УДК 004.054.53
DOI: 10.33764/2618-981X-2020-6-2-182-188

ВЫЯВЛЕНИЕ УГРОЗ ИНФОРМАЦИИ ЧЕРЕЗ ВОЛОКОННО-ОПТИЧЕСКИЙ КАНАЛ СВЯЗИ

Кирилл Евгеньевич Щелкин
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения; тел. (905)936-36-63, e-mail: shchelkin94@gmail.com

Глеб Владимирович Попков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры информационной безопасности, тел. (913)478-91-30, e-mail: glebpopkov@rambler.ru

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

Ключевые слова: оценка эффективности, волоконно-оптические каналы связи, система защиты информации, система обнаружения вторжений.

DETECTION OF INFORMATION LEAKAGE THREATS IN FIBER OPTICAL COMMUNICATION CHANNEL

Kirill E. Shchelkin
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (905)936-36-63, e-mail: shchelkin94@gmail.com

Gleb V. Popkov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (913)478-91-30, e-mail: glebpopkov@rambler.ru

The paper discusses the possibility of detecting an information leakage channel in standard fiber-optic communications by monitoring optical radiation. Any abnormal light emission can create a potential threat of speech information leakage, as well as regular light streams modulated at acoustic frequencies.

Key words: efficiency evaluation, fiber optic communication channels, information security system, intrusion detection system.

Введение

Все нынешние технологии удаленных и локальных систем связи, используемые кабельной системой, их структура состоит на основе оптических систем передачи данных. Одно из основных направлений усовершенствования включает в обеспечении широкополосного абонентского доступа, который осуществляется на основе оптических сетей, в перспективе – полностью пассивных (passive optical

network). Технологии волокно в здание/дом, в офис и к рабочему месту приводят к тому, что оптоволокно замещает электрические кабеля в ближнем окружении пользователя [1, 2]. Кроме способов связи, оптоволокно активно применяется в измерительных приборах для систем безопасности. Волоконно-оптические распределенные измерительные сети способствуют контролю основных физических полей в режиме реального времени с наивысшей восприимчивостью и точностью [3]. Одним из основных направлений использования оптоволокна в системах безопасности является применение оптических интерфейсов для увеличения выделенных линий связи в системах видеонаблюдения. Большее появление оптических кабельных систем в жизни человека влияет на появление новых угроз безопасности информации, обрабатывающейся в здании, офисе, на рабочем месте. Одна из угроз связана с возможностью снятия звуковой информации конфиденциальных разговоров с использованием воздействия акустических полей на прохождение света в волокне. Оптоволокно успешно применяют при создании датчиков и распределенных измерительных систем, и штатная оптоволоконная кабельная система в здании является распределенной измерительной сетью, с помощью которой можно проводить измерения различных физических полей, в том числе и акустического поля.

Методы и материалы

Несанкционированный съем звуковой (речевой) информации методом пользования оптоволоконных коммуникаций разного назначения является одним из актуальных способов акустического разведывания, который называется акустооптическим (волоконным) каналом утечки информации [4, 5]. Появление каналов утечки информации связано с тем, что акустическое поле от носителя информации воздействует на оптоволокно информационных систем и вызывает модуляцию светового потока при прохождении через оптоволокно, пассивные элементы или активное волоконно-оптическое оборудование на акустических частотах. Модуляция такого потока в оптическом канале связи может возникать по фазе, амплитуде, частоте и поляризации в результате влияния акустического поля на физические свойства оптоволокна. На методах акусто-оптических переходов осуществлены волоконно-оптические приборы акустического поля. Модулированный речью световой поток может выйти далеко за пределы выделенного помещения по местному оптоволокну. После чего в результате негативного воздействия правонарушитель может получить доступ к закрытой информации организации.

Основными каналами утечки являются световые потоки в оптоволоконном кабеле линии связи. Световые потоки возможно разнести на штатные, связанные с физическим осуществлением протокола передачи данных, и нештатные, специально образованные нарушителем для несанкционированного съема звуковой информации. Штатные световые потоки, формируемые, например, при цифровых способах предоставления информации, позволяют создать канал утечки без деструктивного воздействия всей системы, так как уровень звукового влияния на штатный световой поток уменьшает отношения шума к сигналу. К нештатным потокам относятся любые излучения, образованные источниками света, несанкционированно подключенными к оптоволоконным сетям связи.

