РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 428 798** (13) **C2**

(51) МПК
H04B 10/12 (2006.01)
G01R 29/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2009134092/09, 14.09.2009**

(24) Дата начала отсчета срока действия патента:
14.09.2009

Приоритет(ы):
(22) Дата подачи заявки: **14.09.2009**

(43) Дата публикации заявки: **20.03.2011** Бюл. № 8

(45) Опубликовано: **10.09.2011** Бюл. № **25**

(56) Список документов, цитированных в отчете о поиске: **RU 2362271 C1, 20.07.2009. RU 2230435 C1, 10.06.2004. RU 2128885 C1, 10.04.1999. US 5073982 A, 17.12.1991. US 5161044 A, 03.11.1992.**

Адрес для переписки:
117216, Москва, бул. Дм. Донского, 9, корп.4, кв.2, В.В. Гришачеву

(72) Автор(ы):
Гришачев Владимир Васильевич (RU)

(73) Патентообладатель(и):
Гришачев Владимир Васильевич (RU)

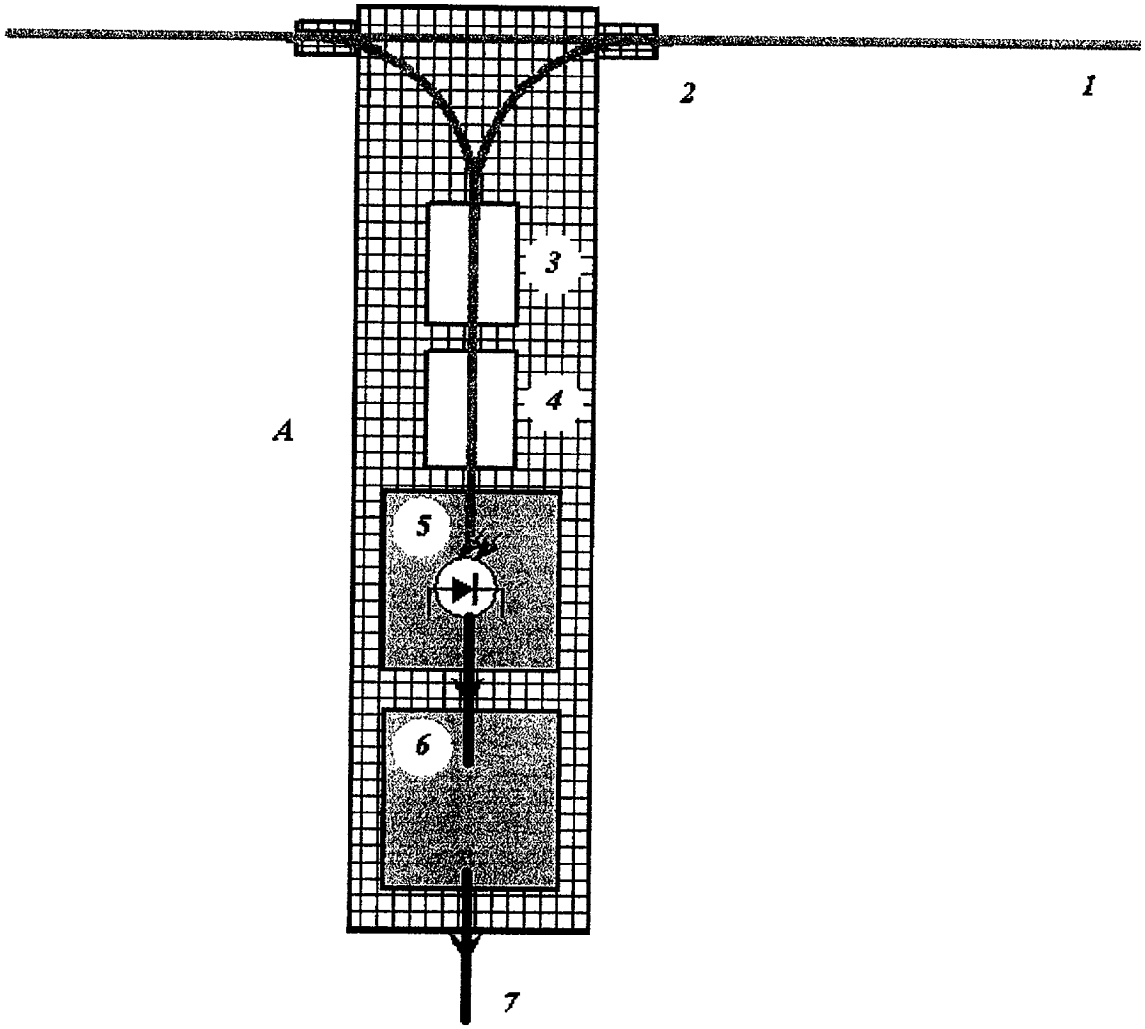
(54) ВОЛОКОННО-ОПТИЧЕСКИЙ ДЕТЕКТОР УГРОЗ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ЧЕРЕЗ ВОЛОКОННО-ОПТИЧЕСКИЕ КОММУНИКАЦИИ

