РАЗРАБОТКА МЕТОДА КОМПЛЕКСНОГО КОНТРОЛЯ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ ПЕРЕДАЧИ И ЕГО РЕАЛИЗАЦИЯ В КОНТРОЛЛЕРЕ ЗАЩИТЫ

К. И. Балашов, В. В. Шубин

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

В докладе представлен новый метод комплексного контроля волоконно-оптических линий передачи, совмещающий в себе методы обратного рассеяния и прямого детектирования. Предлагаемый метод реализует все необходимые функции защиты: обнаружение и быструю реакцию на попытку съема сигнала, локализацию места нарушения. Предложена практическая реализация метода в комплексном контроллере защиты. Разработаны его структурная и принципиальная электрическая схемы, алгоритм работы. Изготовлен макет устройства, приведены результаты экспериментальных исследований, подтверждающие правильность предложенного метода.

Введение

Для создания распределенных автоматизированных систем специального назначения требуются высокоскоростные каналы передачи информации. Волоконно-оптические системы передачи (ВОСП) благодаря уникальным возможностям по пропускной способности, малому затуханию информационного сигнала, невосприимчивости к электромагнитным помехам являются наилучшим проводным каналом передачи больших объемов информации с высокой скоростью.

Высокая эксплуатационная надежность ВОСП удачно сочетается с высокой степенью защиты передаваемой информации по сравнению с электрическими кабелями, радиорелейными линиями и спутниковой связью. Однако сегодня теоретически доказано и экспериментально подтверждено, что с обычной волоконно-оптической линии передачи (ВОЛП) можно снять оптический сигнал без прерывания передачи, отводя через боковую поверхность оптического волокна (ОВ) менее 1 % мощности передаваемого сигнала. В материалах Э. Сноудена, упоминается о том, что спецслужбы США и их британские коллеги прослушивают не только наземную связь, но также снимают информацию с подводных кабелей, по которым идет значительная часть международного интернет трафика. Для этого, в частности, используется специализированная подлодка «Джимми Картер» (США) [1]. Также известны случаи обнаружения подключений к оптическим линиям в аэропорту Франкфурта, на оптической сети компании Verizone [2] и другие. Поэтому проблема защиты информации в ВОСП является актуальной.

Подходы к защите информации в ВОЛП

Для защиты информации передаваемой по волоконно-оптическим линиям передачи (ВОЛП) можно выделить два различных подхода [3]:

1) защита передаваемой информации шифрованием в сетях общего пользования;

2) защита оптического канала передачи (защищенные ВОСП) в выделенных сетях.

В первом случае криптография является единственным способом защиты информации. Сети общего пользования применяются для предоставления вычислительных ресурсов удаленным пользователям, организации служебной связи и так далее. В этом случае информация ограниченного доступа должна быть надежно защищена от перехвата. Криптография не препятствует съему оптического сигнала, а лишь затрудняет получение информации из перехваченного сообщения. Современные системы шифрования с открытым ключом (например, RSA) обеспечивают защиту лишь только на время, которое требуется для обнаружения нарушителем закрытого ключа. Развитие вычислительной техники непрерывно уменьшает это время, а появление квантовых компьютеров привело к снижению этого времени до нескольких минут. Увеличение длины ключа является временной мерой, не гарантирующей надежную защиту. Кроме того в сетях общего пользования необходимо обеспечивать защиту ВОСП от разнообразных удаленных сетевых атак, количество которых непрерывно возрастает.

Средства криптографической защиты информации (СКЗИ) ограничивают скорость передачи информации. СКЗИ зарубежного производства обеспечивают защиту информации для скоростей передачи до 10 Гбит/с, но их использование для государственных предприятий запрещено положением о средствах защиты информации. Скорости передачи отечественных сертифицированных СКЗИ не превышают 1 Гбит/с.

Развиваемая в настоящее время квантовая криптография также пока не обеспечивает высоких скоростей распределения квантовых ключей. Кроме того квантово-криптографические системы имеют

уязвимости, которые подтверждены результатами экспериментальных исследований.

