

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

3
(86)

Москва
2009
Основан
в 1974 г.

СОДЕРЖАНИЕ

Криптография

- Молдовяну П. А., Молдовян Д. Н., Дернова Е. С.* Гомоморфизм и многомерная цикличность конечных групп векторов в синтезе алгоритмов ЭЦП .. 2
- Щербаков В. А., Костина А. А., Молдовяну П. А., Молдовян Н. А.* Примитивы цифровой подписи: конечные группы с трехмерной цикличностью 9

Биометрические методы и средства защиты информации

- Алгулиев Р. М., Имамвердиев Я. Н., Мусаев В. Я.* Методы обнаружения живучести в биометрических системах 16

Выявление и предотвращение возможной утечки информации

- Гришачев В. В., Халяпин Д. Б., Шевченко Н. А.* Волоконно-оптический телефон в акусто-оптоволоконном канале утечки конфиденциальной речевой информации 22
- Иванов В. П.* Активная защита информативных наводок средств вычислительной техники 31

Автоматизированные системы, технологии и программные средства защиты информации от несанкционированного доступа

- Скиба В. Ю.* Структурно-функциональная схема распределенных автоматизированных информационных систем в защищенном исполнении 35

Общие вопросы безопасности информации и объектов

- Кабулов Б. Т., Лим В. Г., Колотилов Ю. В.* Использование методов визуализации многомерных данных для оценки информационных рисков 39
- Любимов А. В.* Методика инжиниринга стандартов информационной безопасности 47
- Ермошин В. Г.* Методы защиты конфиденциальной компьютерной информации организаций от внутренних угроз 53
- Фомин А. А.* Исследование и оптимизация алгоритмов аудита информационной безопасности организации 57
- Осипов В. Ю., Емелин В. И.* Оптимальное управление информационной безопасностью социально-технических систем 64

- Рефераты из проблемно ориентированной базы данных ФГУП "ВИМИ" по вопросам защиты информации 68

Главный редактор

В. Н. Везиров, д-р техн. наук, советник директора ФГУП "ВИМИ"

Редакционный совет:

А. Л. Балыбердин, зам. начальника Департамента Аппарата Правительства РФ;
Е. А. Беляев, советник директора Федеральной службы по техническому и экспортному контролю (ФСТЭК); **В. А. Коняевский**, д-р техн. наук, член научного совета при Совете Безопасности Российской Федерации; **И. В. Никульшин**, отв. секретарь, ФГУП "ВИМИ"; **Ю. Н. Лаврухин**, канд. техн. наук, начальник Управления ФСТЭК; **А. А. Найда**, канд. техн. наук, научный редактор, ФГУП "ВИМИ"; **С. П. Панащенко**, канд. техн. наук, начальник отделения разработки программного обеспечения фирмы "Анкад"; **П. Б. Петренко**, д-р техн. наук, заместитель заведующего кафедрой "Защита информации", МГТУ им. Н. Э. Баумана; **В. Н. Пожарский**, начальник Управления инженерно-технических средств охраны службы безопасности ОАО "Газпром"; **А. А. Репин**, генеральный директор ГП Российского центра "Безопасность".

Вопросы защиты информации: Науч.-практ. журн./ФГУП "ВИМИ", 2009. Вып. 3 (86). С. 1—72.

Редакторы *Н. П. Кундиус, Л. К. Андрианова*
Корректор *Н. С. Кузьмина*
Компьютерная верстка
И. А. Жамальдинова

Подписано в печать 8.09.2009.
Формат 60x84 1/8.

Бумага офсетная. Печать офсетная. Усл. печ. л. 8,37.

Уч.-изд. л. 9,5. Тираж 500 экз.

Заказ 1569. Цена договорная.

Отпечатано в ФГУП "ВИМИ".

125993, Москва.

E-mail: office@vimi.ru

http://infogoz.vimi.ru/main_izd.php

Индекс 79187.

Свидетельство о регистрации

ПИ № ФС 77-35665 от 24.03.2009 г.

© Федеральное государственное унитарное предприятие "Всероссийский научно-исследовательский институт межотраслевой информации — федеральный информационно-аналитический центр оборонной промышленности" (ФГУП "ВИМИ"), 2009

ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВОЗМОЖНОЙ УТЕЧКИ ИНФОРМАЦИИ

УДК 004.056

Волоконно-оптический телефон в акусто-оптоволоконном канале утечки конфиденциальной речевой информации

В. В. Гришачев, канд. физ.-мат. наук;

Д. Б. Халяпин, канд. техн. наук; Н. А. Шевченко

Институт информационных наук и технологий безопасности,
Российский государственный гуманитарный университет,
Москва, Россия

Представлены общий теоретический и экспериментальный анализы акусто-оптоволоконного канала утечки конфиденциальной речевой информации на основе промышленно выпускаемого волоконно-оптического тестера-телефона "Рубин-021". Полученные результаты показывают высокую степень опасности современных волоконно-оптических технологий для обеспечения безопасности информации. Предложены способы борьбы с заявленными угрозами.

Ключевые слова: волоконно-оптическая линия связи, канал утечки речевой информации, волоконно-оптический телефон, защита акустической (речевой) информации.

Акусто-оптоволоконный канал утечки конфиденциальной речевой информации

Выявление новых каналов утечки в современных информационных системах является важной задачей. Развитие новых технологий обработки, хранения и передачи информации происходит быстрыми темпами, внедряются новые уникальные технологии, что создает реальные угрозы появления неучтенных каналов утечки информации, не защищенных существующими техническими средствами. Постоянный мониторинг создаваемой и разрабатываемой информационной техники дает возможность успешно противодействовать возникающим новым угрозам информационной безопасности.

