V Выводы

Общие принципы механизмов безопасности создаваемой Единой Национальной Сети Оперативной Конфиденциальной Подвижной Радиосвязи Украины (ЕНС КОПРС) должны основываться на требованиях законов Украины «О государственной тайне», «О защите информации в автоматизированных системах», Указе Президента Украины «Положение о криптографической защите информации в Украине», а также соответствующих документах ISO [3].

Как следует из проведенного анализа, этим требованиям в большей степени удовлетворяет стандарт на цифровую транкинговую систему TETRA, принятый всеми странами Евросоюза в качестве базового при построении национальных корпоративно-ведомственных сетей подвижной связи специального назначения. Выбор в качестве базовой системы при построении ЕНС КОПРС цифровой транкинговой системы стандарта TETRA будет не только способствовать построению в Украине новейшей высокотехнологичной системы оперативной конфиденциальной подвижной связи, но и заложит прочный фундамент эффективной интеграции отечественной системы связи в европейские и мировые телекоммуникационные структуры.

Литература: А. Г. Мильковский, О. Н. Кононенко. Об эффективности использования частотного спектра в системах стандартов TETRA и TETRAPOL/ "Зв'язок", № 4, 1999, с. 17-18. 2. В. Л. Банкет, В. А. Іванов. Аналіз ефективності систем цифрового рухомого радіозв'язку. // Зв'язок, № 6, 1999, с. 21-25. 3. ISO 7498-2 (1989): "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture". 4. Radio Equipment and Systems (RES) / Trans-European Trounced Radio (TETRA) / Voice plus Data (V+D) / Part 7: Security / ETS 300 392-7 December 1996. 5. TETRAPOL Specifications; Part 16: Security; Part 1: Security services PAS 0001-16-1 Version: 2.1.0 Date: 30 January 1998. 6. TETRAPOL Specifications; Part 16: Security; Part 2: KSW – KMC interface PAS 0001-16-2 Version: 2.1.0 Date: 30 January 1998. 7. TETRAPOL Technical Report; Part 1: Guide to TETRAPOL features; Part 1: System Technical Report; TTR 0001-1-1 Version: 1.0.0 Date: 25 June 1997. 8. Trans European Trounced Radio (TETRA) system; Technical requirements specification Part 3: Security aspects ETR 086-3 January 1994. 9. TETRA security – the fundamental of the high performance system / Gert Roelofsen/ PTT Telecom/KPN Research – Chairman ETSI Project TETRA Working Group. 10. Terrestrial Trounced Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface FINAL DRAFT pr ETS 300 812 September 1998. 11. TETRAPOL Specifications; Part 16: Security; +Part 3: Mechanisms, messages and algorithms. PAS 0001-16-3 Version: 2.1.0 Date: 30 January 1998.

УДК 621.391.052

ЗАЩИТА ИНФОРМАЦИИ НА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Александр Манько, Виктор Каток, Михаил Задорожний

Научно-инженерный центр линейно-кабельных сооружений Киевского института связи при Государственном комитете связи и информатизации Украины, г. Киев

Аннотация: **Рассматриваются особенности распространения электромагнитной энергии в оптическом волокне, а также возможности и основные пути обеспечения защиты информации от несанкционированного доступа на волоконно-оптических линиях связи.**

Summary: **In work is considered the features of electromagnetic power propagation in an optic fiber (OF), and also possibility and fundamental ways of provision of protection of the information from the non-authorized access on fiber-optic links of communication.**

Ключевые слова: **Защита информации, волоконно-оптические линии связи, несанкционированный доступ.**

Введение

В последнее время одним из наиболее перспективных и развивающихся направлений построения сети связи в Украине и в мире являются волоконно-оптические линии связи (ВОЛС). В области систем передачи информации с большой информационной емкостью и высокой надежностью работы ВОЛС не имеют конкурентов. Это объясняется тем, что они значительно превосходят проводные по таким показателям, как пропускная способность, длина регенерационного участка, а также помехозащищенность.

