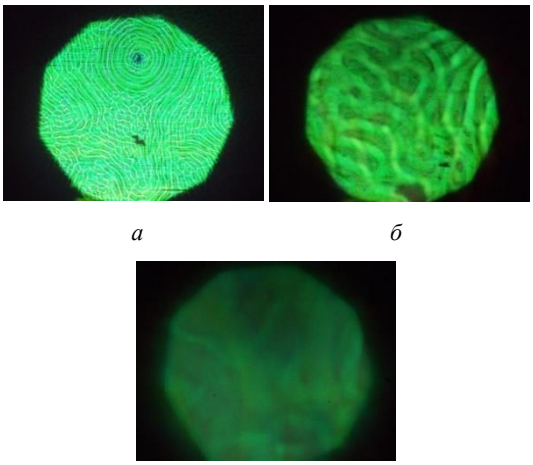

а *б* *в*

Рисунок 3 – Оптическое изображение дефектной области с увеличением ×10 (*а*), ×40 (*б*) и ×100 (*в*)

Результаты исследований показали, что исследование поверхности анодного оксида алюминия методом сканирующего зонда Кельвина позволяет эффективно выявлять и локализовать области концентрации структурных дефектов, при этом регистрируемые зондом значения КРП могут использоваться как условная количественная характеристика степени дефектности участка поверхнотси. Для уточнения вида дефектов могут использоваться дополняющие методы, такие как оптическая или атомно-силовая микроскопия, обеспечивающие более высокое пространственное разрешение, но малое (недостаточное для начальной локализации дефектов) поле контроля.

Благодарности. Работа выполнена в рамках задания 1.10 ГПНИ «Фотоника и электроника для инноваций».

Литература

1. Zharin, A. L. Contact Potential Difference Techniques as Probing Tools in Tribology and Surface Mapping // Applied Scanning Probe Methods. – 2010. – V. 14. – P. 687–720.

2. Растровая сканирующая фотостимулированная электрометрия для контроля прецизионных поверхностей / Р. И. Воробей [и др.] / Известия ТулГУ. Технические науки. 2021. Вып. 10. – С. 66–73.

УДК 621.391

ТЕСТИРОВАНИЕ ИНФОРМАЦИОННОЙ УЯЗВИМОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ

Завадская Т. Е.

Московский государственный технический университет имени Н. Э. Баумана
Москва, Российская Федерация

Аннотация. Показаны критичность волоконно-оптической линии связи (ВОЛС) к несанкционированному доступу (НСД), который может осуществляться неинтрузивными способами. Показана примерная соответствующей лабораторной установки.

Ключевые слова: волоконно-оптическая линия связи, несанкционированный доступ, уязвимость линии, требования безопасности.

TESTING THE INFORMATION VULNERABILITY OF FIBER-OPTIC COMMUNICATION LINES

Zavadskaya T.

Bauman Moscow State Technical University
Moscow, Russian Federationn Federation

Abstract. The criticality of a fiber-optic communication line (fiber optic line) to unauthorized access (NSD), which can be carried out in non-intrusive ways, is shown. An approximate model of the corresponding laboratory installation is shown.

Key words: fiber-optic communication line, unauthorized access, vulnerability of the line, security requirements.

Адрес для переписки: Завадская Т. Е., ул. Вторая Бауманская, 5, г. Москва 107005, Российская Федерация
e-mail: zavadskay@bmstu.net

Почти все преимущества ВОЛС не вызывают сомнений, но тезис о хорошей защищенности волоконно-оптической линии связи от несанкционированного доступа (НСД) требует разъяснений. Определимся, что применительно к ВОЛС это означает невозможность перехвата информации без физического нарушения целостности волоконно-оптической линии и отсутствие паразитных наводок [1].

В Центре компетенций компании «Открытые технологии» был собран стенд для исследования возможной уязвимости ВОЛС, представляющий собой модель распределенного центра обработки данных. Оптическая магистраль имитировалась кросс-панелью с петлей из разделанного многожильного оптического кабеля для внешней проводки. В качестве перехватчика использовалось пассивное устройство типа «ответвитель-прищепка» FOD 5503. Такое устройство создает микроизгиб в волокне и ответвляет сигнал, который может быть получен через имеющийся патч-корд. В процессе тестирования удалось перехватить сигнал, передаваемый в одном направлении.