• *Волоконно-оптические инфокоммуникации* [1–3]. Одно из важных направлений развития техники передачи информации — переход на волоконно-оптические технологии, которые позволяют достичь более высокие скорости передачи при значительном повышении надежности и защищенности. Это развитие имеет интенсивный и экстенсивный характер. Одновременно с улучшением технических показателей оборудования при переходе на волоконно-оптические технологии в телекоммуникационных (глобальных) системах связи происходит замена существующих электронных технологий в локальных системах связи. На оптоволоконно переходят инфокоммуникации террито-

рий, зданий и офисов, в связи с чем появляются новые угрозы безопасности информации на самых разных уровнях.

• *Новый тип канала утечки речевой информации* [4, 5]. Возникающие опасности защите информации формируются на самых разнообразных физических принципах, которые недостаточно изучены относительно их информационной защищенности и требуют новых технических решений. Одной из таких опасностей является акусто-оптоволоконный канал утечки конфиденциальной речевой информации (рис. 1). Его суть заключается в возможности модуляции речью от носителя конфиденциальной информации светового потока в волоконно-оптической кабеле, проложенном через комнаты для конфиденциальных переговоров, технические помещения коммерческих и государственных учреждений.

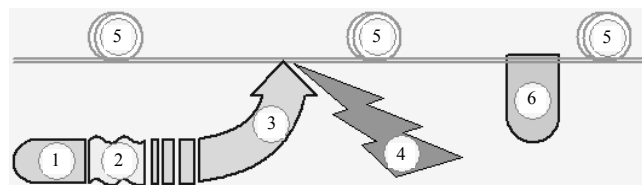


Рис. 1. Общая структура акусто-оптоволоконного канала утечки конфиденциальной речевой информации:

1 — источник речевой конфиденциальной информации;
2 — воздушная среда; 3 — вибрационные (структурные) волны; 4 — акустические помехи; 5 — волоконно-оптический кабель; 6 — ТСП конфиденциальной информации

Параметры светового потока в оптоволокне зависят от состояния внешней среды — температуры, звукового поля и др. [6, 7].

Специальным воздействием на кабель или его элементы злоумышленник может значительно повысить чувствительность волокна к звуку на отдельных участках. Используя собственный трафик локальной сети или иницируя внешние световые потоки, можно вывести промодулированное излучение далеко за пределы охранной зоны учреждения и получить конфиденциальную информацию.

В формировании канала утечки большое значение имеют отдельные волоконно-оптические элементы структурированной кабельной системы, которые могут быть использованы для эффективной модуляции светового потока звуковым полем [2, 3]. Все элементы можно разделить на три типа (А, В, С) в соответствии с конструктивными особенностями линии связи, каждому из которых будут отвечать свои особенности формирования канала утечки речевой информации.

- *Каналы утечки типа А.* Связаны с разрывными соединениями кабеля [8]. Механические соединения оптических волокон позволяют создавать локальные системы связи с перестраиваемыми элементами, что имеет большое значение при изменении и развитии конфигурации сети. Любое разъемное соединение является одним из наиболее опасных элементов для формирования канала утечки, так как дает возможность без видимых изменений повышать чувствительность к звуковому полю проходящего светового потока. Например, ослабление механического соединения, повышение упругих свойств контакта и другие изменения повышают чувствительность к звуку.

- *Каналы утечки типа В.* Определяются конструктивными особенностями свободного волоконно-оптического кабеля и связаны с восприимчивостью оптоволокна к механическим воздействиям (вибрациям) и звуковым колебаниям воздуха. Уменьшение влияния внешнего воздействия в современных волоконно-оптических кабелях достигается путем заключения волокна внутри специальной защитной оболочки. Любое нарушение однородности в структуре кабеля, например путем введения под оболочку специального уплотнения или пережатия кабеля, может на локальном участке разрушить звукоизоляцию оптоволокна и создать эффективный канал утечки речевой информации.

- *Каналы утечки типа С.* Вызваны особенностями монтажа кабеля в специальные короба, лотки и необходимостью их механического крепления к конструкциям здания. Упругий механический контакт с элементами здания повышает чувствительность оптоволокна к виброакустическим колебаниям, которые вызываются звуковым полем в помещении, повышая эффективность модуляции световых потоков в кабеле.

- *Технические средства реализации канала утечки* [9–11]. Реализация акусто-оптоволоконного канала утечки требует специальных технических средств разведки (ТСР). К ним можно отнести, во-первых, технические средства ввода речевой информации в волоконно-оптический канал, т. е. средства регистрации конфиденциальной речевой информации, к которым относятся инженерно-технические мероприятия по изменению состояния линии связи в целях повышения виброакустической чувствительности и специальные устройства (закладки), модулирующие световой поток; во-вторых, технические средства вывода речевой информации из волоконно-оптического канала, т. е. средства получения информации, включающие устройства демодуляции речи, находящиеся за пределами охранной зоны.

Для рассматриваемого канала утечки ТСР могут быть специально промышленно изготовлены, может быть использовано такое контрольно-измерительное волоконно-оптическое оборудование, применяемое при строительстве, монтаже, тестировании и эксплуатации волоконно-оптических линий связи. Такие устройства наиболее незаметны, не привлекают внимание, в некоторых ситуациях являются естественным атрибутом работы технических специалистов по обслуживанию структурированных кабельных систем. Все это делает их опасными для применения злоумышленником.

