ФИЗИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ПЕРЕДАВАЕМОЙ ПО ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИИ СВЯЗИ

Киличов Жасур Рузикулович
Самаркандский филиал ТУИТ, Узбекистан
Хаджаев Мухаммадзоир Сафармаматович
Самаркандский филиал ТУИТ, Узбекистан
Хидиров Абдували Махмадалиевич
Самаркандский филиал ТУИТ, Узбекистан
abduvali.xidirov@mail.ru

Аннотация: Произведен анализ известных способов формирования каналов утечки информации и физические методы защиты информации, передаваемой по волоконно-оптических линиях связи. Предложены способы повышения защищенности оптического волокна при передаче данных, а также предложена и описана модель системы защиты информации в волоконно-оптической линии на основе устройства рефлектометра.

Ключевые слова: методы защита информации, оптоволокно, информационной безопасность, несанкционированный доступ, рефлектометр.

В настоящее время для передачи информации широко используются волоконно-оптические линии связи (ВОЛС) по ряду причин: высокая пропускная способность (10 Гбит/с и выше) [1], помехоустойчивость, защищенность, долговечность (номинальный срок работы порядка 25 лет) [2], меньший коэффициент затухания сигнала (до 0,18-0,19 дБ/км на частоте 1550 нм) [2] и малый вес по сравнению с медным кабелем (2200 кг/м^3 против 8900 кг/м^3), следовательно, актуальными являются вопросы защиты информации, передаваемой с помощью оптических систем связи.

Оптоволокно – это обычное стекло, передающее электромагнитную энергию в виде света инфракрасного диапазона. Излучение наружу практически отсутствует. Перехватить сообщение можно, только физически подключившись к волокну. Поэтому, на первый взгляд, проблема информационной безопасности окончательно решена.

Однако не все так просто. Оптоэлектроника (особенно для поддержки высокоскоростных приложений, систем видеонаблюдения и видеоприложений) стоит дорого и во многих случаях не снимает проблемы излучения электромагнитной энергии в окружающее пространство, поскольку рабочие станции, серверы, интерфейсные карты, концентраторы и другие сетевые устройства также являются активным оборудованием и задают собственный уровень излучений. Поэтому, принимая решения об использовании оптоволоконных кабельных систем (ОКС), важно представлять фактическое состояние дел по вопросам безопасности.

Появилась информация о создании специальных роботов, которые управляются дистанционно, могут самостоятельно передвигаться по кабельным канализациям и без непосредственного участия человека подключаться к

оптоволоконному кабелю для последующей трансляции циркулирующих в ОКС данных. Для противодействия злоумышленникам, вооруженным специальной техникой, предложено использовать в качестве сигнальных проводов внутренние силовые металлические конструкции оптоволоконных кабелей. Чтобы получить доступ к оптоволокну, необходимо нарушить целостность указанных конструкций. Это приводит к немедленному срабатыванию сигнализации в центре контроля за ОКС.

Условно можно выделить три основные группы методов, предотвращающих или снижающих до минимума влияние посторонних подключений:

1. Физические средства защиты информации;
2. Криптографическая защита информации;
3. Аппаратные средства защиты информации [3].

В данной стати мы рассмотрим физические средства защиты информации. Физические методы защиты информации, передаваемой по ВОЛС можно разделит на две группы:

- Первая группа работ связана с разработкой конструкционных, механических и электрических средств защиты от несанкционированного доступа (НД) к оптическим кабелям (ОК), муфтам и оптическим волокнам (ОВ) [4]. Одни из видов средств защиты этой группы построены так, чтобы затруднить механическую разделку кабеля и воспрепятствовать доступу к ОВ. Подобные средства защиты широко используются и в традиционных проводных сетях специальной связи. Также перспективным представляется использование пары продольных силовых элементов ОК, которые представляют собой две стальные проволоки, размещенные симметрично в полиэтиленовой оболочке, и используемые для дистанционного питания и контроля датчиков, установленных в муфтах, и контроля НД. Целесообразно также применение комплекта для защиты места сварки, который заполняет место сварки непрозрачным затвердевающим гелем. Одним из предложенных методов защиты является использование многослойного оптического волокна со специальной структурой отражающих и защитных оболочек. Конструкция такого волокна представляет собой многослойную структуру с одномодовой сердцевиной.

Подобранное соотношение коэффициентов преломления слоев позволяет передавать по кольцевому направляющему слою многомодовый контрольный шумовой оптический сигнал. Связь между контрольным и информационным оптическими сигналами в нормальном состоянии отсутствует. Кольцевая защита позволяет также снизить уровень излучения информационного оптического сигнала через боковую поверхность ОВ (посредством мод утечки, возникающих на изгибах волокна различных участков линии связи). Попытки проникнуть к сердцевине обнаруживаются по изменению уровня контрольного (шумового) сигнала или по смешению его с информационным сигналом. Место НД определяется с высокой точностью с помощью рефлектометра.

- Вторая группа работ в этом направлении связана с мониторингом горячих волокон и разработкой различных устройств контроля параметров оптических сигналов на выходе ОВ и отраженных оптических сигналов на входе ОВ.

