ПРИБОРЫ И ТЕХНИКА ЭКСПЕРИМЕНТА, 2020, № 4, с. 145–148

ФИЗИЧЕСКИЕ ПРИБОРЫ ДЛЯ ЭКОЛОГИИ, МЕДИЦИНЫ, БИОЛОГИИ

УДК 621.372.8: 621.396: 621.315

ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИЗИЧЕСКИХ КАНАЛОВ ОПТИЧЕСКИХ СЕТЕЙ ДОСТУПА[1]

© 2020 г. Н. И. Горлов[a],*, И. В. Богачков[b]

[a] *Сибирский государственный университет телекоммуникаций и информатики*
Россия, 630102, Новосибирск, ул. Кирова, 86

[b] *Омский государственный технический университет*
Россия, 644050, Омск, просп. Мира, 11

**e-mail: gorlovnik@yandex.ru*

Поступила в редакцию 03.03.2020 г.
После доработки 12.03.2020 г.
Принята к публикации 13.03.2020 г.

Рассматривается проблема защиты информации от несанкционированного доступа и представлены результаты сравнительного анализа методов извлечения информации из оптического волокна. Предложена методика обнаружения факта формирования каналов утечки информации, проводимого различными способами, для успешной борьбы с несанкционированным доступом. Из проанализированных способов формирования каналов утечки информации в волоконно-оптической линии связи наиболее простым является изгиб оптического волокна для нарушения условий полного внутреннего отражения. В этом случае в системе мониторинга для обнаружения изгибов волокон необходимо отслеживать внесенные потери.

DOI: 10.31857/S0032816220040278

Волоконно-оптические линии связи (в.о.л.с.) в начале развития считались неуязвимыми к несанкционированному доступу, что обуславливалось физическими принципами распространения электромагнитной волны в световоде. Однако со временем была исследована и доказана принципиальная возможность физического съема информации с оптического волокна. Впоследствии общественности стали известны факты обнаружения подслушивающих устройств на в.о.л.с. европейских телекоммуникационных компаний. Очевидным стал факт, что в.о.л.с. лишь изначально имеют более высокую степень защиты информации от физического съема, чем линии связи других типов.

Во-первых, это связано с тем, что электромагнитное излучение без внешнего воздействия выходит за пределы оптического волокна на расстояние не более длины волны [1]. Так создается обязательное условие для съема информации – физический контакт.

Во-вторых, оптические кабели имеют сложную конструкцию: множество волокон с упрочняющими и защитными элементами (в отдельных случаях металлической броней). Также существуют специальные кабели, оснащаемые дополнительными защитными механизмами (например, газовой оболочкой или электромагнитным полем). В результате физический доступ к отдельному волокну становится сложным и трудоемким процессом.

В-третьих, оптические каналы характеризуются высокой скоростью передачи информации (сотни Гбит/с), что достигается использованием коротких световых импульсов (десятки и сотни пикосекунд). Это формирует повышенные требования к характеристикам аппаратуры детектирования [2].

Несмотря на технологическую сложность, процесс несанкционированного подключения к в.о.л.с. возможен. В настоящее время хорошо известно несколько способов, которые представлены на рис. 1.

Способ несанкционированного съема информации посредством сгибания основывается на нарушении внутреннего отражения оптической волны. Для достижения полного внутреннего отражения угол падения сигнала оптической волны на переходе между сердцевиной и оболочкой должен быть больше, чем критический.

Значение критического угла определяется значениями профилей коэффициентов преломления сердцевины и оболочки по формуле

[1] Результаты данного исследования были представлены и обсуждены на третьей международной конференции “Оптическая рефлектометрия, метрология и сенсорика 2020” (http://or-2020.permsc.ru/, 22–24 сентября, Россия, Пермь).

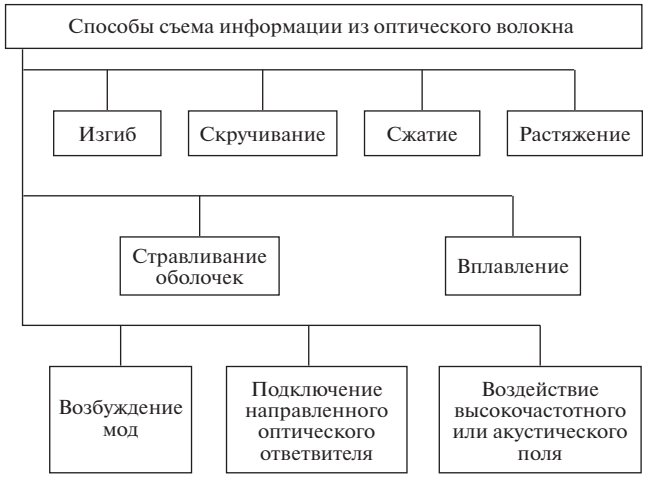

Рис. 1. Способы несанкционированного съема информации из оптического волокна.

$$\theta_к = \cos^{-1}\left(\frac{n_2}{n_1}\right), \quad \text{причем } n_2 < n_1, \qquad (1)$$

где $\theta_к$ – критический угол, n_1 – коэффициент преломления сердцевины, n_2 – коэффициент преломления оболочки.