Следует отметить, что описанные действия можно выполнить без применения специализированного дорогостоящего инструмента (приемлемая стоимость средств перехвата позволяет их использовать не только организациям, но и частным лицам) и за сравнительно небольшое время. Линии связи остались без разрывов: в процессе подготовки стенда кабель был освобожден лишь от внешних защитных оболочек, а волокна находились в защитном цветном буфере толщиной 250 мкм [2].

Из результатов эксперимента следует такой вывод: уязвимость ВОЛС доказана на практике. А потому в связи с возможностью компрометации передаваемых данных или их модификации необходимо использовать средства криптографической защиты информации, передаваемой по ВОЛС. Для криптографической защиты следует выбрать средства, которые не вносят существенных временных задержек при криптографическом преобразовании передаваемой/принимаемой информации и обеспечивают шифрование/расшифровку для всего диапазона скоростей передачи данных, характерного для каналов SONET/SDH [3].

Рисунок 1 – Схема испытательного стенда

В качестве таких средств были выбраны устройства SafeEnterprise SONET Encryptor компании SafeNet. Они осуществляют шифрование всего трафика SDH на канальном уровне на скорости от OC-3 (155,5 Мбит/с) до OC-48 (2,4 Гбит/с). Их применение прозрачно для протоколов вышележащих уровней и, следовательно, не должно вносить существенной задержки в сигнал. Это предположение было решено проверить серией тестов [4].

Для проведения новой серии испытаний был собран стенд, имитирующий нагрузку на магистраль передачи данных между основным ЦОД и резервным. Оборудование шифрования трафика SafeEnterprise SONET Encryptor OC3/OC12 подключалось к магистрали SDH и обеспечивало прозрачное для конечных устройств шифрование трафика. Для тестирования использовались встроенные средства OS Sun Solaris, которые создавали нагрузку на дисковую подсистему и измеряли ее параметры. Параметры нагрузки варьировались как по видам нагрузки, так и размерам блока передаваемых данных (8 Кбайт и 1 Мбайт). Измерения последовательно проводились для двух конфигураций испытательного стенда: канал 100 Мбит/с с шифрованием и канал с той же пропускной способностью без шифрования [5].

Исходя из проведенных исследований можно сформировать краткую информацию по требованиям безопасности, предъявляемой к информации, передаваемой по ВОЛС, представленной в таблице 1.

Таблица 1 – Требования безопасности, предъявляемые к информации, передаваемой по ВОЛС, и методы защиты

Требование безопасности	Методы защиты, выполняющие требование безопасности
Обеспечение контроля штатных параметров сигнала с информацией, передаваемой по ВОЛС	Мониторинг при помощи рефлектометров, дальномеров, интерферометров, специальных автоматизированных систем мониторинга
Обеспечение безопасности оптоволоконного канала в местах механических соединениях оптоволокна	Введение дополнительного зашумления, маскирования и кодирования проходящего сигнала, введение дополнительных внешних методов защиты оптоволокна
Обеспечение безопасности оптоволоконного канала от внешней среды и механических воздействий	Использование специальных покрытий, усиленного бронирование к применяемому оптоволокну
Обеспечение безопасности оптоволоконного канала от внешнего излучения	Использование специальных покрытий, усиленного бронирование к применяемому оптоволокну
Обеспечение безопасности оптоволоконного канала от внешнего излучения	Использование специальных покрытий, усиленного бронирование к применяемому оптоволокну
Обеспечение безопасности информации, передаваемой по оптоволоконному каналу, на протяженных участках прокладки оптоволокна	Использование специальных покрытий, усиленного бронирование к применяемому оптоволокну, введение кодирование и мониторинга на концах участков

Полученные данные позволяют сформулировать основную информацию о текущей ситуации в сфере обеспечения информационной безопасности ВОЛС и разработать на их основе математическую постановку задачи и алгоритм программного обеспечения.

Литература

1. Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for detection and Prevention, Keith Shaneman & Dr. Stuart Gray, IEEE Military Communications Conference, 2004.

2. Широкополосные телекоммуникационные средства с кодовым разделением каналов на основе хаотических сигналов / Ю. В. Гуляев и др. // Радиотехника. – 2014. – № 10. – С.3–15.

