УДК 004.322

Розоринов Г.Н., Фендри Мохаммед Аймен

ЗАЩИТА ИНФОРМАЦИИ В ОПТОВОЛОКОННЫХ КАБЕЛЬНЫХ СЕТЯХ

Рассмотрены технические методы несанкционированного подсоединения к оптическому волокну. Показано, что существуют разные сценарии скрытного подсоединения, выполнимые при помощи доступных технологий.Проанализированы три основных класса методов, предотвращающих или снижающих до минимума влияние посторонних подключений. Сделан акцент на то, что явная легкость доступа к оптоволокну требует определенных предосторожностей при проектировании сетей оптоволоконной связи.

Ключевые слова: оптическое волокно, защита информации, скрытное подсоединение, мониторинг сигналов, оптические рефлектометры.

Введение

В истории развития техники немного можно найти отраслей, развитие которых происходило так стремительно как волоконно-оптическая связь в период начала третьего тысячелетия. В то время как прогресс в электрической связи, включая временное мультиплексирование TDM (Time Division Multiplexing) и электрическую маршрутизацию, более или менее следовал закону Мура, то развитие оптико-волоконной техники вышло за его рамки. Достаточно отметить, что скорость передачи на каждый затраченный доллар возрастала в два раза за каждые 9 месяцев, а скорость передачи на каждой используемой длине волны удваивалась за период в 12 месяцев [1].

Одним из преимуществ волоконно-оптических кабельных сетей считается тот факт, что такая среда передачи информации более безопасна, чем металлические провода. Однако, развитие этой технологии показывает, что этот факт уже не может являться бесспорным.

На основании результатов проведенных до настоящего времени исследований можно утверждать, что новые и недорогие технологии сделали кражу данных легко возможной и трудно определимой. Представители бизнеса и различные организации, которые отправляют конфиденциальную информацию по волоконно-оптическим кабелям, могут вдруг обнаружить, что их данные уязвимы, поскольку большая часть кабельных сетей легко доступна и не очень надёжно защищена. Данные, посылаемые организациями, как государственными, так и частными, могут быть подвергнуты перехвату или прослушиванию, не только в военных целях, но чаще всего конкурентами: промышленный шпионаж в этих секторах стоит миллиарды долларов.

Публикаций по стороннему подключению к оптоволокну относительно мало в силу определенной специфики такой тематики [2]. Однако, специалистам, отвечающим за вопросы безопасности коммуникаций, необходимо знать об основных источниках угроз в оптоволоконных сетях и методах противодействия им. Данная статья представляет собой попытку привлечь внимание к существующим проблемам в области безопасности оптоволоконных коммуникаций.

Основная часть

Известно несколько методов подсоединения к оптическому волокну [3]:

– сгибание оптоволокна;
– оптическое расщепление;
– использование неоднородных волн;
– V-образный вырез;
– рассеяние.

При использовании ***метода сгибания*** оптический кабель разбирается до волокна. Метод основан на принципе распространения световых волн по волокну посредством полного внутреннего отражения. При этом угол падения света на переход между ядром волокна и его оболочкой должен быть больше, чем критический угол полного внутреннего отражения. В противном случае, часть света будет излучаться через оболочку ядра.

Значение критического угла $\theta_{кр}$ является функцией показателей преломления ядра $\beta_{я}$ и его оболочки $\beta_{об}$ и определяется следующим образом: $\theta_{кр} = \cos\theta - 1\ (\beta_{об}/\beta_{я})$, причем $\beta_{об} < \beta_{я}$.

Сгибание волокна приводит к тому, что угол отражения становится меньше критического, и свет начинает проникать через оболочку. Очевидно, что могут быть два типа изгибов оптического волокна: микроизгиб и макроизгиб (рис. 1).

Приложение внешнего усилия приводит к острому, но при этом микроскопическому искривлению поверхности волокна, приводящему к осевым смещениям на несколько микрометров и пространственному смещению длины волны на несколько миллиметров (рис.1, а). Через дефект проникает свет, и он может использоваться для съема информации.

