

# Современные методы разработки информационной безопасности ВОЛС

*Н.Р.Рахимов, В.А.Трушин, Д.И.Бакиун, В.А.Кнутов  
ФГБОУ ВПО НГТУ, Новосибирск, Россия*

**Аннотация:** В данной работе исследованы методы обеспечения защиты информации в ВОЛС. Указано, что в зависимости от особенностей распространения света в ВОЛС различают три типа формирования каналов утечки информации.

**Ключевые слова:** оптическое волокно, защита информации, оптический контакт, генератор помех, нарушенное полное внутреннее отражение, модуляции интенсивности света, лазерный диод.

## ВВЕДЕНИЕ

Целенаправленная и эффективная организация обмена информацией в современном обществе приобретает все большее значение и в первую очередь это связано с интенсификацией практической деятельности человечества. Объем информации, необходимой для успешного функционирования современного общества, растет пропорционально квадрату увеличения производительных сил [1]. И это в первую очередь связано с самим понятием информации как отражение реальности окружающего нас мира, описывающее как свойства индивидуальных объектов и процессов, так и результат их взаимодействия. 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. Требования, предъявляемые к современным системам передачи информации, такие как высокая скорость передачи данных, защищенность от помех, высокая надежность и другие, приводят неоспоримому преимуществу волоконно-оптических линий связи (ВОЛС) перед любыми другими видами. В ближайшем будущем, и в России ВОЛС могут полностью заменить другие типы передачи данных в магистральных линиях связи. В связи с широкой распространенностью волоконно-оптических линий связи возникают проблемы информационной безопасности при их эксплуатации. Изначально, ВОЛС имеют более высокую степень защищенности информации от несанкционированного доступа, чем какие либо другие линии связи. Это связано с физическими

принципами передачи информации, которые основываются на модуляции света распространяющегося в оптическом волноводе. Электромагнитное излучение оптического диапазона выходит за пределы волокна на расстояния не более длины волны (менее 2 мкм) при ненарушенном канале связи, поэтому в пространстве, окружающем волновод, отсутствуют поля на оптических частотах несущие информацию.

Защита информации от утечки по ВОЛС - это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

В современных системах ВОЛС самый перспективный способ передачи информации основан на модуляции интенсивности света. Это наиболее простой способ передачи информации по ВОЛС. При этом способе передачи каналы утечки информации напрямую связаны с интенсивностью светового потока. Волоконно-оптический кабель представляет собой сложную конструкцию с несколькими слоями покрытия оптического волновода. Параметры его таковы, что в пространстве, окружающем кабель, информативное оптическое излучение практически не создает каких-либо электромагнитных полей диапазона близкого к частоте модуляции. Вследствие этого для формирования канала утечки информации требуется физический контакт с оптическим каналом передачи информации – оптоволоком. Это требование является одним из главных факторов защищенности информации в волоконно-оптических системах передачи [1-5]. В данной работе мы будем обсуждать только формирование каналов утечки информации, основанное на оптическом контакте с оптоволоком без нарушения канала связи.

## 1. ПРИНЦИПЫ РАЗРАБОТКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЛС

Угрозы, основанные на оптическом контакте, можно разделить на пассивные и активные. Пассивные угрозы направлены в основном на несанкционированное использование ВОЛС, не оказывая при этом влияния на ее функционирование [2]. Активные

угрозы имеют целью нарушение нормального функционирования ВОЛС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, нарушение работы линий связи, утечка информации (Рис. 1) и т. д. В работе рассматривается метод, предусматривающий защиту, как от пассивных так и от активных угроз.

В зависимости от особенностей распространения света в ВОЛС различают три типа формирования каналов утечки информации:

1) Использующие нарушение полного внутреннего отражения (НПВО).

2) Использующие регистрацию рассеянного излучения.

