

БЕЗОПАСНОСТЬ ДАННЫХ В ОПТОВОЛОКОННЫХ КАБЕЛЬНЫХ СЕТЯХ

Со стремительным развитием информационных технологий и ростом потоков информации вопрос безопасности и надёжности систем передачи данных становится как никогда актуальным. С уверенностью можно сказать, что на сегодняшний день не существует ни одного государственного либо частного учреждения, в котором бы не использовались современные информационно-коммуникационные системы — от телефонной связи до компьютерных сетей. Информация, передающаяся посредством информационно-коммуникационных систем зачастую может иметь служебный либо конфиденциальный характер, соответственно, предопределяющую роль играет защищённость и безопасность сетей, используемых в информационно-коммуникационной системе. Наиболее надёжными системами передачи информации специалисты называют системы с использованием оптоволоконных кабельных сетей (ОКС).

Современное оптоволокно, используемое в оптоволоконных системах, представляет собой прозрачные стеклянные волокна, передающие электромагнитную энергию в виде света инфракрасного диапазона с минимальными потерями, благодаря эффекту полного внутреннего отражения. Конструктивно, такое оптоволокно состоит из ядра, оптической оболочки и защитной оболочки (Стерлинг Дональд Дж. Техническое руководство по волоконной оптике. — М.: Лори, 1998. — 195 с.)

Для волоконно-оптического кабеля характерны следующие конструктивные особенности:

- наличие центрального силового элемента;
- размещение в полимерной трубке-модуле;
- количество оптических волокон в одном модуле — от 1 до 12;
- заполнение пространства между модулями упрочняющими элементами — корделями из стеклонитей или нитей из кевлара и гидрофобным гелем;
- покрытие всех этих элементов и модулей промежуточной полимерной оболочкой;
- внешняя защита оболочки из полиэтилена или металла; возможно наличие двух защитных оболочек — металлической и полиэтиленовой.

Кроме указанных общих характеристик оптические кабели различных фирм могут также иметь дополнительные скрепляющие ленты, антикоррозионные и водозащитные обмотки, гофрированные металлические оболочки и т. д.

Учитывая сложность конструкции, подключиться к оптоволоконному кабелю в полевых условиях и, тем более, не повредить его трудно. Кроме того, практически отсутствует излучение наружу, соответственно, перехватить сообщение можно, только физически подключившись к волокну.

Таким образом, на сегодняшний день именно ОКС большинством специалистов считаются наиболее безопасными системами передачи информации, а к их основным преимуществам можно отнести быструю скорость передачи данных и практически нулевой уровень излучения.

Однако стоит отметить, что неотъемлемой частью ОКС являются сетевые устройства — рабочие станции, серверы, интерфейсные карты, концентраторы и т.д., — которые задают собственный уровень излучений. Таким образом, проблема излучения электромагнитной энергии в окружающее пространство не решается полностью. Поэтому, принимая решения об использовании оптоволоконных кабельных сетей, важно представлять фактическое состояние дел по вопросам безопасности (Мельников В. Защита информации в компьютерных системах. — М.: Финансы и статистика, Электронинформ, 1997—368 с.).

Значительно расширяющиеся сферы использования ОКС повлекли за собой разработку и доведение до коммерческого использования многочисленных инноваций в технике монтажа. Это улучшенные инструменты и приспособления для сплавления волокон, быстрозатвердевающие эпоксидные смолы, специальные коннекторы и т. п. Указанные технологии с одной стороны значительно упрощают и удешевляют сам процесс монтажа и установки ОКС, а с другой стороны — делают оптоволоконные системы более уязвимыми, увеличивая вероятность несанкционированного доступа к данным.

Кроме того, среди специалистов появилась информация о создании специальных роботов, которые управляются дистанционно, могут самостоятельно передвигаться по кабелю и без непосредственного участия человека подключаться к ОКС для последующей трансляции циркулирующих в системе данных. Аналитики IDC утверждают, что подобные технологии, хоть и сравнительно малозатратны, делают легкодоступной кражу данных из ОКС без риска обнаружения, путём простого извлечения света из ультратонких волокон. После успешного проведения этой процедуры sniffеры пакетов и другое ПО для анализа и мониторинга трафика могут перехватывать данные (Оптоволоконные сети уязвимы к взлому[Электронный ресурс] // Журнал «Хакер». — Режим доступа: <http://www.hacker.ru/post/49063/>. Дата доступа: 23.04.2014).

Для противодействия злоумышленникам, вооружённым специальной техникой, следует использовать в качестве сигнальных проводов внутренние силовые металлические конструкции оптоволоконных кабелей. В таком случае, чтобы получить доступ к оптоволокну, необходимо нарушить целостность указанных металлических конструкций.

Это приводит к немедленному срабатыванию сигнализации в центре контроля за ОКС. Для реализации подобной охранной системы практически не требуется использование дополнительного оборудования или создание специальных условий. Например, нет необходимости прокладывать оптоволоконный кабель в трубопроводах, где поддерживается высокое давление (в этом случае сигнал тревоги срабатывает при разгерметизации защитного трубопровода) как это часто делают с медными кабелями. (Доценко С. М. Безопасность оптоволоконных кабельных систем // С. М. Доценко. — «Конфидент», 1999 — № 6. [Электронный ресурс]. — Режим доступа: <http://www.bnti.ru/showart.asp?aid=222&lvl=04.02.04.&p=1>).

Итак, вопреки сформировавшемуся ложному мнению о полной безопасности данных систем, более корректен другой подход: выбор оптоволоконных кабельных систем является лишь частичным решением проблемы обеспечения безопасности передачи данных. Он позволяет сделать нежелательный доступ к сети извне значительно более трудным, чем в случае использования системы со стандартными неэкранированными линиями, применяемыми в современных сетях.