Считается, что ВОЛС, в силу особенностей распространения электромагнитной энергии в оптическом

волокне (ОВ), обладают повышенной скрытностью. Это объясняется тем, что оптическое излучение, являющее носителем информации, распространяется в ОВ согласно закону полного внутреннего отражения, а за ОВ электромагнитное излучение экспоненциально спадает. Участки, где возможна утечка электромагнитного излучения и несанкционированный съем информации (НСИ), относительно малочисленны, «классическими» радиотехническими методами (приемо-передающая аппаратура, регенерационные пункты) изучены и локализованы. По этой причине эти участки сравнительно легко могут быть поставлены под контроль.

Рассмотрим ВОЛС и ее основные параметры (рис. 1) [1, 2].

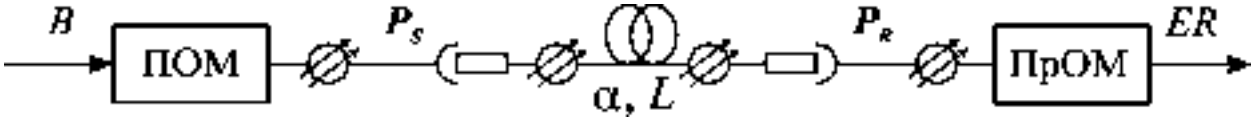

Рисунок 1 – Структурная схема ВОЛС

В состав ВОЛС входит: передатчик оптической мощности (ПОМ) с выходной мощностью *Ps*, приемник оптической мощности (ПрОМ), обеспечивающий при входной оптической мощности *Pr* прием и преобразование оптического сигнала с заданным коэффициентом ошибок *ER*, и волоконно-оптический линейный тракт (ВОЛТ), имеющий длину *L* и затухание α. Приемо-передающая пара (ПОМ-ПрОМ) имеет энергетический потенциал *E*, который зависит от мощности ПОМ, спектральной плотности шума, чувствительности ПрОМ и скорости передачи *B*. Заданный энергетический потенциал *E* ограничивает длину волоконно-оптического тракта *L*, затухание которого (с учетом эксплуатационного запаса) не должно превосходить энергетический потенциал *E*. Очевидно, что для того, чтобы осуществить НСИ, необходимо добраться до самого волокна ВОЛТ и каким-либо образом считать информацию, сняв часть оптической мощности P_{RX} через разветвитель оптический (РО) в точке с мощностью P_X, внеся потери α_X и не нарушая при этом функционирование канала связи (рис. 2).

Рассмотрим воздействие на параметры ВОЛТ съема информации при пассивном локальном не санкционированном доступе (НД) [1, 2]. Введем следующие обозначения: P_S , P_R , P_X , P_{RX} - мощности оптических сигналов, соответственно на выходе ПОМ (в начале ВОЛТ), на входе ПрОМ (в конце ВОЛТ), в месте съема информации и на входе ПрОМ НД, α [дБ/км] - затухание ВОЛТ, *E* - энергетический потенциал приемопередатчиков ВОЛС.

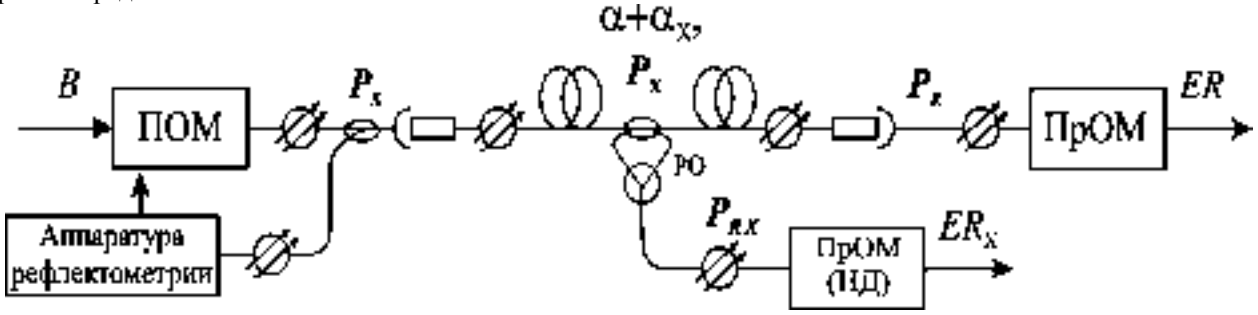

Рисунок 2 – ВОЛС с пассивным НД

При НСИ в результате воздействия на ОВ возникает неоднородность, при этом из ОВ излучается оптический сигнал Δ*P*x, часть которого P_{RX} подается на ПрОМ НД, и в ВОЛТ вносится дополнительное затухание α_X.