(57) Реферат:

Изобретение относится к области обеспечения информационной безопасности переговоров в выделенных помещениях путем выявления возможных угроз по формированию каналов утечки акустической (речевой) информации через волоконно-оптические системы связи и может быть использовано в системах защиты конфиденциальной речевой информации. Обнаружение канала утечки акустической (речевой) информации проводится путем контроля оптических излучений в штатных волоконно-оптических коммуникациях. Для служб безопасности появление любых нештатных световых излучений или появление модуляции на акустических частотах штатных световых потоков является показателем возможности угрозы утечки речевой информации и принятия мер по их нейтрализации. Устройство для реализации данного метода содержит приемник оптического излучения, систему регистрации (демодуляции) и анализа принятых акустических сигналов. 18 з.п. ф-лы, 2 ил.

RU 2428798 C2

RU 2428798 C2



Фиг. 1

RU 2428798 C2

RU 2428798 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 428 798** (13) **C2**

(51) Int. Cl.
H04B 10/12 (2006.01)
G01R 29/08 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2009134092/09, 14.09.2009**

(24) Effective date for property rights:
14.09.2009

Priority:
(22) Date of filing: **14.09.2009**

(43) Application published: **20.03.2011** Bull. 8

(45) Date of publication: **10.09.2011 Bull. 25**

Mail address:
117216, Moskva, bul. Dm. Donskogo, 9, korp.4, kv.2, V.V. Grishachevu

(72) Inventor(s):
Grishachev Vladimir Vasil'evich (RU)

(73) Proprietor(s):
Grishachev Vladimir Vasil'evich (RU)

(54) FIBRE OPTIC DETECTOR OF VOICE INFORMATION LEAKAGE THREATS VIA FIBRE OPTIC COMMUNICATIONS

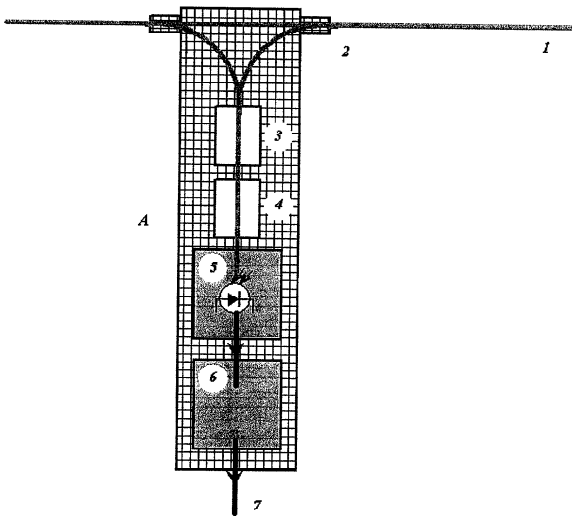
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: detection of acoustic (speech) information leakage channel is carried out monitoring of optical radiations in standard fibre optic communications. For security departments appearance of any non-standard light radiations or occurrence of modulation at acoustic frequencies of standard light flows is a parameter of possible threat of voice information leakage and taking measures for their neutralisation. The device to realise this method comprises a receiver of optical radiation; a system of registration (demodulation) and analysis of received acoustic signals.

EFFECT: increased throughput capacity.