- *Волоконно-оптический телефон и его применение* [12, 13]. Одним из таких устройств является волоконно-оптический телефон (рис. 2), используемый для звуковой связи между специалистами.

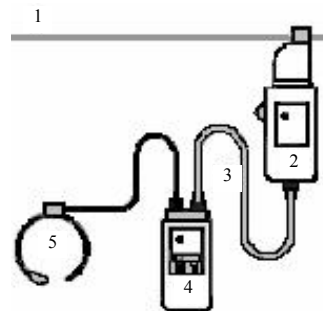


Рис. 2. Блок-схема волоконно-оптического телефона:

- 1 — волоконно-оптический кабель инфокоммуникаций;
- 2 — устройство ввода/вывода света в/из оптоволокна;
- 3 — соединительный волоконно-оптический кабель;
- 4 — модулятор/демодулятор света на звуковых частотах;
- 5 — микрофон/наушники

Это прибор акустической модуляции/демодуляции оптического излучения в оптоволокне с волоконно-оптическим входом/выходом. Например, волоконно-оптический тестер-телефон "Рубин-021" позволяет осуществлять устойчивую голосовую связь по оптическому волокну на расстоянии более 200 км, с автономным питанием не менее 50 ч, при этом массогабаритные параметры составляют 300 г и 95×158×33 мм³, соответственно.

Подключение телефона к оптоволокну может производиться через разъемное волоконно-оптическое соединение в штатной кабельной системе. Возможно также подключение к линии без разрыва, которое осуществляется с помощью специального устройства ввода/вывода света через боковую поверхность оптоволокна путем его микроизгиба. В области изгиба происходит нарушение полного внутреннего отражения (рис. 3) вследствие уменьшения угла падения до значений, меньших критических, и свет может частично входить в сердцевину или выходить из сердцевины оптоволокна.

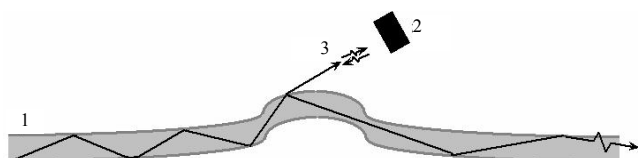


Рис. 3. Физические принципы ввода и вывода оптического излучения в волоконно-оптическом телефоне без разрыва оптоволокна:

- 1 — оптоволокно; 2 — регистрирующий/излучающий полупроводниковый фото-, светодиод;
3 — ввод/выход света на микроизгибе

В данной работе обсуждаются опасности применения волоконно-оптического телефона как технического средства разведки и меры противодействия реализации акусто-оптоволоконного канала утечки конфиденциальной речевой информации.

Структура канала утечки на основе волоконно-оптического телефона

Возможности применения волоконно-оптического телефона как технического средства разведки определяются такими его параметрами, как простота конструкции, надежность, автономность, доступность, быстрая установка, малые размеры и масса. Причем он может применяться в качестве устройства как ввода (закладка), так и вывода речевой информации из канала утечки. Обсудим принципы работы подобных акусто-оптоволоконных каналов утечки. В них волоконно-оптический телефон может использоваться только для съема речевой информации и располагаться далеко за пределами зоны охраны учреждения. Несмотря на то, что схемы на основе одного телефона более сложны, они более скрыты и эффективны.

- *Ввод и вывод речевой информации в канале утечки.* Простейшая система подслушивания может содержать два волоконно-оптических телефона, первый из которых располагается на месте конфиденциальных переговоров, а второй, соединенный с первым оптоволоком, — за его пределами. Волоконно-оптический телефон используется как простое устройство регистрации речевой информации и модуляции света, т. е. как заклад-

ное устройство. Существующие подключения устройств к оптоволокну делятся на схемы с разрывом линии связи и без разрыва.

Структурированная кабельная система, как правило, содержит много разъемных соединений, в том числе и в специальных помещениях в виде распределительных схем, переходных соединений, соединений с активным оборудованием и т. п. В этом случае возможно использование разъемного соединения оптоволоконного кабеля для реализации простейшего канала утечки на основе двух волоконно-оптических телефонов путем вставки одного из них в оптическую схему в специальном помещении, а другого — на другом конце оптоволокна за ее пределами. Такая схема проста, но и легко обнаруживается.

Кроме разрывного соединения возможно присоединение с помощью специального устройства ввода/вывода излучения из оптоволокна на микроизгибе. С помощью специального зажима оптоволокно изгибается, и из него часть излучения можно выводить или в него вводить. Размещение в месте зажима источника света, интенсивность которого промодулирована речью, позволяет ввести излучение в оптоволокно, причем при противоположных направлениях освещения изгиба основная часть излучения будет распространяться в оптоволокне в противоположных направлениях, что позволит выбирать положение устройства вывода излучения.

Другой наиболее скрытный, трудно обнаруживаемый способ ввода информации (модуляции светового потока в оптоволокне) состоит в изменении чувствительности оптоволокна к внешним акустическим полям, например, путем повышения упругих свойств механических соединений, специального изменения конструкции кабеля или его прокладки.

Волоконно-оптический телефон может применяться как устройство вывода речевой информации (демодуляция) с помощью оптоволокна за пределами охранной зоны. Это наиболее эффективный способ получения информации, так как он легко создается простым, быстрым подключением и отключением от линии связи. В этой схеме возможно использование как присоединение с разрывом линии, так и без разрыва с выводом излучения на микроизгибе.

