ВЫЯВЛЕНИЕ УГРОЗ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ЧЕРЕЗ ВОЛОКОННО-ОПТИЧЕСКИЕ КОММУНИКАЦИИ

В.Гришачев, к.ф.-м.н., Российский Государственный Геологоразведочный Университет, Москва, grishachev@mail.ru

В работе обсуждается возможность обнаружения канала утечки акустической (речевой) информации в штатных волоконно-оптических коммуникациях путем мониторинга оптических излучений. Потенциальную угрозу утечки речевой информации могут создавать любые нештатные световые излучения, так же как и штатные световые потоки, модулированные на акустических частотах.

Современные технологии дальней и локальной кабельных систем связи строятся на основе оптических систем передачи данных, что связано с преимуществами оптического кабеля по сравнению с электрическим кабелем как транспортной среды. Одно из основных направлений развития состоит в обеспечении широкополосного абонентского доступа, который осуществляется на основе оптических сетей, в перспективе – полностью пассивных (passive optical network, PON). Технологии волокно в здание/дом (fiber to the building/home, FTTB/FTTH), в офис (fiber to the office, FTTO) и к рабочему месту (fiber to the workplace/desk, FTTD/FTTD) приводят к тому, что волокно замещает проводные технологии в ближнем окружении пользователя [1,2]. Кроме технологий связи волокно активно применяется в измерительных системах и системах безопасности. Волоконно-оптические распределенные измерительные сети позволяют контролировать все основные физические поля в реальном времени с высокой чувствительностью и точностью [3]. Одним из активных направлений применения волокна в системах безопасности является использование оптических интерфейсов для удлинения специальных линий связи в системах видеонаблюдения при охране периметра и в кабельных системах телевидения.

Продвижение оптических кабельных систем ближе к человеку создает новые угрозы безопасности информации, циркулирующей в здании, офисе, на рабочем месте. Одна из угроз связана с возможностью подслушивания конфиденциальных разговоров с использованием влияния акустических полей на прохождение света в волокне. Оптическое волокно успешно применяют при создании датчиков и распределенных измерительных сетей, и штатная оптическая структурированная кабельная система в здании является не чем иным как распределенной измерительной сетью, с помощью которой можно проводить измерения различных физических полей, в том числе и акустического поля.

Таким образом, в зданиях коммерческих и государственных структур возникает необходимость защиты конфиденциальных переговоров в кабинете руководителя, в служебных помещениях, комнатах для переговоров и других выделенных помещениях от утечки акустической (речевой) информации через оптические структурированные кабельные системы. Настоящая проблема является новой, недостаточно изученной в связи с чем, очень опасной.

ФИЗИЧЕСКИЕ ПРИНЦИПЫ ПОДСЛУШИВАНИЯ

Несанкционированный съем акустической (речевой) информации путем использования штатных волоконно-оптических коммуникаций различного назначения является одним из новых способов акустической разведки, который называется акустооптическим (волоконным) каналом утечки информации [4,5]. Формирование канала утечки связано с тем, что

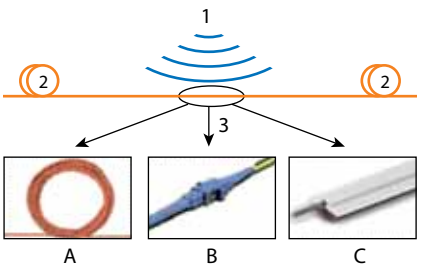

Рис.1. Модель акустооптического (волоконного) канала утечки информации: 1 – источник звука; 2 – оптический кабель; 3 – элемент оптической кабельной системы, подвергаемый звуковому воздействию, включающий свободный оптический кабель (A), разъемное оптическое соединение (B), кабель с виброакустическим контактом с конструкциями здания (C)

акустическое поле от носителя информации воздействует на оптоволокно штатных информационных систем и вызывает модуляцию светового потока при прохождении через оптоволокно, пассивные элементы или активное волоконно-оптическое оборудование на акустических частотах, а также при отражении от неоднородностей в них (рис.1). Модуляция светового потока в оптоволокне может происходить по амплитуде, фазе, поляризации и частоте в результате воздействия акустического поля на физические параметры оптического волокна. На принципах акустооптической модуляции реализованы волоконно-оптические датчики акустического поля в гидролокации, датчики вибраций и другие устройства. Модулированный речью световой поток может выйти далеко за пределы выделенного помещения по штатным волоконно-оптическим коммуникациям. После чего в результате демодуляции злоумышленник может получить доступ к функционирующей в учреждении конфиденциальной информации.