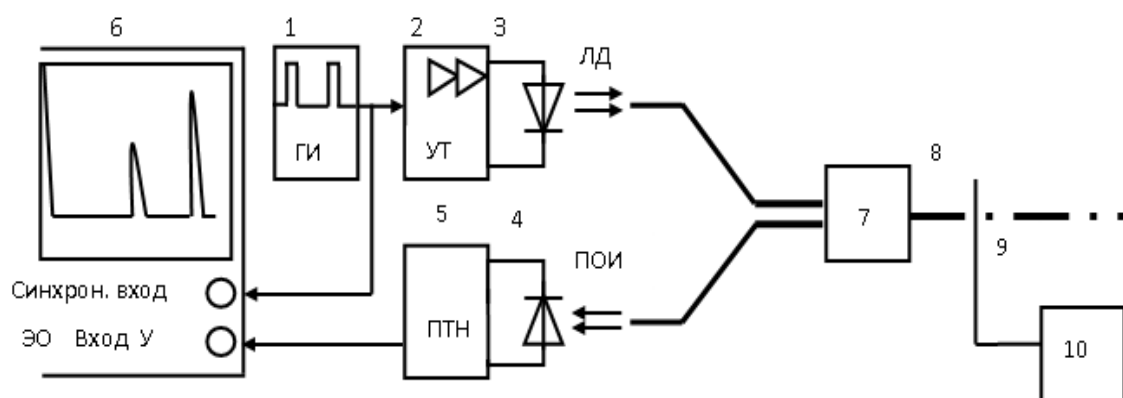


Рис. 1. Применение волоконно-оптического рефлектометра для определения каналов утечки информации в волоконно-оптических линиях связи: 1 - Генератор импульсов (ГИ). 2 - Усилитель тока (УТ). 3 - Лазерный диод (ЛД). 4 - Приемник оптического излучения (ПОИ). 5 - Преобразователь тока. 6 - Осциллограф. 7- Y-образный разветвитель. 8 - Оптический кабель. 9 - механическое, оптическое или специальные воздействия на оптоволокно. 10 - Устройство для прослушивания

Данное устройство работает следующим образом. В исследуемое ОВ вводится через ЛД мощный короткий импульс, который вырабатывает ГИ и усиливает УТ. Затем на этом же конце регистрируется излучение, рассеянное в обратном направлении на различных неоднородностях. По интенсивности этого излучения 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 осциллографе и 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 волоконно-оптического рефлектометра с анализом отраженного сигнала на основе метода импульсной рефлектометрии являются:

1. Значительное снижение динамического диапазона рефлектометров и уменьшение

3) Использующие параметрические методы регистрации проходящего излучения.

В первом случае для измерения больших уровней отражения необходимо подключать рефлектометр к линии с помощью аттенюатора, который позволяет уменьшить уровень сигнала с тем, чтобы отраженный сигнал не влиял на точность измерений.

В случаях использующих регистрацию рассеянного излучения для контроля величины мощности сигнала обратного рассеяния в ОВ используется метод импульсного зондирования, применяемый во всех образцах отечественных и зарубежных рефлектометров (Рис.1).

контролируемого участка ВОЛС при высоком разрешении сигнала по длине оптического тракта (что имеет важное значение для обнаружения локальных неоднородностей при фиксации НД).

2. Затруднение проведения контроля оптического тракта во время передачи информации, содержащей мощные импульсы, что снижает возможности волоконно-оптического рефлектометра, либо усложняет и удорожает систему диагностики.

3. Ограниченный ресурс источников мощных зондирующих импульсов недостаточный для длительного непрерывного контроля ВОЛС.

4. Значительное удорожание стоимости волоконно-оптического рефлектометра из-за использования специализированных источников зондирующего оптического излучения, широкополосной и быстродействующей аппаратуры приемного блока рефлектометров.

Эффективность систем защиты определяется как открытием новых, так и совершенствованием технологий волоконно-оптического рефлектометра, использующих уже известные физические явления.

С течением времени могут появиться новые методы перехвата. Возникнет необходимость дополнять защиту. Это неприменимо для криптографических методов защиты, которые рассчитываются на достаточно длительный срок.

