

реагувати на всі зміни, що відбуваються на атакованому об'єкті. Подібні віддалені атаки найбільше характерні для розподілених обчислювальних мереж.

На відміну від атак із зворотнім зв'язком, віддаленим атакам без зворотнього зв'язку не потрібно реагувати на будь-які зміни, що відбуваються на атакованому об'єкті. Атаки даного виду звичайно здійснюються шляхом передачі на атакований об'єкт одиночних запитів, відповіді на які нападнику не потрібні. Подібну віддалену атаку можна називати однонаправленою віддаленою атакою. Прикладом однонаправленої атаки є типова віддалена атака "Відмова в обслуговуванні".

По розташуванню суб'єкта атаки щодо атакованого об'єкта:

- внутрішньосегментне;
- міжсегментне.

Суб'єкт атаки (або джерело атаки) - програма-нападник, або оператор, що безпосередньо здійснює вплив, комп'ютер мережі (робоча станція) тощо.

Сегмент мережі - фізичне об'єднання комп'ютерів мережі. Наприклад, сегмент мережі утворюють сукупність комп'ютерів мережі, під'єднаних до сервера за схемою "загальна шина". При такій схемі підключення кожний комп'ютер мережі має можливість надавати аналізу будь-який пакет у своєму сегменті.

Отже, при організації технічного захисту інформації, що циркулює в системі технологічного управління, не можна копіювати заходи забезпечення безпеки, що були розроблені для менш пріоритетних автоматизованих та комп'ютерних систем; навпаки, має бути визначений індивідуальний комплекс заходів, що найбільш повно враховував би особливості СТУ. Саме така робота проводиться при розробці керівних нормативних документів, що стосуються СТУ.

Література: 1. Trusted Computer System Evaluation Criteria (TCSEC), US DoD 5200.28-STD, 1993.. 2. Information Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom.- Department of Trade and Industry, London, 1991. 3. Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.. 4. В. Г. Кононович, А. О. Севостьяненко. Основы организации службы ТЗИ в галузі телекомунікацій. Тези доповіді на конференції "Современные и будущие информационные технологии Украины", К.: УДЭНТЗ, 2000, с. 3.. 5. НД ТЗИ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. 6. НД ТЗИ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 7. НД ТЗИ 2.5-005-99. Класифікація автоматизованих систем та стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

УДК 621.391.052

ВОСП И ЗАЩИТА ИНФОРМАЦИИ

Сергей Авдеев, Андрей Свинцов, Анатолий Свинцов

г. Королев, РКК «Энергия», г. Москва, МГТУ им. Баумана, г. Москва, ТОО «Прогноз+»

Анотация: Рассматриваются особенности и основные пути обеспечения защиты информации от НСИ в ВОСП

Ключевые слова: ВОСП, системы диагностики состояния, ЧМЗ, рефлектометрия

Волоконно-оптические системы передачи (ВОСП) благодаря уникальной пропускной способности, малому затуханию волоконных световодов (ВС) и успехам в технологии элементов ВОСП являются наиболее перспективными информационными системами. В области стационарных систем передачи информации с большой информационной емкостью и высокой надежностью ВОСП не имеют конкурентов. Радио системы, в том числе для подвижной связи, и спутниковые системы связи имеют свои преимущества, но по комплексу параметров (скорость передачи, помехоустойчивость, защищенность информации) ВОСП являются наилучшими информационными системами.

Высокая эксплуатационная надежность ВОСП удачно совмещается с высокой степенью защиты передаваемой информации. Это объясняется тем, что в наиболее протяженном и уязвимом для несанкционированного съема информации (НСИ) участке ВОСП - волоконно-оптическом тракте (ВОТ) для передачи используется оптический носитель информации, а с поверхности волоконных световодов электромагнитное поле не излучается. Участки, где возможна утечка электромагнитного излучения, и возможен НСИ "классическими" радиотехническими методами (приемо-передающая аппаратура, регенерационные пункты) известны, локализованы и относительно малочислены. По этой причине эти каналы утечки информации сравнительно легко могут быть поставлены под контроль.