Во втором случае защита информации осуществляется защитой оптического канала путем снижения мощности сигнала, обнаружением попыток съема, быстрой реакцией на нарушение и локализацией места подключения. Для организации защиты оптических каналов в РФЯЦ-ВНИИЭФ разработаны, сертифицированы (ФСТЭК России [4]) и поставлены на серийное производство универсальные контроллеры защиты FOBOS-100GL, предназначенные для обнаружения и быстрой реакции на нарушение (рис. 1).

Рис. 1. Контроллер защиты FOBOS-100GL

Контроллеры могут быть включены в одноканальные и многоканальные (WDM технологии) ВОСП любого стандарта, работающие на скоростях передачи от 100 Мбит/с до 100 Гбит/с и более. При этом контроллеры не снижают скорость передачи информации, обеспечиваемую приемо-передающей аппаратурой. Для локализации места нарушения в настоящее время используются дополнительные средства защиты – промышленные оптические рефлектометры.

Сравнение методов прямого детектирования и обратного рассеяния

Работа всех ранее разработанных устройств FOBOS основана на методе прямого детектирования, который состоит в анализе проходящего через оптическое волокно (ОВ) контрольного сигнала. Специальная цифровая обработка сигнала методом обнаружения сигналов на фоне случайных помех обеспечивает высокую чувствительность и скорость обнаружения сигнала съема во входной реализации сигнала. Но метод прямого детектирования имеет следующие недостатки:

– непрямое измерение локальных потерь в ОВ (ограничивается точность);

– зависимость времени наблюдения от стабильности контрольного сигнала;

– невозможность локализации попыток съема (обнаружение места нарушения).

Недостатки обусловлены тем, что при прямом детектировании измеряется и анализируется временная зависимость мощности принимаемого контрольного сигнала, которая изменяется не только при отводе мощности из ОВ, но и от флуктуаций передаточных характеристик всех активных элементов ВОСП: передатчика, регенераторов, приемника.

Для устранения вышеизложенных недостатков предложено использовать метод обратного рассеяния. Метод позволяет сразу измерять зависимость коэффициента затухания от длины ОВ, что повышает точность измерения. Прямой зависимости анализируемого сигнала от стабильности передаточных характеристик активных компонентов ВОСП нет. А это в свою очередь позволяет увеличивать время наблюдения, которое определяется стационарностью и эргодичностью анализируемого сигнала.

Кроме того метод обратного рассеяния позволяет обнаружить расстояние, на котором появились новые локальные потери, связанные с нарушением ОВ. Для определения места нарушения (локализация) в исследуемую линию посылают мощный зондирующий импульс и измеряют мощность и время запаздывания импульсов, вернувшихся обратно. Затем время запаздывания пересчитывается в расстояние от начала линии, и определяется удаленность места нарушения от входного полюса ВОЛП. Точность определения расстояния зависит от длительности зондирующего импульса: чем короче импульс, тем выше точность.

Но метод обратного рассеяния имеет существенный недостаток, который ограничивает его использование в системах защиты ВОЛП. Малая мощность обратно рассеянного сигнала требует его накопления, что занимает значительное время. Поэтому метод имеет большую инерционность, которая значительно превышает требуемое время реакции на нарушение. В настоящее время прямое детектирование используется для автоматического обнаружения нарушений и отключения (переключения) передачи оптических сигналов, а метод обратного рассеяния - для последующей локализации нарушений и обнаружения «закладок».

Предлагается метод комплексного контроля ВОЛП, совмещающий в себе методы обратного рассеяния и прямого детектирования, алгоритм и контроллер защиты, реализующие данный подход.

Описание метода комплексного контроля

Максимальная длина ВОЛП без применения оптических усилителей может достигать 160 км [5]. Мощность оптического сигнала по мере его распространения по волокну уменьшается. Злоумышленнику приходится производить съем оптического сигнала в месте, где уровень мощности сигнала достато-

чен для его регистрации и расшифровки, то есть как можно ближе к оптическому передатчику. Таким образом, начальный участок ВОЛП является наиболее вероятным местом подключения аппаратуры перехвата.