Из приведенного анализа можно заключить, что наиболее эффективен канал утечки конфиденциальной речевой информации с модификацией оптоволокна для повышения виброакустической чувствительности и выводом информации с помощью волоконно-оптического телефона.

По модуляции в оптоволокне светового потока звуком в месте проведения конфиденциальных переговоров все схемы можно разделить на два типа: с модуляцией проходящего или отраженного света (рис. 4).

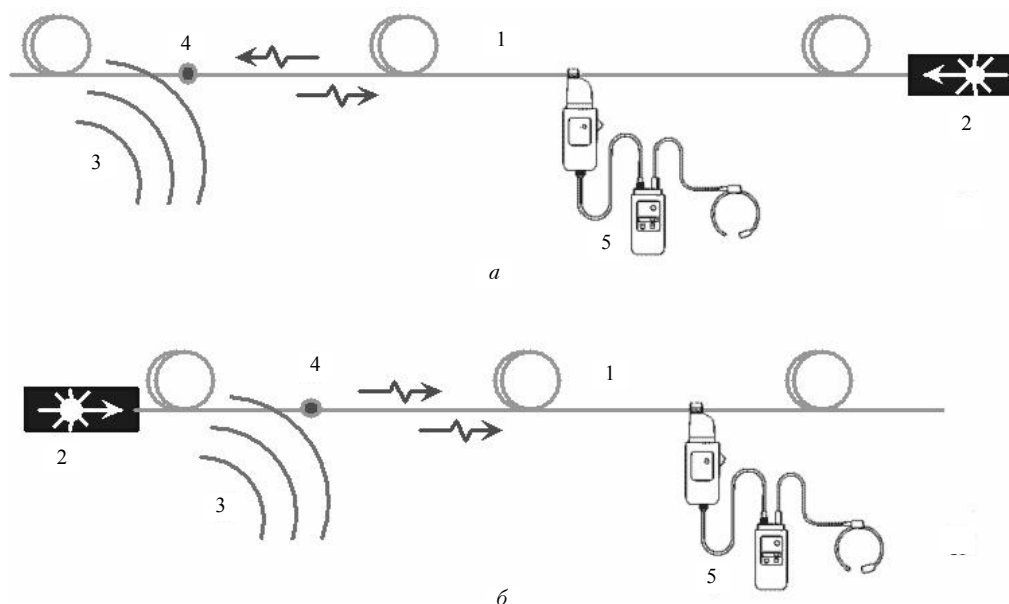


Рис. 4. Структура акусто-оптоволоконного канала утечки с применением волоконно-оптического телефона для вывода конфиденциальной речевой информации:

a — схема на прохождение оптического излучения; *б* — схема на отражение оптического излучения;
 1 — волоконно-оптический кабель инфокоммуникаций; 2 — непрерывный источник света (лазер);
 3 — источник конфиденциальной речевой информации; 4 — чувствительный к виброакустическому воздействию участок волоконно-оптической линии связи; 5 — волоконно-оптический телефон с устройством ввода/вывода света из оптоволоконна;

Рассмотрим возможные схемы реализации канала утечки.

- *Канал утечки на прохождение оптического излучения* (см. рис. 4, *a*). В зависимости от структуры кабельной системы реализация схемы утечки на прохождение светового потока может создаваться как за счет собственного трафика, так и посредством подключения внешнего источника света.

Первый способ осуществляется при включенном активном сетевом волоконно-оптическом оборудовании, таком как адаптеры, коммутаторы, конвертеры и др., расположенном в комнате переговоров или рядом с ней.

Функционирование канала возможно при достаточно большом трафике в сети.

Второй способ используется при прокладке волоконно-оптического кабеля через комнату переговоров, когда с одной стороны комнаты размещается источник света, а с другой — волоконно-оптический телефон. Для его активации не требуется работа сетевого оборудования, достаточно подключения к линии внешнего источника света злоумышленником.

Вывод информации производится с помощью волоконно-оптического телефона. Все структурные элементы канала утечки располагаются за пределами охранной зоны. Каждая схема канала имеет свои преимущества и недостатки. В первом случае по отношению ко второму требуется меньшее число операций, меньше условий для функционирования, но он менее надежен, зависит от трафика сети. Во втором случае требуется доступ к нераз-

рывному волокну с двух сторон от защищаемой зоны.

- *Канал утечки на отражение оптического излучения* (см. рис. 4, *б*). Наиболее эффективной может быть схема канала утечки с отражением от чувствительных к звуку участков оптоволоконна, расположенного в специальных помещениях, комнате переговоров. Этот канал не требует активного состояния сети, может быть реализован из одного места вне охраняемой зоны. В этом случае световое излучение вводится в оптоволоконно в направлении контролируемого местоположения источника речевой информации (звука); промодулированное обратно отраженное или рассеянное световое излучение регистрируется в месте ввода излучения. Подобный канал утечки требует доступа только в одном месте локальной сети, что повышает его скрытность.

Расстояние, с которого можно проводить съем речевой информации по обсуждаемым схемам, определяется структурой кабельной системы, и при определенных условиях может составлять десятки и более километров.

Экспериментальная оценка эффективности акусто-оптоволоконного канала утечки

Возможности реализации акусто-оптоволоконного канала утечки проверялись на стенде, созданном на основе промышленно выпускаемого волоконно-оптического тестера-телефона "Рубин-021" и его аналогах. Оптическая схема макета повторя-

ла описанные выше каналы утечки на основе отражения и прохождения светового излучения.

