DOI: 10.22184/1993-7296.FRos.2022.16.6.484.500

Проблема информационной безопасности волоконно-оптических технологий

В. В. Гришачев А. Д. Заболотская
Российский государственный гуманитарный университет, Институт информационных наук и технологий безопасности, Москва, Россия

В работе представлен анализ угроз безопасности информации критической информационной инфраструктуры, функционирующей на основе волоконно-оптических технологий. В предложенной модели выделены три направления угроз конфиденциальности – перехват трафика в оптических сетях; волоконно-оптический канал утечки информации, циркулирующей на защищаемом объекте; несанкционированный доступ к информации с помощью волоконно-оптических средств технической.

Ключевые слова: информационная безопасность волоконно-оптических технологий, перехват трафика в оптических сетях, волоконно-оптический канал утечки информации, волоконно-оптические средства технической разведки

Статья получена: 05.04.2022
Статья принята: 04.05.2022

ВВЕДЕНИЕ

Совершенствование технологической базы информационных систем, телекоммуникационных сетей, автоматизированных систем управления приводит к созданию новых ранее неизвестных угроз информационной безопасности. Особую опасность несут технологии реализации информационных процессов на новых физических принципах. В новых технологиях и технике проявляется внутреннее противоречие, связанное с неизученностью всех особенностей

Information Security Concern of Fiber-Optic Technologies

V. V. Grishachev, A. D. Zabolotskaya
Russian State University for the Humanities, Institute of Information Science and Security Technologies, Moscow, Russia

The paper presents an analysis of information security threats to the critical information infrastructure operating on the basis of fiber-optic technologies. The proposed model identifies three areas of privacy threats, including traffic interception in the optical networks; fiber optic channel of information leakage circulating at the protected facility; unauthorized access to the information using the fiber-optic technical intelligence means.

Key words: information security of fiber-optic technologies, traffic interception in the optical networks, fiber-optic information leakage channel, fiber-optic technical intelligence means

Received on: 05.04.2022
Accepted on: 04.05.2022

INTRODUCTION

Improvement of the processing base of information systems, telecommunication networks, automated control systems leads to the occurrence of previously unknown new threats to information security. The information process technologies based on new physical principles are of particular danger. An internal contradiction is manifested in new technologies and techniques related to the lack of knowledge about all the functioning features. On the one part, introduction of new technologies creates an illusion of greater information security that is associated with novelty of the principles used, for which the threat models have not yet been developed. On the other part, there is a danger of occurrence of the leakage channels that have not yet been identified and that are based on the physical principles not previously considered in the regulatory and methodological documents.

функционирования. С одной стороны, внедрение новых технологий создает иллюзию большей защищенности информации, что связывается с новизной используемых принципов, для которых еще не разработаны модели угроз. С другой стороны, существует опасность появления каналов утечки не выявленных, функционирующих на физических принципах, не рассматриваемых ранее в нормативных и методических документах.

Подобная проблема возникает с применением фотонных технологий в системах сбора, обработки, передачи и хранении информации, в частности, в связи с успешным внедрением волоконно-оптических технологий в системах связи, измерения и безопасности, которые несут значительные преимущества по сравнению с другими технологиями. Решение проблемы возможно при осуществлении физико-технического анализа возможных каналов утечки информации в новых технологиях, построение актуальных моделей угроз, разработке современных технических средств и систем защиты информации, доведение знаний до широкого круга специалистов в области обеспечения безопасности.

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЙ

Фотоника одно из основных направлений развития не только в информационной, но и в общей технике. В ней условно можно выделить лазерные, оптоэлектронные, волоконно-оптические и интегрально-оптические технологии. В информатике находит широкое применение волоконно-оптические технологии связи (в настоящее время, кабельные инфраструктуры в основном строятся на волоконно-оптических технологиях). Все новые телекоммуникации проектируются и строятся на оптическом кабеле [1]. Наиболее перспективным абонентским доступом (первая/последняя миля) является оптический доступ в виде пассивных оптических сетей (*Passive Optical Network, PON*), который позволяет связать оптоволокном без промежуточного активного оборудования центральный сетевой терминал с абонентом. В будущем, вся система связи как локальная, так и дальняя, должны стать полностью оптическими (*All-Optical Network, AON*). Доля оптической составляющей в современной связи определяется уровнем развития информационной составляющей на данной территории и непрерывно растет.

A similar problem occurs due to the use of photonic technologies in the data collection, processing, transmission and storage systems, in particular, in connection with the successful introduction of fiber-optic technologies in the communication, measurement and security systems that have significant advantages in comparison to other technologies. The problem can be solved by a physical and technical analysis of possible information leakage channels in the new technologies, generation of the relevant threat models, development of the up-to-date technical facilities and information security systems, and notification of a wide range of security specialists.

1. INFORMATION SECURITY OF FIBER-OPTIC TECHNOLOGIES

Photonics is one of the main areas of development not only in the field of information technology, but also in the general technological field. It can conditionally be divided into the laser, optoelectronic, fiber-optic and integrated-optical technologies. The fiber-optic communication technologies are widely used in computer science. At present, the cable infrastructures are mainly based on the fiber-optic technologies. All new telecommunications are designed and developed using the optical cables [1]. The most promising subscriber access (first/last mile) is optical access in the form of passive optical networks (*PON*) that allows to use fiber optics for connection of the central network terminal with the subscriber without any intermediate active equipment. In the future, the entire communication system (both local and distant), must be all-optical (*All-Optical Network*, *AON*). The share of the optical component in modern communications is determined by the development level of the information component in a given territory; moreover, it is constantly growing.

