа.

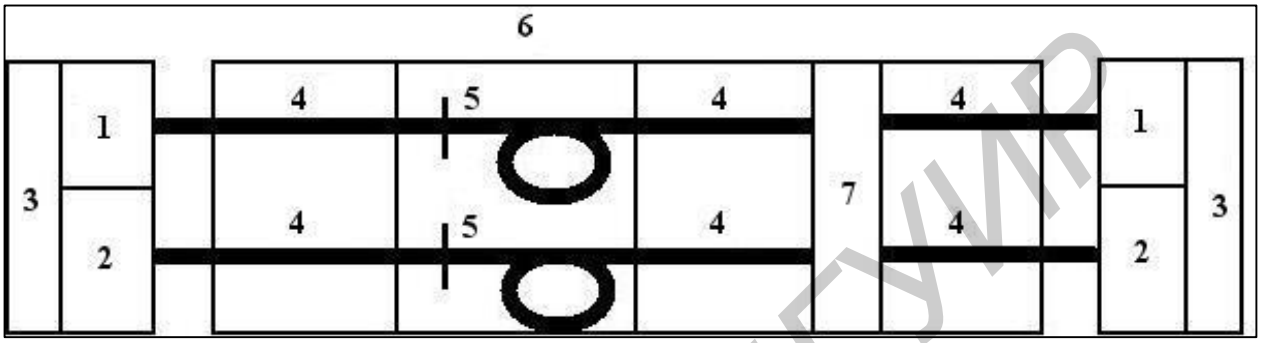


Рисунок 1.3 - Потенциально-возможные места съема сигнала в ВОСП
1 – передатчик оптического сигнала; 2 – приемник оптического сигнала; 3 – оборудование мультиплексирования; 4 – оптическое волокно; 5 – сварное соединение двух оптических волокон на местах стыка строительных длин; 6 – соединительная муфта, в которую помещаются сростки оптических волокон; 7– пункт регенерации/ усиления оптического сигнала.

Сварное соединение 5 располагается в соединительной муфте 6. При некачественном сварном соединении происходит рассеяние излучения, которое может быть зафиксировано злоумышленником. Также рассеяние возможно из-за малого радиуса изгиба волокна при уплотнении кабеля в муфтах.

Однако в ходе дальнейших исследований все же выяснилось, что несанкционированный съем информации с волоконно-оптического кабеля все-таки возможен, правда, при условии физического доступа к кабелю. Поэтому проблема защиты информации от несанкционированного доступа является актуальной и для волоконно-оптических линий связи.

Во 2-ой главе рассмотрены особенности многоволновых систем DWDM и методы несанкционированного доступа с использованием стандартных мультиплексоров:

1) методы физического съема информации;

2) способы несанкционированного доступа.

Существует три способа осуществления НСД:

– разрывный способ. При этом способе аппаратура злоумышленника, отводящая мощность с волокна (приемник перехвата), внедряется в намеренно

созданный разрыв оптического кабеля, с которого осуществляется съем информации;

– безразрывный без принудительного отвода мощности. В этом способе для съема сигнала используется излучение, возникающее естественным образом в результате рассеяния света на муфтах, соединителях, устройствах ввода и вывода оптической мощности, самом оптическом волокне.

– безразрывный с принудительным отводом мощности. Путем какого-либо воздействия на волоконный световод пытаются добиться изменения его оптических свойств, что и приводит к выводу части излучения из световода.

Чтобы осуществить отвод оптического информационного сигнала с кабеля на каком-либо участке, используется локальное воздействие на его волоконные световоды. При таком воздействии изменяются их оптические свойства, что и приводит к «вытеканию» сигнала. Методов воздействия на волокно можно перечислить несколько:

– изгиб волокна;

– изменение диаметра волокна (например, путем давления);

– микроизгибы волокна;

– воздействие химическими реактивами.