Введем следующие коэффициенты: *К*с = P_{RX}/P_X – коэффициент связи устройства НСИ; *К*в = $P_{RX}/\Delta P_X$ – коэффициент отбора устройства НСИ; *К*зч = P_{R0}/P_{RX0} – коэффициент запаса чувствительности устройства НСИ, где P_{R0}, P_{RX0} – чувствительность соответственно фотоприемников ВОЛС и устройства НСИ.

Энергетический потенциал ВОЛС *E* и координата x от начала ВОЛТ до места съема информации для устройства НД с заданным коэффициентом запаса чувствительности *К*зч определяют коэффициент связи *К*с устройства НСИ. В зависимости от конструктивных особенностей и технологии изготовления устройства вывода-ввода для НСИ обеспечивается некий уровень *К*в, что вызывает дополнительное вносимое затухание ВОЛТ α_X.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Основная часть

Всегда существует принципиальная возможность съема информации с ОВ оптического кабеля. Несанкционированный доступ к ВОЛС, несмотря на сложность и дороговизну, все-таки возможен. Способы съема, которые могут быть использованы для перехвата информации с ВОЛС, можно условно разделить на несколько групп [3, 4]:

1. по способу подсоединения:
   1.1 безразрывный;
   1.2 разрывный;
   1.3 локальный;
   1.4 протяженный.
2. по способу регистрации и усиления:
   2.1 пассивные – регистрация излучения с боковой поверхности ОВ;
   2.2 активные – регистрация излучения, выводимого через боковую поверхность ОВ с помощью специальных средств, меняющих параметры сигнала в ВОЛТ;
   2.3 компенсационные – регистрация излучения, выводимого через боковую поверхность ОВ с помощью специальных средств с последующим формированием и вводом в ОВ излучения, компенсирующего потери мощности при выводе излучения;

Основным и наиболее популярным способом безразрывного локального НД является способ линзовой фокусировки сингулярных (вытекающих) мод на изгибе волокна. Этот способ нашел применение в аппаратах для сварки ОВ (и юстировки) [3].

Устройства разрывного НД позволяют осуществлять более надежный съем информации. Однако разрывное подключение требует временного выключения линии, что может сигнализировать о наличии самого доступа. Вероятно, “для маскировки”, параллельно с подключением могут быть осуществлены и умышленные повреждения кабеля. Возможная схема организации разрывного НД приведена в [4].

Пассивные способы обладают высокой скрытностью, так как практически не меняют параметры распространяющегося по ОВ излучения, но имеют низкую чувствительность. Поэтому для перехвата информации используют участки, на которых уровень бокового излучения повышен. Даже после формирования стационарного распределения поля в волокне небольшая часть рассеянного излучения все же проникает за пределы оболочки и может быть каналом утечки передаваемой информации. Возможность существования побочных оптических излучений с боковой поверхности ОВ обусловлена рядом физических, конструктивных и технологических факторов (рис. 3):