Such a prospect is related primarily to the advantages of photonic transport over electronic transport in the cable networks. It means the lower energy losses, greater information capacity of the communication channel, durability, reliability, inertness to the superimposed fields and aggressive mediums. Very important advantages include the well-established installation and operation technologies for the optical cable networks. The construction produce-ability of the optical networks of different levels is related to a wide range of installation, testing and operational equipment that allows the construction of underwater, underground, overhead telecommunication lines. The total length

Подобная перспектива связана в первую очередь с преимуществами фотонного транспорта над электронным в кабельных сетях. Это меньшие энергетические потери, большая информационная емкость канала связи, долговечность, надежность, инертность к внешним полям и агрессивным средами. Не маловажным преимуществом является отлаженность технологий монтажа и эксплуатации оптических кабельных сетей. Технологичность строительства оптических сетей разного уровня связывается с широким ассортиментом монтажного, испытательного и эксплуатационного оборудования, которое позволяет проводить строительство подводных, подземных, воздушных телекоммуникаций. Общая протяженность оптических кабельных сетей превышает 4 миллиарда километров, пересекая континенты и океаны.

Кроме информационных коммуникаций волоконно-оптические технологии находят применение в системах измерений [2, 3]. На оптоволокне можно построить широкий набор датчиков, распределенных измерительных систем практически всех физических величин для механических воздействий, акустических, тепловых, радиационных, электромагнитных полей и т.д. Преимуществом оптоволокна как датчика является высокая чувствительность к внешним полям и воздействиям, распределенность измерений, возможность создания датчика нескольких величин на одном оптоволокне. На основе оптоволокна возможно построение распределенных измерительных сетей для контроля экологического состояния территорий и технологического состояния промышленных объектов. Например, прокладывая оптоволокно внутри дорожного покрытия автострад можно контролировать состояние покрытия. Аналогичные задачи могут решаться в железнодорожном, трубопроводном транспорте, в строительном мониторинге. Одно из важных применений оптоволокна является использование его для решения задач безопасности [4, 5]. Используя преимущества оптического кабеля, его применяют в системах видеонаблюдения, для контроля доступа, охране периметра, в системах пожарной сигнализации и других областях.

Столь широкое распространение волоконно-оптических технологий формирует новые виды угроз безопасности информации, которые можно разделить на три направления:

- угрозы перехвата трафика в оптических сетях различного назначения;

of optical cable networks exceeds 4 billion kilometers, while traversing the continents and oceans.

In addition to the information communications, fiber optic technologies are widely applied in the measurement systems [2, 3]. Fiber optics can be used to produce a wide range of sensors, distributed measuring systems of almost all physical values for mechanical impacts, acoustic, thermal, radiation, electromagnetic fields, etc. The advantage of an optical fiber as a sensor is its high sensitivity to the superimposed fields and influences, distribution of measurements, and possible provision of several values on a single optical fiber. The optical fiber can be used as a basis for possible generation of distributed measuring networks to control the environmental condition of territories and the process condition of industrial facilities. For example, it is possible to monitor the coating condition by laying fiber optics inside the motorway coating. Similar problems can be solved in the field of railway and pipeline transport, or construction monitoring services. One of the important applications of optical fiber is its use for solving the security problems [4, 5]. By using the advantages of optical cable, it can be applied in the video surveillance systems, access control, perimeter guarding, fire alarm systems and other areas.

Such a widespread use of fiber optic technologies leads to the new types of information security threats that can be divided into three groups:

- threats of traffic interception in the optical networks for various purposes;
- threats of unauthorized data collection at the facilities using the standard optical networks;
- threats to use the technical intelligence means based on the fiber-optic technologies.

The classification provided makes it possible to cover all aspects of the problem, each of which has an important significance with some independent technical implementation of both attack and defense instruments.

2. THREATS OF TRAFFIC INTERCEPTION IN THE OPTICAL NETWORKS [6–11]

Traffic interception is an illegal information sourcing using a technical tool that detects, receives and processes the informative signals from the data networks (Fig. 1). When intercepted, the object of threat is information transmitted over the regular optical networks.

The optical cable system of the facility can include not only telecommunications and local networks, but also the special-purpose networks such as audio communications, cable TV, video surveillance

- угрозы несанкционированного сбора информации на объектах через штатные оптические сети;
- угрозы применения средств технической разведки на основе волоконно-оптических технологий.

Представленная классификация позволяет охватить все аспекты проблемы, каждая из которых имеет самостоятельное значение с некоторой независимой технической реализацией как средств нападения, так и защиты.

2. УГРОЗЫ ПЕРЕХВАТА ТРАФИКА В ОПТИЧЕСКИХ СЕТЯХ [6–11]

Перехват трафика – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов из информационных сетей (рис. 1). При перехвате объектом угрозы является информация, передаваемая по штатным оптическим сетям.

