Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 8, Is. 2, pp. 55-61, 2016

DOI: 10.13187/vesp.2016.8.55
www.ejournal21.com

Technical Means

UDC 004.056.53

Channels Analysis of Leakage Information with the VOLS and Methods of Protection Multimode Fiber

[1] Xenia A. Kudryavtseva
[2] Natalya S. Ralnikova

[1-2] ITMO University, Russian Federation
Kronverkskiy prospekt, 49, Saint-Petersburg 197101
[1] E-mail: kudriavtseva.ksyu@yandex.ru
[2] E-mail: natalya.ralnikova@gmail.com

Abstract

This article examines the ways in which it can be intercepted information sent via fiber optic channels, particular attention is paid to the violation of total internal reflection, also the maximum bending radius for multimode and single-mode fiber and to determine methods of protecting the first of them. In conclusion the authors came to the conclusion that there is a real possibility of covert interception with the VOLS, which can be done while in physical contact with the optical fiber, but without violating the integrity of his shell. The most effective and practical method is for fiber bending, which are most susceptible to multimode optical fiber. Since optical fiber is now considered the most perfect physical environment for information transfer, it is necessary to conduct various activities for its protection.

Keywords: information security, optical signal, fiber optic link, frustrated total internal reflection, multimode fiber.

Введение

В основе деятельности любого государства лежит информация, поэтому обеспечение ее безопасности является важнейшей задачей правоохранительных органов. Информация, передаваемая от её источника к получателю, всегда подвержена риску несанкционированного перехвата и для каждого из способов её передачи существуют вполне определённые каналы утечки.

В последнее время все большую популярность набирают волоконно-оптические линии связи (ВОЛС). ВОЛС представляет собой канал связи, основанный на использовании оптических диэлектрических волноводов, известных как "оптическое волокно". Само оптоволокно представляет собой прозрачную нить из стекла или пластика, которая переносит внутри себя свет посредством явления полного внутреннего отражения.

ВОЛС применяются как в больших магистральных линиях передачи, так и в локальных компьютерных сетях. Свое широкое распространение оптоволокно получило

благодаря ряду преимуществ над другими каналами связи, такими как коаксиальный кабель или витая пара, главным из которых является, несомненно, огромная пропускная способность.

Изначально ВОЛС имеют более высокую степень защищенности информации от несанкционированного доступа, чем какие-либо другие линии связи. Это связано с физическими принципами передачи информации, которые основываются на модуляции света, распространяющегося в оптическом волноводе. Благодаря явлению полного внутреннего отражения электромагнитное излучение оптического диапазона выходит за пределы волокна на расстояния не более длины волны при ненарушенном канале связи, поэтому считалось невозможным снять информацию с ВОЛС, не нарушив целостности волокна. Однако недавние исследования показали, что существуют и другие каналы утечки информации, которые формируются без разрыва кабеля, с помощью которых возможно организовать скрытный перехват информации.

Материалы и методы

Основным источником для написания данной статьи стали официальные документы, регламентирующие действия правоохранительных органов для обеспечения безопасности информационных потоков, а также последние достижения в сфере создания технических средств защиты ВОЛС.

Методологическую основу данного исследования составили логические приемы, определения, описания, анализа и синтеза. Также использован общенаучный метод анализа.

Обсуждение

В оптоволоконных линиях связи основной способ передачи информации основан на модуляции интенсивности света, поэтому каналы утечки информации напрямую связаны с интенсивностью светового потока. Рассмотрим возможные каналы утечки без нарушения целостности волокна.

1. Нарушение полного внутреннего отражения. В идеальном случае свет не выходит из оптического волокна вследствие полного внутреннего отражения на его границах. Любые отклонения в распространении света приводят к выходу части излучения из волновода, которое образует канал утечки информации. Вариантами формирования такого канала утечки могут являться механическое воздействие (потери на изгибе волокна), акустическое воздействие, специальные напыляемые покрытия и оптические смазки, воздействие стационарных магнитных полей.