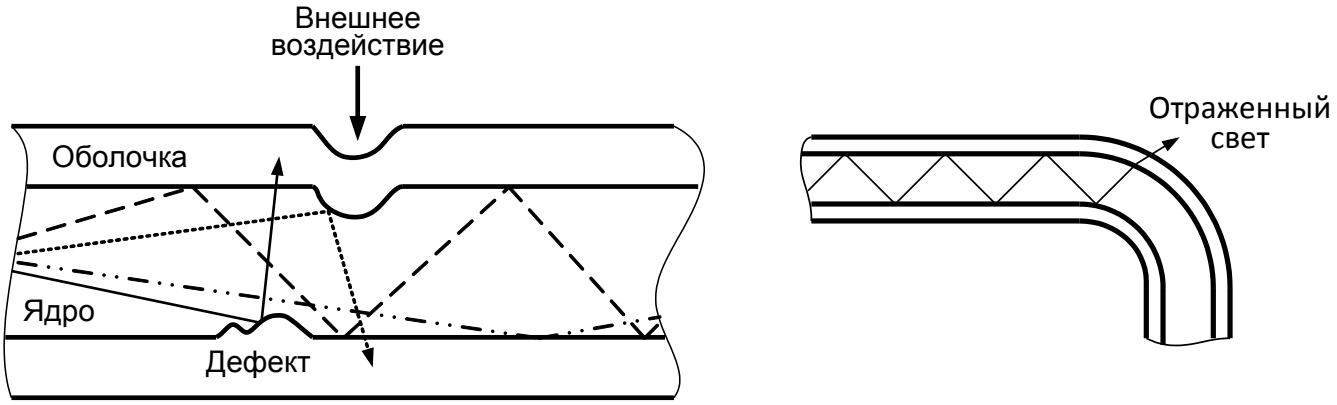

Рис. 1. Изгибы оптического волокна: а – микроизгиб, б – макроизгиб

Для каждого типа волокна существует минимально допустимый радиус изгиба. Это свойство также может использоваться для съема информации. Если волокно сгибается при меньшем радиусе, то возможен пропуск света (рис.2, б), достаточный для съема информации. Обычно минимальный радиус изгиба одномодового волокна составляет 6,5…7,5 см, за исключением волокна специального типа. Многомодовое волокно может быть изогнуто до 3,8 см.

При использовании ***метода оптического расщепления*** оптоволокно вставляется в оптический разветвитель, который отводит часть оптического сигнала. Этот метод является ***интрузивным***, поскольку требует разрезания волокна, а это, в свою очередь, вызовет срабатывание систем безопасности. Однако, необнаруженное подключение такого типа может работать годами.

Метод неоднородных волн (Evanescent Coupling) используется для перехвата сигналов от волокна-источника в волокно-приемник посредством локальной полировки оболочки волокна-источника до поверхности ядра и затем точного совмещения волокна-приемника с местом полировки. Это позволяет некоторой части сигнала проникать в волокно-приемник. Естественно, данный метод трудновыполним в полевых условиях.

V-образный вырез (V Groove Cut) – это специальная выемка в оболочке волокна близкая к ядру, сделанная таким образом, что угол между светом, распространяющимся в волокне и проекцией V-выреза больше критического угла. Это создает условия полного внутреннего отражения, при котором часть света будет уходить из основного волокна через оболочку и V-образный вырез.

При ***методе рассеяния*** на ядре волокна создается решетка Брэгга, с помощью которой достигается отражение части оптического сигнала от волокна. Это реализуется путем наложения и интерференции ультрафиолетовых лучей, создаваемых лазером с ультрафиолетовым возбуждением.

В работе [3] сделана попытка точно оценить потери при сгибании оптоволокна типа

SMF-28. Для этого волокна радиус ядра $r_я = 4{,}15$ мкм, а показатель преломления $\beta_я = 1{,}4493$; для оболочки эти значения равны, соответственно: $r_{об} = 62{,}25$ мкм, $\beta_{об} = 1{,}444$. Коэффициент преломления воздуха принимался равным 1. Радиус изгиба ρ определялся по оси x, вектор поляризации моды направлен по оси y, а распространение световой волны шло по оси z (рис. 2).