Оптическая кабельная система объекта может включать не только телекоммуникационные и локальные сети, но и такие сети специального назначения как аудиосвязи, кабельного телевидения, систем видеонаблюдения, различных измерительных систем и другие кабельные системы. Передаваемый по оптическим кабелям трафик носит конфиденциальный характер и имеет важное значение для функционирования объекта не зависимо от вида сети. Трафик может подвергаться различным опасностям: нарушению конфиденциальности, целостности и доступности. Угрозы реализуются различными способами, но одним из основных способов является перехват посредством несанкционированного съема информации, т.е. нарушение конфиденциальности при передаче информации с помощью средств технической разведки. При перехвате нарушитель обладает техническими возможностями на уровне современной техники и способен реализовать любой сценарий по получению доступа к конфиденциальной информации, не противоречащий законам физики [6–8].

systems, various measuring systems and other cable systems. The traffic transmitted over the optical cables is confidential, and therefore, it is important for the facility operation, regardless of the network type. Traffic can be exposed to various hazards such as breach of confidentiality, integrity, and availability. The threats are perpetrated in various ways, but one of the main methods is interception through the unauthorized data retrieval, i.e. breach of confidentiality during data transmission using the technical intelligence tools. When intercepted, the intruder has technical capabilities at the modern technological level and is able to implement any scenario for gaining access to the confidential information that does not contradict the physics laws [6–8].

The informative signals and access methods to them play an important role in the interception structure. In the optical networks, the parameter registration methods for an informative signal can be divided into the contact and remote ones. In the case of contact access, the intruder needs to gain physical access to the optical fiber in the cable, including the need to search for the cable, destroy the protective sheaths, select the required fiber, and then remove part of the optical informative signal by installing a special fiber optic insert into the fiber optic gap or by influencing the optical fiber for output of the optical signal parts, for example, at the fiber bend, optical tunneling, etc. In the case of remote interception, the intruder requires the

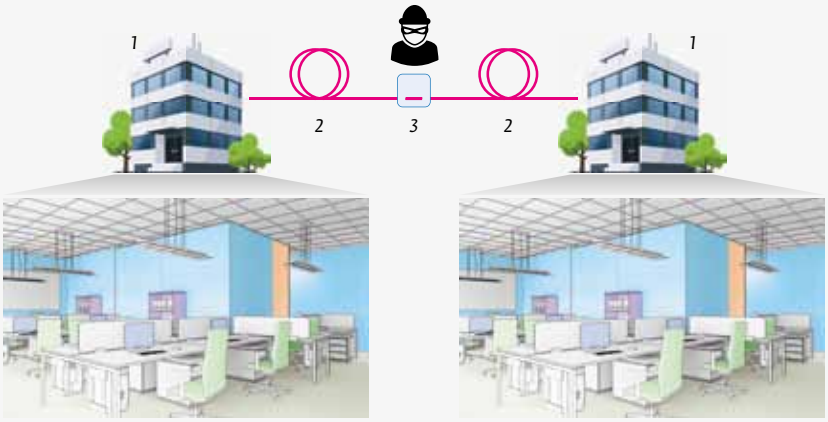


Рис. 1. *Принципиальная схема перехвата трафика: защищаемые объекты (1), волоконно-оптическая линии связи (2), нарушитель со средствами технической разведки (3)*

Fig. 1. *Circuit diagram of traffic interception: protected facilities (1), fiber-optic communication lines (2), an intruder with the technical intelligence tools (3)*

В структуре перехвата важную роль играют информативные сигналы и методы получения доступа к ним. В оптических сетях методы регистрации параметров информативного сигнала можно разделить на контактные и дистанционные. При контактном доступе нарушителю требуется получить физический доступ к оптоволокну в кабеле, что включает необходимость поиска кабеля, разрушения защитных оболочек, выделение требуемого оптоволокна с последующим отводом части оптического информационного сигнала путем установки специальной волоконно-оптической вставки в разрыв оптоволокна или путем воздействия на оптоволокно для вывода части оптического сигнала, например, на изгибе волокна, оптическом туннелировании и др. При дистанционном перехвате нарушителю требуется максимально близкий контакт с оптическим кабелем, только без разрушения или незначительном разрушении его защитных оболочек на основе побочных оптических излучений, паразитных электромагнитных излучений и т. д. Обсудим основные типы перехвата.

Модель угроз контактного перехвата трафика в оптических сетях

1. Контактный перехват с разрывом волокна

Наиболее простой и эффективный метод регистрировать информационный сигнал связан с использованием штатного устройства контроля за трафиком – волоконно-оптического перехватчика трафика (*Fiber Channel Traffic Access Point, TAP*), который может быть вставлен в штатный разрыв сети или подключен с помощью сварного соединения в созданный разрыв волокна. Вставка может быть реализована на основе оптических ответвителей.

2. Контактный перехват путем воздействия на волокно без разрыва [9]

Условие распространения оптического излучения в волокне определяется полным внутренним отражением на границе раздела сердцевина-оболочка, любые воздействия могут вызывать нарушение полного внутреннего отражения и появление побочных оптических излучений, выходящих из волокна. Наиболее просто это реализуется при механическом воздействии путем изгиба волокна. Устройства ввода/вывода на изгибе, например, волоконно-оптическая прищепка FOD-5503, используется при монтаже оптических сетей для аудиосвязи между монтажниками с помощью волоконно-оптических телефонов, не разрывая оптическую линию.

closest possible contact with the optical cable, only without destruction or with slight destruction of its protective sheaths based on the spurious optical radiation, spurious electromagnetic radiation, etc. Further, we will discuss the main types of interception.