Изгиб оптического волокна (о.в.) должен быть таким, чтобы угол отражения стал меньше критического. При этом оптическая волна станет проходить сквозь оболочку оптического волокна.

Обнаружение несанкционированного подключения при использовании нарушителем способов первой группы затруднено, поскольку параметры излучения практически не меняются. При этом мощность бокового излучения достаточно мала, что ухудшает достоверность приема перехваченных оптических волн, и это вынуждает непосредственно использовать участки в.о.л.с. с высоким уровнем излучения. Высокие уровни излучения находятся на участках соединения оптической линии, местах изгиба оптического кабеля и на участках со значительным давлением грунта. Следует отметить, что чем больше вводимая мощность, тем сильнее будут изменяться параметры канала передачи данных и, следовательно, легче обнаружить несанкционированное подключение.

В способах, использующих для вывода накладные *Y*- и *X*-образные ответвители, регулировка отводимой мощности затруднена. Способы третьей группы (рис. 1) связаны со значительными техническими трудностями при их реализации с выводом излучения оптической волны и ее обратным вводом, представляющими сложную техническую задачу. Они имеют высокую скрытность.

Системы мониторинга в.о.л.с. на базе оптического рефлектометра являются весьма эффективными для обнаружения несанкционированного подключения. Они позволяют осуществлять непосредственный мониторинг любой ветви в оптической сети доступа. Структурная схема такой системы представлена на рис. 2.

Модуль управления режимами работы необходим для управления и синхронизации модулей мониторинга состояния в.о.л.с. 1, в.о.л.с. 2 и модуля анализа текущих изменений в режиме передачи оптического сигнала. В случае, когда значения увеличения затухания контрольных сигналов ненулевые, то модуль анализа изменений параметров в.о.л.с. принимает решение о гипотетических причинах изменения параметров линии передачи данных. В модуле определения изменений параметров обрабатываются данные, которые поступают от модуля мониторинга состояний в.о.л.с. 1. В.о.л.с. 2 является резервной и используется системой обнаружения несанкционированного подключения для определения эталонных параметров оптической сети доступа.

Алгоритм диагностики увеличения затухания сигнала оптической волны представлен на рис. 3.

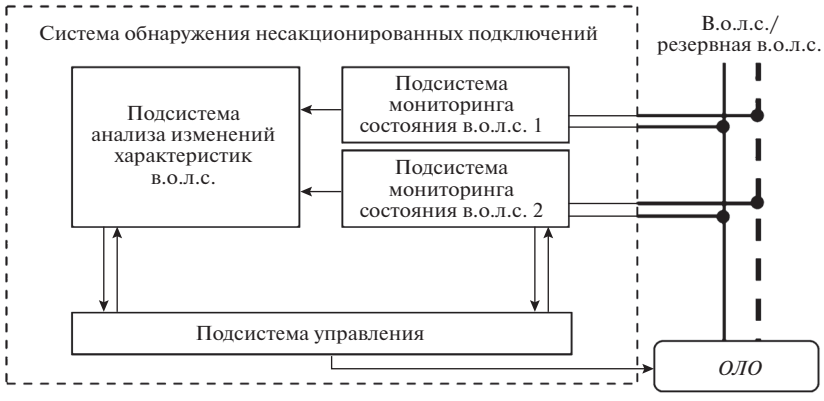

Рис. 2. Структурная схема системы обнаружения несанкционированного подключения. *ОЛО* – оптическое линейное окончание.

Система обнаружения должна иметь тесную интеграцию с архитектурой оптической сети доступа и модульный принцип построения.

К преимуществам описанной системы обнаружения можно отнести:

– наличие базы данных (б.д.) позволяет хранить измеряемые характеристики и данные характеристики относятся к определенному интервалу времени;

– система позволяет идентифицировать местоположение несанкционированного подключения к в.о.л.с.

К недостаткам описываемого способа относятся большее количество элементов, которые позволяют устанавливать координаты неоднородностей и макроизгибов о.в.