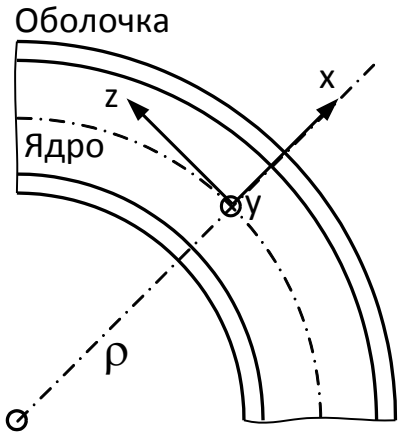

Рис. 2. Модель распространения световой волны по изгибу

Потери по мощности на изгибе как функция радиуса изгиба оптоволокна длиной 1 м показаны в виде графика на рис. 3.

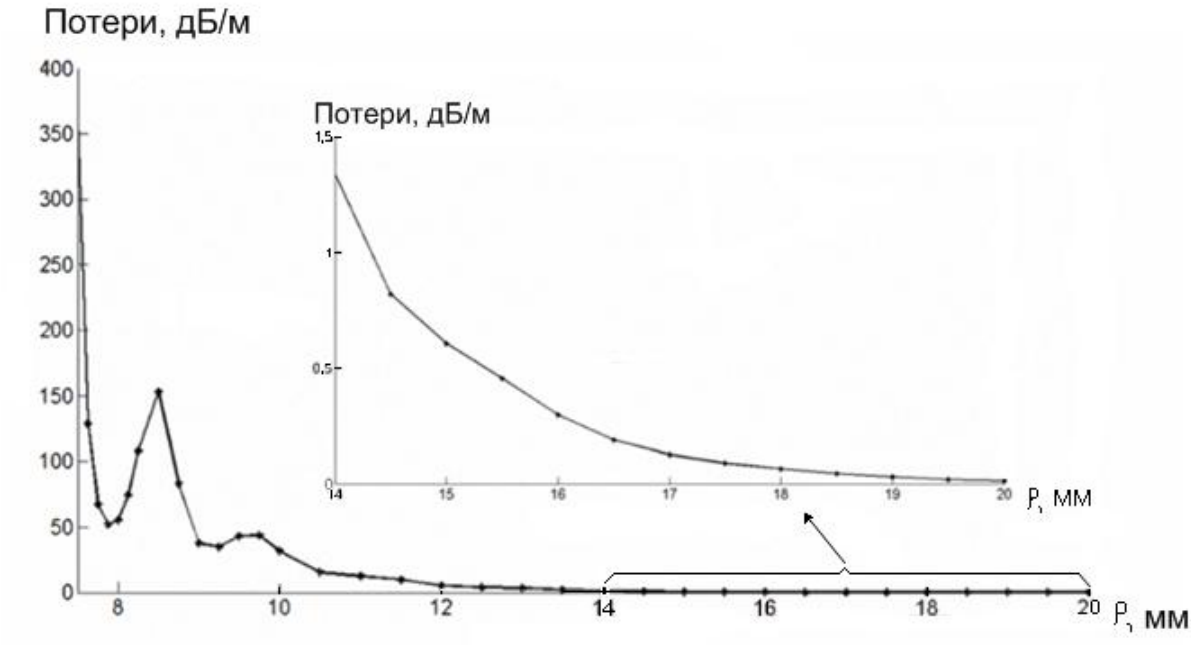

Рис. 3. Зависимость потерь по мощности от радиуса изгиба оптоволокна

На рис. 3 в увеличенном масштабе показан участок для обычных радиусов изгиба $\rho =$ 14…20 мкм. Из рисунка видна явно выраженная логарифмическая зависимость потерь от

радиуса изгиба. Для малых радиусов изгиба ($\rho < 10$ мм) потери превышают 40 дБ/м. При обычных радиусах изгиба ($\rho > 15$ мм) потери составляют меньше, чем 1 дБ/м.

Важно отметить, что сама процедура подсоединения к оптоволокну включает в себя несколько последовательных операций, а именно:

– съем оптического сигнала с волокна;

– детектирование оптического сигнала;

– определение метода передачи (декодирование протокола передачи);

– программная обработка обнаруженных фреймов/пакетов и извлечение из них необходимых данных.