Threat Models of Contact Traffic Interception in the Optical Networks

1. Contact Interception with Fiber Breakage

The simplest and most effective registration method for information signal is related to the use of a standard traffic control device that is a fiber channel traffic access point (*TAP*). It can be inserted into a regular network breakage or connected using a welded joint to a fiber breakage made. The insert can be made on the basis of optical couplers.

2. Contact Interception by Influencing the Fiber Without Breakage [9]

The condition for the optical radiation propagation in a fiber is determined by total internal reflection at the core-cladding boundary. Any influences can cause impairment of total internal reflection and occurrence of the spurious optical radiation coming from the fiber. It can be easily implemented under mechanical impact by bending the fiber. The bend I/O devices, such as the FOD-5503 fiber optic pin, are used in the optical networking for audio communications between the installers using the fiber optic phones without breaking the optical line.

3. Contact Interception Based on the Optical Tunneling [10]

Optical tunneling represents the transition of part of the optical radiation from one channel to another closely located channel separated by an optical layer with a lower refractive index, providing the total internal reflection. In the case of this phenomenon, the couplers are made using the lateral fiber fusion technology without the optical channel crossing. When intercepted by this method, the fibers of the communication and leakage channels are brought into a fixed optical contact that does not require significant damage to the protective sheaths of the cable and fiber. Using a thin metal tube, the communication channel fiber is captured. Then the optical adhesive and the leakage channel fiber are introduced through the tube. When the adhesive is set, a fixed optical contact is established between the fibers of the communication and leakage channels (Fig. 2).

3. Контактный перехват на основе оптического туннелирования [10]

Оптическое туннелирование проявляется в переходе части оптического излучения из одного канала в другой близко расположенный отделенный оптическим слоем с меньшим показателем преломления, обеспечивающим полное внутреннее отражение. На данном явлении функционируют ответвители выполненные по технологии с боковым сплавлением волокон без пересечения оптических каналов. При перехвате данным методом, волокна каналов связи и утечки приводят в фиксированный оптический контакт, для чего не требуется значительных разрушений защитных оболочек кабеля и волокна. С помощью тонкой металлической трубки захватывается волокно канала связи, далее через трубку вводится оптический клей и волокно канала утечки, при затвердении клея формируется фиксированный оптический контакт между волокнами каналов связи и утечки (рис. 2).

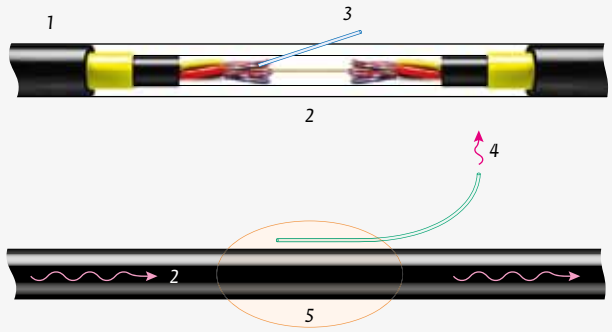


Рис. 2. *Модель контактного перехвата на основе оптического туннелирования: оптический кабель с защитными оболочками (1), оптоволокно канала связи (2), капиллярная трубка (3), оптоволокно канала утечки (4), оптический клей (5)*

Fig. 2. *Contact interception model based on the optical tunneling: an optical cable with the protective sheaths (1), fiber optics of the communication channel (2), a capillary tube (3), fiber optics of the leakage channel (4), an optical adhesive (5)*

Модель угроз дистанционного перехвата трафика в оптических сетях

1. Дистанционный перехват на основе вытекающих мод

Вытекающими модами называют выходящее из канала связи оптическое излучение при несогласованном соединении источника света и волокна, когда апертура источника превышает апертуру волокна. Вводимое в волокно оптическое излучение, выходящее за апертуру волокна, будет падать на границу раздела сердцевина-оболочка под углами меньшими критического и испытывать френелевское отражение с не нулевым преломлением. Эффект вытекающих мод может наблюдаться не только для входного информационного сигнала, но и по всей волоконно-оптической линии связи в местах подключения усилителей, повторителей, а также в местах дефектного соединения волокон или волокон с различающимися апертурами. Формирование дистанционного канала утечки возможно при наличии оптических окон в защитных оболочках кабеля или частичной оптической прозрачностью оболочек.