19 cl, 2 dwg



Фиг. 1

RU 2428798 C2

RU 2428798 C2

Область техники, к которой относится изобретение

Изобретение относится к области обеспечения информационной безопасности переговоров в выделенных помещениях от угроз утечки акустической (речевой) информации через волоконно-оптические коммуникации путем контроля оптических потоков в штатных линиях связи и выявления возможной модуляции их акустическими полями. Изобретение может быть использовано в системах защиты конфиденциальной речевой информации.

Уровень техники.

Защита речевой информации является важной проблемой современного общества, что связано с важностью информации, функционирующей в коммерческих и государственных учреждениях при проведении конфиденциальных переговоров. С появлением новых технологий передачи информации, таких как волоконно-оптические технологии, появляются новые угрозы информационной безопасности. Современные волоконно-оптические каналы связи широко используются в различных системах передачи информации от магистральных и региональных линий связи до локальных сетей, структурированных кабельных систем, передачи видеосигнала в системах видеонаблюдения, системах кабельного телевидения и др. Таким образом, оптоволокно приходит в дом, офис, учреждение и располагается вблизи/внутри выделенных помещений, где могут проводиться конфиденциальные переговоры. В связи с чем возникают опасности формирования новых каналов утечки речевой информации, которым не уделялось должного внимания ранее.

Одним из таковых является акустооптоволоконный канал утечки, связанный с несанкционированным съемом речевой информации (подслушиванием) через штатные волоконно-оптические каналы передачи информации различного назначения данного учреждения (см. Гришачев В.В., Халяпин Д.Б., Шевченко Н.А., Мерзликин В.Г. Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС // Специальная техника, 2009, №2, с.2-9). В этом канале утечки акустическое поле от носителя информации воздействует на оптоволокно штатных информационных систем, построенных на волоконно-оптических технологиях, и вызывает модуляцию светового потока в оптоволокне или волоконно-оптическом оборудовании на акустических частотах. Таким образом, модулированный речью световой поток по штатным волоконно-оптическим коммуникациям может выйти далеко за пределы от места переговоров, где может быть произведена демодуляция и злоумышленник получит доступ к конфиденциальной информации.

Основой канала 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, например, формируемые при цифровых методах передачи информации, которые наиболее часто применяемы в современных системах связи, позволяют создать канал утечки без нарушения работы всей системы, так как уровень акустического воздействия на штатный световой поток незначительно уменьшает отношение сигнал/шум. Также для съема речевой информации могут быть использованы переменные по интенсивности световые потоки, применяемые для синхронизации на физическом уровне работы приемопередающего активного оборудования, действующие между передачей данных. К нештатным потокам относятся любые источники света, несанкционированно подключенные к волоконно-оптическим коммуникациям.

В настоящее время существует много методов и технических решений защиты речевой информации от утечки по побочным электромагнитным излучениям и наводкам, виброакустическим и акустическим каналам. Использование нового вида канала утечки речевой информации - акустооптоволоконного - может создать серьезные проблемы системам защиты, что связано с широким распространением новых технологий передачи информации на основе волоконно-оптического кабеля, а также с нестандартными физическими принципами формирования канала, техническое противодействие которым на настоящий момент в полном объеме не существует. Все методы нейтрализации нового канала утечки можно разделить на пассивные (например, звукоизоляция волоконно-оптического канала связи) и активные методы (различные способы фильтрации, зашумления).

Эффективность любой защиты зависит от обнаружения угроз безопасности информации. Учитывая малые размеры канала, направленность излучения и отсутствия побочных световых потоков, можно предложить простой и эффективный способ обнаружения несанкционированного съема информации (подслушивания) путем контроля существующих в канале световых потоков. Для предотвращения подслушивания необходимо выполнение следующих правил.

Во-первых, штатные световые потоки не должны быть модулированы звуком.

Во-вторых, не должно быть нештатных потоков, не предусмотренных физической реализацией протокола передачи данных в сети, а при их наличии, они не должны быть модулированы звуком.

Все эти простые правила дают возможность обнаружить атаку на систему безопасности.