На рис. 4 показана возможная схема подсоединения к оптоволокну методом его сгибания. В этом случае оптоволокно разделывается до оболочки и помещается в так называемый оптический каплер (coupler), где волокно сгибается.

Из-за нарушения принципа полного внутреннего отражения из волокна выходит некоторое количество света, которое снимается с помощью дополнительного волокна и направляется в однонаправленный конвертер (например, Ethernet).

Затем фреймы Ethernet обрабатываются и из них реконструируется передаваемый сигнал на дополнительном компъютере.

Для захвата пакетов можно воспользоваться промышленным анализатором протоколов, а для реконструкции передаваемого сигнала из захваченных пакетов – соответствующим программным обеспечением.

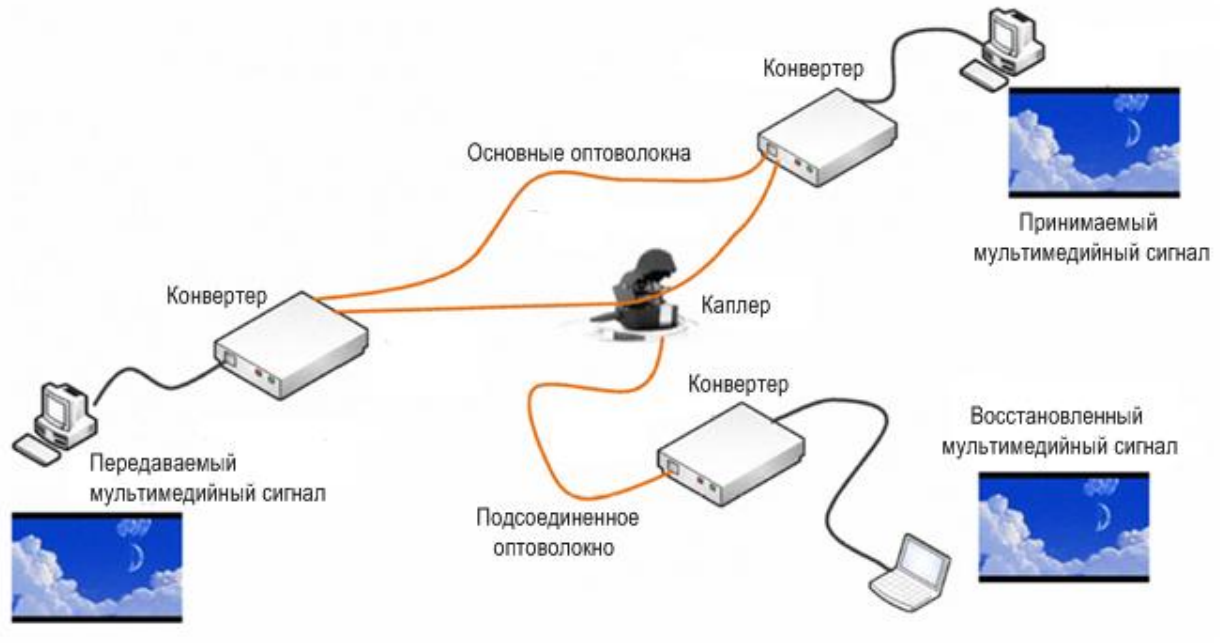

Рис. 4. Возможная схема для подсоединения к оптоволокну методом его сгибания

Вполне очевиден и вариант подсоединения к оптоволокну с удаленной обработкой (рис.5).

Рис. 5. Вариант подсоединения к оптоволокну с удаленной обработкой

Ценная информация может быть получена из сетей передачи данных, таких как SDH и SONET — двух основных стандартов оптической передачи данных по магистральным каналам связи и метросетям. Информацию из высокоскоростных сетей достаточно сложно сохранять и обрабатывать, но на рынке доступны высокотехнологичные анализаторы SDH-протоколов, которые могут быть использованы для получения низкоуровневых исходных сигналов [4].Частично это упрощает задачу, связанную со скоростью передачи данных. Такие устройства могут быть доработаны для получения различных типов трафика, проходящего через сеть.