Основой системы фиксации НД является система диагностики состояния (СДС) оптического тракта. СДС можно построить с анализом либо прошедшего через оптический тракт сигнала, либо отраженного сигнала.

СДС с анализом прошедшего сигнала является наиболее простой диагностической системой. На приемной части ВОЛС анализируется прошедший сигнал. При НД происходит изменение сигнала, это изменение фиксируется и передается в блок управления ВОЛС. При использовании анализатора коэффициента ошибок на приемном модуле ВОЛС СДС реализуется при минимальных изменениях аппаратуры ВОЛС, так как практически все необходимые модули имеются в составе аппаратуры ВОЛС.

Недостатком является относительно низкая чувствительность к изменениям сигнала. Основным недостатком СДС с анализом прошедшего сигнала является отсутствие информации о координате появившейся неоднородности, что не позволяет проводить более тонкий анализ изменений режимов работы ВОЛС (для снятия ложных срабатываний системы фиксации). СДС с анализом отраженного сигнала (рефлектометрические СДС) позволяют в наибольшей степени повысить надежность ВОЛС.

Для контроля величины мощности сигнала обратного рассеяния в ОВ в настоящее время используется метод импульсного зондирования, применяемый во всех образцах отечественных и зарубежных рефлектометров.

Суть его состоит в том, что в исследуемое ОВ вводится мощный короткий импульс, и затем на этом же конце регистрируется излучение, рассеянное в обратном направлении на различных неоднородностях, по интенсивности которого можно судить о потерях в ОВ, распределенных по его длине на расстоянии до 100 - 120 км. Начальные рефлектограммы контролируемой линии фиксируются при разных динамических параметрах зондирующего сигнала в памяти компьютера и сравниваются с соответствующими текущими рефлектограммами. Локальное отклонение рефлектограммы более чем на 0,1 дБ свидетельствует о вероятности попытки несанкционированного доступа к ОВ в данной точке тракта.

Применяя данные способы защиты ВОЛС комплексно, при помощи так же организационных методов, можно быть уверенными, что возможность перехвата информации мала, но не стоит забывать про актуализацию средств защиты, так как с каждым годом злоумышленники находят новые методы несанкционированного подключения и волоконно-оптические технологии не остаются без их внимания.

Использованная литература:

1. Барашко, Е. Н. Сравнительный анализ новых технологий и систем проводной и беспроводной связи / Е. Н. Барашко, Н. В. Крепский, А. В. Трибельгон // European Scientific Conference : сб. ст. XV Междунар. науч.-практ. конф., Пенза, 07 мая 2019 г. – Пенза : Наука и Просвещение (ИП Гуляев Г.Ю.), 2019. – С. 52–55.

2. Листвин, А. В. Оптические волокна для линий связи : учеб. пособие / А. В. Листвин, В. Н. Листвин, Д.В. Швырков. – М. : ЛЕСАРарт, 2003. – 106 с.

3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : Питер, 2011.
4. FTTH Council Europe Webinar [Electronic resours] – April 23rd, 2020. – Mode of access: https://www.telepolis.pl/images/2020/04/swiatlowod-eu-092019.pdf. – Date of access: 29.08.2021.

АЛГОРИТМ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ ДЛЯ МАГНИТООПТИЧЕСКИХ ВОЛНОВОДНЫХ ЛОГИЧЕСКИХ ЭЛЕМЕНТОВ

Хидиров Абдували Махмадалиевич
Самаркандский филиал ТУИТ, Узбекистан
к.ф.-м.н. Эгамов Шухрат Ваххабович
Самаркандский филиал ТУИТ, Узбекистан
к.ф.-м.н., доцент Жуманов Хакберди Ахмедович
Самаркандский филиал ТУИТ, Узбекистан
jumanov56@mail.ru

Аннотация: Для криптообработки информации с использованием шифрования Вернам разработан рабочий симулятор логического элемента *XOR*, основанный на тех же принципах, что и магнитооптические логические элементы. Проведена экспериментальная проверка устройства-имитатора с использованием кодирования *ASCII* и разработан алгоритм шифрования и дешифрования текстовой информации.
Ключевые слова: Логические элементы, криптография, шифрование данных, алгоритм шифрования Вернама.

Обмен информацией, как открытой, так и закрытой, происходит в основном с использованием цифровых технологий и персональных компьютеров, поэтому есть возможность использовать все преимущества программного обеспечения, разработанного для обработки сигналов в цифровом и аналоговом формате. Суть шифрования с помощью шифра Вернама легко понять и реализовать на компьютере. Для того чтобы зашифровать открытый текст, вам просто нужно объединить двоичный код открытого текста с двоичным кодом ключа с помощью операции *XOR*, результирующий двоичный код, представленный в символьной форме, будет шифрованием шифра Вернама. Если мы попытаемся снова зашифровать шифрование, полученное шифром Вернама, с помощью того же ключа, мы снова получим открытый текст. Фактически, шифрование шифра Вернама идентично его расшифровке, что говорит нам о том, что шифр Вернама является симметричным шифром [1].

Давайте кратко рассмотрим шаги, которые мы непосредственно использовали для создания макета устройства для шифрования и дешифрования текстовой информации в кодировке двоичного формата *ASCII*. Поскольку одной из целей этого проекта было найти механизм, позволяющий кодировать (для