Рассмотрим градацию функционирования злоумышленника по сбору акустической информации через оптоволоконные сети связи и дадим общие описание используемых специальных технических средств. Организация акусто-оптического канала утечки информации маловероятно без физического воздействия на оптоволоконный кабель, который проходит через контролируемую зону. Данная сеть должна быть свободна от активного оптоволоконного оборудования на отрезке между злоумышленником и источником происхождения звуковой информации, что связано с перезапуском основных сигналов и подавлением шумовых составляющих в активном оборудовании. Между злоумышленником и источником звуковой информации должна размещаться оптоволоконная линия связи с пассивными оптическими элементами, которые не изменяют существенным образом модуляцию светового потока. К пассивным оптическим элементам, кроме оптического кабеля, относятся адаптеры, розетки, ответвители, делители. Надо отметить, что данная конструкция оптоволоконной сети связи является наиболее перспективной для абонентского доступа и активно развивается в виде технологии пассивных оптических сетей.

Оптическая схема сбора акустической информации может быть реализована несколькими вариантами. Во-первых, могут быть применены специализированные зондирующие источники света, которые не предусмотрены штатной линией. Зондировать можно таким способом как отражение, так и пропускание зондирующего луча сквозь место модуляции. В этом случае можно совместить источник света с приемо-передающим излучением. Во-вторых, для несанкционированного съема информации может быть использовано штатное излучение, применяемое для передачи данных внутри линии связи.

Опасность канала утечки можно определить по результатам акустической модуляции в месте размещения воспроизводителя информации. Акустическое поле вызывает различные варианты перехода световых потоков в оптоволокне. Выбирая критерии демодуляции светового потока (амплитуду, фазу, поляризацию или частоту) всегда можно достичь значительной эффективности канала утечки акустической (речевой) информации. Еще одна угроза связана с доступностью монтажного спецоборудования, которое может быть использовано как индивидуальное техническое средство для несанкционированного съёма информации. Например, для речевой связи между монтажниками сети используются волоконно-оптические телефоны, которые позволяют при прямом присоединении к оптоволокну реализовывать акустическую связь на дистанции более 200 км. Волоконно-оптические телефоны могут подключаться к оптоволоконной сети связи без разрыва с помощью макроизгиба оптоволоконной линии. На том же принципе соединения работает определитель 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 несанкционированного съема информации может быть использован измеритель уровня возвратного отражения, предназначенный для проверки марки обработки одномодовых оптоволоконных соединителей и измерения уровня обратного отражения от иных эле-

ментов выделенной линии связи. Еще большими возможностями обладает рефлектометр – основное устройство проверки техсостояния оптоволоконной линии связи. Названные инструменты являются общедоступными и широко используются при монтаже оптоволоконных линий, что повышает уровень угрозы их применения в канале утечки [6].

Все основные методы препятствия для утечке звуковой информации через оптоволоконные линии связи условно можно разделить на следующие вариации:

– 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 метод имеет свои минусы и плюсы, но общая результативность любой защиты во многом зависит от технических возможностей [9] обнаружения угроз безопасности информации. Технические средства, позволяющие выявлять событие несанкционированного съема информации или подготовки инструментов для его осуществления, несомненно, повышают безопасность системы защиты. В случае оптоволоконной линии связи следует учитывать физические особенности волоконно-оптического канала связи, такие как наименьшие линейные размеры, направленность излучения и отсутствие побочных световых потоков, выходящих за пределы канала.

Предотвращение несанкционированного съема информации выполняется соблюдением представленных ниже требований. Во-первых, штатные световые потоки не должны быть преобразованы на звуковых частотах. Во-вторых, не должны присутствовать нештатные потоки, не предусмотренные физической реализацией протокола передачи информации в системе, а при их наличии они не должны быть преобразованы звуком. Эти стандартные требования предоставляют вероятность более эффективно обнаружить атаку на систему безопасности и предотвращать угрозу.

Задача обнаружения возможности утечки звуковой информации через штатные оптоволоконные сети связи решаются путем установки специальных технических средств, фиксирующих световые потоки в оптоволоконной линии связи. Осуществление происходит на основе стандартных или специализированных компонентов, в которые включено фотоприемное устройство, подключаемое к оптоволоконному каналу связи; оптический, электронный и оптико-электронный аналитический элемент для выделения акустических колебаний критериев регистрируемого оптического излучения. Устройство защищенности может быть выполнено в двух вариантах: в виде отдельного блока, имеющего собственный инструмент обнаружения угроз, или блока, встроенного в активное оборудование, имеющего информационное взаимодействие с главным оборудованием.