Как известно [6], с удалением места нарушения от начала линии величина внесенных дополнительных потерь, необходимых для получения сигнала требуемой мощности, будет увеличиваться. Зависимость требуемых дополнительных потерь $A_д$ для перехвата информации от расстояния L для ОВ с коэффициентом затухания 0,25 дБ/км на длине волны 1625 нм приведена на рис. 2.

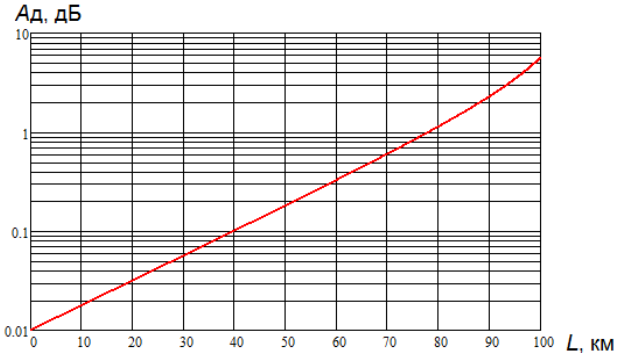

Рис. 2. Зависимость дополнительных потерь от расстояния

На расстоянии свыше 100 км от входного полюса ВОЛП для вывода информации нарушителю потребуется ввести дополнительные прямые потери около 50 дБ. Мощность оптического сигнала при таких потерях недостаточна для съема. На расстоянии свыше 100 км от входного полюса ВОЛП съем информации методом изгиба ОВ при коэффициенте затухания 0,25 дБ/км невыполним. Однако существует вероятность ввода в ОВ, поэтому необходимо обеспечить контроль всей длины ВОЛП.

Таким образом, на начальном участке ВОЛП достаточно контролировать внесение дополнительных прямых потерь величиной около 0,01 дБ.

Для уменьшения инерционности метода обратного рассеяния предлагается увеличить частоту следования зондирующих импульсов, что приведет к наложению обратно рассеянных сигналов от нескольких зондирующих импульсов и формированию суммарного сигнала обратного рассеяния. Такой подход позволит контролировать не только начальный участок ВОЛП, но и всю линию целиком, но с худшими параметрами (большая величина обнаруживаемых дополнительных потерь и большее время реакции контроллера). Это потребовало разработки способа обнаружения локальных потерь, который состоит в следующем (рис. 3) [7]. Период следования коротких зондирующих импульсов $T_и$ выбирают из условия:

$$T_и = \frac{T}{M} \qquad (1)$$

где T – заданное время обнаружения нарушения; M – требуемое количество вычислений среднего значения.

Величину локальных дополнительных потерь для участка на рефлектограмме до обратно-отраженного импульса определяют по формуле:

$$A_{д_0} = 5\log\frac{\sum_{n=1}^{N} 10^{-0{,}1\frac{ca}{n_c}nT_и}}{\sum_{n=1}^{k-1} 10^{-0{,}1\frac{ca}{n_c}nT_и} + 10^{-0{,}2A_д}\cdot\sum_{n=k}^{N} 10^{-0{,}1\frac{ca}{n_c}nT_и}} \qquad (2)$$

а для участка на рефлектограмме после обратно-отраженного импульса по формуле:

$$A_{д_0} = 5\log\frac{\sum_{n=1}^{N-1} 10^{-0{,}1\frac{ca}{n_c}nT_и}}{\sum_{n=1}^{k-1} 10^{-0{,}1\frac{ca}{n_c}nT_и} + 10^{-0{,}2A_д}\cdot\sum_{n=k}^{N-1} 10^{-0{,}1\frac{ca}{n_c}nT_и}} \qquad (3)$$

где N – количество зондирующих импульсов, посланных за время прихода обратно – рассеянного сигнала с округлением до большего значения; n – текущий номер участка обратно-рассеянного сигнала, начиная с рассматриваемого участка с отсчетом в обратную сторону; k – номер участка обратно-рассеянного сигнала, на котором обнаружены локальные дополнительные потери; c – скорость света в вакууме; a – коэффициент затухания в волокне на рабочей длине волны; n_c – показатель преломления сердцевины оптического волокна на рабочей длине волны.