Из этих методов наиболее интересным является метод изгиба волокна, потому что он, в отличие от остальных, позволяет организовать направленный вывод излучения. При изменении диаметра световода, а также акустическом или химическом воздействии вышедшее излучение распространяется по многим направлениям и труднее поддается сбору. В случае же изгиба вышедшее излучение распространяется вдоль одного направления, поэтому оно может быть собрано при помощи различных линзовых систем. Вот почему изгиб волокна является популярным вариантом при осуществлении НСД.

Существует множество исследований, посвященных проблеме НСД в традиционных, электрических линиях связи. В них для защиты от НСД предлагается использовать различные методы кодирования, затрудняющие расшифровку информации в случае малых уровней сигнала, но в то же время не влияющие на прием, если уровни сигнала большие. Развитие таких методов привело к появлению «концепции кодового зашумления», которая основывается на теории канала с отводом, впервые введенной Вайнером в 1975 г. Конструктивное развитие данной концепции, разработка методов оценки защищенности, алгоритмов кодирования/декодирования, исследование эффективности кодового зашумления проведено В.И. Коржиком, В.А. Яковлевым с 1981 г. по настоящее время.

Можно предполагать, что применение кодового зашумления в сочетании с вышеописанной системой контроля даст возможность повысить

эффективность ее работы и тем самым увеличить защищенность волоконно-оптических линий связи от попыток НСД.

Добиться изменения угла падения можно механически воздействуя на ОВ, например, изгиб. При изгибе ОВ изменяется угол падения электромагнитной волны на границе с сердцевиной и оболочкой. Угол падения изменяется и может становиться меньше предельно допустимого угла, что будет означать выход некой части электромагнитного излучения из световода (рисунок 1.4).

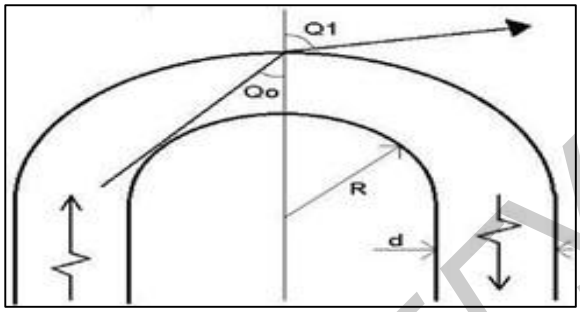


Рисунок 1.4 - Формирование канала утечки при изгибе радиусом R оптоволокна с диаметром сердцевины d
$Q_0$- угол падения; $Q_1$ - угол преломления

Исходя из этого, можно сделать вывод, что изгиб приводит к сильному побочному излучению на месте изгиба, что тем самым создает угрозу съема информации.

Вероятность существования побочных оптических излучений с боковой поверхности ОВ вызвана некими физическими, технологическими и конструктивными факторами:

– излучение вытекающих и излучательных мод на всем ОВ из-за рэлеевского рассеяния на неоднородностях материала ОВ, размеры которых намного меньше самой длины волны излучения;

– существование вытекающих мод на первоначальном участке ОВ, вызванное возбуждением его источником излучения с пространственным распределением, превышающим апертуру волокна;

– изменение направляемых мод в вытекающие благодаря локальным изменениям волноводного параметра на волноводных нерегулярностях волокна: микроизгибах и макроизгибах.

Микроизгиб – приложение внешнего усиления ведет к резкому, но микроскопическому изменению кривизны поверхности, к пространственному смещению длины волны на минимальное расстояние (миллиметры) и к осевым смещениям на несколько микрон. Через получившийся дефект проходит свет, и его можно использовать для съема данных.

Макроизгиб – у каждого типа волокна есть свой минимально допустимый радиус изгиба. Благодаря этому свойство также можно иметь возможность незаконного съема информации. Если сгибать волокно при меньшем радиусе, то возможен пропуск света, которого достаточно для съема информации. Минимально допустимый радиус изгиба ОВ равен 6.5-7.5 см. Многомодовое волокно имеет минимально допустимый радиус уже 3.8 см.