2. Дистанционный перехват на основе побочных оптических излучений

Побочным оптическим излучением можно назвать все локализованные по оптическому каналу связи излучения, вызванные рэлеевским рассеянием, френелевским отражением на опти-

Threat Models of Remote Traffic Interception in the Optical Networks

1. Remote Interception Based on the Tunnelling Modes

The tunnelling mode is the optical radiation emerging from the communication channel when the junction of the light source and fiber is unmatched and the source aperture exceeds the fiber aperture. The optical radiation introduced into the fiber and went out beyond the fiber aperture, will fall on the core-cladding

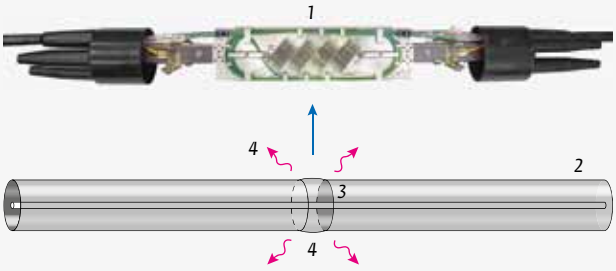


Рис. 3. *Дистанционный перехват на основе побочных излучений: соединительная муфта (1), сращиваемое волокно (2), место сращивания волокон (3), побочное излучение (4)*

Fig. 3. *Remote interception based on the spurious emissions: a coupler (1), a spliced fiber (2), a fiber splicing place (3), spurious radiation (4)*

ческих неоднородностях и др., которые могут выходить за пределы волокна и кабеля через оптические окна сквозь защитные оболочки и слои кабельной системы (рис. 3).

В частности, побочные излучения могут формироваться при несогласованном сварном соединении волокон. Такие случаи наступают, когда волокна смещены друг относительно друга, сварены под углом друг к другу и др. Даже качественное соединение дает локализованные потери порядка 0,01 дБ, из которых некоторая часть захватывается волокном, а другая может выходить за пределы оболочек волокна. Сращенные волокна размещаются в кабельных муфтах подземной, подводной и воздушной проводки телекоммуникационных сетей, которые могут располагаться через каждые 3–5 км, что позволяет нарушителю выбрать наиболее подходящее место перехвата, при этом требуется наличие оптических окон в кабеле и муфте.

3. Дистанционный перехват на основе паразитных электромагнитных излучений [11]

Паразитные электромагнитные излучения формируются в оптическом волокне вследствие нелинейно-оптических преобразований, приводящих к демодуляции информационного оптического сигнала на частотах близких к частоте модуляции оптической несущей. Это возникает в миллиметровом и сантиметровом диапазоне длин волн, для которых диэлектрические защитные оболочки кабеля могут быть прозрачны. Мощность паразитных электромагнитных излучений определяется когерентностью прямого и величиной рассеянного информационного оптического потока.

4. Дистанционный перехват на основе параметрических методов

Параметрические методы регистрации информационного сигнала в оптическом канале связи вызываются модуляцией параметров волокна оптическим излучением информационного сигнала. Это может быть модуляция прецессии электронных или ядерных магнитных моментов, акустооптических эффектов, рентгеноструктурных эффектов и другое. В структуре параметрического перехвата используются внешние электромагнитные, рентгеновские, акустические поля, которые могут проходить защитные оболочки кабеля без его разрушения, что позволяет реализовать дистанционный перехват без прямой необходимости разрушения кабеля.

boundary at the angles smaller than the critical one. It will be also exposed to the Fresnel reflection with non-zero refraction. The effect of tunnelling modes can be observed not only for the input information signal, but also along the entire fiber-optic communication line at the connection points of amplifiers and repeaters, as well as at the defective connection points of the fibers or fibers with various apertures. Generation of a remote leakage channel is possible in the presence of optical windows in the protective cable sheaths or partial optical transparency of the sheaths.

2. Remote Interception Based on the Spurious Optical Radiation

The spurious optical radiation can be any radiation localized along the optical communication channel, caused by the Rayleigh scattering, Fresnel reflection on optical inhomogeneities, etc. that can go beyond the fiber and cable through the optical windows of the protective sheaths and the cable system layers (Fig. 3).

In particular, the spurious radiations can be generated in the case of an inconsistent welded joints of fibers, i.e. when the fibers are displaced relative to each other, welded at an angle to each other, etc. Even a high-quality connection leads to the localized losses of about 0.01 dB. Some of them are captured by the fiber, and other can go beyond the fiber cladding. The spliced fibers are placed in the cable glands of underground, underwater and overhead telecommunication networks that can be located every 3–5 km. It allows the intruder to select the most suitable interception point, while requiring the available optical windows in the cable and gland.

3. Remote Interception Based on the Spurious Electromagnetic Radiation [11]

The spurious electromagnetic radiation is generated in the optical fiber due to the nonlinear optical transformations, leading to demodulation of the information optical signal at the frequencies close to the optical carrier modulation frequency, i.e. in the millimeter and centimeter wavelength range, for which the dielectric protective cable sheaths can be transparent. The spurious electromagnetic radiation power is determined by the coherence of the direct information optical flow and the value of the scattered information optical flow.

4. Remote Interception Based on the Parametric Methods

The parametric methods for the information signal registration in an optical communication channel

Оценим зону разведывательной доступности для дистанционного перехвата по побочным оптическим излучениям, как наиболее эффективным из описанных методов. Пусть побочное излучение формируется плоской неоднородностью в сердцевине волокна вследствие френелевского отражения величиной 30 дБ (т.е. 1/1000 от информационного сигнала), из-за дифракционной расходимости излучения ослабление составит 100 дБ на расстоянии 1 м от неоднородности размером порядка 10 мкм. Если другими потерями пренебречь, то в грубом приближении интенсивность информативного побочного оптического излучения составит –130 дБ от интенсивности информационного сигнала. Таким образом, зона разведывательной доступности не превысит цилиндр радиусом порядка 1 м с осью в виде кабеля. Поэтому выделение в модели угроз дистанционного перехвата можно считать условным, т.к. эффективный перехват возможен при прямом физическом контакте с оптическим кабелем.