Основными каналами утечки являются световые потоки в оптическом кабеле линий связи. Все световые потоки можно разделить на штатные, связанные с физической реализацией протокола передачи данных, и нештатные, специально сформированные нарушителем для несанкционированного съема речевой информации. Штатные световые потоки, формируемые, например, при цифровых методах передачи информации, позволяют создать канал утечки без нарушения работы всей системы, так как уровень акустического воздействия на штатный световой поток незначительно уменьшает отношение сигнал/шум. К нештатным потокам относятся любые излучения, формируемые источниками света, несанкционированно подключенными к волоконно-оптическим коммуникациям.

Исследование эффективности утечки речевой информации проводилось артикуляционным методом, в котором определяется разборчивость речи W(%) как отношение числа правильно понятых слов на выходе канала к числу слов, произнесенных на входе канала утечки. Они показали высокую опасность нового метода подслушивания. Оценка эффективности проводилась для амплитудной модуляции проходящих световых потоков в линии связи, содержащей основные элементы пассивных оптических сетей: оптический кабель, – свободный и прикрепленный к конструкциям зданий, разъемные соединения, аттенюаторы и т.д. В результате проведенных исследований на стандартном общедоступном оборудовании показана возможность подслушивания через волоконно-оптические коммуникации речи с уровнем звукового давления порядка 60 дБ с разборчивостью W до 80%. Глубина модуляции интенсивности проходящего светового потока достигала насыщения при уровне звукового давления выше 90 дБ и составляла 0,3%.

СЦЕНАРИЙ УГРОЗЫ ПОДСЛУШИВАНИЯ

Обсудим общую последовательность действий нарушителя по сбору акустической информации через волоконно-оптические коммуникации и дадим общую характеристику используемых специаль-

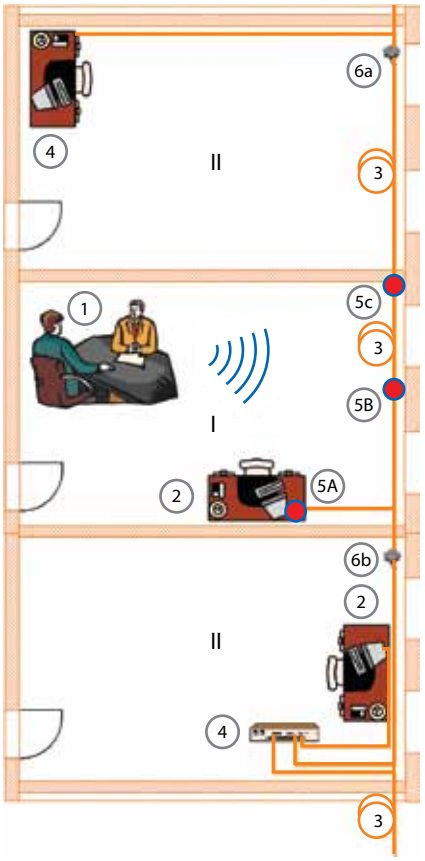

Рис.2. Обобщенный сценарий утечки акустической (речевой) информации через волоконно-оптические коммуникации (модель акустооптического (волоконного) канала утечки): I – выделенное помещение, II – вспомогательные помещения, 1 – место конфиденциальных переговоров; 2 – рабочая станция (компьютер) с волоконно-оптическими коммуникациями, 3 – волоконно-оптические коммуникации, 4 – штатное активное волоконно-оптическое оборудование, 5 – место возможного расположения каналов утечки типа A, B, C, 6 – техническое средство акустической разведки: a (источник) и b (приемник) в случае канала утечки на прохождение; a или b (источник и приемник в одном месте) в случае канала утечки на отражение