Изменения угла падения можно добиться не только изменением формы оптоволокна при механическом воздействии, но и акустическим воздействием на оптическое волокно. В сердцевине оптоволокна создается дифракционная решетка периодического изменения показателя преломления, которая вызвана воздействием звуковой волны. Электромагнитная волна отклоняется от своего первоначального направления, и часть ее выходит за пределы канала распространения, причем воздействие осуществляется на канал определенной длины волны. Такую задачу осуществляет дифракция Брэгга на высокочастотном звуке (>10 МГц), длина волны $\Lambda$ которого удовлетворяет условию: ($\lambda L/\Lambda^2$), где $\lambda$ - 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 решеткой (рисунок 1.5).

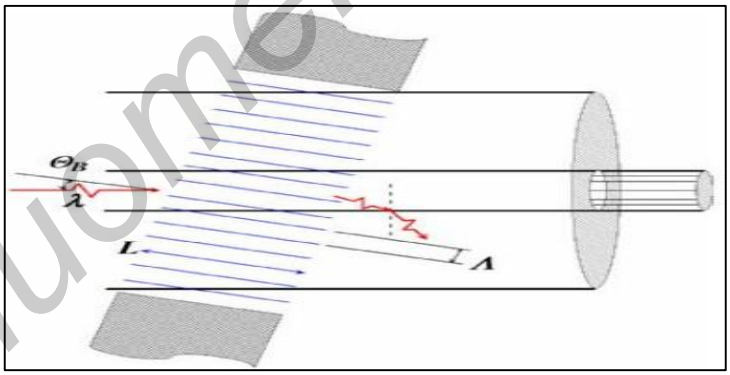


Рисунок 1.5 - Формирование дифракционной решетки в сердцевине оптоволокна звуковой волной

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

$$I = I_0 \sin^2\left(\frac{\pi}{2}\sqrt{J_0 M_2}\frac{L}{\lambda}\right), \quad (1.1)$$

где $J_0$ – интенсивность звуковой волны,

$M_2$=1,51×10$^{-15}$ сек$^3$/кг - акустооптическое качество кварца.

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

Для фильтрации применяется свойство селективности анизотропного Брэгговского рассеяния света на акустической волне. Если на акустооптическую ячейку падает световой поток со сплошным спектром, то дифрагирует лишь та составляющая, длина волны которой удовлетворяет условию Брэгга на данной акустической частоте. При фиксированном угле падения света и изменении частоты ультразвука происходит перестройка устройства, так как Брэгговское условие становится справедливым уже для другой длины волны света.

В 3-ей главе рассмотрены методы обнаружения НСД в оптических каналах многоволновых ВОСП. Все методы обнаружения НСД в оптических волокнах делятся на две группы: методы светопропускания и методы обратного рассеяния.

Имеются два способа выполнения измерений по методике с использованием светопропускания (рисунок 1.6): метод обрыва и метод вносимых потерь.

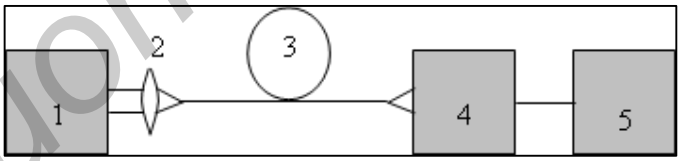


Рисунок 1.6 – Метод светопропускания

1 – Источник света; 2 – Оптическое устройство ввода; 3 – Волоконный световод; 4 – Фотодетектор; 5 – Устройство оценки данных

При методе обрыва определяется световая мощность в двух точках световода: $L_1$ и $L_2$. Обычно точка $L_2$ находится на дальнем конце световода, а точка $L_1$ – очень близко к его началу. При проведении измерений световая мощность P сначала измеряется на конце в точке $L_2$ (км), а затем в точке $L_1$ (км), причем световод должен быть обрезан в точке $L_1$, но при этом не должны изменяться условия ввода между источником света (передатчиком) и световодом. Затем коэффициент затухания $\alpha$ (дБ/км) световода рассчитывается по формуле:

$$\propto = \frac{10}{L_2 - L_1} Lg \frac{P(L_2)}{P(L_1)}, \quad (1.2)$$

Этот метод не лишен недостатков, так как необходимо отрезать короткий кусок волоконного световода, что, например, при использовании волоконно-оптических кабелей с соединителями нецелесообразно.