Самый простой пример механического воздействия на волокно – это изгиб. При изгибе волокна уменьшается угол падения света на границе, который может оказаться меньше предельного угла, и как следствие – нарушение полного внутреннего отражения, то есть часть светового потока выходиит из оптоволокна.

Максимальный радиус изгиба, при котором наблюдается побочное излучение в точке изгиба световода с диаметром сердцевины d, связанное с нарушением полного внутреннего отражения, определяется выражением:

$$R \leq d \frac{n_2}{n_1 - n_2}, \quad (1)$$

где R – максимальный радиус изгиба,

d – диаметр сердцевины световода,

n1, n2 – показатели преломления сердцевины и оболочки световода [1].

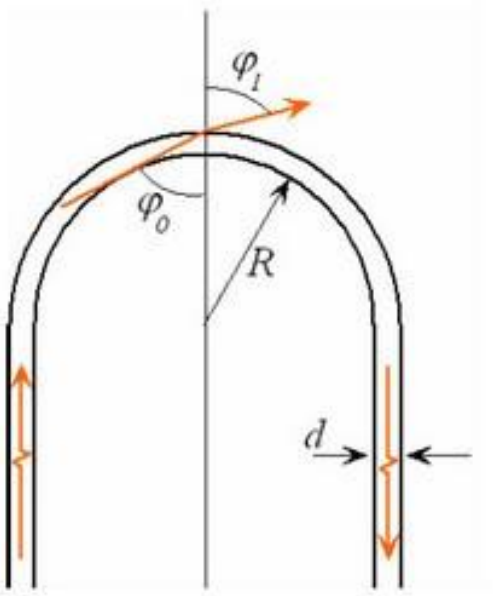

Рис. 1. Формирование канала утечки при изгибе радиусом R оптоволокна с диаметром сердцевины d, φ – угол падения, φ_r – угол преломления

Интенсивность электромагнитной волны, выходящей из волокна в точке изгиба, определяется по формулам Френеля для p- и s-поляризаций, соответственно,

$$I_p = I_0 \frac{\sin 2\varphi_0 \sin 2\varphi_1}{\sin^2(\varphi_0+\varphi_1)\cos^2(\varphi_0-\varphi_1)}, (2)$$

$$I_s = I_0 \frac{\sin 2\varphi_0 \sin 2\varphi_1}{\sin^2(\varphi_0+\varphi_1)}, (3)$$

где I_0 – интенсивность падающего излучения,

I_p, I_s – интенсивности прошедшего излучения для p- и s-поляризаций [1].

Существует специальное устройство подключения на изгибе волокна, так называемый ответвитель-прищепка. При подключении прищепки образуется изгиб и в результате некоторая часть излучения покидает светопроводящую сердцевину и выходит наружу. Регулируя радиус изгиба можно добиться как полного выхода или входа излучения, так и частичного.

Способом, который позволяет захватывать часть электромагнитного излучения, выходящего за пределы сердцевины информационного оптического волокна дополнительным световодом является оптическое туннелирование.

Явление оптического туннелирования состоит в прохождении оптического излучения из среды с показателем преломления n1 через слой с показателем преломления n2 меньшим n1 в среду с показателем преломления n3 при углах падения, больших угла полного внутреннего отражения [1].