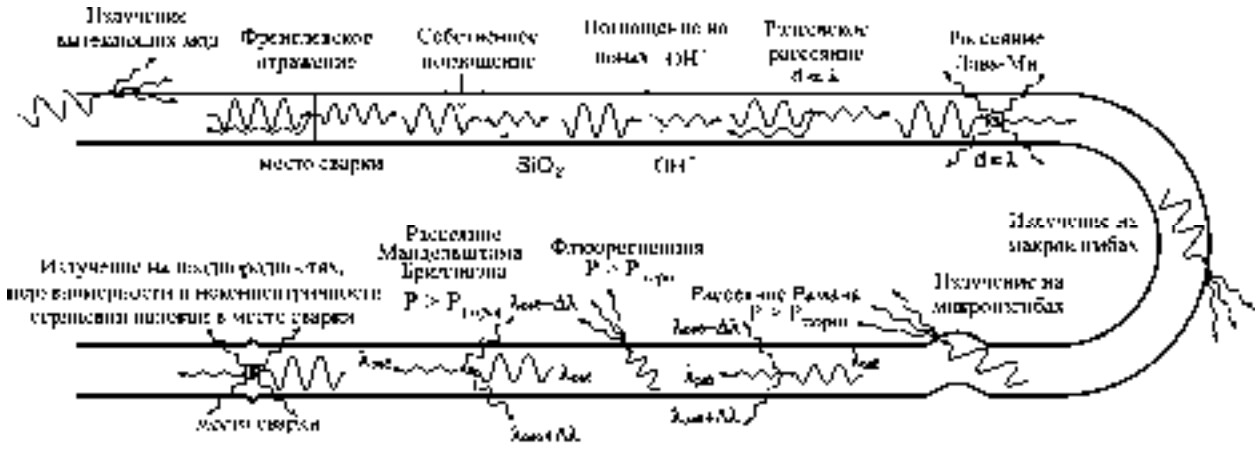

Рисунок 3 – Причины излучения и рассеивания в ОВ

- существование вытекающих мод на начальном участке волокна, обусловленное возбуждением его источником излучения с пространственным распределением, превышающим апертуру волокна;
- излучение вытекающих и излучательных мод на всем протяжении ОВ за счет рэлеевского рассеяния на структурных неоднородностях материала ОВ, характерные размеры которых существенно меньше длины волны излучения;
- преобразование направляемых мод в вытекающие за счет локальных изменений волноводного параметра на волноводных нерегулярностях волокна: микроизгибах (радиус изгиба сравним с диаметром

ОВ) и макроизгибах (радиус изгиба намного больше диаметра ОВ);

- возникновение распределенных и локальных давлений на ОВ.

Использование вытекающих мод в местах стыковки ОВ представляет достаточную опасность с точки зрения защиты информации, т. к. имеется возможность организовать режим «прозрачности» НСИ, когда ВОЛС «не замечает» отбор достаточно большого оптического сигнала из ВОЛТ. В этом случае трудно фиксировать съем сигнала. Однако, ввиду ограниченного и известного числа и расположения таких мест на трассе ВОЛТ обеспечение защиты информации относительно просто достигается организационно-техническими мероприятиями (охрана, наблюдение таких участков).

Активные способы позволяют вывести через боковую поверхность ОВ излучение значительно большей мощности. Однако при этом происходит изменение параметров распространяющегося по ОВ излучения (уровень мощности в канале, модовая структура излучения), что может быть легко обнаружено. К способам этой группы относятся: механический изгиб ОВ, вдавливание зондов в оболочку, бесконтактное соединение ОВ, шлифование и растворение оболочки, подключение к ОВ фотоприемника с помощью направленного ответвителя, термическое деформирование геометрических параметров ОВ и формирование неоднородностей в ОВ.

Компенсационные способы принципиально сочетают в себе преимущества первых двух групп – скрытность и эффективность, но сопряжены с техническими трудностями при их реализации. Вывод излучения, формирование и обратный ввод через боковую поверхность должны осуществляться с коэффициентом передачи, близким к единице. Однако статистический характер распределения параметров ОВ по длине (диаметров, показателей преломления сердцевины и оболочки и др.), спектральной полосы полупроводникового лазера и характеристик устройства съема приводит к тому, что разность между выведенным и введенным обратно уровнями мощности носит вероятностный характер. Поэтому коэффициент передачи может принимать различные значения. Практические устройства, реализующие компенсационные способы съема информации с боковой поверхности ОВ, в настоящее время неизвестны.

Следует отметить, что защитные оболочки и элементы конструкции кабеля существенно ослабляют боковое излучение. Поэтому перехват информации любым из вышеперечисленных способов возможен только при нарушении целостности внешней защитной оболочки кабеля и непосредственном доступе к оптическим волокнам.

Интересным является также протяженный безразрывный съем информации, который можно осуществить или на пологом изгибе волокна или на прямом волокне под воздействием низких температур. Дело в том, что при низких температурах происходит изменение коэффициентов преломления стекла, в результате чего в сердцевине может повыситься уровень рассеяния.

Конфиденциальность передаваемой по ВОЛС информации может быть обеспечена применением специальных методов и средств защиты линейного тракта от НД. К основным достоинствам применения защищенных ВОЛС относятся:

- независимость от структуры передаваемых цифровых сигналов;
- независимость от скорости передачи цифровых сигналов;
- относительно низкая стоимость;
- универсальность применения в локальных, абонентских или зоновых сетях связи.