В технике обслуживания волоконно-оптических систем связи существуют приборы, фиксирующие наличие оптического излучения в волокне. Например, определитель наличия оптического сигнала в волокне Fujikura FID-20R/21R (Япония, http: //www.fujikura.ru/), который позволяет определять наличие и направление распространения оптического сигнала в волокне с покрытием 250 мкм, 900 мкм, а также в стандартных оптических шнурах толщиной до 3 мм.

Известны способы обнаружения наведенной акустическим полем модуляции электромагнитного излучения радиодиапазона или электрического информационного сигнала в проводных линиях, так называемое высокочастотное навязывание, для борьбы с которым используются детекторы электромагнитного поля. Например, комплекс радиомониторинга «Кассандра», который предназначен для постоянного, периодического или оперативного мониторинга радиообстановки и обнаружения несанкционированных радиоизлучений из проверяемых помещений (Кассандра. Руководство по эксплуатации. / Группа компаний «STT», www.detektor.ru).

Однако подобные методы обнаружения подслушивания через волоконно-оптические каналы передачи информации неизвестны, что связано с новизной проблемы. В связи с чем прототипов изобретению не существует.

Раскрытие изобретения

Сущность изобретения как технического решения

Сущность изобретения как технического решения состоит в том, что для обнаружения акустооптоволоконного канала утечки конфиденциальной речевой информации в волоконно-оптическом канале передачи информации регистрируются все световые потоки и проводится анализ возможности подслушивания. Опасность утечки акустической (речевой) информации определяется по следующим признакам:

i) нештатный световой поток обнаруживается в канале передачи информации;

ii) штатный световой поток имеет акустическую модуляцию по одному из параметров оптического излучения (амплитуде, фазе, поляризации, частоте) и/или одновременно по нескольким параметрам;

iii) нештатные световые потоки, разделенные по оптическому спектру, имеют акустическую модуляцию на данной оптической длине волны по одному из параметров оптического излучения (амплитуде, фазе, поляризации, частоте) и/или одновременно по нескольким параметрам.

Выполнение хотя бы одного из этих условий достаточно для формирования канала утечки акустической (речевой) информации и может быть использовано для оценки угроз информационной безопасности.

Задача, на решение которой направлено изобретение, с указанием технического результата

Изобретение решает задачу обнаружения возможности утечки речевой информации через штатные волоконно-оптические коммуникации путем установки специальных технических средств, регистрирующих световые потоки в волоконно-оптическом канале передачи информации. Устройство для обнаружения может быть выполнено в виде отдельного блока и/или встроено в штатное сетевое волоконно-оптическое оборудование и позволяет детектировать все виды атак по акустооптоволоконному каналу утечки.

Признаки, используемые для характеристики способов

Признаки предлагаемых способов защиты сводятся к следующему. Любая атака на систему безопасности через волоконно-оптический канал для получения доступа к акустической (речевой) информации связана с оптическими потоками в нем. Контроль световых потоков в канале, их характеристик позволяет выявить любую возможность несанкционированного съема. Для этого требуется регистрировать проходящее по волоконно-оптическим элементам излучение, произвести выделение санкционированных носителей информации (штатное излучение), выявить несанкционированные потоки (нештатное излучение) и модуляции на акустических частотах. Нештатное излучение (от внешних источников) может иметь спектральный состав как пересекающийся со штатным излучением, так и непересекающийся с ним, которое модулируется внешним акустическим сигналом с конфиденциальной информацией. Эти признаки акустооптоволоконного канала утечки позволяют обнаружить и нейтрализовать утечку.

Признаки, используемые для характеристики устройств

Реализация предлагаемых способов осуществляется на основе стандартных или специально созданных элементов, в число которых входят: блок питания; фотоприемное устройство, подключаемое к волоконно-оптическому каналу; оптического, электронного и оптико-электронного аналитического элемента для выделения акустических колебаний параметров регистрируемого оптического излучения.