Существуют две важных причины использовать удаленную обработку:

– при подключении к протяженным высокоскоростным (несколько Гбит/с) каналам связи, роль хранилища данных становится крайне важной. Захваченные пакеты заполняют запоминающие устройства крайне быстро;

– привлечение сетевых экспертов для работы в полевых условиях может оказаться весьма затратным. Более удобно организовать их работу в удаленном центре обработки, где имеется любое необходимое оборудование.

Можно воспользоваться различными вариантами работы с удаленными данными, к числу которых принадлежат:

– использование беспроводного интернета. При использовании Wi-Fi, дополнительный компъютер может находиться в другом помещении или в автомобиле, за пределами здания, где реализовано подключение. Эксперт может работать в относительной безопасности с возможностью доступа ко всем ресурсам:

– использование микроволнового или спутникового канала (рис. 5);

– вставка сигнала. Применив метод рассеяния, теоретически возможно создать устройство, позволяющее передавать сигнал внутрь волокна посредством видоизмененной технологии оптического каплинга. Можно разработать технологии для ввода помех или неверной информации в волокно без разрыва в связи.

Есть три основных класса методов, предотвращающих или снижающих до минимума влияние посторонних подключений.

А. Наблюдение за кабелем и мониторинг.

1. Мониторинг сигналов вблизи оптоволокна.

Для реализации этого метода оптический кабель снабжается дополнительными волокнами, по которым передается специальный сигнал мониторинга. Использование такого метода увеличивает стоимость кабеля, но любая попытка согнуть кабель вызывает потерю сигнала мониторинга, и вызывает срабатывание сигнала тревоги [5].

2. Электрические проводники.

Такой метод основан на включении в кабель электрических проводников, и если оболочка кабеля нарушена, то изменяется емкость между электрическими проводниками, что и используется для срабатывания тревоги.

3. Мониторинг мощности мод.

Этот метод применим к многомодовому оптоволокну, в котором затухание является функцией моды распространения световой волны. Подсоединение к оптоволокну существенно влияет на некоторые моды, но при этом затрагивает и другие моды. Это приводит к перераспределению энергии от проводящих мод к непроводящим, что меняет соотношение энергии в ядре волокна и его оболочке. Изменение энергии в модах может быть обнаружено на приемной стороне соответствующим измерением, что является основой для принятия решения о подключении к кабелю [4].

4. Измерение оптически значимой мощности.

В волокне может осуществляться мониторинг уровня оптически значимой мощности. В том случае, если она отличается от установленного значения, срабатывает сигнал тревоги. Однако, для этого требуется соответствующая модуляция сигнала, при которой в волокне присутствует постоянный уровень сигнала, не зависящий от наличия передаваемой информации [4].

5. Оптические рефлектометры.

Поскольку подсоединение к волокну забирает часть оптического сигнала, для обнаружения подключений могут использоваться оптические рефлектометры. С их помощью можно установить расстояние по трассе, на котором обнаруживается падение уровня сигнала (рис. 6) [4].

Рис. 6. Обнаружение подключения на оптической трассе с помощью оптического рефлектометра

6. Использование пилотного тона.

Пилотные тоны проходят по оптоволокну так же, как и сигналы передачи. Их можно использовать для обнаружения перерывов в передаче. Пилотные тоны позволяют обнаружить атаки, связанные с постановкой помех. Если несущие частоты пилотных тонов не затрагиваются, то их применение не является эффективным при обнаружении такого рода атак. О наличии подключения можно судить только по существенной деградации уровня сигнала пилотного тона [6].

Б. Сильногнущееся волокно.

Существуют специальные виды волокна, обычно называемые волокном с малыми потерями и сильным изгибом, которые защищают сеть передачи данных, путем ограничения величины потерь, возникающих при прокалывании волокна или при его сгибании. Кроме того, для светового потока в таком волокне становятся менее повреждающими такие факторы как вытягивание, перекручивание и другие физические воздействия. Известны и другие типы оптоволокна, основанные на иных технологиях производства [7].

В. Шифрование.

Хотя шифрование никак не препятствует подсоединению к волокну, оно делает украденную информацию малополезной для злоумышленников. Шифрование обычно классифицируют по уровням 2 и 3.