Для решения задач третьего типа предлагаем новый метод обеспечения информационной безопасности в волоконо - оптических линиях связи. Передаваемая информация преобразуется в оптическое излучение и фокусируется на вход ВОЛС, имеющей два выхода. Преобразованная в оптическое излучение информация проходит всю длину линии и с первого выхода фокусируется на чувствительную площадь ПОИ. На второй выход ВОЛС фокусируется шумоподобный электрический сигнал, вырабатываемой генератором помехи (преобразованный в оптический сигнал с помощью полупроводникового лазера). Шумоподобный оптический сигнал, пройдя через второй выход внутрь ВОЛС, создает в ней помеху. Таким образом, по всей длине ВОЛС в обратном направлении относительно информационного сигнала, распространяется шумоподобная оптическая помеха. Поток, поступающий на чувствительную площадь ПОИ, состоит из суммы двух потоков излучения: информационного и шумоподобного.

Фотоэлектрический сигнал на выходе ПОИ тоже состоит из суммы двух сигналов: информационного и шумоподобного. Выделение информационного сигнала из суммарного фотоэлектрического сигнала производится с помощью сумматора. Для этого на один его вход подается суммарный фотоэлектрический сигнал, а на второй – противофазный шумоподобный оптический сигнал с выхода генератора помехи. Благодаря противофазе, шумоподобные сигналы, поступающие на разные входы сумматора от генератора помехи и ПОИ, при условии равных амплитуд компенсируют друг друга. В результате остаётся только информационный сигнал. При попытке несанкционированного съема информации с любого участка волоконо - оптической линии, оптический сигнал будет содержать шумоподобный, сигнал который не даст возможность выделить информационный сигнал из суммарного сигнала. Таким образом, рассмотренный метод позволяет производить защиту информации, передаваемой по волоконо - оптической линии связи, и осуществлять контроль за несанкционированным доступом к ВОЛС.

## 2. ШУМОВОЙ ДВУНАПРАВЛЕННЫЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ В ВОЛС

На *Рис.2* приведена функциональная схема реализации данного способа защиты информации. Рассмотрим её работу. Микрофон

– МИК1 преобразует речевой сигнал в электрический, который усиливается с помощью микрофонного усилителя УЗЧ1 и передается на первый источник излучения речевого сигнала ИИС1. В результате ИИС1 излучает световой поток  $\Phi_{C1}$  закон изменения которого соответствует закону изменения речевого сигнала. Сформированный поток излучения ИИРС1 фокусируется на вход оптического кабеля ВОК1 (световода). Данный световой поток проходит через участок ВОК1 и поступает на светочувствительную площадь первого приемника оптического излучения ПОИ1. Далее сигнал с выхода ПОИ1 усиливается с помощью первого фотоэлектрического усилителя ФУ1 и подается на один из входов первого сумматора СУМ1. Результирующий сигнал подается на вход первого усилителя мощности звуковой частоты УМ1. С выхода УМ1 сигнал, усиленный до требуемого уровня, подается на вход первой динамической головки ДГ1.

1. Рассмотрим обеспечение защиты информации в приемной линии. Генератор помех ГП1 вырабатывает шумоподобный электрический сигнал с прыгающей частотой. Этот сигнал подается на вход первого источника излучения помехи ИИП1. В результате ИИП1 излучает шумоподобный световой поток  $\Phi_{П1}$  который распространяется по всей длине волоконно-оптического кабеля ВОК1. И в оптическом кабеле ВОК1 формируется оптический сигнал, состоящий из двух компонент:  $\Phi_{C1} + \Phi_{П1}$  (первый из которых создаётся звуковым сигналом, поступающим от передающей части, а второй - шумоподобным сигналом, излучаемым источником ИИП1). В результате сложения обоих компонент оптического сигнала, принимаемый сигнал становится практически не распознаваемым. Для выделения полезного сигнала на второй вход сумматора СУМ1 подается шумоподобный сигнал с противофазного выхода ГП1. При этом шумоподобные сигналы, поступающие на оба входа сумматора, являются противофазным. Когда амплитуды шумоподобных сигналов, поступающих на первый и второй вход сумматора одинаковы, сигналы помех компенсируют друг друга, и на выходе сумматора формируется электрический сигнал, соответствующий электрическому сигналу на выходе первого микрофона МИК1. (вышеупомянутой квантовой криптографии).