В фотоприемном устройстве используются стандартные фотодиоды, используемые в активном оборудовании для регистрации штатных световых потоков. Регистрация световых потоков спектрального оптического диапазона вне штатных спектральных полос производится фотоприемниками с максимумом спектральной чувствительности в области видимого диапазона, например кремниевые p-i-n-фотодиоды. Для регистрации слабых оптических сигналов утечки информации используются фотоэлектронный умножитель, лавинный фотодиод и другие высокочувствительные фотоэлектронные преобразователи. Подключение к волоконно-оптическому каналу

может быть осуществлено напрямую через разъемное соединение, или через неразъемное соединение на основе механического сращивания или сварки волокон, или через устройство ввода/вывода излучения на изгибе волокна таким образом, чтобы световое излучение проходило через устройство без значительных оптических потерь, соответствующими обычным соединениям. Также устройство может располагаться в конце оптического канала в месте преобразования в электрический сигнал (ресивер/трансивер) и быть встроено в существующее активное волоконно-оптическое оборудование. В случае подключения со свободным прохождением потоков света необходимо отводить излучение как прямом, так и обратном направлении для контроля каналов утечки во всех (двух) направлениях. В случае подключения к ресиверу/трансиверу необходим контроль как по приемному, так и передающему тракту, что связывается с возможность использования каждого из них в обоих направлениях.

Аналитический элемент выполняется для предварительного анализа оптического излучения, например, с целью выделения спектрального диапазона (см. Калинин В.А., Пресленев Л.Н. Оптические волокна и пассивные компоненты волоконно-оптических линий связи: уч. пос. // СПб: Гос. Университет Аэрокосмического Приборостроения, 2008. - 80 с. или Семенов А.Б. Волоконно-оптические подсистемы современных СКС // М: ДМК-Пресс, 2007. - 631 с.), в котором канал утечки максимально чувствителен к внешнему акустическому воздействию. Повышенная чувствительность может быть связана с конструктивными особенностями волокна, его нелинейно-оптическими свойствами, интерференционными процессами при выводе сигнала. А также спектральное выделение необходимо из-за возможности применения злоумышленником оптических источников с узкой полосой излучения, работающих в области длин волн вне пределов штатных излучателей. Предварительно обработанный оптический сигнал возможного канала утечки поступает на фотоприемник, а затем в электронную систему обработки. Например, после оцифровки сигнал поступает в компьютер со специальным программным обеспечением анализа звуковых сигналов, в котором измеряется общий уровень акустического сигнала утечки, его спектральный состав, или в систему аналоговой обработки - селективный усилитель - для выделения акустического сигнала на характерных для речи других звуков частотах.

Краткое описание чертежей

В дальнейшем предлагаемое изобретение поясняется конкретными примерами его выполнения и чертежами, на которых:

фиг.1. Принципиальная оптико-электронная схема способа детектирования каналов утечки: А - детектор атаки, 1 - штатная оптоволоконная линия, 2 - разъемные или неразъемные волоконно-оптические присоединения к детектору атаки, 3 - оптический фильтр, пропускающий штатные или нештатные световые потоки, 4 - анализатор спектра оптического излучения, 5 - линейка фотоприемников на выделенные спектры излучения, 6 - аналого-цифровой преобразователь на каждый выделенный оптический канал, 7 - выходной электрический цифровой сигнал, поступающий в компьютер для обработки и определения степени опасности.

фиг.2. Принципиальная оптико-электронная схема детектора угроз утечки, встроенного в активное оборудование штатной сети: А - детектор атаки, В - штатное активное оборудование сети, С - штатный ресивер/трансивер с отводом излучения в детектор, 1 - штатная оптоволоконная линия, 2 - разъемные или неразъемные волоконно-оптические присоединения к штатному активному оборудованию, 3 -

оптический фильтр, пропускающий штатные и отражающий нештатные световые потоки, 4 - анализатор спектра оптического излучения на основе дифракционной решетки, 5 - линейка фотоприемников на выделенные спектры излучения, 6 - аналого-цифровой преобразователь на каждый выделенный оптический канал, 7 - выходной электрический цифровой сигнал, поступающий в компьютер для обработки и определения степени опасности, 8 - аналоговая обработка сигнала с системой индикации уровня опасности, 9 - цифровой электрический вход/выход ресивера/трансивера, 10 - аналоговый электрический выход ресивера, 11 - аналоговый электрический выход детектора атаки.