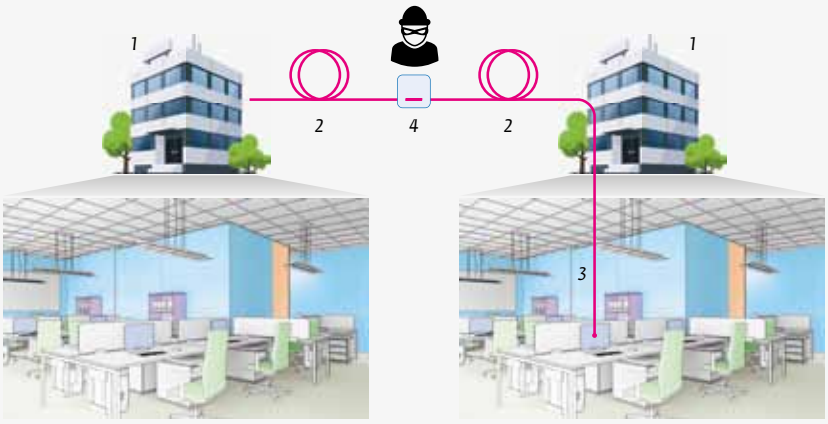


Рис. 4. *Принципиальная схема несанкционированного сбора информации через штатные оптические сети: защищаемые объекты (1), волоконно-оптическая линии связи (2), локальная оптическая сеть (3), нарушитель со средствами технической разведки (4)*

Fig. 4. *Circuit diagram of unauthorized data collection through the regular optical networks: protected facilities (1), fiber-optic communication lines (2), local optical network (3), an intruder with technical intelligence tools (4)*

Технические средства защита информации (трафика) могут строиться на особенностях оптического канала связи – его малом поперечном сечении, когда весь информационный сигнал в виде светового потока заключен внутри волокна, кабеля. Первый эшелон защиты связан с техническими средствами контроля доступа к кабелю, к волокну, а также состояния оптического канала связи. Другой способ защиты трафика состоит в зашумлении или искажении сигнала при его передаче в канале связи и очистке от шума или восстановлении его при приеме из канала связи.

В волоконно-оптической линии связи для защиты трафика могут быть применены стандартные методы шифрования, которые применяются для любых других систем связи. В последнее время разрабатываются и предлагаются на рынок системы защиты передаваемой информации от перехвата на основе квантовой криптографии. Есть основания считать такие системы защиты абсолютными по самой природе реализации.

are caused by modulation of the fiber parameters by the optical radiation of the information signal. It can be the precession modulation of electronic or nuclear magnetic moments, acousto-optic effects, X-ray diffraction effects, etc. The parametric interception structure applies the superimposed electromagnetic, X-ray, acoustic fields that can pass through the protective cable sheaths without its destruction that makes it possible to implement remote interception without the direct need to destroy the cable.

We will assess the reconnaissance accessibility area for remote interception using the spurious optical radiation as the most efficient of the described methods. Let the spurious radiation be formed by a plane discontinuity in the fiber core due to the Fresnel reflection of 30 dB (i.e. 1/1000 of the information signal). Due to the diffraction divergence of radiation, the attenuation will be 100 dB at a distance of 1 m from the discontinuity with a size of about 10 μm. If other losses are neglected, then, as a rough approximation, the intensity of the informative spurious optical radiation will be –130 dB of the information signal intensity. Thus, the reconnaissance accessibility area will not exceed a cylinder with a radius of about 1 m and an axis in the form of a cable. Therefore, determination of the remote interception in the threat model can be considered conditional, since the efficient interception is possible with the direct physical contact with the optical cable.

3. УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО СБОРА ИНФОРМАЦИИ ЧЕРЕЗ ШТАТНЫЕ ОПТИЧЕСКИЕ СЕТИ

Несанкционированный сбор информации – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов из контролируемой зоны на основе конвергенции функций передачи и измерения в штатных оптических сетях (рис. 4). В этом случае объектом угрозы является информация, циркулирующая на объекте вблизи оптических сетей в виде различного типа физических полей – речь, тепло, электромагнитные поля, радиационные поля и др.

На объектах конфиденциальностью обладает не только внутренний и внешний трафик, но также и информация, циркулирующая внутри объекта в виде речи сотрудников, различных звуков работающего оборудования, электромагнитных полей, физических параметров окружающего пространства и т.д. Штатные волоконно-оптические коммуникации являются распределенной волоконно-оптической измерительной сетью с нештатными измерительными возможностями. Располагаясь внутри объекта, коммуникации проходят через или вблизи защищаемых помещений, в которых может свободно циркулировать конфиденциальная информация. Нарушитель может получить доступ к ней через штатные оптические сети, используя штатные световые потоки сети или внешние зондирующие излучения. В отличие от угрозы трафику, такой канал утечки информации можно считать техническим (ТКУИ), использующим не декларируемые, или не известные, или не контролируемые возможности оптической кабельной инфраструктуры в следствие конвергенции транспортных и измерительных функций сети.