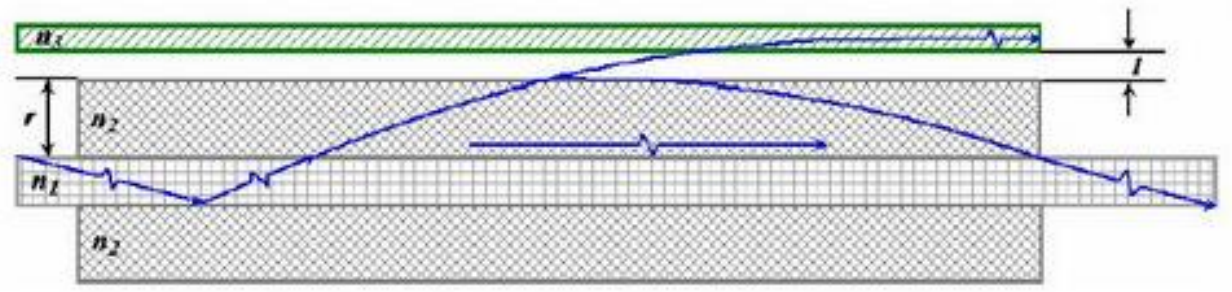

Рис. 2. Формирование канала утечки оптическим туннелированием.
n1 и n2 – показатели преломления сердцевины и оболочки оптоволокна,
n3 – показатель преломления дополнительного оптоволокна

При распространении света в оптическом волокне часть светового потока выходит за пределы сердцевины оптоволокна. Интенсивность излучения вышедшего из сердцевины в оболочку оптоволокна на расстояние r=(D-d)/2 в зависимости от угла падения на границе сердцевина-оболочка φ определяется выражением:

$$I = I_0 \exp(-4\pi n_1 \left(\frac{r}{\lambda}\right) \sqrt{sin^2\varphi - sin^2\varphi_r}), \quad (4)$$

Интенсивность излучения переходящего в дополнительный волновод определяется выражением:

$$I = I_0 sin^2(kS) \ , \quad (5)$$

где k – коэффициент связи оптических волокон,

S – длина оптического контакта двух волокон [1].

Сформировать канал утечки данным способом можно при помощи специального оптического соединителя, работающего на принципе оптического туннелирования. Отличительной особенностью оптического туннелирования является отсутствие обратно рассеянного излучения, что затрудняет детектирование несанкционированного доступа к каналу связи. Этот способ съема информации наиболее скрытный.

2. Регистрация рассеянного излучения. Даже в стационарном режиме в обычных условиях небольшая часть рассеянного излучения всё же проникает за пределы волокна, то есть излучается. Основной идеей формирования данного канала утечки является увеличение интенсивности этого излучения. Для несанкционированного доступа к информации с использованием такого рода методов необходимо использовать места усиленного бокового излучения, то есть следует снимать излучение в местах изгибов, сварных соединений, соединения с усилителями.

Основными причинами излучения световой энергии в окружающее пространство в местах соединения оптических волокон являются:

• смещение (осевое несовмещение) стыкуемых волокон;
• наличие зазора между торцами стыкуемых волокон;
• непараллельность торцевых поверхностей стыкуемых волокон;
• угловое рассогласование осей стыкуемых волокон;
• различие в диаметрах стыкуемых волокон [2].

Также участком рассеянного излучения являются участки соединения оптоволокна с усилителями. Современные оптические волноводы обладают очень маленькими потерями – это позволяет передавать информацию на значительные расстояния без необходимости усиления сигнала. Расстояния между участками ретрансляции составляет более 100 км, что требует генерации световых импульсов значительной мощности. Высокие мощности входного светового потока создают большое по величине рассеяние на ближайших к ретрансляторам участках, которые можно использовать для формирования каналов утечки информации.

3. Использование параметрических методов регистрации проходящего излучения. Оптическое излучение, являющееся носителем информации, при распространении по оптоволоконной линии вызывает изменение его физических свойств. С помощью специальных устройств можно регистрировать все эти изменения. Существующая в настоящее время техника измерений позволяет регистрировать даже самые малые изменения свойств волокна. Модуляция свойств оптоволокна является основой для формирования канала утечки информации. Можно использовать такие свойства волокна как: показатель преломления; показатель поглощения при прохождении света; малые изменения геометрических размеров; регистрация модуляции свойств поверхности волокна [3].

Результаты

Из представленных выше методов формирования каналов утечки информации с ВОЛС наиболее интересным является нарушение полного внутреннего отражения, а именно изгиб. Достоинство этого метода состоит в том, что он, в отличие от остальных, позволяет организовать направленный вывод излучения, а также является высоко эффективным. Ведь изменяя радиус изгиба волокна, злоумышленник может добиться снятия таких величин оптической мощности, которой ему будет вполне достаточно для перехвата

информации, но недостаточно для обнаружения утечки, так как будут соизмеримы с величинами естественных потерь.