1. Шифрование третьего уровня

Примером шифрования третьего уровня является протокол IPSec. Он реализуется на стороне пользователя, так что это вызывает определенные задержки в обработке. Протокол используется в начале приема и общая реализация может быть весьма сложной, если в работу вовлечено большое число сетевых элементов. В первоначальной версии связь между различными узлами и элементами была вообще не защищенной. Позже в эту версию был встроен протокол IPSec, так как технологии нижнего уровня не предлагали никакого шифрования.

2. Шифрование второго уровня.

Шифрование второго уровня освобождает элементы третьего уровня от любого шифрования информации. Один из возможных источников шифрования второго уровня – это оптический формат CDMA, который считается относительно безопасным [8-10]. Данное допущение базируется на методах дешифрования грубой силой и упускает из виду более продвинутые методы. Вероятность успешного перехвата данных является функцией нескольких параметров, включая отношение сигнал/шум, и фрагментацию доступной системной емкости. В [10] показано, что повышение сложности кода может увеличить отношение сигнал/шум всего лишь на несколько дБ, которое требуется злоумышленникам чтобы выполнить декодирование. В то же время обработка менее чем 100 бит со стороны злоумышленников может уменьшить отношение сигнал/шум на 12 дБ. Скачки по длинам волн, распределение сигнала во времени и использование формата O-CDMA обеспечивают достаточный уровень секретности, но он сильно зависит от структуры системы и параметров ее реализации.

Заключение

Подсоединение к оптоволокну является реальной угрозой интересам национальной безопасности, финансовым организациям а также частной собственности и свободам. После подключения, получаемая информация может быть использована многими способами, в зависимости от мотивации злоумышленника и его технических возможностей. В данной

работе рассмотрены варианты подключения к оптоволокну методом сгибания, а также продемонстрирована возможность существования разных вариантов подключения, выполнимых при помощи доступных в настоящее время технологий. Помимо получения информации с оптоволокна, существует ряд методов, позволяющих вставлять информацию в него, как в случае с разделением на неоднородных волнах и достигнуть постановки помех или вброса неверной информации. Явная легкость доступа к оптоволокну требует определенных контрдействий, предотвращающих или снижающих до минимума влияние посторонних подключений. В статье описаны три основных класса таких методов.

ЛИТЕРАТУРА

1. Фриман Р. Волоконно-оптические системы связи / Пер. с англ. Под ред. Н.Н. Слепова – М.: Техносфера, 2003. – 448 с.

2. Каток В.Б., Манько А.А., Задорожный М.Д. Защита информации на уровне линейных сооружений волоконно-оптических линий связи от несанкционированного доступа // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Тезіси докладів науково-технічної конференції. – Київ, Вип. 3, 2000. – С. 205-213.

3. Iqbal M.Z., Fathallah H., Belhadj N. Optical fiber tapping: Methods and precautions // High Capacity Optical Networks and Enabling Technologies (HONET), 19-21 Dec. 2011, pp. 164 – 168.

4. Корнейчук В. И., Панфилов И. П. Волоконно-оптические системы передачи: учебн. Пособ. – Одесса: УГАС, 2001. – 436 с.

5. Jedidi R., Pierre R. High-Order Finite-Element Methods for the Computation of Bending Loss in Optical Waveguides, lLT, Vol. 25, No. 9, September, 2007, pp. 2618-2630.

6. Розорінов Г.М., Соловйов Д.О. Високошвидкісні волоконно-оптичні лінії зв'язку: навч. посіб. – 2-е вид., перероб. і допов. – К.: Кафедра, 2012. – 344 с.

7. Draka Elite, BendBright-Elite Fiber for Patch Cord, Draka Communications, July, 2010.

8. Ford W. Computer Communications Security: principles, standard protocols, and techniques.– Upper Saddle River, NJ: Prentice-Hall, 1994. – 494 p.

9. Stinson D. R. Cryptography: Theory and Practice. – CRC Press, Boca Raton, 1995 (first edition). – 340 p.; 2002 (second edition). – 360 p.; 2005 (third edition). – 600 p.

10. Ferguson N., Schneier S. Practical Cryptography. – Indianapolis, IN: Wiley, 2003. – 410 p.

Надійшла: 29.11.2013р.

Рецензент: д.т.н., професор Єрохін В.В.