Обобщенная структура ТКУИ на основе волоконно-оптических коммуникаций объекта требует штатной/нештатной системы ввода/вывода зондирующего оптического излучения с формированием информативных сигналов утечки при воздействии на оптоволокно физического поля, связанного с конфиденциальной информации. Воздействие вызывает модуляцию светового потока в оптоволокне, которое переносит информацию за пределы контролируемой зоны, т.е. является информативным сигналом для модулирующего поля. Преобразующие возможности оптоволокна определяют уровень опасности волоконно-оптического ТКУИ. В угрозе

The technical information (traffic) security facilities can be based on the features of an optical communication channel, such as its small cross section, when the entire information signal in the form of a light flux is enclosed inside the fiber or cable. The first safety layer is related to technical means for controlling access to the cable and to the fiber, as well as the optical communication channel condition. Another way to protect traffic is the noise contamination or signal distortion when it is transmitted through the communication channel and its cleaning from noise or restoration when received from the communication channel.

The standard encryption methods can be applied in a fiber-optic communication line to protect traffic. Such methods can be used for any other communication systems. Recently, the transmitted data protection systems against interception based on the quantum cryptography have been developed and offered at the market. There are some reasons to consider such protection systems absolute by the very nature of their implementation.

3. THREATS OF UNAUTHORIZED DATA COLLECTION THROUGH THE REGULAR OPTICAL NETWORKS

Unauthorized data collection is an illegal information sourcing using the technical tool that detects, receives and processes informative signals from the controlled area based on the convergence of transmission and measurement functions in the regular optical networks (Fig. 4). In this case, the object of threat is information circulating at the facility near the optical networks in the form of various physical fields, such as speech, heat, electromagnetic fields, radiation fields, etc.

At the facilities, not only internal and external traffic is confidential, but also information circulating inside the facility in the form of the employees' speech, various sounds of operating equipment, electromagnetic fields, physical parameters of the external environment, etc. The regular fiber optic communications are the distributed fiber optic measuring networks with non-standard measuring capabilities. Being located inside the facility, the communications pass through or near the protected premises where the confidential information can freely circulate. An intruder can gain access to it through the regular optical networks, using the regular light fluxes of the network or external probe radiation. In contrast to the traffic threat, such an information leakage channel can be considered a technical one (TCIL), using the undeclared, or unknown, or uncontrolled capabilities of the optical

безопасности информации большую роль играет топология сети, так как прокладка оптического кабеля вблизи или через защищаемые помещения существенным образом влияет на защищенность от утечек.

Другие особенности связаны с возможностью использования для формирования информативного сигнала в дополнение к штатным излучениям еще и внешних нештатных источников, создающих зондирующие излучения. При этом трудности подключения к оптоволокну сохраняются, оптическая схема может быть усложнена, но повышаются возможности нарушителя вследствие варьирования параметров источника излучения. Сценарии по реализации ТКУИ через волоконно-оптические коммуникации могут быть различны в зависимости от возможности модуляции света в оптоволокне информативными полями и целей преследуемых нарушителем.

Таким образом, в структуре волоконно-оптического ТКУИ выделяются основные направления реализации угроз – это методы зондирования штатной оптической сети, с помощью которой регистрируются информативные сигналы, и объекты оптической сети, на которых происходит модуляция зондирующего излучения. По методам и объектам зондирования можно построить модель угроз безопасности информации, циркулирующей на защищаемом объекте.

Модель угроз несанкционированного сбора информации через штатные оптические сети

1. Методы зондирования оптической сети

По существующей волоконно-оптической технике, используемой в несанкционированном сборе информации, можно выделить технику разведки

- на прохождение, т.е. измерение параметров оптического излучения, прошедшего зондируемый объект, используемое для регистрации информативного сигнала на небольших расстояниях между источником и приемников, когда шумовые модуляции не превышают величины информативного сигнала;
- на отражение, т.е. оптическая рефлектометрия зондируемого объекта, используемое для регистрации информативного сигнала на максимальных расстояниях, определяемых техникой оптической рефлектометрии, так как позволяет выделить отклик от конкретного объекта зондирования;

cable infrastructure due to the convergence of the transport and measurement network functions.

The generalized TCIL structure based on the facility's fiber-optic communications requires a regular/irregular input/output system for the probe optical radiation with generation of the informative leakage signals when the optical fiber is exposed to the physical field related to the confidential information. The impact causes the light flux modulation in the optical fiber that transfers data outside the controlled area, i.e. being an informative signal for the modulating field. The transforming capabilities of fiber optics determine the danger level of fiber-optic TCIL. The network topology plays an important role in the threat to information security, since the optical cable laying near or through the protected premises significantly affects the protection against leaks.

Other features are related to the possible use of external non-regular sources creating the probe radiation in addition to the regular radiation for the informative signal generation. Moreover, the difficulties of connecting to an optical fiber are remained, the optical circuit can be complicated, but the intruder's capabilities are increased due to variation in the radiation source parameters. The TCIL implementation scenarios using the fiber-optic communications can differ depending on the possible light modulation in the optical fiber by the informative fields and the aims pursued by the intruder.