В данном случае полезным является метод вносимых потерь, при котором измеряется световая мощность на дальнем конце испытуемого световода, а затем она сравнивается со световой мощностью на конце короткого отрезка световода. Такой отрезок световода служит эталоном и должен быть сопоставим с испытываемым световодом по структуре и характеристикам. Во время проведения измерения следует позаботиться о том, чтобы условия возбуждения эталонного отрезка были одинаковыми, насколько возможно с условиями ввода для испытуемого отрезка световода. Из-за этих ограничений точность и воспроизводимость метода вносимых потерь менее предпочтительны, чем у метода обрыва.

Можно считать недостатком то, что речь идет о суммарном измерении по всему отрезку световода, которое не дает информации о локальных измерениях затухания по длине световода. Кроме того, должен иметься доступ к обоим концам волоконного световода.

При методе обратного рассеяния свет вводится и выводится на одном конце волоконного световода (рисунок 1.7). Дополнительно можно получить информацию о процессе затухания вдоль световода.

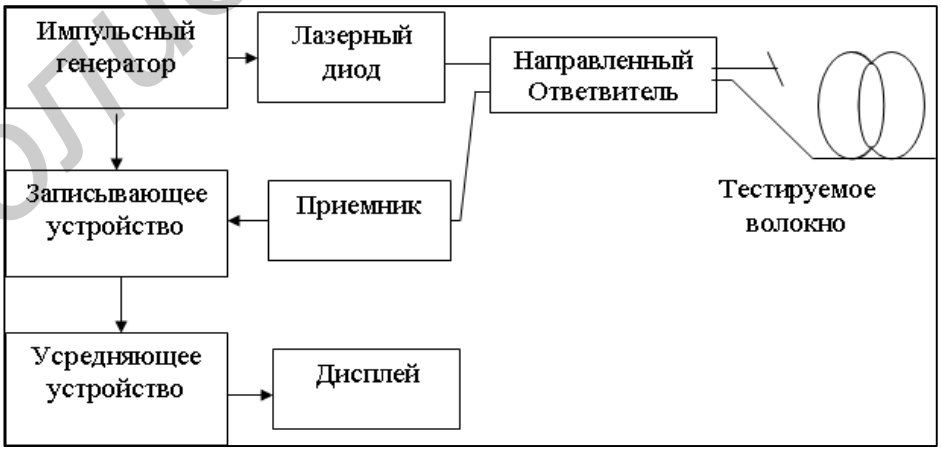


Рисунок 1.7 – Метод обратного рассеяния

В основу метода положено Рэлеевское рассеяние. В то время как основная часть рассеиваемой мощности распространяется в направлении «вперед»,

небольшая ее часть рассеивается назад к передатчику. Эта мощность обратного рассеяния по мере прохождения назад по волоконному световоду также претерпевает затухание. Оставшаяся часть мощности при помощи направленного ответвителя, расположенного перед световодом, выводится и измеряется. По этой световой мощности обратного рассеяния и времени прохождения по световоду можно построить кривую, на которой наглядно видно затухание по всей длине световода (рисунок 1.8).