Таким образом, волоконно-оптические системы передачи информации благодаря своему принципу работы обеспечивают высокий уровень защиты от несанкционированного съема передаваемой информации.

Однако, и в ВОСП имеется возможность трудноконтролируемого НСИ, в том числе съема информации с ВОТ, путем физического *локального воздействия* на ВС ВОТ и отвода части оптического сигнала, распространяющегося по ВС [1-3].

Принципы работы ВОСП (передача информации при помощи оптического сигнала посредством волоконных световодов), высокая степень развития техники и технологии ВОСП и реализация высокого уровня технических параметров (высокие скорости передачи, малые затухания волоконных световодов, большие длины регенерационных участков) в значительной мере затрудняют несанкционированный съем информации в ВОСП.

Несанкционированный съем информации в ВОСП возможен. При НСИ в ВОСП необходимо в результате локального воздействия вывести из ВС оптический сигнал и собрать его. При локальном выводе сигнала, в той или иной мере изменяются параметры ВОТ, фиксация которых позволяет фиксировать НСИ и обеспечивать защиту информации от НСИ путем прерывания ее передачи.

Защита информации в ВОСП

При защите информации в ВОСП можно выделить несколько «рубежей обороны»:

- 1) защита *информации* от расшифровки;
- 2) защита *оптического сигнала* от физического снятия.

В первом случае используются как криптографические методы, так и защита оптического сигнала от дешифровки на физическом уровне (когерентные [4], поляризационные или спектральные методы передачи информации в ВОСП).

Во втором случае происходит защита оптического сигнала от *снятия* либо путем затруднения отвода сигнала с ВС ВОТ ВОСП, либо путем фиксации попыток отвода и пресечения этих попыток.

Наиболее перспективными ВОСП, с точки зрения защиты информации, являются модернизированные серийные ВОСП с системами фиксации НСИ на основе анализа состояния ВОТ.

Таким образом, для защиты информации в ВОСП оптимальным является использование специально спроектированных ВОСП на основе серийных элементов с системой фиксации НСИ .

Основой системы фиксации НСИ является система диагностики состояния (СДС) волоконно-оптического тракта. СДС можно построить с *анализом* либо *прошедшего* через ВОТ сигнала, либо отраженного сигнала (*рефлектометрические* СДС).

СДС с анализом прошедшего сигнала является наиболее простой диагностической системой. На приемной части ВОСП анализируется прошедший сигнал. При НСИ происходит изменение сигнала, это изменение фиксируется и передается в передающую часть ВОСП в блок управления.

При использовании анализа коэффициента ошибок на приемном модуле ВОСП СДС реализуется при минимальных изменениях аппаратуры ВОСП, т.к. практически все необходимые модули имеются в составе аппаратуры ВОСП. Недостатком является относительно низкая чувствительность к изменениям сигнала.

Для повышения чувствительности в состав СДС с анализом прошедшего сигнала необходимо использовать фотоприемное устройство с предельной чувствительностью не хуже 10 пВт и нелинейностью преобразования не хуже 0.0001 [5], а также обеспечивать высокую стабильность передающего блока СДС, либо организовывать работу с опорным каналом и измерять отношение оптических сигналов [6].

Основным недостатком СДС с анализом прошедшего сигнала является отсутствие информации о координате появившейся неоднородности, что не позволяет проводить более тонкий анализ изменений режимов работы ВОСП для снятия ложных срабатываний системы фиксации НСИ.

СДС с анализом отраженного сигнала (*рефлектометрические* СДС) позволяют в наибольшей степени повысить надежность ВОСП.

Аппаратура оптической рефлектометрии является основой СДС с анализом отраженного сигнала. В настоящее время наиболее развит метод импульсной рефлектометрии (OTDR). Основным преимуществом СДС с анализом отраженного сигнала на основе метода импульсной рефлектометрии является высокая степень

технической проработки (серийно выпускаются приборы).

