УДК 621.3.078

ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОПТОВОЛОКОННЫХ СЕТЯХ ПРИ ПОМОЩИ НЕЙРОННЫХ СЕТЕЙ

Старовойтов Р.Д., магистрант; Червинский В.В., доц., к.т.н., доц.
(ГОУ ВПО «Донецкий национальный технический университет», г. Донецк, ДНР)

Выбор показателей оценки защищенности оптоволоконных сетей является сложной исследовательской задачей и в постановочном плане относится к области принятия решения. Сложность выбора показателей, позволяющих дать адекватную оценку защищенности волоконно-оптической линии связи (ВОЛС), определяется [1]:

- необходимостью контроля большого количества средств и элементов защиты, а также мероприятий, направленных на обеспечение безопасности конфиденциальной информации;
- случайностью внешних воздействий и внутренних угроз в системе обработки информации и системе ее защиты;
- отсутствием показателей, учитывающих специфику ВОЛС и особенности ее функционирования;
- необходимостью получения не только качественной, но и количественной оценки защищенности ВОЛС.

Основными параметрами, определяющими показатели защищенности информации, являются:

- количество и характеристики тех показателей ВОЛС, в которых оценивается защищенность информации;
- количество и характеристики дестабилизирующих факторов, которые потенциально могут проявиться и оказать негативное воздействие на защищаемую ВОЛС;
- количество и характеристики применяемых методов защиты;
- число и категории лиц, которые потенциально могут быть нарушителями правил защиты.

Рассмотрим некоторые методы обнаружения угроз в оптических сетях [2, 3].

Контроль состояния оптического кабеля на основе оптической рефлектометрии регистрирует факт присоединения к оптическому каналу по изменениям рефлектограммы. Работа 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 несанкционированного доступа (НД) является система диагностики состояния (СДС) ВОЛС. СДС можно построить с анализом либо прошедшего через ВОЛС 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. 1) 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.

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.

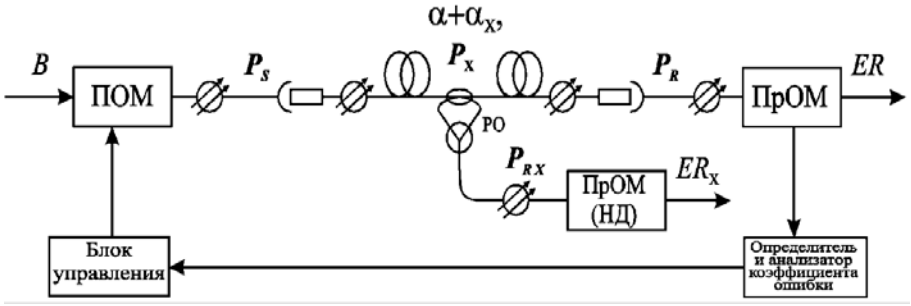

Рисунок 1 – Схема диагностики по анализу коэффициента ошибок

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. 2).

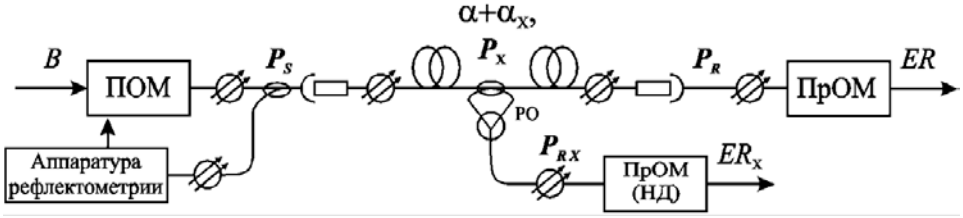

Рисунок 2 – ВОЛС с рефлектометрическими системами диагностики

Суть его состоит в том, что в исследуемую ВОЛС 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 ВОЛС. 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 ВОЛС.

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

— при высоком разрешении по длине ВОЛС значительно снижается динамический диапазон рефлектометров и уменьшается контролируемый участок;

— мощные зондирующие импульсы затрудняют проведение контроля ВОЛС 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.

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.

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. 3. Величина времени задержки зависит от типа RZ кода, и для RZ-25% составляет T/2, где T – длительность тактового интервала.

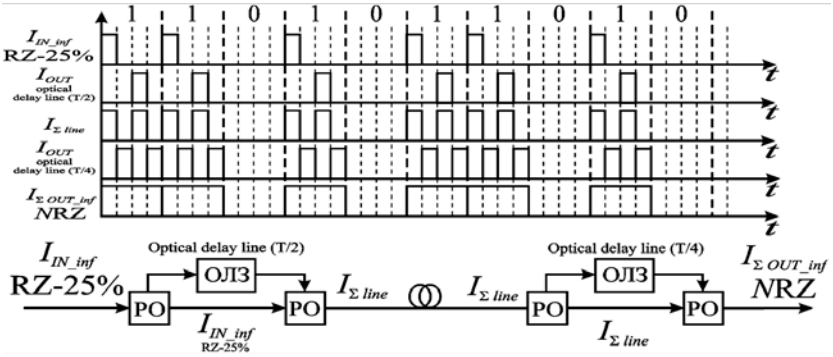

Рисунок 3 – Маскировка линейного кода

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 [4].

Таким образом, возникает задача комплексной оценки возможных угроз безопасности для оптической сети. Одним из вариантов системы, осуществляющей подобную оценку, является система, использующая нейронные сети [5].