Местоположение локальных дополнительных потерь определяют по формуле:

$$z = \frac{c\left(t + nT_и\right)}{2n_c} \qquad (4)$$

где t – время от посылки зондирующего импульса до появления локальных дополнительных потерь.

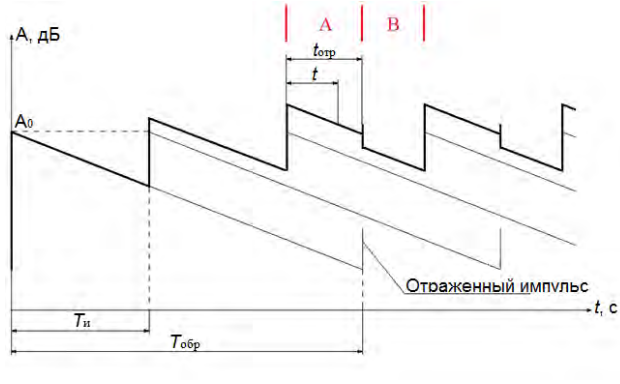

Рис. 3. Схема формирования суммарного сигнала обратного рассеяния

Расчеты по формулам (1–4) показывают, что метод обратного рассеяния позволяет надежно контролировать первые 20 км ВОЛП и обнаруживать требуемое значение дополнительных прямых потерь в 0,01 дБ [3] при времени реакции контроллера менее 1с. Однако на большем расстоянии метод обратного рассеяния не позволяет обнаруживать необходимую величину дополнительных прямых потерь в 0,03 дБ (рис. 3) при сохранении времени реакции контроллера менее 1с. Поэтому необходимо применение метода прямого детектирования в дополнение к методу обратного рассеяния.

Из рис. 2 видно, что если первые 20 км контролируются методом обратного рассеяния, то методом прямого детектирования достаточно контролировать величину дополнительных прямых потерь $A_д \geq 0{,}03$ дБ, что обеспечить при спектральном разделении информационных и контрольных сигналов достаточно просто [3].

Таким образом, предлагаемый способ позволяет вести контроль методом обратного рассеяния на первых 20 км, обнаруживая дополнительные прямые потери $A_д \geq 0{,}01$ дБ, и методом прямого детектирования на расстоянии до 160 км, контролируя дополнительные прямые потери $A_д > 0{,}03$ дБ. Время наблюдения при методе обратного рассеяния не зависит от внешних факторов и значительно превышает время наблюдения для метода прямого детектирования. Локализация мест нарушений возможна на первых 20 км ВОЛП с разрешением в 100 м.

Структурная схема ВОЛП с комплексными контроллерами защиты

На основе предлагаемого метода разработана структурная схема контроллера защиты. На рис. 4 приведена схема защищенной ВОЛП.

На противоположных концах контролируемой ВОЛП, в пределах контролируемой зоны, расположено по одному устройству контроля [8]. МК 1 формирует периодические зондирующие импульсы длительностью 1 мкс с периодом 200 мкс, которые поступают на лазерный диод ЛД 2 и преобразуются в оптические сигналы. После этого контрольные сигналы через оптический циркулятор ОЦ 3 передаются на вход WDM - мультиплексора 4, где складываются с информационными оптическими сигналами, которые передаются на рабочих длинах волн в диапазоне от 1260 до 1565 нм, а контроль осуществляется на длине волны 1625 нм.

Суммарный оптический сигнал поступает в ВОЛП через выходной полюс T_{line}. Отраженное и обратно рассеянное излучение с ВОЛП поступает обратно. Через WDM-мультиплексор 4, ОЦ 3 излучение поступает на фотодиод ФД 6, где преобразуются в фототок. Логарифмирование и масштабирование сигнала производится в логарифмическом усилителе ЛУ 7. После этого сигнал поступает на вход аналого-цифрового преобразователя (АЦП) МК 1, где преобразуется в цифровую форму и обрабатывается по специальной программе. Так происходит контроль методом обратного рассеяния.