ных технических средств (рис.2). Формирование акустооптического (волоконного) канала утечки информации практически невозможно без физического доступа к оптическому кабелю, проходящему через выделенные помещения. Кабельная сеть должна быть свободна от активного волоконно-оптического оборудования на участке между нарушителем и источником акустической информации, что связано с восстановлением формы штатных сигналов и подавлением шумовых составляющих излучения в активном оборудовании. Между нарушителем и источником акустической информации должен располагаться оптический кабель с пассивными оптическими элементами, которые не изменяют существенным образом модуляцию светового потока. К пассивным оптическим элементам, кроме оптического кабеля, относятся розетки, адаптеры, делители, ответвители, аттенюаторы. Надо отметить, что подобная структура оптической кабельной сети является наиболее перспективной для абонентского доступа и активно развивается в виде технологии пассивных оптических сетей.

Реализация канала утечки требует применения технических средств подключения к кабелю и регистрации оптического излучения. Подключение осуществляется через штатные разъемные соединения, которые используются для соединения отдельных частей сети между собой, для присоединения к стационарным (optical line terminal, OLT) и сетевым (optical network terminal, ONT) терминалам. Соединение разъединяется и в него вставляется вставка с вводом зондирующего излучения и ответвителя части излучения. Другой способ присоединения состоит в применении ответвителя излучения на макроизгибе оптического кабеля. Все предложенные способы не требуют применения специальных технических средств, распростра-

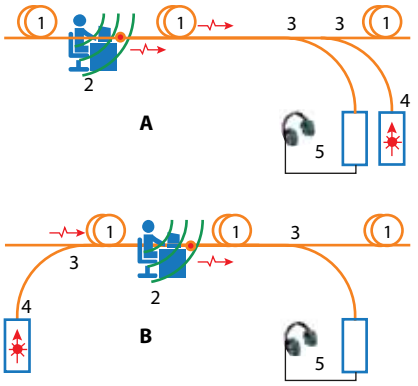

Рис.3. Структура акустооптического (волоконного) канала утечки в схеме на отражение оптического излучения (A) и в схеме на прохождение оптического излучения (B): 1 – волоконно-оптическая кабельная сеть, 2 – источник конфиденциальной речевой информации с чувствительным к виброакустическому воздействию участком волоконно-оптического кабеля, 3 – волоконно-оптический ответвитель, 4 – источник света (лазер), 5 – аналоговый волоконно-оптический приемник излучения с акустическим демодулятором и наушниками