- *Лабораторно-исследовательский стенд акусто-оптоволоконного канала утечки.*

Практическое изучение различных способов реализации акусто-оптоволоконных каналов утечки проводилось на специально созданном стенде, который позволял экспериментально моделировать его функционирование с применением различных технических средств разведки. К основным элементам канала относятся устройства ввода (модуляции), передачи и вывода (демодуляции) речевой информации (рис. 5), которые включены в реальную волоконно-оптическую линию связи. Все основные элементы канала утечки накладывались на модельный канал связи и вместе образовывали стенд.

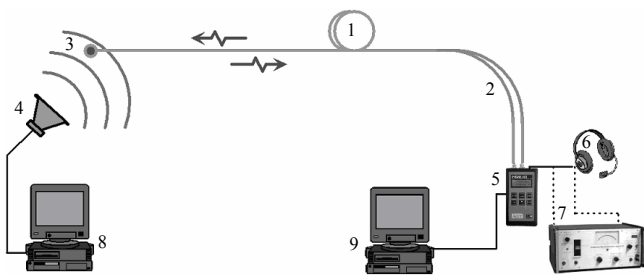


Рис. 5. Общая блок-схема лабораторно-исследовательского стенда по исследованию эффективности акусто-оптоволоконного канала утечки конфиденциальной речевой информации:

- 1 — двоянный волоконно-оптический кабель;
- 2 — ответвитель для оптической схемы на отражение;
- 3 — модулятор света на звуковых частотах; 4 — источник звука; 5 — волоконно-оптический тестер-телефон "Рубин-021";
- 6 — головная гарнитура; 7 — селективный нановольтметр;
- 8, 9 — компьютеры управления

Волоконно-оптический канал передачи информации моделировался типичным двоянным волоконно-оптическим кабелем со стандартной структурой в защитной пластиковой оболочке (кожухе) общим диаметром 3 мм с одиночным одно- или многомодовым оптоволоконном длиной более 25 м. Трафик линии связи моделировался непрерывным световым потоком от лазерного источника излучения "Рубин-021" с волоконно-оптическим выходом, соединенным с кабелем на одном конце, а на другом конце кабель оптически замыкался, образуя волоконно-оптическую петлю из двоянного кабеля.

Контроль оптической мощности производился приемником того же устройства "Рубин-021" на втором конце двоянного кабеля. Источник и приемник излучения вместе моделировали приемопередающее оборудование линии связи.

Моделирование канала утечки производилось различными способами в зависимости от решаемых задач в месте оптического замыкания двоянного кабеля. Он включал источник речевой информации, приспособления ввода в канал связи, переда-

чу сигнала, вывод информации и ее регистрацию оператором.

Моделирование конфиденциального разговора производилось акустической системой компьютера; для формирования речи использовался стандартный компьютерный речевой движок, параметры которого не изменялись. Акустическую систему располагали в непосредственной близости от чувствительного участка волоконно-оптического кабеля. Эффективность модуляции светового потока в кабеле зависела от уровня давления звука вблизи кабеля и контролировалась шумомером.

Ввод речевой информации, т. е. модуляция светового потока в оптоволоконке звуком, является основой любого канала утечки речевой информации. В реальных условиях место ввода должно обладать максимальной чувствительностью к акустическому воздействию и не иметь отличительных особенностей. Таким местом выбирался свободный участок волоконно-оптического кабеля, зажатый между двумя твердыми поверхностями (канал утечки типа С), который функционировал как модулятор светового потока в волокне на прохождение или отражение излучения.

Как показали исследования, этот канал ввода наиболее эффективен для модуляции оптического излучения. Он может быть легко реализован на практике путем использования реальных креплений, применяемых при монтаже структурированной кабельной системы. В целях анализа применялись и другие типы каналов утечки А и В.

Другой элемент канала утечки речевой информации — вывод речевой информации, т. е. демодуляция светового потока в оптоволоконке. Он располагается за пределами зоны наблюдения и может быть реализован на отражение от чувствительного участка линии связи или на прохождение через него. В обеих схемах на прохождение и отражение света использовались возможности тестера "Рубин-021" как переговорного устройства.

В схеме на прохождение источник света отключался от микрофона, и непрерывное излучение, проходя через замкнутый двоянный волоконно-оптический кабель в виде петли, поступал на приемник света со звуковым демодулятором. В схеме на отражение, ввод/вывод оптического излучения осуществлялся с помощью волоконно-оптического ответвителя типа 1—2, т. е. один вход — два выхода или наоборот один выход — два входа.

Ответвитель располагался в месте ввода основного излучения, моделирующего трафик сети, соединяя двоянный волоконно-оптический кабель с источником света тестера. Другой выход ответвителя соединялся с приемником тестера-телефона "Рубин-021", в котором осуществлялась демодуляция светового потока.

Распознавание перехваченного речевого сообщения производилось оператором с помощью головной гарнитуры волоконно-оптического телефо-

на, которое также можно было записать с помощью второго управляющего компьютера. Дополнительно для предварительной обработки сигнала использовался селективный усилитель звуковых колебаний, который повышал эффективность канала утечки и увеличивал предельные расстояния его действия.

• *Оценки эффективности канала утечки по артикуляционному методу* [14–16].

Любой канал утечки речевой информации связан с возможностью смыслового распознавания произнесенного текста озвученной информации. В простейшем случае, когда канал не содержит сложного оборудования, которое позволяет записать, применить специальные фильтры для получения распознавания конфиденциальной речевой информации, достаточно нарушителю иметь возможность услышать разговор и распознать его смысл с определенной степенью разборчивости речи. Как правило, этого достаточно для наиболее простой оценки эффективности канала утечки, что и составляет суть артикуляционного метода. Метод позволяет не только качественно оценить эффективность утечки информации, но и определить его количественную меру.