В последние время проводятся интенсивные работы по созданию ВОЛС, обеспечивающих защиту передаваемой информации от НД. Можно выделить три основных направления этих работ:

- разработка технических средств защиты от НД к информационным сигналам, передаваемым по ОВ;
- разработка технических средств контроля НД к информационному сигналу, передаваемому по ОВ [1, 2];
- разработка технических средств защиты информации, передаваемой по ОВ, реализующих принципы маскировки [8,9], добавления помех, оптической и квантовой криптографии.

Первая группа работ связана с разработкой конструкционных, механических и электрических средств защиты от НД к оптическим кабелям (ОК), муфтам и ОВ. 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 [3]. Конструкция такого волокна представляет собой многослойную структуру с одномодовой сердцевиной.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

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 приникнуть 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) ВОЛТ. СДС можно построить с анализом либо прошедшего через ВОЛТ сигнала, либо отраженного сигнала (рефлектометрические СДС).

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 (рис. 4) СДС реализуется при минимальных изменениях аппаратуры ВОЛС, т. к. практически все необходимые модули имеются в составе аппаратуры ВОЛС. Недостатком является относительно низкая чувствительность к изменениям сигнала.

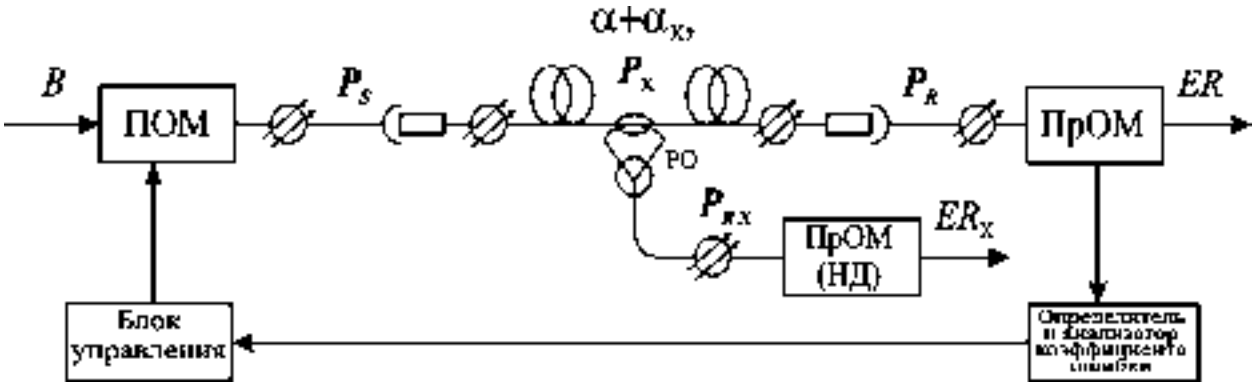

Рисунок 4 – ВОЛС с системой диагностики по анализу коэффициента ошибок

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 НСИ).

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 (рис. 5).

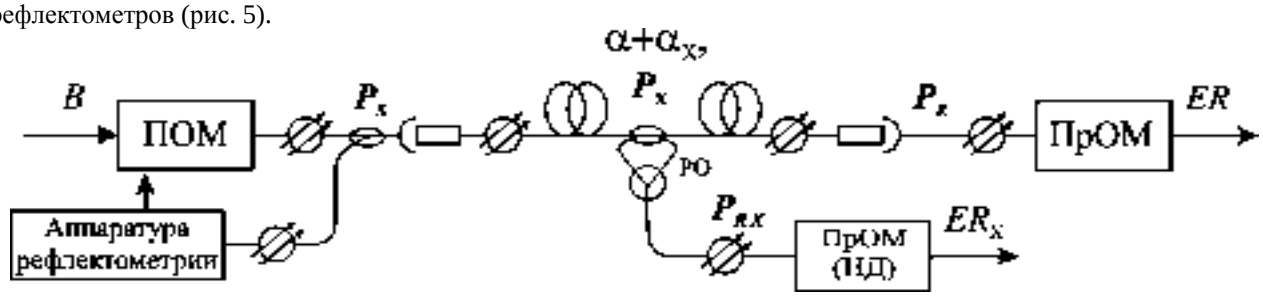

Рисунок 5 – ВОЛС с рефлектометрическими системами диагностики состояния ВОЛТ

ISBN 966-622-022-9

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. В качестве такого рефлектометра может быть использован оптический рефлектометр Минского института радиоэлектроники, выполненный на базе компьютера типа note-book (возможно использование и персонального компьютера семейства IBM) с соответствующим программным обеспечением. Начальные рефлектограммы 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.