Суммарный оптический сигнал, распространяющийся по ВОЛП по обратному каналу, попадает на вход R_{line} устройства контроля. WDM - демультиплексор 8 разделяет сигналы на контрольные и информационные сигналы по длинам волн. Контрольные сигналы принимаются ФД 9, преобразуются в фототок, логарифмируются, масштабируются в ЛУ 10 и поступают на вход АЦП МК 1, где преобразуется в цифровую форму и обрабатывается по специальной программе. Так происходит контроль методом прямого детектирования.

В случае появления на рефлектограмме, сформированной МК 1, локального дефекта с потерями большими установленного порога, или, в случае отклонения контрольного сигнала на величину больше порогового значения, МК 1 формирует сигнал отключения ОП 5 и включает блок индикации БИ 11. ОП 5 переводится в разомкнутое состояние, передача

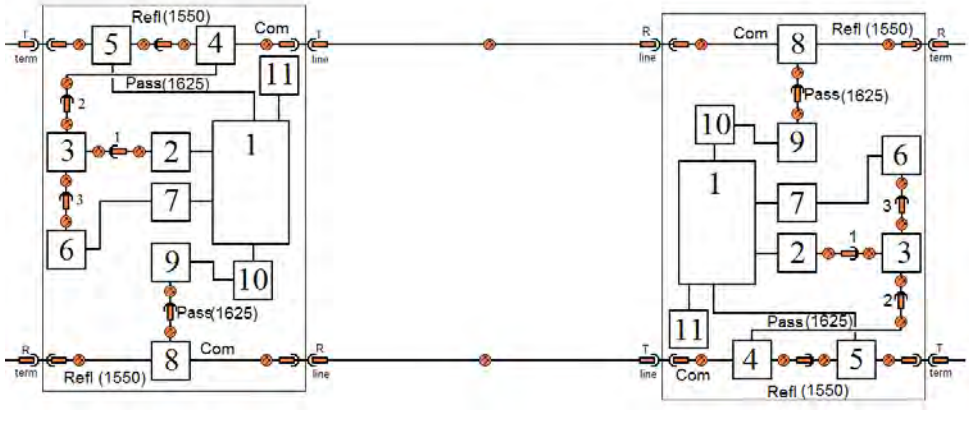

Рис. 4. Структурная схема защищенной ВОЛП: 1 – микроконтроллер (МК) с аналого-цифровым преобразователем (АЦП); 2 – лазерный диод (ЛД); 3 – оптический циркулятор (ОЦ); 4 – WDM-мультиплексор; 5 – оптический переключатель (ОП); 6, 9 – pin-фотодиод (ФД); 7, 10 – логарифмический усилитель (ЛУ); 8 – WDM-демультиплексор; 11 – блок индикации (БИ)

информационных сигналов с входного полюса T_{term} на выходной T_{line} не производится. Контрольные сигналы также не посылаются. В случае обнаружения нарушения на первых 20 км, МК формирует файл, содержащий информацию о месте нарушения. Файл копируется на внешнее запоминающее устройство.

Реализация контроллера защиты и алгоритма его работы

По структурной схеме комплексного контроллера защиты произведены выбор элементной базы и разработка принципиальной электрической схемы. На основе принципиальной электрической схемы была разработана и выпущена печатная плата, которая может быть установлена в корпус контроллера FOBOS-100GL. По разработанной конструкторской документации было произведено макетирование разработанного устройства. На рис. 5 приведен внешний вид макета контроллера защиты.

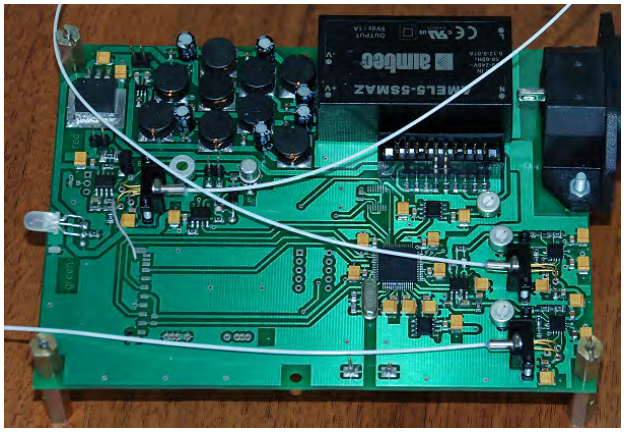

Рис. 5. Внешний вид макета комплексного контроллера защиты

На рис. 6 приведена блок-схема алгоритма работы контроллера защиты. В исходном состоянии контроллер находится в состоянии ВЫКЛЮЧЕН. Переход в режим ВКЛЮЧЕНИЕ осуществляется автоматически с подачей напряжения питания.