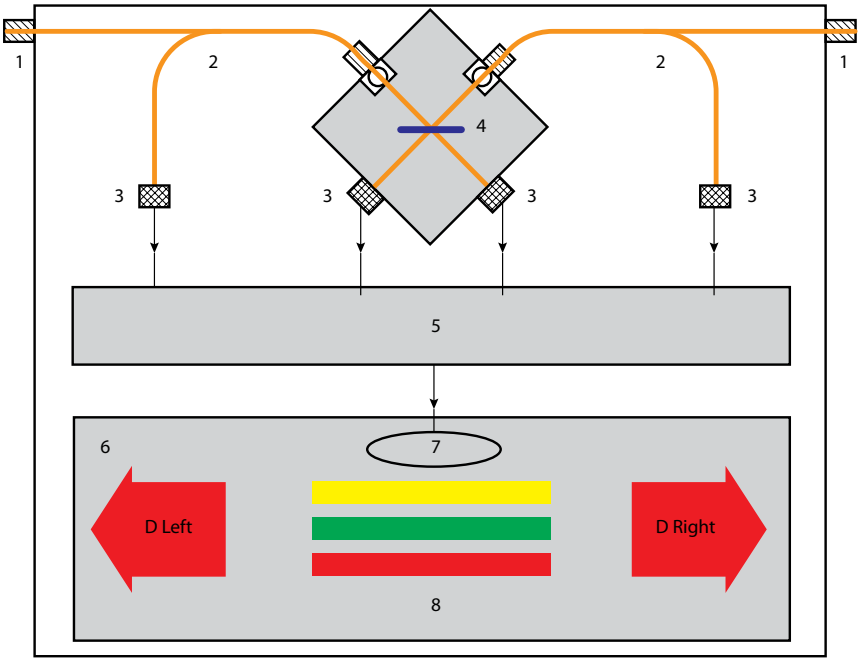

Рис.4. Индикатор атаки внешний: 1 – волоконно-оптические входы, 2 – волоконно-оптические ответвители, 3 – фотодетекторы, 4 – спектроделитель, 5 – спектроанализатор, 6 – блок индикации, 7 – звуковой индикатор атаки, DLeft – индикатор атаки слева, DRight – индикатор атаки справа, 8 – цветовые индикаторы опасности

нение которых регламентировано нормативными документами – такие приспособления используются при монтаже оптической сети. Еще один способ использует нештатный разрыв кабеля с вставкой ответвителя путем сварки волокон.

Оптическая схема подслушивания может быть реализована несколькими способами (рис.3). Во-первых, могут быть применены специальные зондирующие источники света, которые не предусмотрены штатной сетью. Зондировать можно методом отражения или пропускания зондирующего луча сквозь место модуляции. В этом случае можно совместить его с приемо-передающим излучением. Во-вторых, для подслушивания может быть использовано штатное излучение, применяемое для передачи трафика внутри сети.

Опасность канала утечки можно определить по эффективности акустической модуляции в месте расположения источника информации. Акустическое поле вызывает различные виды модуляции световых потоков в оптическом волокне. Подбирая параметры демодуляции светового потока (амплитуду, фазу, поляризацию или частоту) всегда можно добиться очень высокой эффективности канала утечки акустической (речевой) информации. Еще одна опасность связана с доступностью монтажного оборудования, которое может быть использовано как специальное техническое средство акустической разведки. Например, для речевой связи между монтажниками сети используются волоконно-оптические телефоны, которые позволяют при прямом присоединении к волокну осуществлять звуковую связь на расстоянии более 200 км. Волоконно-оптические телефоны могут подключаться к оптическому кабелю без его разрыва с помощью макроизгиба оптоволокна. На том же принципе присоединения работает определитель наличия оптического сигнала в волокне, который позволяет устанавливать направление распространения оптического сигнала в волокне с покрытием 250 мкм, 900 мкм, а также в стандартных оптических шнурах толщиной до 3 мм без их разрыва. Для подслушивания может быть использован измеритель уровня обратного отражения, предназначенный для контроля качества полировки одномодовых волоконно-оптических соединителей и измерения уровня обратного отражения от других компонентов линий связи. Еще большими возможностями обладает рефлектометр – основное устройство контроля состояния оптического кабеля. Названные приборы являются общедоступными и широко используются при монтаже оптических кабельных систем, что повышает опасность их применения в канале утечки [6].

ПРОФИЛАКТИКА УГРОЗ ПОДСЛУШИВАНИЯ

Все основные способы противодействия утечки речевой информации через волноводные каналы условно можно разделить на следующие виды:

- звукоизоляция среды канала передачи – пассивный способ, заключающийся в уменьшении влияния акустического поля на среду канала передачи;
- фильтрация носителя информации в канале передачи – способ, заключающийся в непропускании через канал нештатных сигналов

и модуляций с конфиденциальной речевой информацией;

- маскировка носителя информации в канале передачи – способ, заключающийся в ее сокрытии посредством добавления специального маскирующего сигнала и модуляций;
- зашумление среды канала передачи – активный способ, заключающийся в создании искусственных помех и шумов на акустических частотах [7, 8].

Каждый способ имеет свои недостатки и достоинства, но общая эффективность любой защиты во многом зависит от технических возможностей обнаружения угрозы безопасности информации [9]. Технические средства, позволяющие выявить сам факт подслушивания или подготовки оборудования для его осуществления, несомненно, повышают надежность системы защиты. В случае волоконно-оптических коммуникаций следует учитывать физические особенности волоконно-оптического канала связи, такие как малые линейные размеры, направленность излучения и отсутствие побочных световых потоков, выходящих за пределы канала.