3. Документация SafeNet SONET Encryptor [Электронный ресурс]. – Режим доступа: http://www.askon.cz/downloadFile.php?ID=23.

4. Румянцев, К. Е. Защита сообщений в фотонных телекоммуникационных системах – новая технология передачи данных / К. Е. Румянцев, И. Е. Хайров // Сборник докладов и статей регионального научно-практического семинара «Информационная безопасность Юг России». – Таганрог, 2003.

5. Fietcher, P. Light pulses sent over optical fibers create «Invulnerable» encryption / P. Fietcher // Electron Des. – 1995. –V. 43, – № 26. – P. 38–40.

6. Румянцев, К. Е. Передача конфиденциальной сообщений по волоконно-оптическим линиям связи, защищенная от НСД / К. Е. Румянцев, И. Е. Хайров // Информационное противодействие угрозам терроризма. – 2003. – № 1.

УДК 621.3.049.77: 681.586

ЦИФРОВОЙ ЛАЗЕРНЫЙ ДАЛЬНОМЕР С РАДИОИНТЕРФЕЙСОМ ПЕРЕДАЧИ ДАННЫХ

Здоровцев С. В., Кушнеров Д. П., Шевченко А. В.

Открытое акционерное общество «МНИПИ»
Минск, Республика Беларусь

Аннотация. Представлены результаты разработки цифрового лазерного дальномера для определения положения (измерения расстояния) объекта. Прибор обеспечивает беспроводную передачу данных на удаленный ПК по радиоканалу за счет встроенного радиоинтерфейса.

Ключевые слова: цифровой лазерный дальномер, определение положения объекта, беспроводная передача данных.

DIGITAL LASER RANGEFINDER WITH A RADIO DATA TRANSMISSION INTERFACE

Zdorovtsev S., Kushnerov D., Shevchenko A.

MNIPI Open Joint-Stock Company
Minsk, Republic of Belarus

Abstract. The results of the development of a digital laser rangefinder for determining the position (distance measurement) of an object are presented. The device allows wireless data transmission to a remote PC via a radio channel by means of the built-in radio interface.

Key words: digital laser rangefinder, determining the object position, wireless data transmission

Адрес для переписки: Здоровцев С. В., ул. Я. Коласа, 73, г. Минск 220113, Республика Беларусь
e-mail: zgk@mnipi.by

Оптические приборы являются самой распространенной группой приборов для измерения положения и перемещения объектов. Оптические приборы позволяют выполнять бесконтактное измерение, определять положение объектов, перемещающихся с большой скоростью. Расстояние обнаружения может достигать сотен метров, а точность определения положения объекта достигать десятых долей микрона.

В настоящее время широкое распространение получили лазерные дальномеры для измерения расстояния и положения объектов, а также различные системы контроля и обеспечения безопасности на основе лазерных датчиков [1–3].

В работе представлены результаты разработки цифрового лазерного дальномера, предназначенного для измерения положения объекта с возможностью беспроводной передачи данных за счет использования встроенного радиоинтерфейса.

Структурная схема дальномера представлена на рисунке 1.

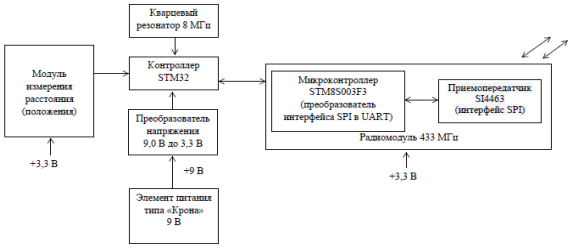

Рисунок 1 – Структурная схема цифрового лазерного дальномера

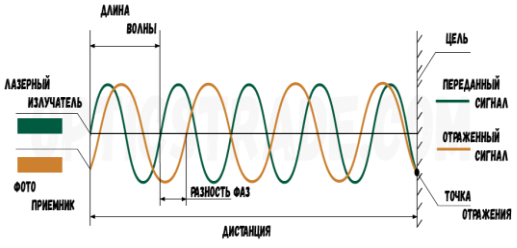

Рисунок 2 – Принцип работы лазерного дальномера