Осуществление изобретения

Изобретение, относящееся к способу и устройству

Пример 1. Общее описание функционирования способа дано на фиг.1. В оптическую линию (1) с помощью стандартных разъемов или соединений (2) включается устройство (детектор утечки - А). Световые потоки, проходящие через линию в обоих направлениях, выводятся в систему оптической обработки (3, 4). С помощью оптического фильтра (3) происходит разделение на штатные и нештатные световые потоки, что позволяет упростить анализ. Например, появление нештатных световых потоков уже является основанием для вывода об атаке на систему безопасности. В этом случае происходит спектральное разложение оптического сигнала на составляющие, каждая из которых исследуется на акустическую модуляцию по отдельности. Это связано с возможностью применения злоумышленником узкополосных источников света в области, не применяемой для передачи данных. Сложный спектральный анализ в акустической области модуляции можно производить обычными методами вычислительной техники, для чего сигнал на акустических частотах из системы фотоприемников (5) на каждый оптический канал оцифровывается (6) и поступает в компьютер. На основе программной обработки акустического сигнала принимается решение об опасности утечки речевой информации. В простейших случаях анализ может производиться по таким параметрам, как общий уровень акустического сигнала, появление спектральных составляющих, характерных для голоса человека и др. В частности, уровень акустического сигнала дает общее представление об эффективности канала утечки: чем выше уровень, тем выше опасность.

Пример 2. В качестве устройства, реализующего способ детектирования каналов утечки, рассмотрим детектор атаки (А), встроенный в штатное активное оборудование сети (фиг.2), такое, например, как сетевой адаптер, медиаконвертор и др. (В). В любом активном оборудовании присутствует преобразователь оптического сигнала в электрический и обратно - ресивер/трансивер (С). С помощью селективных зеркал (3) отводится нештатное излучение из входящего излучения, а в канале передатчика пропускается штатное излучение и отводится любое излучение, идущее в обратном направлении - к передатчику, которое по определению является нештатным. Излучения отводятся в детектор атаки (А) на элемент (4) оптического анализа излучения - дифракционную решетку. Спектрально разделенное оптическое нештатное излучение от дифракционной решетки поступает на линейку фотодетекторов (5) с акустическим фильтром на выходе. Далее аналоговый электрический сигнал акустического диапазона по одному каналу поступает в аналогово-цифровой преобразователь (6) и затем в компьютер (7), а по другому каналу - в электрическую систему аналоговой обработки сигнала (8). Аналоговая обработка электрического сигнала включает интегрирующую цепочку, которая

вырабатывает сигнал атаки - присутствия нештатного излучения. Здесь же параллельно производится селективное разделение сигналов по спектру по фиксированным акустическим частотам, например, 2, 3, 4, 5, 6 кГц, уровень сигнала которых также дает возможность определить уровень опасности. Уровень опасности из трех степеней - безопасно, осторожно и тревога - выводится в световой индикации на панель активного оборудования, а также поступает в компьютер (11). Аналогичному анализу подвергается аналоговый электрический сигнал (10), поступающий от штатного ресивера (В) в систему аналоговой обработки сигнала (8). Таким образом, проводится предварительный аналоговый анализ на атаку системы безопасности по волоконно-оптическому каналу.

Более точный анализ проводится с помощью вычислительных средств системы безопасности, размещаемых здесь же или в другом месте, куда цифровая информация об акустических сигналах поступает по тем же каналам связи.

Пример 3. Пояснение к п.4 формулы. Одним из возможных способов повышения отношения сигнал/шум при регистрации акустического сигнала при демодуляции света в оптическом волокне нарушителем может быть применена высокочастотная модуляция зондирующего оптического излучения на ультразвуковых частотах. Например, зондирующее оптическое излучение модулируется на частоте 100 МГц по одному из параметров излучения - амплитуде, фазе, поляризации, частоте, тогда при демодуляции сигналов акустического диапазона применение в регистрирующей аппаратуре узкополосного фильтра на этой частоте может значительно увеличить отношение сигнал/шум. Поэтому наличие высокочастотной модуляции проходящего излучения является повышенной опасностью подслушивания. В детектор атаки требуется включить анализ высокочастотной составляющей акустического сигнала на наличие конфиденциальной информации, для чего в спектре регистрируемого акустического сигнала ограничиваются не только звуковым спектром, но и проводят анализ ультразвуковых составляющих.