Особенности волоконно-оптического канала позволяют предложить простой и эффективный способ обнаружения несанкционированного съема информации (подслушивания) путем контроля существующих в канале световых потоков. Любая атака на систему безопасности через волоконно-оптический канал для получения доступа к акустической (речевой) информации связана с оптическими потоками в нем. Контроль параметров световых потоков в канале позволяет выявить любую возможность несанкционированного съема. Для этого требуется регистрировать проходящее по волоконно-оптическим элементам излучение, выделять санкционированные носители информации (штатное излучение), выявлять несанкционированные потоки (нештатное излучение) и модуляции на акустических частотах в любом из них. Нештатное излучение (от внешних источников) имеет спектральный состав, которое может как пересекаться со штатным излучением, так и не пересекаться с ним. При этом штатное излучение модулируется внешним акустическим сигналом с конфиденциальной информацией.

Предотвращение подслушивания достигается выполнением следующих правил. Во-первых, штатные световые потоки не должны быть модулированы на звуковых частотах. Во-вторых, должны отсутствовать нештатные потоки, не предусмотренные физической реализацией протокола передачи данных в сети, а при их наличии они не должны быть модулированы звуком. Эти простые правила дают возможность обнаружить атаку на систему безопасности и нейтрализовать ее. Таким образом, степень опасности утечки акустической (речевой) информации определяется по следующим признакам:

- нештатный световой поток обнаруживается в канале передачи информации;
- штатный световой поток имеет модуляцию по одному из параметров оптического излучения

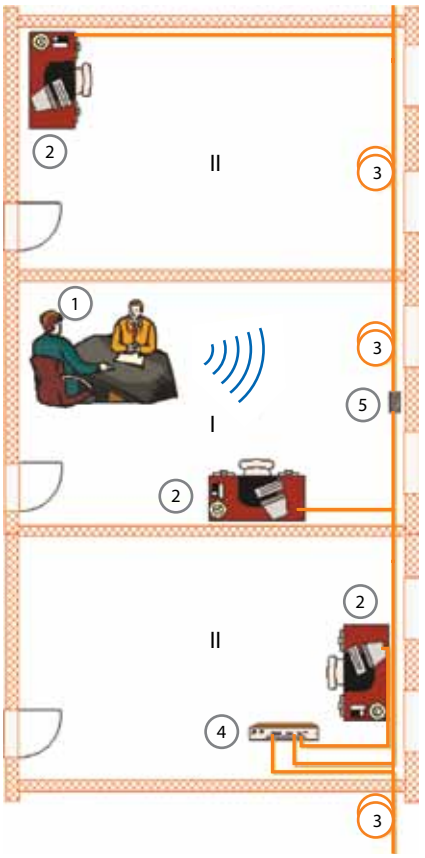

Рис. 6. Принципиальная схема построения системы защиты от утечки речевой информации через волоконно-оптические коммуникации на основе детектора атаки: I – выделенное помещение, II – вспомогательные помещения; 1 – место конфиденциальных переговоров, 2 – рабочее место, 3 – волоконно-оптический кабель, 4 – активное волоконно-оптическое сетевое оборудование, 5 – место включения детектора атаки