Оценим радиус изгиба для многомодового волокна с диаметром сердцевины d=50 мкм и оптической оболочки – D=125 мкм (n1=1,481, n2=1,476). Получаем, что при R≤3,5 см начинает наблюдаться сильное прохождение излучения в точке изгиба (при оценке изгиба не учитывалась форма светового потока, цилиндрическая форма преломляющей поверхности и другие эффекты, изменяющие показатель преломления оптоволокна, например, фотоупругий эффект). Если же оценивать радиус изгиба для одномодового волокна, то получим R≤0,27 см.

Таким образом, можно сделать вывод о том, что одномодовое волокно менее подвержено такому методу реализации канала утечки как нарушение полного внутреннего отражения.

Теперь определим, какие методы защиты многомодового оптоволокна можно применить для локализации рассмотренных выше каналов утечки.

Самый простой и действенный способ для службы безопасности компании это контроль доступа к оптическому кабелю.

Это метод контроля, в котором регистрируется физический доступ к оптическому кабелю возможных злоумышленников по их воздействию на оптический кабель, в виде вибраций, виброакустических и других полей создаваемых нарушителем [4].

В настоящее время разработана и широко используется измерительная аппаратура, позволяющая не только определять с высокой точностью величину полных потерь в линии (мультиметры), но и распределение потерь вдоль неё (оптические рефлектометры).

Мультиметр может использоваться как стабилизированный источник излучения, измеритель оптической мощности и затухания оптического сигнала в процессе прокладки, эксплуатации и ремонта волоконно-оптических линий связи. С применением этого прибора можно установить общие параметры работающей ВОЛС.

Так же используются оптические тестеры.

Оптический тестер — это приборы, использующиеся для диагностики состояния оптоволоконных сетей и определения параметров, объединяет в себе измеритель оптической мощности, источник излучения.

Оптические тестеры позволяют проводить измерения, запоминать и передавать результаты замеров потерь канала, потерь на отражение на канале и длины канала.

Подробнее рассмотрим оптические рефлектометры, упоминаемые выше. Их работа в данной области обусловлена применением импульсной рефлектометрии. Это область измерительной техники, которая основывается на получении информации об измеряемой линии по анализу её реакции на зондирующее (возмущающее) воздействие, с возможностью определения расстояния до неоднородности в канале.

Метод импульсной рефлектометрии позволяет определить зону повреждения (в пределах погрешности измерения) и применить отдельные трассовые методы обнаружения только на небольших участках трассы, что позволяет существенно сократить время точного определения места дефекта.

С помощью оптического рефлектометра можно определить полную величину потерь в линии, местоположение обрыва волокон, участки линии с большими значениями потерь, коэффициенты отражения от соединительных разъемов и т.д. Используя для этого рефлектограмму [5].

С помощью оптического рефлектометра можно определить не только где и в каких объемах потерян трафик, но и вид дефекта ОК, от чего и происходят данные потери.

Помимо мониторинга можно применить такой метод как кодовое зашумление.

Это метод, заключающийся в применении специально подобранных преобразований передаваемой информации, которые гарантируют уменьшение вероятности правильного приема сообщений при оптимальном декодировании сигналов, получаемых из канала утечки информации.

Защита информации обеспечивается не за счет воздействия на параметры каналов утечки, а за счет вероятностного преобразования информации перед передачей по каналу связи. Невозможность восстановления информации злоумышленником основана на том свойстве, что канал утечки имеет меньшую пропускную способность, чем штатный канал

пользователя. Способ кодирования выбирается так, чтобы в канале утечки количество возникающих ошибок сильно возрастало, обеспечивая эффект зашумления передаваемого сигнала, в то время как в основном канале обеспечивалась надежная связь [6].