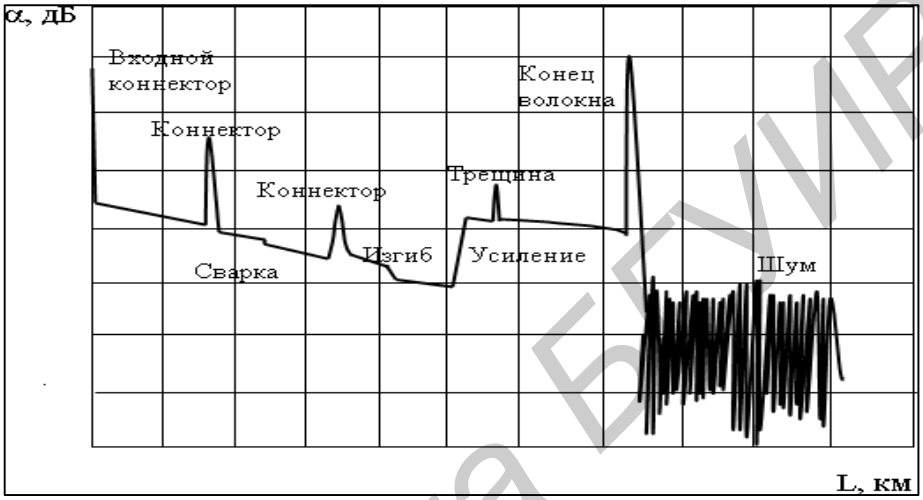


Рисунок 1.8 – Типовая рефлектограмма ВОЛС

В 4-ей главе рассмотрены требования к системам телекоммуникаций:

– конфиденциальность информации – обеспечение просмотра информации в приемлемом формате только для пользователей, имеющих право доступа к этой информации;

– целостность информации – обеспечение неизменности информации при ее передаче;

– аутентичность информации – обеспечение надежной идентификации источника сообщения, а также гарантия того, что источник не является поддельным;

– доступность информации – гарантия доступа санкционированных пользователей к информации.

В данной главе также описаны три основные категории методов, предотвращающих или снижающих до минимума влияние посторонних подключений:

– наблюдение за кабелем и мониторинг;

– сильногнущееся волокно;

– шифрование.

В 5-ой главе произведены измерения потерь в многоволновых ВОСП (измерения потерь в сварных соединениях, на изгибах оптических волокон и измерение потерь отражательных событий), представлены результаты испытаний по методу обратного рассеяния и методу светопропускания. Также в данной главе дано описание рефлектометра *FTB-100B MINI-OTDR,* его технические характеристики, особенности эксплуатации.

В заключении, по результатам испытаний, подведены итоги исследовательской работы. Анализ полученных данных позволяет с уверенностью утверждать, что оптоволоконная техника, в период стремительного развития интернета и связи, представляет огромный интерес не только у пользователей, но и у злоумышленников.

## ЗАКЛЮЧЕНИЕ

На сегодняшний день в период стремительного развития интернета и связи получила достаточно высокое развитие оптоволоконная техника. ВОЛС проложены почти везде. Раннее считалось, что в отсутствии излучения организовать несанкционированный доступ в оптическом кабеле вообще не представляется возможным, но как показывают исследования это возможно. Да и злоумышленники не сидят на месте, поэтому необходимо защищать свои персональные данные от взлома. Принятые законы РБ не всегда останавливают людей от перехвата информации.

Результаты, полученные в ходе исследования позволяют сделать вывод, что волоконно-оптический кабель в данном случае, как показывает эксперимент, справляется от НСД на достаточно высоком уровне.

Подводя итоги проделанного исследования, мы видим, что, поскольку доступ к информации возможен, для пользователя линии могут представлять интерес меры по выявлению и пресечению несанкционированного подключения. Аппаратура контроля НСД, устанавливаемая для этого на приемной стороне линии, производит слежение за уровнем принимаемого сигнала. Если она выявляет его уменьшение, то это может являться признаком нелегального подключения: ведь злоумышленник отбирает мощность из линии. Поскольку отбираемая мощность мала, то обнаружить подключение достаточно сложно. Вот еще одна причина, почему злоумышленник не может отвести большие объемы мощности: достоверность перехваченной информации это бы повысило, но на приемной стороне это вызвало бы большое падение мощности, и для аппаратуры контроля такое подключение было бы проще обнаружить.

## СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1 – 55 юбилейная научная конференция аспирантов, магистрантов и студентов БГУИР. «Защита многоволновых ВОСП от несанкционированного доступа»/ Дудак М.Н., Урядов В.Н.

2 – 56 научная конференция аспирантов, магистрантов и студентов БГУИР. «Способы несанкционированного доступа в волоконно-оптических линиях передачи»/ Дудак М.Н., Урядов В.Н.