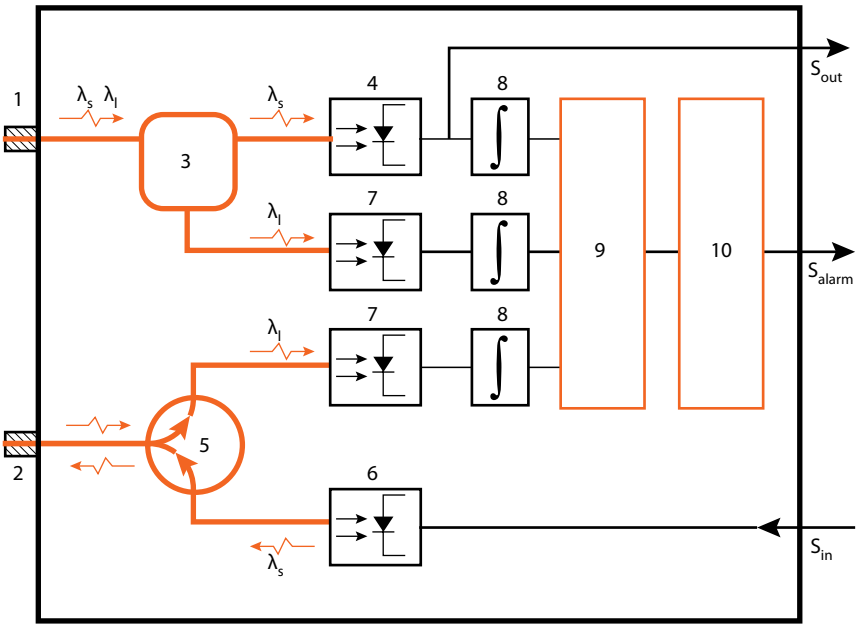

Рис.5. Индикатор атаки встроенный: 1 – оптический вход, 2 – оптический выход, 3 – мультиплексор, разделяющий информационный сигнал на длине волны λ_s и зондирующий световой поток на длине волны λ_l, 4 – штатный фотоприемник с входным информационным сигналом Sout, 5 – ответвитель, 6 – штатный передатчик с выходным информационным сигналом Sin, 7 – дополнительные фотоприемники контроля, 8 – интегрирующие элементы, 9 – анализатор спектра, 10 – аналого-цифровой преобразователь, вырабатывающий сигнал опасности

(амплитуде, фазе, поляризации, частоте) и/или одновременно по нескольким параметрам внешним акустическим сигналом;

- нештатные световые потоки, разделеные по спектру, модуллируются внешним акустическим сигналом (на данной оптической длине волны) по одному из параметров оптического излучения (амплитуде, фазе, поляризации, частоте) и/или одновременно по нескольким параметрам.

Если хотя бы одного из этих условий выполняется, этого бывает достаточно для того, чтобы сформировать канал утечки акустической (речевой) информации. Этот факт можно использовать для оценки угрозы информационной безопасности.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ЗАЩИТЫ

Задача обнаружения возможности утечки речевой информации через штатные волоконно-оптические коммуникации решается путем установки специальных технических средств, регистрирующих световые потоки в волоконно-оптическом канале передачи информации. Реализация может быть осуществлена на основе стандартных или специально созданных элементов, в число которых входит фотоприемное устройство, подключаемое к волоконно-оптическому каналу; оптический, электронный и оптико-электронный аналитический элемент для выделения акустических колебаний параметров регистрируемого оптического излучения. Устройство защиты может быть выполнено в двух конструктивных решениях: в виде отдельного блока, имеющего собственную систему сигнализации угрозы, или блока, встроенного в активное оборудование, имеющего информационную связь с основным оборудованием. Обсудим возможную реализацию устройств и особенности их функционирования.

Внешнее устройство индикации угрозы (рис.4) включается в оптический канал с помощью стандартных оптических разъемов и замыкает линию связи без существенного влияния на проходящий трафик. Основную опасность несет нештатное зондирующее излучение, отделение которого от штатного излучения производится спектроделителем. Падающее излучение на штатной длине волны отражается, а нештатное излучение на иных длинах волн проходит через него и регистрируется фотоприемником. Часть прошедшего через спектроделитель штатного излучения отводится и регистрируется другим фотоприемником. Полученные на выходе фотоприемников сигналы анализируются на существование нештатного зондирующего излучения и на возможные амплитудные модуляции излучения. По полученным данным принимается решение об опасности – каков уровень опасности и с какой стороны от индикатора он исходит. Высший уровень опасности соответствует существованию нештатного излучения или амплитудной модуляции штатного излучения. Средний уровень соответствует наличию амплитудной модуляции штатного излучения на уровне шумов в оптическом канале. Отсутствие нештатных излучений и какой-либо нештатной модуляции соответствует безопасному режиму работы.