Рассмотрим в качестве примера инфокоммуникационную сеть доступа типа LR-PON, приведенную на рис. 4.

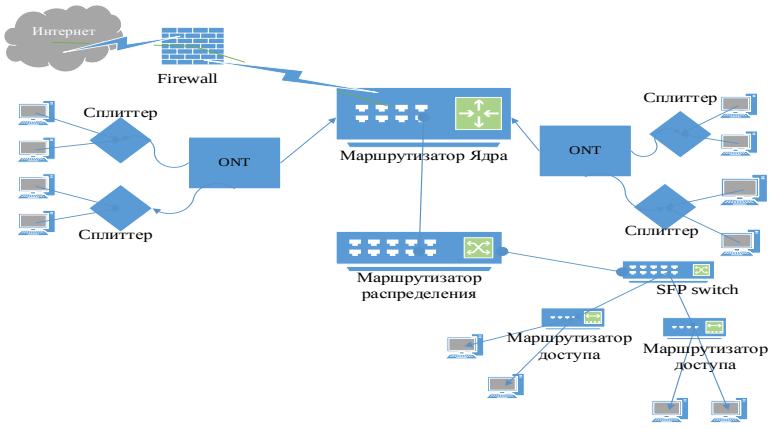

Рисунок 4 – Схема моделируемой сети доступа LR-PON

Для более точного обнаружения НСД в ОВ сетях можно предложить систему на основе нейронной сети, которая будет суммировать и сортировать данные, полученные несколькими методами обнаружения НСД, проводить анализ, идентифицировать и выдавать точную информацию о наиболее вероятных атаках для модельной сети.

Порядок оценки ожидаемого ущерба выглядят следующим образом:

- первоначально рассматривается средний ущерб от проявления угроз и принимается нормальная функция его распределения;

- по данным наблюдения за проявлениями угроз и размером фактического ущерба на нескольких интервалах времени различной продолжительности корректируются параметры распределения среднего ущерба;

- выделяя неопределенные параметры из функции распределения вероятностей ущерба, строят окончательное распределение размера ожидаемого ущерба.

Произведение вероятностей возникновения угрозы и возможного причиняемого ущерба характеризуется понятием риск. Чем больше вероятность угроз и причиняемого ущерба, тем выше риск. Таким образом, если бы удалось собрать достаточное количество фактических данных о проявлениях угроз и их последствиях, то рассмотренную модель можно было бы использовать для решения достаточно широкого круга задач защиты ВОЛС.

Построение оптимальных стратегий сводится к достижению максимальных трудностей для получения прибыли со стороны злоумышленника и минимизации потерь со стороны защитников ВОЛС.

Основными факторами, влияющими на результативность процесса борьбы с незаконным воздействием на защищаемую сеть, являются:

— многовариантность НСД в отношении объектов преступного посягательства, по способу, по месту совершения, по способу реализации и т.д.;

— многоисходность и многонаправленность защитных действий: предупреждение, пресечение или недопущение, раскрытие или не раскрытие;

— вероятностный характер событий – заранее трудно предвидеть, какие конкретные действия совершит злоумышленник, или в течение какого времени и как отреагирует оперативная группа на действия нарушителя;

— динамичность, которая выражается в том, что и НСД и процесс борьбы с ними протекают в реальном времени. Для реализации благоприятного исхода защитные действия должны соответствовать по временным интервалам НСД.

Перечень ссылок

1. Козьминых, С. И. Моделирование систем и процессов обеспечения информационной безопасности в органах внутренних дел [Электронный ресурс] / С. И. Козьминых, П. С. Козьминых // Вестник Московского университета МВД России, 2016. – № 2.– С.161-168. – Режим доступа : https://cyberleninka.ru/article/v/modelirovanie-sistem-i-protsessov-obespecheniya-informatsionnoy-bezopasnosti-v-organah-vnutrennih-del .

2. Гришачев, В. В. Информационная безопасность волоконно-оптических технологий. Часть II [Электронный ресурс] – Режим доступа : http://www.analitika.info/public/files/grishachev-lectures_isfot_part_2.pdf .

3. Tsang, T. Performance Modeling and Analysis for Dynamic Bandwidth Distribution Scheme Using Real-Time Probabilistic System [Электронный ресурс] / Tony Tsang // International Journal of Computer Networks & Communications (IJCNC).– Vol. 3, Issue 4, Jul-Aug 2013, pp.2314-2317 – Режим доступа : http://www.ijera.com/papers/Vol3_issue4/MY3423142317.pdf .

4. Болонная, Е. И. Комбинирование характеристик существующих квантовых криптографических систем в целостный комплекс передачи [Электронный ресурс] / Е. И. Болонная, П. М. Шпатарь // Universum: Технические науки : электрон. научн. журн. 2013. № 1 (1). – Режим доступа : http://7universum.com/ru/tech/archive/item/784 .

5. Зинкевич, А. В. Система обнаружения вторжений с использованием нейронной сети для анализа данных [Электронный ресурс] / А. В. Зинкевич, К. Ю. Еремин // Электронное научное издание «Ученые заметки ТОГУ», 2017. – Том 8, № 4. – С.514-519. Режим доступа : http://pnu.edu.ru/media/ejournal/articles-2017/TGU_8_339.pdf .