В настоящее время оптические рефлектометры имеют динамический диапазон измерения до 41.5дБ и разрешение до 0.001 дБ (AQ7250) [7]. В состав рефлектометров, кроме источника мощного зондирующего сигнала малой длительности, фотоприемника и разветвителя входит мощный блок обработки, обеспечивающий широкие функциональные возможности рефлектометров приборов (получение, обработку, запись, хранение и анализ рефлектограмм).

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

- при высоком разрешении по длине ВОТ (что имеет важное значение для обнаружения локальных неоднородностей при фиксации НСИ) значительно снижается динамический диапазон рефлектометров и уменьшается контролируемый участок ВОТ (например, в рефлектометре НР8147 для разрешения $\Delta x=1$ м динамический диапазон снижается до 9 дБ с 28 дБ для $\Delta x = 1000$ м) ;
- мощные зондирующие импульсы затрудняют проведение контроля ВОТ 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 ВОСП;
- специализированные источники зондирующего оптического излучения, широкополосная и быстродействующая аппаратура приемного блока рефлектометров значительно удорожает СДС.

СДС с анализом отраженного сигнала на основе метода ЧМЗ [8,9,10] является наиболее перспективной для диагностики состояния и фиксации НСИ. Это, в основном, обусловлено следующими особенностями подобных систем:

- обеспечивается наибольшая чувствительность приемного блока ЧМЗ рефлектометра, выигрыш в чувствительности тем больше, чем лучше пространственное разрешение рефлектометра;
- имеется возможность использовать для зондирующего излучения СДС серийный, связной источник излучения;
- имеется возможность проводить диагностику ВОТ во время передачи информации;
- использование относительно дешевых компонент в СДС позволяет реализовать системы значительно более дешевые, чем на основе импульсных рефлектометров;

Необходимо отметить отсутствие в настоящее время серийно выпускаемых рефлектометров на основе метода ЧМЗ, низкий уровень решенных задач для реализации возможностей метода ЧМЗ в приложении к диагностике ВОТ ВОСП.

Литература: 1. А.В. Яковлев Волоконно-оптическая система передачи конфиденциальной информации // Электросвязь -№10,1994г., 2. Leung Chung-Jec et. al. Protection of multimode optical fiber communication // Proc. 14 Congr. Int. Comm. Opt. - Quebec, Aug. 23-28.-1987 - S.1.1987 - p 203., 3. Mit dem Ohr am Licht / Funkschau - 1984 N22- S 49, 4. В.Н. Рыжневин, М.В. Лазарев «Скрытность передаваемой информации при электрооптической модуляции света и когерентном уплотнении информации в волоконно-оптических линиях связи» // Волоконно-оптическая техника -№2,1993 г., 5. Свинцов А.Г. "Фотометр", Патент от 25.11.1988 г., 6. Свинцов А.Г., Канцырев В.Л., Симаковский А.Н. "Фотометр", авторское свидетельство от 26.11.87 г., 7. Комаров М.Ю. «Контрольно-измерительное оборудование для монтажа и эксплуатации волоконно-оптических линий связи» // Волоконно-оптическая техника №8. 1998г., 8. Свинцов А.Г., Яковлев М.Я. Патент РФ "Волоконно-оптическая система передачи информации", N1729263 с приоритетом от 19. 04. 1990г, 9. Свинцов А.Г. «ВОСП и защита информации». Тезисы докладов научно-технической конференции «Правовое, нормативное и метрологическое обеспечение систем защиты информации в Украине», г. Киев, 1998 г., 10. Свинцов А.А., Свинцов А.Г. «Численное моделирование систем диагностики состояния волоконно-оптического тракта «ВОСП» ». Тезисы докладов научно-технической конференции «Правовое, нормативное и метрологическое обеспечение систем защиты информации в Украине», г. Киев, 1998 г.