Хотя устройство регистрирует только амплитудную модуляцию оптических излучений и не регистрирует другие виды модуляции, надо учитывать, что другие виды модуляции могут эффективно наблюдаться только при использовании нештатного зондирующего излучения. Поэтому можно утверждать, что путем регистрации нештатного излучения обеспечивается контроль всех видов модуляции. Еще одна возможность, которой обладает данное устройство, – его включение выполняет роль фильтра нештатных оптических излучений: штатное излучение проходит индикатор угрозы, а нештатное не проходят. Подобное свойство значительно ограничивает применение оптической схемы на прохождение, которая эффективнее схемы на отражение. Отраженный сигнал всегда слабее прямого зондирующего излучения. Схема на отражение для нарушителя требует более интенсивного излучения, чтобы достичь приемлемого отраженного сигнала. Но для индикатора угрозы любой зондирующий сигнал является прямым, идущим либо слева либо справа от него, таким образом его регистрация будет намного надежнее, чем у нарушителя, регистрирующего только отраженный сигнал.

Внутреннее устройство индикации угрозы (рис.5) может встраиваться непосредственно в активное оборудование оптической сети. Оно может быть интегрировано в оборудование или присоединяться через съемные модули – трансиверы. В последнем случае физического изменения основного оборудования не требуется, изменяется только драйвер самого трансивера. Основная проблема подобного преобразования состоит в размещении дополнительных оптических элементов в требуемом форм-факторе трансивера. Обсудим структуру и работу устройства индикации, интегрированного в активное двухпортовое оборудование с раздельными оптоволоконными входом (канал приемника) и выходом (канал передатчика). На каждое волокно ставиться своя система контроля в виде дополнительного фотоприемника. В порте приемника сигнал разделяется на штатное и нештатное излучение с помощью оптического циркулятора. Информационный сигнал штатного приемника обрабатывается обычными средствами по каналу передачи, а также поступает на интегратор, на выходе которого вырабатывается аналоговый сигнал от штатного излучения с возможной модуляцией на акустических частотах. Выделенное нештатное излучение регистрируется собственным приемником и преобразуется в аналоговый сигнал. В порте передатчика нет входящих излучений, поэтому в канале не требуется разделение излучений на штатное и нештатное, они разделены по направлению распространения. Фотоприемник подключен к каналу передатчика через ответвитель, и сигнал от него также интегрируется. Таким образом, система контроля содержит три приемника с интегрирующими устройствами, формирующими три аналоговых сигнала, по которым и делается вывод об угрозе подслушивания. Суть анализа – определить наличие нештатных излучений или обнаружить в спектрах сигналов характерные составляющие речи – форманты. По его результату вырабатывается сигнал опасности.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

В настоящее время реализации описанных выше способов выявления угроз утечки речевой информации не существует. Как видно из общего описания принципов функционирования устройств защиты, создание рабочих макетов для обнаружения подслушивания через волоконно-оптические коммуникации возможно на основе стандартного оборудования. Основным элементом системы защиты является волоконно-оптический фотоприемник с усилителем на звуковых частотах, который присутствует в любом аналоговом волоконно-оптическом телефоне. Стандартный аналоговый волоконно-оптический телефон обладает высокой чувствительностью, что позволяет регистрировать очень малые колебания интенсивности и выявлять попытки подслушивания. Однако он имеет и существенные недостатки для систем защиты, одним из которых является смещение чувствительности в инфракрасную область спектра, что не позволяет регистрировать с высокой надежностью зондирующие световые потоки видимой области спектра. На расстояниях в несколько сотен метров общие оптические потери составят несколько децибел на длинах волн видимого диапазона в стандартных кварцевых волокнах, что не позволяет надежно детектировать слабое оптическое излучение штатными фотоприемниками. Другой недостаток – необходимость дополнительных волоконно-оптических элементов для регистрации модуляции по поляризации, частоте и фазе. Но в любом случае принципы функционирования волоконно-оптического телефона делают его наиболее близким к использованию в системах защиты от прослушивания через волоконно-оптические коммуникации.