Таким образом, практический анализ эффективности канала утечки речевой информации можно определять по артикуляционному методу, количественная оценка которого состояла в нахождении вероятности W распознавания оператором слов речи, прошедших акусто-оптоволоконный канал утечки, величина которой определялась по формуле

$$W = \frac{N_1}{N_0},$$

где N_0 — число произнесенных слов на входе канала утечки;

N_1 — число распознанных слов на выходе канала утечки.

Артикуляционный метод — наиболее эффективный способ экспериментального выявления канала утечки речевой информации без сложного теоретического анализа его принципов функционирования.

Как показывают исследования, для понимания речи с различной степенью требуется распознать определенное число слов в общем объеме, составляющем речевую информацию. В зависимости от числа правильно понятых слов можно составить отчет о содержании переговоров, в частности, при словесной разборчивости:

• менее 60–70 % — невозможно составление подробной справки о содержании перехваченных переговоров;

• менее 40–50 % — перехваченное сообщение позволяет составить краткую справку, отражающую предмет, проблему и общий смысл перехваченного разговора;

• порядка 20–30 % — можно установить предмет разговора;

• менее 20 % — условие проведения конфиденциальных переговоров, голос говорящего не идентифицируется, тема разговора не определяется, анализ перехваченного сообщения позволяет определить только факт наличия речи.

Методика расчета словесной разборчивости речи, рекомендованная Гостехкомиссией России для оценки и контроля защищенности речевой информации, позволяет рассчитать и дать достаточно точную оценку допустимой разборчивости речи в зависимости от октавных уровней защищаемого речевого и акустического (вибрационного) шумового сигнала.

Точность измерения по артикуляционному методу зависит от многих параметров, и для сертификационных измерений требует специально подготовленных специалистов. Соблюдение всех условий в исследовательской работе не представляет смысла. Наши измерения проводились только одним оператором, что позволило получить объективные результаты, точность которых мы оцениваем порядка 5 %. Такие значения были получены при сравнении результатов исследования с другими операторами. Основные параметры источника речи определялись используемым компьютерным речевым движком и оставались неизменными, что повышало объективность экспериментального сравнения различных типов каналов утечки.

Результаты исследования по артикуляционному методу и их анализ

В работе были проведены исследования влияния уровня звукового давления на разборчивость речи при формировании канала утечки информации на основе механического соединения *FC-FC* (канал утечки типа *A*), специально созданной неоднородности на свободном волокне (канал утечки типа *B*) или зажатом между поверхностями волокна (канал утечки типа *C*).

На рис. 6 представлены результаты измерений. Разборчивость речи носит пороговый характер и при величине звукового давления около 50 дБ достигает 70 %. Попытки увеличить разборчивость речи селективным усилением на определенных частотах не привели к значительному улучшению результатов, что может быть связано с малыми расстояниями до локальной неоднородности на волоконно-оптическом кабеле. С увеличением расстояния до места съема речевой информации широкополосное усиление не дает подобных результатов, так как отношение сигнал/шум будет значительно выше. В этом случае применение селективного усиления может привести к росту возможностей по использованию канала утечки.

С учетом затухания в оптоволокне такие расстояния составят порядка нескольких километров.

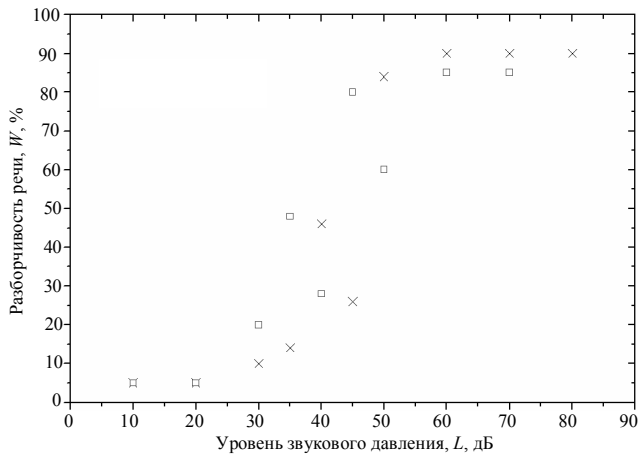


Рис. 6. Экспериментальное исследование зависимости разборчивости речи W от уровня звукового давления L вблизи канала утечки типа B на расстоянии 30 м:

× — без усилителя; □ — с усилителем

На разборчивость речи влияют также мощность источника лазерного зондирующего излучения (рис. 7) и его длина волны. При росте интенсивности излучения растет и отношение сигнал/шум, что связано с нелинейностью эффекта воздействия звука на оптоволокно. Основной механизм модуляции света в оптоволокне связан с микроизгибами, возникающими при вибрациях. При достижении интенсивности света определенных значений (в нашем случае -15 дБм) в модуляцию начинают давать вклад другие механизмы, не связанные со звуком, например неоднородности оптоволокна и др.