Пример 4. Пояснение к пп.13, 14, 15 формулы. Одним из основных способов повышения отношения сигнал/шум для злоумышленника является выделение полезного сигнала и уменьшение вклада шумов. Эта задача может решаться путем выделения сигнала по одному из параметров световой волны - частоте, поляризации, фазе (п.6 формулы).

Частотная селекция технически реализуется спектральными волоконно-оптическими элементами, например, с помощью волоконно-оптических демультиплексоров, создаваемых волоконным циркулятором, дифракционной решеткой, дисперсионной призмы и иными волоконно-оптическими устройствами демультиплексирования оптического сигнала, а также с помощью фильтрации оптического сигнала на базе волоконной брегговской решетки (см. Убайдуллаев Р.Р. Волоконно-оптические сети // М.: Эко-Трендз, 2001. - 268 с.; Бударагин Р.В., Майстренко В.К., Назаров А.В., Раевский С.Б. Интегральная оптика: уч. пос. // Н.Новгород: Нижегородский Гос. Тех. Университет, 2008. - 105 с.).

Селекция сигналов по поляризации и по фазе также проводится стандартными волоконными элементами. Для поляризации используются специальные волокна удерживающие поляризацию, скрученные волокна, и другие элементы (см. Кульчин Ю.Н. Распределенные волоконно-оптические измерительные системы // М.: ФИЗМАТЛИТ, 2001. - 272 с.)

Селекция по фазе может быть выполнена на базе стандартных волоконно-оптических интерферометров (Окоси Т. и др. Волоконно-оптические датчики. Пер. с

япон. // Л.: Энергоатомиздат, 1990. - 256 с.).

Такие устройства широко используются в системах волоконно-оптической связи, измерительных системах и серийно выпускаются промышленностью. Они могут быть применены без существенных изменений в детекторе атаки.

Формула изобретения

1. Способ выявления утечки речевой информации через волоконно-оптические коммуникации выделенных помещений, приводящий к несанкционированной передаче речевой информации, заключающийся в том, что производится регистрация с демодуляцией на акустических частотах параметров оптического излучения, проходящего через элементы волоконно-оптических коммуникаций, и определяется утечка речевой информации.

2. Способ по п.1, отличающийся тем, что осуществляется разделение регистрируемого оптического излучения на излучение, которое относится к световым потокам для передачи данных в кабельной системе, и/или на излучение, которое не относится к световым потокам для передачи данных в кабельной системе и имеет искусственное и/или естественное происхождение от внешних и/или внутренних источников.

3. Способ по п.1, отличающийся тем, что осуществляется спектральное разложение или сканирование регистрируемого оптического излучения и выделяются излучения на оптических длинах волн, на которых существует наиболее эффективная акустическая модуляция параметров оптического излучения.

4. Способ по п.1, отличающийся тем, что при осуществлении демодуляция оптического излучения электрический сигнал анализируется на частотах, смещенных в ультразвуковую область акустического спектра, который несет или может нести конфиденциальную акустическую информацию и/или модулирован звуковым сигналом.

5. Способ по п.1, отличающийся тем, что осуществляется регистрация световых потоков, проходящих через элементы волоконно-оптических коммуникаций в прямом и/или обратном направлении распространения.

6. Способ по п.1, отличающийся тем, что осуществляется демодуляция световых потоков в волоконно-оптических коммуникациях по амплитуде, и/или фазе, и/или поляризации, и/или частоте и выявляются колебания на акустических частотах.

7. Способ по п.1, отличающийся тем, что осуществляют спектральный анализ акустических колебаний демодулированного светового потока, выделяя характерные спектральные составляющие для речи, звуков.

8. Способ по п.1, отличающийся тем, что осуществляется анализ акустических колебаний демодулированного светового потока по интегральному уровню звукового сигнала.

9. Способ по п.1, отличающийся тем, что осуществляется анализ акустических колебаний демодулированного светового потока по артикуляционному методу прослушиванием выделенного сигнала оператором.

10. Способ по п.1, отличающийся тем, что осуществляется регистрация оптического излучения через волоконно-оптический трансивер активного оборудования сети, такого как медиаконвертор, адаптер, концентратор, маршрутизатор.