Принцип действие второго канала разработанного устройства аналогичен к принципу действие первого канала.

При сравнении предлагаемого авторами метода с подобными методами защиты информации можно выделить следующие преимущества:

1. Шумоподобный сигнал подается не со стороны передатчика волоконно-оптической

линии связи, а со стороны приемника информации. Это позволяет выделить информационный сигнал даже при очень сложных законах изменения зашумлений, а также осуществлять контроль за несанкционированным доступом к ВОЛС.

2. Реализация данного способа защиты

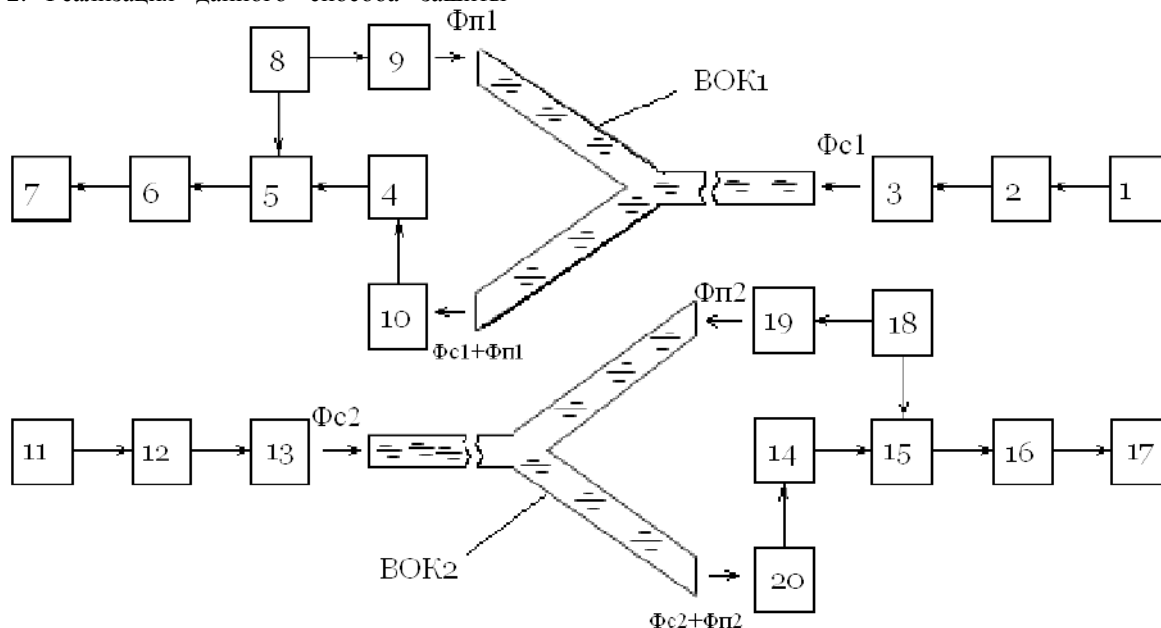


Рис. 2. Блок схема устройства для методов обеспечения защиты информации в ВОЛС: 1 - микрофон – (МИК1); 2 - усилитель звуковой частоты (УЗЧ1); 3 - источник излучения речевого сигнала (лазер) (ИИРС1); 4 - фотоэлектрический усилитель (ФУ1); 5 - сумматор (СУМ1); 6 - усилителя мощности звуковой частоты (УМ1); 7 - динамическая головка (ДГ1); 8 - генератор помех (ГП1); 9 - источник излучения помехи (ИИП1); 10 - приемник оптического излучения (ПОИ1); волоконно-оптический кабель (ВОК1) 11 - МИК2; 12 - УЗЧ2; 13 - ИИРС2; 14 - ФУ2; 15 - СУМ2; 16 - УМ2; 17 - ДГ2; 18 - ГП2; 19 - ИИП2; 20 - ПОИ2.