На этапе ИНИЦИАЛИЗАЦИЯ осуществляется установка режимов работы микроконтроллера, проверка подключения ОВ к полюсам T_{line} и R_{line}. Если по истечении 15 минут этап не завершается, то производится переход на этап ТРЕВОГА.

После этапа ИНИЦИАЛИЗАЦИЯ происходит автоматический переход на этап НАСТРОЙКА, на котором производится проверка стабильности контрольного сигнала для методов обратного рассеяния и прямого детектирования. В случае если этап НАСТРОЙКА не завершается в течение 15 минут, то происходит переход на этап ТРЕВОГА.

На этапе КОНТРОЛЬ происходит автоматическое обнаружение сигналов попытки съема или ввода оптического сигнала по специальному алгоритму, реализованному в программном обеспечении микроконтроллера. В случае превышения любого из порогов обнаружения контроллер переходит на этап ТРЕВОГА.

В режиме ТРЕВОГА производится отключение передачи информационных оптических сигналов, срабатывает звуковая и световая сигнализация. Если нарушение произошло на первых 20 км контролируемой ВОСП, то на SD карту памяти записывается файл, позволяющий определить расстояние от начала линии до места нарушения. После этого контроллер автоматически переходит в режим ОЖИДАНИЕ. В этом режиме передача информационных оптических сигналов запрещена. Из состояния ОЖИДАНИЯ контроллер может вывести отключение и последующее включение напряжения питания.

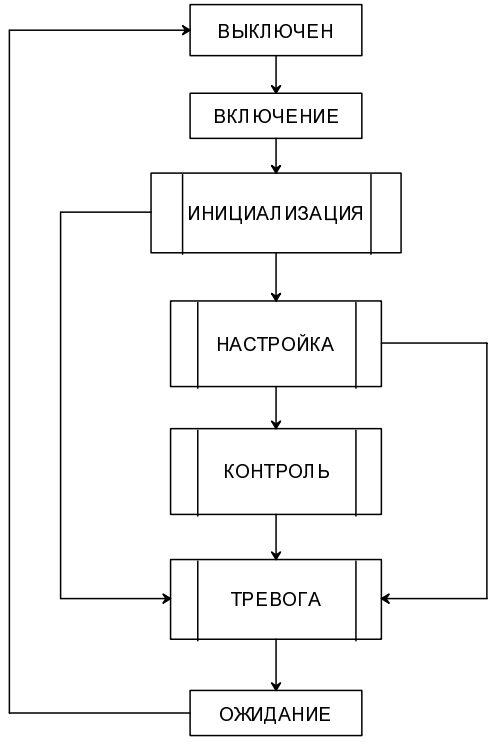

Рис. 6. Блок-схема алгоритма работы контроллера защиты

Результаты экспериментальных исследований макета контроллера защиты

С помощью макета была произведена экспериментальная проверка правильности его работы. Для исследования была использована ВОЛП, состоящая из двух катушек с ОВ SMF-28e общей длиной 51,9 км соединенных между собой с помощью сварного соединения. Потери вносились ответвителем-прищепкой FOD 5503 на удалении 26 км от входного полюса ВОЛП. На рис. 7 приведен внешний вид стенда для экспериментальных исследований.

Рис. 7. Внешний вид стенда для экспериментальных исследований макета

На рис. 8 приведены результаты измерений: наложенные друг на друга рефлектограммы ВОЛП, полученные с помощью макета контроллера защиты до и после внесения дополнительных потерь.