Основными недостатками СДС с анализом отраженного сигнала на основе метода импульсной рефлектометрии являются следующие:

- при высоком разрешении по длине ВОЛТ (что имеет важное значение для обнаружения локальных неоднородностей при фиксации НД) значительно снижается динамический диапазон рефлектометров и уменьшается контролируемый участок ВОЛТ ;
- мощные зондирующие импульсы затрудняют проведение контроля ВОЛТ во время передачи информации, что снижает возможности СДС, либо усложняет и удорожает систему диагностики;
- источники мощных зондирующих импульсов имеют ресурс, недостаточный для длительного непрерывного контроля ВОЛС;
- специализированные источники зондирующего оптического излучения, широкополосная и быстродействующая аппаратура приемного блока рефлектометров значительно удорожает СДС.

Методы этой группы хорошо сочетаются со многими другими методами защиты.

Представляет интерес метод, основанный на использовании кодового зашумления передаваемых сигналов. При реализации этого метода применяются специально подобранные в соответствии с требуемой скоростью передачи коды, размножающие ошибки. Даже при небольшом понижении оптической мощности, вызванном подключением устройства съема информации к ОВ, в цифровом сигнале на выходе ВОЛС резко возрастает коэффициент ошибок, что достаточно просто зарегистрировать средствами контроля ВОЛС. Интересным также является метод, основанный на использовании пары разнознаковых компенсаторов дисперсии на ВОЛС. Первый компенсатор вводит в линию диспергированный сигнал, а на приемном конце второй компенсатор восстанавливает форму переданного сигнала.

При использовании маскировки информационного сигнала может применяться система, использующая спектральное разделение каналов [8, 9].

Для маскировки линейного кода в оптическом тракте при использовании кода типа *RZ* можно применить оптическую линию задержки (ОЛЗ), которая подключается на входе оптического тракта с помощью разветвителей оптических (РО) в соответствии с рис. 6 [8. 9]. Величина времени задержки зависит от типа *RZ* кода, и для *RZ*-25% составляет *T*/2, где *T* – длительность тактового интервала.