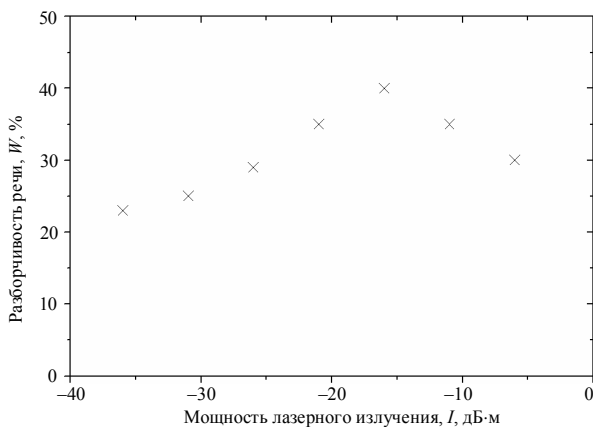


Рис. 7. Экспериментальное исследование влияния мощности лазерного излучения I на величину разборчивости речи W при фиксированном уровне звукового давления 50 дБ и расстоянии 30 м до канала утечки типа A

Волоконно-оптический тестер-телефон "Рубин-021" дает возможность проводить измерения на длинах волн 1310 и 1550 нм, а при использовании излучателя "Рубин-104" — еще и на 850 нм.

Приемник тестера-телефона рассчитан на диапазон длин волн от 800 до 1700 нм. При измерениях было обнаружено влияние длины волны на разборчивость речи. Уменьшение длины волны понижает уровень шумов, и речь легче понимается оператором. Но как показывают исследования, такая зависимость наблюдается при каналах утечки типа B , в других случаях многое зависит от способа создания неоднородности и ее величины.

Сравнительный анализ эффективности канала утечки на основе разъемных соединений (канал утечки типа A) из разных материалов показал, что разборчивость речи зависит от того, из какого материала изготовлен корпус-наконечник адаптера. При одинаковых условиях для адаптера $SC-SC$ из пластика-керамики разборчивость речи составляла 45 %, а для металлокерамического адаптера понижалась до 35 % на уровне громкости 40 дБ.

Все представленные исследования проводились в схеме на прохождение, но все каналы утечки реализуемы и по схеме на отражение. В этом случае значительно увеличиваются шумы, что требует дополнительной обработки сигнала, но работа канала утечки возможна.

Таким образом, проведенный экспериментальный анализ эффективности акусто-оптоволоконного канала утечки показывает высокую угрозу конфиденциальным переговорам даже при использовании простого общедоступного волоконно-оптического оборудования. Это показывает высокую угрозу информационной безопасности при внедрении новых видов линий связи.

Методы противодействия угрозам информационной безопасности

Предотвращение атак с применением описанного канала может быть эффективно проведено многими способами. Обсудим наиболее простые и наименее затратные методы.

- Особенности построения волоконно-оптической структурированной кабельной системы.

Основными эффективными способами противодействия подобным угрозам являются правильное проектирование, аккуратный монтаж и эффективная эксплуатация структурированной кабельной системы здания, учреждения, офиса.

Этап проектирования структурированной кабельной системы может существенно повысить защищенность речевой информации. Перед началом проектирования необходимо определить особенности структурированной кабельной системы, влияющие на возможности формирования канала утечки. Во-первых, необходимо учесть, что канал утечки формируется только на свободном от активного оборудования участке волоконно-оптического кабеля. Любое оборудование, изменяющее условия распространения света, может быть

непреодолимым препятствием для создания данного канала утечки. Во-вторых, наиболее опасными являются места механического соединения элементов системы, контакта с конструкцией здания. Например, такие элементы коммуникаций как разъемное подсоединение к активному сетевому оборудованию и соединение между собой, соединительные и распределительные панели, а также крепления к поверхностям кабельных каналов. Учет таких особенностей при проектировании позволяет существенно повысить защищенность от утечки. К другим особенностям относятся конструктивное ограничение доступа к коммуникациям, использование кабельных каналов, отсутствие открытых элементов кабеля и др.

Этап монтажа структурированной кабельной системы на всех участках должен производиться с учетом возможности ее использования для формирования канала утечки. Необходимо исключить незапланированные изменения в структуре кабельной системы, связанные с привязкой к конкретным условиям прокладки коммуникаций. Кабельные каналы, используемые для прокладки, с одной стороны, должны максимально плотно закрывать кабель, чтобы исключить возможность внесения специальных изменений кабеля, его прокладки в целях повышения чувствительности к акустическому полю. С другой стороны, нахождение кабеля в лотках должно быть свободно, чтобы исключить упругого контакта с поверхностью, т. е. сцепление с кабельным лотком.

Любые изгибы кабеля должны быть с максимальной кривизной, а на защищаемых участках должны быть исключены, так как именно на этих конструктивных особенностях можно создать наиболее эффективный канал утечки.

Этап эксплуатации структурированной кабельной системы наиболее важен, так как позволяет сгладить недочеты в проектировании и монтаже. Рекомендации в этом случае состоят в подготовке специалистов с учетом новых опасностей и использования стандартных рекомендаций по организации комплексной защиты информации.

- *Использование специальных устройств защиты информации* [9–11].

Особые меры требуется применять при непосредственной защите конфиденциальных переговоров. В этом случае возможно применение специальных устройств по полному закрытию описанного канала утечки, к которым можно отнести устройства контроля состояния структурированной кабельной системы на защищаемом участке и системы постановки акустических помех.

Контроль состояния волоконно-оптических инфокоммуникаций возможен с помощью методов оптической рефлектометрии.

Современные рефлектометры позволяют надежно контролировать любые изменения состояния линий связи, подключения, конструктивные изме-

нения и т. д. Трудности реализации подобной системы защиты связаны с высокой стоимостью оборудования и необходимостью привлечения большого штата специалистов для обеспечения эффективности работы. Причем однократное привлечение специалистов не способно обеспечить даже кратковременную надежную защиту, что связано с необходимостью непрерывного контроля состояния коммуникаций.