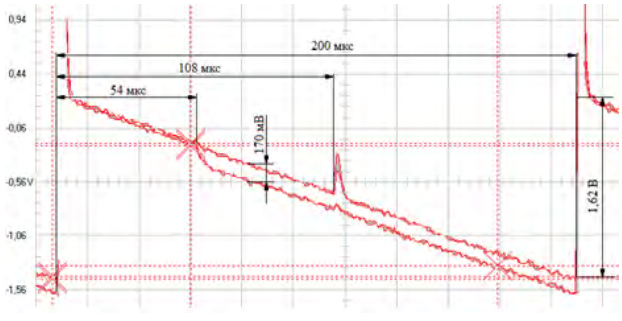

Рис. 8. Рефлектограммы ВОЛП, полученные с помощью макета контроллера защиты

Т. к. период следования зондирующих импульсов меньше времени распространения света в тестируемом волокне (увеличена частота следования зондирующих импульсов), то на рис. 7 представлен суммарный сигнал обратного рассеяния от нескольких зондирующих импульсов. Через 54 мкс на рефлектограмме находится место внесения дополнительных прямых потерь, а через 108 мкс – отраженный от дальнего конца ВОЛП импульс. Т. к. потери внесены на удалении больше, чем 20 км от входного полюса ВОЛП, то на рефлектограмме они приведут к изменению мощности обратно рассеянного сигнала, но на меньшую величину, чем это было бы на первых 20 км. Внесение дополнительных потерь ответвителем-прищепкой FOD 5503 привело к изменению суммарного сигнала обратного рассеяния на 170 мВ, что в пересчете в дБ соответствует 4,53 дБ.

Полученное значение соответствует значению, полученному с помощью рефлектометра FOD 7005 (4,51 дБ).

Пересчитав время, которое прошло от момента ввода зондирующего импульса в волокно, до момента появления на рефлектограмме места внесения дополнительных прямых потерь (200 мкс + 54 мкс) в расстояние, получим 26 км. Место нарушения локализовано.

Таким образом, экспериментально подтверждена правильность предложенного метода контроля и его реализации в комплексном контроллере защиты.

Заключение

Таким образом, предложенный метод комплексного контроля ВОЛП реализует необходимые функции защиты: обнаружение и быструю реакцию на попытку съема оптического сигнала, локализацию нарушения по длине оптического волокна. Разработан способ уменьшения инерционности метода обратного рассеяния, который экспериментально проверен на макете устройства.

Осуществлена практическая реализация метода в комплексном контроллере защиты. Разработаны его структурная и принципиальная электрическая схемы, алгоритм работы. Изготовлен макет устройства, создан стенд, на котором проведены экспериментальные исследования, подтверждающие правильность предложенного метода и его практической реализации.

Литература

1. Ализар А. Как записывают трафик с подводного оптоволокна. [Электронный ресурс]. Режим доступа: https://xakep.ru/2013/07/04/60880/

2. Iqbal M. Z., Fathallah H., Belhadj N. Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networksand Enabling Technologies (HONET). 2011.

3. Шубин В. В. Информационная безопасность волоконно-оптических систем. – Саров: РФЯЦ-ВНИИЭФ, 2015.

4. Система сертификации средств защиты информации по требованиям безопасности информации. № РОСС RU 0001.01БИ00. Сертификат соответствия № 3329 от 30.12.2014.

5. ITU-T Rec. G.692 Optical interfaces for multichannel systems with optical amplifiers, 10/1998.

6. Балашов К. И., Шубин В. В. Контроль нарушений волоконно-оптических линий в распределенных информационно-вычислительных сетях методами интегральной рефлектометрии и прямого детектирования // ВАНТ, сер. Математическое моделирование физических процессов. 2016. Вып. 3. С. 70–79.

7. Пат. 2611588 Российская Федерация, МПК H04B 10/00. Устройство комплексного контроля волоконно-оптических линий / Балашов К. И., Шубин В. В. // Бюл. № 7. 2017.

8. Пат. 2586074 Российская Федерация, МПК H04B 10/00. Защищенная волоконно-оптическая система передачи с селекцией и локализацией аварийных ситуаций / Балашов К. И., Шубин В. В. // Бюл. № 16. 2015.