Защиту выделенного помещения от прослушивания через волоконно-оптические коммуникации можно представить в следующем виде (рис.6). Оптический кабель проходит через выделенное помещение и присоединяется к компьютеру на рабочем месте. Весь кабель вместе с соединительными элементами внутри помещения выступает как система, подвергаемая акустическому воздействию, формируемому речью носителей конфиденциальной информации. Световой поток модулируется речью, выходит за пределы выделенного помещения и может быть зарегистрирован злоумышленником. Опасными для подсоединения технических средств разведки злоумышленника являются все участки сети в выделенном помещении от одного активного оборудования до другого. Определив опасный участок, устанавливаем устройство детектирования атаки в выделенном помещении путем оптической вставки.

Мы проводили модельные прослушивания волоконно-оптической линии связи, состоящей из оптического кабеля со сдвоенным волокном длиной более 25 м и толщиной каждого 3 мм. Световой поток формировался оптическим тестером, гелий-неоновым лазером и регистрировался волоконно-оптическим телефоном с аналоговой модуляцией.

Акустическое воздействие создавалось локально с помощью динамиков компьютера, действующих непосредственно на кабель и элементы сети. Речевой сигнал был

сильно зашумлен, но слова речи распознавались на слух.

Представленные модельные исследования подтверждают возможность реализации подобных схем выявления атаки даже с помощью непрофильного оборудования. Производство специализированного оборудования может более надежно решить проблему выявления подслушивания и помочь службам безопасности защищать речевую информацию в современных условиях быстрого распространения волоконно-оптических технологий связи.

ЗАКЛЮЧЕНИЕ

Настоящая работа является развитием патента на изобретение [9], в котором предлагается решение по обеспечению информационной безопасности переговоров в выделенных помещениях путем выявления возможных угроз по формированию каналов утечки акустической (речевой) информации через волоконно-оптические системы связи и предлагается к использованию в системах защиты конфиденциальной речевой информации. Обнаружение канала утечки акустической (речевой) информации проводится путем контроля оптических излучений в штатных волоконно-оптических коммуникациях. Появление любых нештатных световых излучений или модуляций на акустических частотах штатных световых потоков создает потенциальную угрозу утечки речевой информации.

ЛИТЕРАТУРА

1. **LamC.** Passive Optical Networks: Principles and Practice. – San Diego, California.: Elsevier, 2007.
2. **Trojer E., Dahlfort S., Hood D. and Mickelsson H.** Current and next-generation PONs: A technical overview of present and future PON technology. – Ericsson Review, 2008, №. 2, p. 64.
3. Волоконно-оптические датчики. Вводный курс для инженеров и научных работников. Под редакцией Удда Э. М.: Техносфера, 2008.
4. **Гришачев В., Халяпин Д., Шевченко Н., Мерзликин В.** Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС. – Специальная техника, 2009, №2, с. 2.
5. **Гришачев В., Косенко О.** Практическая оценка эффективности канала утечки акустической (речевой) информации через волоконно-оптические коммуникации. – Вопросы защиты информации, 2010, №2, с.18.
6. Fiber Optic Devices Ltd. (FOD) http://www.fod.ru.
7. Патент РФ № 2 416 167. Способ и устройство активной защиты конфиденциальной речевой информации от утечки по акусто-опто-волоконному каналу на основе внешнего оптического зашумления / **Гришачев В., Халяпин Д., Шевченко Н.**
8. Патент РФ № 2 416 166. Способы и устройства активной защиты речевой информации от прослушивания по акусто-опто-волоконному каналу утечки / **Гришачев В., Халяпин Д., Шевченко Н.**
9. **Гришачев В.** Волоконно-оптический детектор угроз утечки речевой информации через волоконно-оптические коммуникации. – Заявка на изобретение РФ №2009134092 от 14.09.2009 г. Решение о выдаче патента от 18.04.2011.