Как видно из представления правил функционирования системы защиты, создание рабочих моделей для выявления несанкционированного съема информации через оптоволоконные линии связи возможно на основе стандартного оборудования. Основным компонентом системы защиты является волоконно-оптический фотоприемник с усилителем на акустических частотах, который присутствует в любом аналоговом волоконно-оптическом телефоне. Типичный аналоговый волоконно-оптический телефон обладает очень высокой чувствительностью, что позволяет обнаружить даже очень малые колебания интенсивности и выявлять попытки несанкционированного съема информации. Однако он имеет и минусы для систем защиты информации, одним из которых является отклонение чувствительности в инфракрасную область спектра, что не позволяет обнаружить с высокой точностью зондирующие световые потоки видимой области спектра. На дистанции сотни метров общие оптические потери составят несколько децибел на длинах волн видимого диапазона в стандартных кварцевых волокнах, что не позволяет надежно регистрировать слабое оптическое излучение штатными фотоприемниками. Другой недостаток – необходимость дополнительных оптоволоконных компонентов для обнаружения модуляции по поляризации, частоте и фазе. Но в любом случае правила функционирования волоконно-оптического телефона делают его наиболее близким к использованию в системах защиты от несанкционированного съема информации в оптоволоконных линиях связи.

Защиту выделенного помещения от несанкционированного съема информации в оптоволоконных линиях связи можно представить в следующем виде (рис. 1).

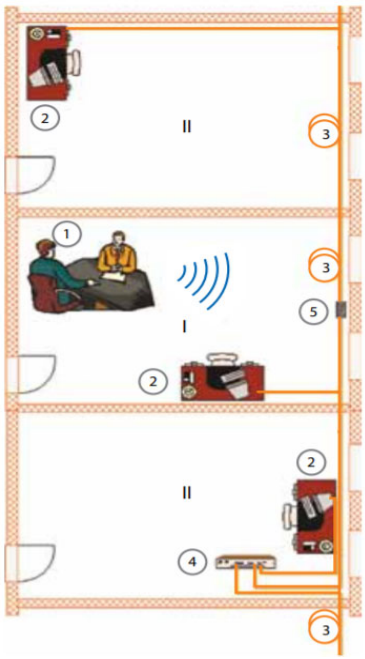

Рис. 1. Принципиальная схема построения системы защиты от утечки звуковой информации в оптоволоконных линиях связи на основе детектора атаки:

I – контролируемая зона, II – вспомогательные помещения; 1 – место закрытых переговоров, 2 – рабочее место, 3 – оптоволоконная линия связи, 4 – активное волоконно-оптическое сетевое оборудование, 5 – место включения детектора атаки.

Оптический кабель проходит через контролируемую зону и присоединяется к компьютеру на рабочем месте. Вся сеть вместе с соединительными компонентами внутри зоны выступает как система, подвергаемая звуковому влиянию, формируемому речью носителей закрытой информации. Световой поток модулируется речью, выходит за пределы контролируемой зоны и может быть зафиксирован нарушителем безопасности информации. Опасными для подсоединения технических средств разведки нарушителя являются все участки системы в контролируемой зоне от одного активного оборудования до другого. Определив наиболее уязвимый диапазон, устанавливаем устройство детектирования атаки в контролируемой зоне путем оптической вставки.

В данном эксперименте проводилось моделирования несанкционированного съема информации в оптоволоконной системе, 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 фиксировался волоконно-оптическим телефоном с аналоговой модуляцией.

Звуковое воздействие создавалось локально с помощью мониторов компьютера, действующих непосредственно на компоненты системы. Речевой сигнал был сильно зашумлен, но слова речи распознавались на слух.

Заключение

Представленная модель исследования подтверждают вероятность осуществление схожих вариаций обнаружения атаки даже с помощью непрофильного оборудования. Производство специализированного оборудования может более надежно решить проблему выявления несанкционированного съема информации и помочь службам безопасности повысить защиту звуковой информацию в современных условиях быстрого распространения оптоволоконной линии связи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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, 56 с.

4. Гришачев В., Халяпин Д., Шевченко Н., Мерзликин В. Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС. – Специальная техника, 2009, №2, 2 с.

5. Гришачев В., Косенко О. Практическая оценка эффективности канала утечки акустической (речевой) информации через волоконно-оптические коммуникации. – Вопросы защиты информации, 2010, №2, 18 с.

6. Fiber Optic Devices Ltd. (FOD) https://www.fod.ru/laser_fault_locator_ru.html.

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.