Архитектура системы обнаружения несанкционированного доступа показана на рис. 4.

Для реализации перечисленных достоинств особо требуются:

– высокая скорость обработки данных;

– стабильность основных узлов системы;

– отказоустойчивость;

– совершенство алгоритмов анализа данных;

– возможность определения причин, которые вызывают отклонения характеристик в.о.л.с.

Чтобы система обработки данных выдавала корректные результаты, необходимо выполнение следующих условий:

– анализ потенциально возможных ситуаций, которые вызывают отклонение анализируемых параметров;

– анализ каждой ситуации по отдельности для установления уникальных свойств, характерных только для возникшей ситуации;

– математическое описание результатов анализа.

Критерием идентификации несанкционированного подключения на макроизгибе оптического волокна является увеличение затухания, которое можно определить как [3]:

$$\Delta\alpha_i = \alpha_{\text{тек}\,i} - \alpha_{\text{ожид}\,i}, \qquad (2)$$

где $\Delta\alpha_i$ – увеличение затухания, $\alpha_{\text{тек}\,i}$ – текущее затухание, $\alpha_{\text{ожид}\,i}$ – ожидаемое затухание.

Погрешность измерения уменьшается благодаря осуществлению нескольких измерений в течение некоторого промежутка времени. Значение увеличения затухания является функцией от длины оптической волны и радиуса изгиба о.в. [4]:

$$\Delta\alpha = f(R_{\text{изгиб}}, \lambda), \qquad (3)$$

где $R_{\text{изгиб}}$ – радиус изгиба о.в., λ – длина волны сигнала оптической волны.

Критерий исходит из предположения, что для заданного типа о.в. теоретически или экспериментально определены следующие аналитические зависимости затухания:

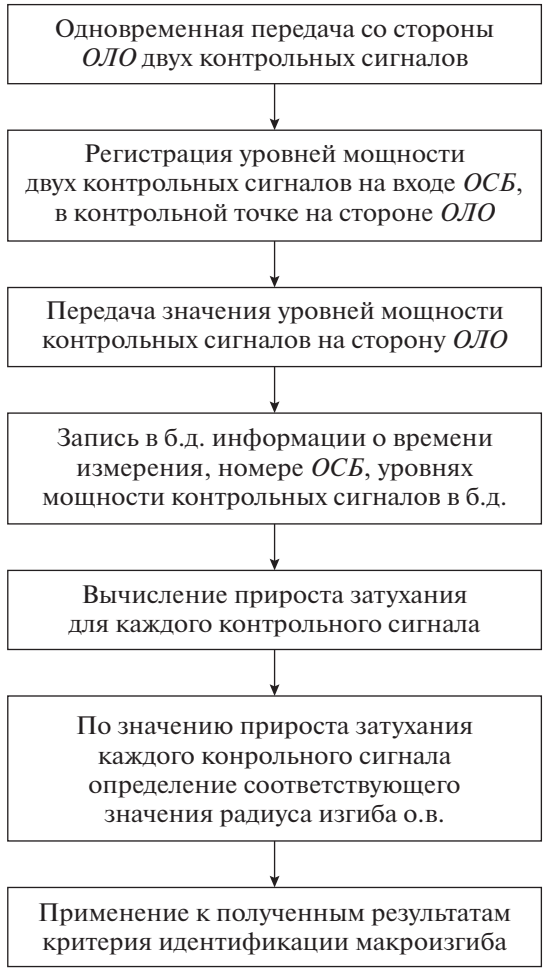

Рис. 3. Алгоритм мониторинга затухания и обнаружения макроизгибов в оптической сети доступа. *ОСБ* – оптический сетевой блок.

$$\Delta\alpha(R_{\text{изгиб}}, \lambda_1), \quad \Delta\alpha(R_{\text{изгиб}}, \lambda_2). \qquad (4)$$

Используя значения критериев (4), для контрольных оптических сигналов с длинами волн λ_1 и λ_2 можно непосредственно вычислить значение увеличения или уменьшения затухания, подставив в ряд возможных значений $R_{\text{изгиб}}$.

Следует отметить, что возможны ситуации возникновения макроизгибов вследствие причин, которые не относятся к несанкционированному подключению, а именно:

– температурные и механические воздействия окружающей среды на в.о.л.с. сети доступа;

– действия персонала по обслуживанию в.о.л.с. сети доступа.