## ЗАКЛЮЧЕНИЕ

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

## ЛИТЕРАТУРА

- [1] Рахимов Н.Р. Рефлектометрический метод определения каналов утечки информации в волоконно-оптических линиях связи. // Сборник материалов VII Международного научного конгресса ГЕО-СИБИРЬ-2011. Т.4.
- [2] Специализированное приборостроение, метрология, теплофизика, микротехника, нанотехнологии. ч.1. Новосибирск. СГГА. 2011. С.221-225.
- [3] Иванов А. Б. Волоконная оптика: компоненты, системы передачи, измерения, М.: Компания Сайрус Системс, 1999.
- [4] Берлин Б. З., Брискер А. С., Иванов В. С. "Волоконно-оптические системы связи на ГТС," М.: "Радио и связь", 1994 г.
- [5] Гуртов В. А. "Оптоэлектроника и волоконная оптика, Петрозаводск, ПетрГУ, 2005 г.
- [6] <http://www.osp.ru/nets/2008/09/5300705/>.
- [7] Рахимов Н.Р., Ушаков О.К. Оптоэлектронные датчики на основе АФН-эффекта. – Новосибирск, 2010г 218 с.

информации в волоконно-оптической линии связи не требует больших расходов (в отличие от вышеупомянутой квантовой криптографии).



**Ньматжон Рахимович Рахимов** – д.т.н., профессор кафедры Специальных устройств и технологий ФГБОУ ВПО «СГГА». E-mail: [nerah@rambler.ru](mailto:nerah@rambler.ru)



**Трушин Виктор Александрович** – Заведующий кафедрой Защиты информации НГТУ, к.т.н, с.н.с. E-mail: [trushin@corp.nstu.ru](mailto:trushin@corp.nstu.ru)



**Бакшун Денис Игоревич** Аспирант первого курса. Кафедра защиты информации.



**Кнутов Вадим Анатольевич,**  
Аспирант первого курса.  
Кафедра защиты информации.

### **Modern methods of developing information security FOL**

**N.R. RAKHIMOV, V.A. TRUSHIN, D.I.  
BAKUNIN, V.A. KNUTOV**

*Abstract.* This paper investigates the methods of ensuring the protection of information in FOL. It is shown that there are three types of formation of channels of information leakage depending on the characteristics of light propagation in the fiber-optic.

*Key words:* optical fiber, data protection, optical contact, interference source, frustrated total internal reflection, light intensity modulation, a laser diode

### **REFERENCES**

- [1] Rahimov N.R. Reflektometricheskij metod opredelenija kanalov utechki informacii v volokonno-opticheskikh linijah svjazi. // Sbornik materialov VII Mezhdunarodnogo nauchnogo kongressa GEO-SIBIR"-2011. T.4.
- [2] Specializirovannoe priborostroenie, metrologija, teplofizika, mikrotehnika, nanotehnologii. ch.1. Novosibirsk. SGGA. 2011. S.221-225.
- [3] Ivanov A. B. Volokonnaja optika: komponenty, sistemy peredachi, izmerenija, M.: Kompanija Sajrus Sistems, 1999.
- [4] Berlin B. Z., Brisker A. S., Ivanov V. S. "Volokonno-opticheskie sistemy svjazi na GTS," M.: "Radio i svjaz", 1994 g.
- [5] Gurtov V. A. "Optoelektronika i volokonnaja optika, Petrozavodsk, PetrGU, 2005 g.
- [6] <http://www.osp.ru/nets/2008/09/5300705/>.
- [7] Rahimov N.R, Ushakov O.K. Optoelektronnye datchiki na osnove AFN-jeffekta. – Novosibirsk, 2010g 218 s.