Заключение

Таким образом, можно сделать вывод о том, что существует реальная возможность скрытного перехвата информации с ВОЛС, которую можно осуществить, находясь в физическом контакте с оптоволокном, но, не нарушая целостности его оболочки. Наиболее эффективным и применимым на практике является метод изгиба волокна, которому наиболее подвержено многомодовое оптическое волокно. Так как оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, необходимо проведение различных мероприятий по его защите.

Примечания:

1. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения // Информационное противодействие угрозам терроризма. 2005. №4. С. 194-204.

2. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина. СПб.: НИУ ИТМО, 2012. 416 с.

3. Рахимов Н.Р. Рефлектометрический метод определения каналов утечки информации в волоконно-оптических линиях связи [Электронный ресурс] // Сборник статей по материалам международного научного конгресса «Интерэкспо Гео-Сибирь». 2010. № 1. Том 5. Режим доступа: http://cyberleninka.ru/article/n/reflektometricheskiy-metod-opredeleniya-kanalov-utechki-informatsii-v-volokonno-opticheskih-liniyah-svyazi

4. Гришачев В.В. Информационная безопасность волоконно-оптических технологий//учебно-методический курс – 3 раздел, Защита РИ в ВОК.

5. M.Z IQBAL, H FATHALLAH, N BELHADJ. 2011. Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networks and Enabling Technologies – 2011.

6. «Перехват данных на оптоволоконной линии, преимущества шифрования». Режим доступа: http://nag.ru

References:

1. Grishachev explosive, Kabashkin V.N., Frolov A.D. Analysis of the channels of the leakage of information in the fiber-optic lines of communications: the disturbance of total internal reflection // the information opposition to threats of terrorism. 2005. №4. S. 194-204

2. Katorin Yu.F., Razumovskiy A.V., Spivak A.I. Protection of information by the technical equipment: Teaching aid / edited by Yu.F. Katorina. St. Petersburg: NIU ITMO, 2012. 416 s.

3. Rahimov N.R. The reflectometric method of determining the channels of the leakage of information in the fiber-optic lines of communications electronic resource is // the collection of the articles based on materials of international scientific congress “Interekspo geo-Siberia”. 2010. №1. Tom 5. Regime of the access: http://cyberleninka.ru/article/n/reflektometricheskiy-metod-opredeleniya-kanalov-utechki-informatsii-v-volokonno-opticheskih-liniyah-svyazi

4. Grishachev v. V. Information safety of fiber-optic tekhnologiy systematic course is – 3 division, protection RI in VOK.

5. M.Z IQBAL, H FATHALLAH, N BELHADJ. 2011. Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networks and Enabling Technologies – 2011.

6. «The interception of data on the optovolokonnoy line, the advantage of coding». Regime of the access: http://nag.ru

УДК 004.056.53

Анализ каналов утечки информации с ВОЛС и методы защиты многомодового волокна

[1] Ксения Александровна Кудрявцева
[2] Наталья Сергеевна Ральникова

[1-2] Университет ИТМО, Российская Федерация
197101 Санкт-Петербург, Кронверский проспект, 49
[1] E-mail: kudriavtseva.ksyu@yandex.ru
[2] E-mail: natalya.ralnikova@gmail.com

Аннотация. В данной статье рассмотрены способы, с помощью которых может быть перехвачена информация, передаваемая по оптоволоконным каналам, особое внимание уделяется нарушению полного внутреннего отражения, также рассчитан максимальный радиус изгиба для многомодового и одномодового оптоволокна и определены методы защиты первого из них. В заключение авторы пришли к выводу, что существует реальная возможность скрытного перехвата информации с ВОЛС, которую можно осуществить, находясь в физическом контакте с оптоволокном, но, не нарушая целостности его оболочки. Наиболее эффективным и применимым на практике является метод изгиба волокна, которому наиболее подвержено многомодовое оптическое волокно. Так как оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, необходимо проведение различных мероприятий по его защите.

Ключевые слова: информационная безопасность, оптический сигнал, оптоволоконная линия связи, нарушение полного внутреннего отражения, многогодовое волокно.