Если на входе некоторого участка наблюдается увеличение или уменьшение затухания, то необ-

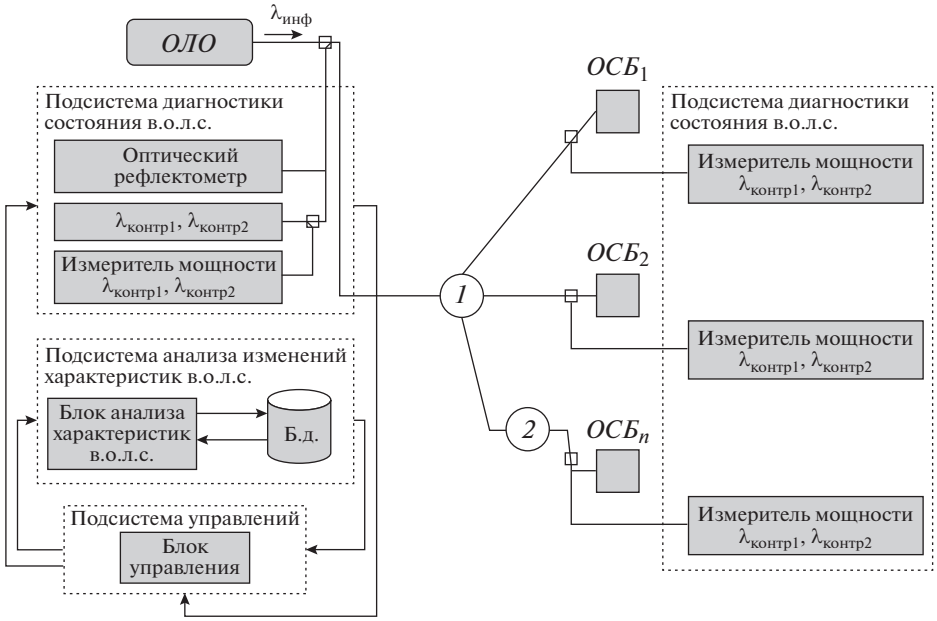

Рис. 4. Архитектура системы обнаружения несанкционированного подключения для оптической сети доступа. *1*, *2* – сплиттеры; $ОСБ_1$–$ОСБ_n$ – оптические сетевые блоки.

ходимо интерпретировать данное событие. Решение о том, является ли изменение затухания следствием макроизгиба о.в., принимается на базе следующих тождеств [5]:

$$\begin{cases} R_{\text{изгиб}}(\Delta\alpha_{\lambda 1}) = R_{\text{изгиб}}(\Delta\alpha_{\lambda 2}) - \text{макроизгиб о.в.} \\ R_{\text{изгиб}}(\Delta\alpha_{\lambda 1}) \neq R_{\text{изгиб}}(\Delta\alpha_{\lambda 2}) - \text{не макроизгиб о.в.} \end{cases} \quad (5)$$

Если любой обнаруживаемый факт изменения затухания принимать как несанкционированный доступ, то это приведет к увеличению количества ложных тревог системы мониторинга в сети доступа.

Для уменьшения количества ложных тревог необходимо использовать специальные критерии, с помощью которых идентифицируется факт несанкционированного подключения:

– время появления изменения затухания не попадает в период, когда на оптической сети доступа осуществляются работы восстановительного или регламентного характера;

– изменение затухания возникло на том участке оптической сети доступа, где не осуществлялись какие-либо работы;

– если на участке не проводятся какие-либо работы восстановительного или регламентного характера, а значение увеличения затухания динамически изменяется во времени в сети доступа.

На первом этапе происходит чтение из б.д. данных и типовых параметров о ветвях оптической сети доступа и времени возникновения тех или иных изменениях затухания. Для увеличения достоверности идентификации несанкционированного доступа следует изменить несущую длину волны зондирующего импульса. Если с увеличением длины волны интенсивность регистрируемого увеличивается, то несанкционированный съем информации осуществляется посредством изгиба о.в.

СПИСОК ЛИТЕРАТУРЫ

1. *Rejeb R., Leeson M.S., Green R.J.* // IEEE Commun. Mag. 2006. V. 44. № 11. P. 79.
2. *Everett B.* Network Security. 2007. V. 207. № 5. P. 13.
3. *Guo S., Zhao Z., Zhang Q.* // Power System Protection and Control. 2017. V. 45. № 17. P. 92.
4. *Gorlov N.I., Bogachkov I.V., Kitova E.T.* // 14-th international scientific-technical conference on actual problems of electronic instrument engineering (APEIE). 2018. P. 140.
5. *Булавкин И.А.* // T-comm – Телекоммуникации и транспорт. 2008. № 3. С. 20.