С точки зрения однократного обеспечения защиты конкретных конфиденциальных переговоров наиболее эффективно применение систем активной защиты — устройства зашумления линии. Такие устройства могут работать также как канал утечки, только на локализованном участке вводится шумовое акустическое воздействие на волоконно-оптический кабель, которое полностью исключает распознавание слов речи даже при формировании канала утечки. С учетом того, что длительность и место переговоров ограничены, то такой способ противодействия наиболее эффективен.

- *Использование волоконно-оптического телефона для зашумления волоконно-оптического канала на акустических частотах.*

Надо отметить, что волоконно-оптический телефон может быть использован не только для формирования канала утечки, но и как защитное устройство. Подключение его к защищаемому оптоволокну кабельной системы и передача акустического шума специального вида могут полностью исключить возможность съема информации по данному каналу. При этом необходимо учесть, что эффективность такого акустического зашумления будет сравнительно низка, если нарушитель сможет применить для формирования канала утечки свет на частотах, не совпадающих со светом, несущим шум, или узкополосный источник света с частотами, смещенными от основных зашумленных световых потоков.

Заключение

Новые угрозы информационной безопасности, возникающие при внедрении новых технологий и техники, требуют новых подходов в их нейтрализации. В настоящей работе исследуются пока широко необсуждаемые каналы утечки конфиденциальной речевой информации по волоконно-оптическим инфокоммуникациям, показана высокая степень опасности возникающих при этом угроз.

Материалы статьи подготовлены в рамках выполнения задания по проекту "Моделирование комплексной защиты конфиденциальной речевой информации национальных языков на объектах коммуникации и информатизации" по аналитической ведомственной целевой программе "Развитие научного потенциала высшей школы (2009–2010 годы) на 2009 год".

Литература

1. Гроднев И. И. Волоконно-оптические линии связи. — М.: Радио и связь, 1990. — 224 с.
2. Семенов А. Б. Волоконно-оптические подсистемы современных СКС. — М.: ДМК Пресс, 2007. — 632 с.
3. Бейли Д., Райт Э. Волоконная оптика: теория и практика: Пер. с англ. — М.: КУДИЦ-ПРЕСС, 2008. — 320 с.
4. Гришачев В. В., Халяпин Д. Б., Шевченко Н. А. Опасности возникновения каналов утечки конфиденциальной речевой информации по волоконно-оптическим структурированным кабельным системам: Матер. X Междунар. науч.-практич. конф. "Информационная безопасность". Ч. 2. — г. Таганрог: Изд-во ТТИ ЮФУ, 2008. — 287 с.
5. Гришачев В. В., Халяпин Д. Б., Шевченко Н. А. Анализ угроз утечки речевой информации через волоконно-оптические коммуникации // Вопросы защиты информации. 2008. № 4. С. 12–17.
6. Снайдер А., Лав Дж. Теория оптических волноводов: Пер. с англ. — М.: Радио и связь, 1987. — 656 с.
7. Кульчин Ю. Н. Распределенные волоконно-оптические измерительные системы. — М.: ФИЗМАТЛИТ, 2001. — 272 с.
8. Семенов А. Б. Оптические разъемы // Фотон-эксперсс, 2005. № 8(48). С. 46–48.
9. Халяпин Д. Б. Защита информации. Вас подслушивают? Защищайтесь. — М.: НОУ ШО "БАЯРД", 2004. — 431 с.
10. Железняк В. К. Защита информации от утечки по техническим каналам: Учеб. пос. — СПб: ГУАП, 2006. — 188 с.
11. Амиров П. Р. и др. Методы и средства защиты речевой информации в системах связи: Справочно-информационное издание. — Уфа: УГАТУ, 2006. — 249 с.
12. Рудницкий В. Б., Сумкин В. Р. Современные волоконно-оптические телефоны // Фотон-Эксперсс, 2005. № 8(48). С. 42–44.
13. Тестер волоконно-оптический "Рубин-021". Руководство по эксплуатации РВПИ.204125.001 РЭ. — С.-Петербург, 2005. — 21 с.
14. Покровский Н. Б. Расчет и измерение разборчивости речи. — М.: Связьиздат, 1962. — 391 с.
15. ГОСТ 16600–72. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений.
16. Цыбулин М. К., Бочаров М. О. Анализ методов оценки качества передачи речевой информации по каналу связи различной структуры // Электросвязь, 2008. № 11. С. 46–48.

Fiber-optic telephone in the audio-optic-fiber covert channel of the confidential voice information

V. V. Grishachev, D. B. Halyapin, N. A. Shevchenko

The Institute of Information Sciences and Security Technologies,
The Russian State University for the Humanities (RSUH),
Moscow, Russia

In the present work the general theoretical and experimental analysis of the audio-optic-fiber covert channel of the confidential speech information on the basis of industrially let out fiber-optical tester-phone of "Rubin-021" is presented. The received results show high danger degree of modern fiber-optical technologies for information safety. Ways of struggle against the declared threats are offered.

Keywords: fiber-optic communication line, covert voice channel, fiber-optic telephone, audio (voice) information security.

Гришачев Владимир Васильевич, доцент.

Тел: (495) 387-20-18. E-mail: grishachev@mail.ru

Халяпин Дмитрий Борисович, профессор.

Тел: (495) 387-20-18.

Шевченко Наталья Андреевна, студентка.

Тел: (495) 387-20-18. E-mail: rgg-shef-nataly@mail.ru