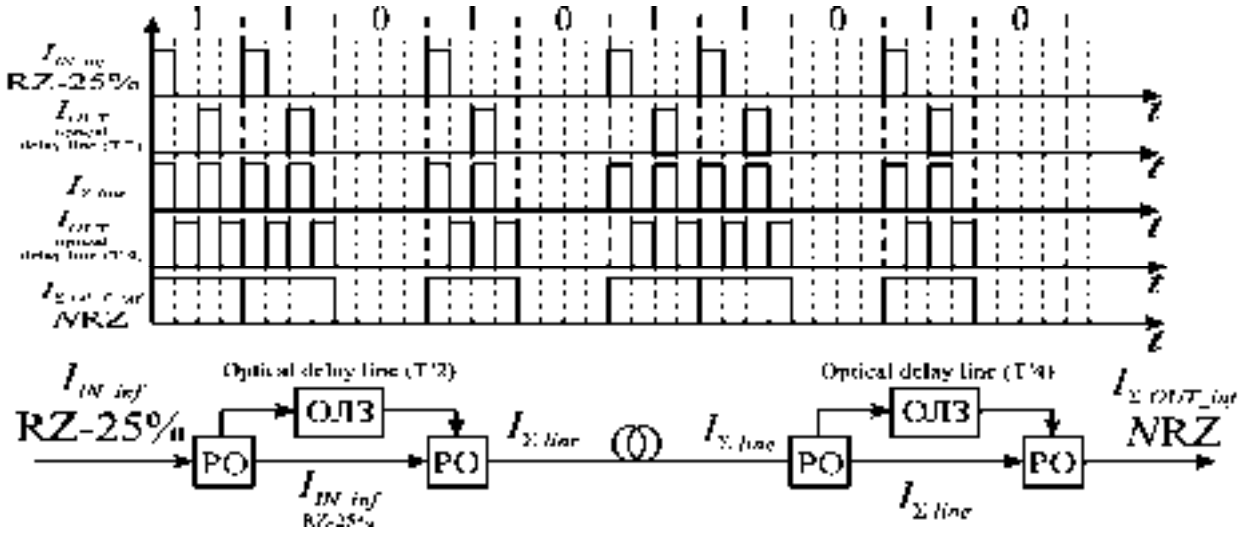

Рисунок 6 – Маскировка линейного кода

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Для выделения сигнала на приемном конце можно использовать аналогичную ОЛЗ, соединенную с двумя РО. При этом на выходе ВОЛС получаем сигнал в коде типа *NRZ*, соответствующий информационному входному сигналу. Также перспективным является использование режима динамического (детерминированного) хаоса, который позволяет обеспечить передачу информации с псевдохаотически изменяющимися частотой и амплитудой несущей. В результате выходной сигнал внешне является шумоподобным, что затрудняет расшифровку.

С развитием науки и техники назрела необходимость и появилась возможность соединить достижения криптографической науки с квантовой механикой и квантовой статистикой. Здесь может возникнуть естественная связь дискретной математики (криптографии) и дискретной (квантовой) механики физических процессов. На этом стыке возникло и интенсивно развивается новое перспективное направление – квантовая криптография.

Методы квантовой криптографии потенциально обеспечивают высокую степень защиты от перехвата информации на линии связи за счет передачи данных в виде отдельных фотонов, поскольку неразрушающее измерение их квантовых состояний в канале связи перехватчиком невозможно, а факт перехвата фотонов из канала может быть выявлен по изменению вероятностных характеристик последовательности фотонов.

Выводы

Возможны различные варианты построения конкретных систем, отличающиеся степенью защиты и контроля НД к передаваемой по ВОЛС информации. Это делает необходимым проведение специальных исследований с целью экспертизы реализованных научно-технических решений и их соответствия требованиям обеспечения защиты информации.

Следует также отметить, что все перечисленные выше методы защиты и их комбинации могут обеспечивать безопасность информации лишь в рамках известных моделей НД. При этом эффективность систем защиты определяется как открытием новых, так и совершенствованием технологий НСИ, использующих уже известные физические явления. С течением времени противник может освоить новые методы перехвата, потребуется дополнять защиту, что не свойственно криптографическим методам защиты, которые рассчитываются на достаточно длительный срок.

В заключение следует отметить, что необходимость практического внедрения и эффективного использования защищенных ВОЛС в сетях связи является задачей сегодняшнего дня.

Литература: 1. Свинцов А. А., Свинцов А. Г. “Численное моделирование систем диагностики состояния волоконно-оптического тракта ВОСП.” Науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, 1998 р. 2. Свинцов А. Г. ”ВОСП и защита информации.” Науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, 1998 р. 3. А. В. Корольков, И. А. Кращенко, В. Г. Матюхин, С. Г, Синев "Проблемы защиты информации, передаваемой по волоконно-оптическим линиям связи, от несанкционированного доступа" // Информационное Общество, 1997 г., № 1. 4. Ю. В. Аграфонов, Д. Б. Липов, А. Н. Малов. "Структура волноводных мод и несанкционированный доступ в волоконно-оптических линиях связи". 5. А. В. Яковлев. Волоконно-оптическая система передачи конфиденциальной информации // Электросвязь, 1994 г., № 10. 6. В. Н. Рыжевнин, М. В.Лазарев. “Скрытность передаваемой информации при электрооптической модуляции света и когерентном уплотнении информации в волоконно-оптических линиях связи” // Волоконно-оптическая техника, 1993 г., № 2. 7. Комаров М. Ю. “Контрольно-измерительное оборудование для монтажа и эксплуатации волоконно-оптических линий связи” // Волоконно-оптическая техника, 1998 г., № 8. 8. Каток В. Б., Манько О. О. “Защита информации в оптических линейных трактах методом спектрального разделения” Ювілейна науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, 9-11 червня 1998 р. 9. Каток В. Б., Манько О. О. Задорожній М. Д. “Нові методи захисту інформації на ВОЛЗ” Науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, квітень 2000 р.

ISBN 966-622-022-9