11. Устройство выявления утечки речевой информации через волоконно-оптические коммуникации выделенных помещений, приводящей к несанкционированной передаче речевой информации, состоящее из приспособления подключения к волоконно-

оптическому каналу и элемента обработки оптического сигнала, после которого оптический сигнал поступает на фотоприемник с усилителем, демодулятором и элемент анализа электрического сигнала.

12. Устройство по п.11, отличающееся тем, что приспособление подключения к волоконно-оптическому каналу выполнено в виде приспособления по выводу/вводу оптического излучения в волокно на его изгибе, или на разъемных соединениях, или волоконно-оптическом ответвителе, или механическом сращивании или сварке волокон.

13. Устройство по п.11, отличающееся тем, что элемент обработки оптического сигнала включает спектральный фильтр и/или демультиплексор.

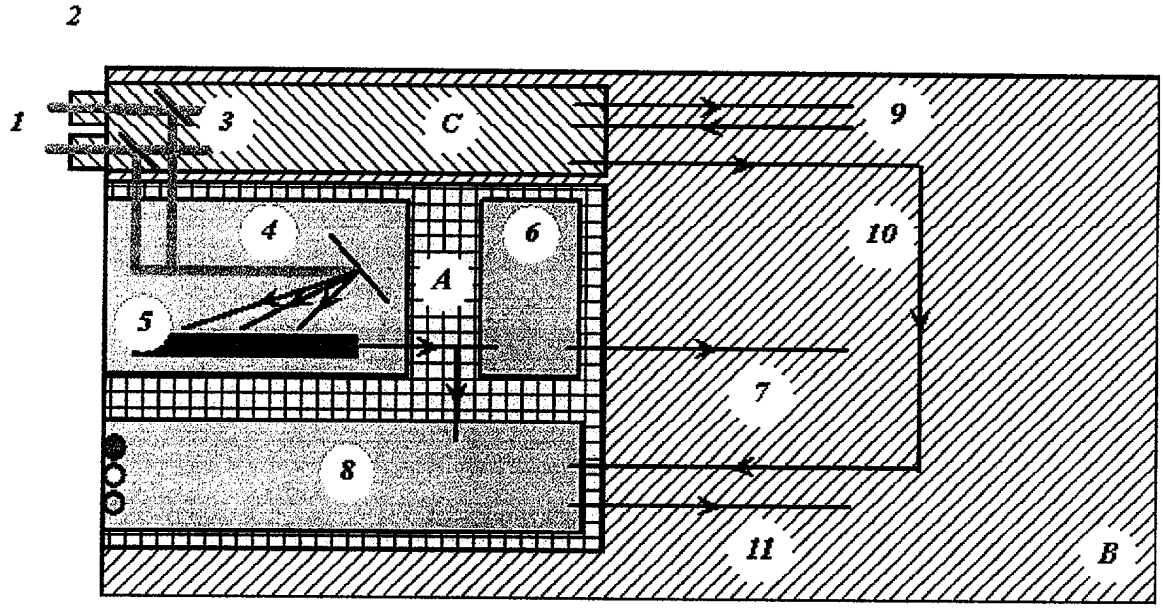
14. Устройство по п.11, отличающееся тем, что элемент обработки оптического сигнала включает анализатор поляризации излучения.

15. Устройство по п.11, отличающееся тем, что элемент обработки оптического сигнала включает волоконно-оптический интерферометр Фабри-Перо, и/или Маха-Цендера, и/или Майкельсона, и/или Саньяка и/или одноволоконный многомодовый.

16. Устройство по п.11, отличающееся тем, что элемент анализа электрического сигнала включает интегрирующий элемент на акустических частотах, и/или селективный усилитель на акустических частотах с регулируемой полосой пропускания, и/или спектроанализатор сигнала на акустических частотах.

17. Устройство по п.11, отличающееся тем, что устройство обнаружения подслушивающих устройств через волоконно-оптические элементы структурированных кабельных систем интегрируется в активное оборудование сети.

18. Устройство по п.11, отличающееся тем, что электрический демодулированный сигнал оцифровывается и для его анализа используются вычислительные ресурсы информационной системы.



Фиг. 2