Thus, the main areas for threat activities can be identified in the structure of the fiber-optics TCIL, including the probing methods for the regular optical network that is used for the informative signal recording, and the optical network facilities, at which the probing radiation is modulated. The probing methods and objects can be used for development of the threat models relating to the data security circulating at the protected facility.

Threat Model of Unauthorized Data Collection Through the Regular Optical Networks

1. Optical method probing methods

Based on the available fiber optic technology used for the unauthorized data collection, the following intelligence techniques can be identified:

- for transmission, i.e. measurement of the optical radiation parameters that has passed through the probed facility, used to record an informative signal at the short distances between the source and the receivers, when the noise modulations do not exceed the informative signal value;

Для зондирования на прохождение и отражение можно использовать все основные параметры оптического излучения и их комбинации – это модуляция интенсивности, фазы, частоты и поляризации, выбираемые исходя из эффективности (глубины) модуляции на объекте зондирования. В некоторых случаях для зондирования может применяться как оптическое излучение от средств технической разведки (нештатных источников), так и от штатных источников. В случае штатных источников и приемников, т.е. трансиверов оптической сети, зондирование обладает высокой скрытностью, но требует доступа к технике оптической сети (внутренний нарушитель).

Основой функционирования канала утечки является оптическая рефлектометрия [3], с помощью которой достигается возможность локализации отклика оптической сети наиболее чувствительной к воздействию информативных сигналов, проведения измерений одного информативного сигнала от нескольких объектов зондирования, повысить отношение сигнал/шум, проводить измерения в реальном времени и т.д. Развитие техники оптической рефлектометрии является одной из наиболее значимых угроз для несанкционированного сбора информации.

2. Объекты зондирования

Пассивные элементы оптической сети являются основными объектами зондирования, определяющие эффективность функционирования канала утечки, их можно разделить на

- штатные пассивные элементы оптической сети, чувствительные к информативным физическим полям,– при изготовлении и монтаже оптической сети, как правило, не проводят исследований на возможный отклик пассивных оптических элементов на все возможные внешние информативные физические поля, таким образом, у них могут существовать не декларируемые возможности не связанные с основными функциями в сети, например, конструкция разъемного соединения во многом совпадает с конструкцией волоконно-оптического микрофона с амплитудной модуляцией, но в декларируемых характеристиках разъемных соединителей акустические параметры не указываются;
- волоконно-оптические закладки, т.е. конструктивные изменения пассивных элементов оптической сети, внесенные с целью повышения чувствительности к окружающим

- for reflection, i.e. optical reflectometry of the probed facility that is used to record an informative signal at the maximum distances determined by the optical reflectometry devices, since it allows to determine the response from a specific probed facility.

All the main optical radiation parameters and their combinations can be used for the transmission and reflection probing, including the intensity, phase, frequency, and polarization modulation, selected based on the modulation efficiency (depth) at the probing facility. In some cases, both optical radiation from the technical reconnaissance equipment (non-regular sources) and regular sources can be used for probing. In the case of regular sources and receivers, i.e. the optical network transceivers, probing is highly concealed, but requires access to the optical network technology (an insider).

The basis for the leakage channel functioning is optical reflectometry [3]. It is used for possible localization of the optical network response that is most sensitive to the influence of informative signals, for measurement of one informative signal from several probing facilities, for increase of the signal-to-noise ratio, for performance of real-time measurements, etc. The development of optical reflectometry technology is one of the most significant threats to unauthorized data collection.

2. Probing Objects

The passive optical network elements are the main objects of probing that determine the leakage channel efficiency. They can be grouped as follows:

- regular passive elements of the optical network that are sensitive to the informative physical fields. During the optical network production and installation, as a rule, no researches of the possible response of passive optical elements to all possible external informative physical fields are conducted, so they may have undeclared opportunities not related to the main network functions, for example, the detachable connection design largely coincides with the design of a fiber-optic microphone with amplitude modulation, but the acoustic parameters are not indicated in the declared specifications of detachable connectors;
- fiber-optic markers, i.e. the structural changes in the optical network passive elements made in order to increase sensitivity to the surrounding informative physical fields that can be introduced into the optical network.

информативным физическим полям, которые могут быть внесены в оптическую сеть;

3. Волоконно-оптические закладки

Конструктивные изменения пассивных элементов оптической сети могут быть произведены при изготовлении, при инсталляции, при эксплуатации оптической сети, каждая из которых имеет свои особенности и возможности, что позволяет произвести разделение угроз по трем направлениям:

- **волоконно-оптические закладки производства** – при производстве оптических элементов изготовитель может внести изменения в конструкцию пассивных элементов, которые не влияют на его функциональные возможности, но повышают чувствительность к внешним физическим полям.

  Вносимые изменения могут относится к оптическому волокну, к защитным оболочкам и другим элементам оптического кабеля. Одной из таких возможностей является создание брэгговских решеток в сердцевине волокна с длиной волны резонансного отражения на длинах волн в области поглощения материала волокна (рис. 5). Учитывая малую спектральную ширину резонансного отражения решетки, она не будет оказывать влияния на прохождение излучения на рабочих длинах волн канала связи в области окон прозрачности материала. Наличие таких решеток через каждые 100–200 м по длине кабеля создает возможность их расположения вблизи информативных сигналов при инсталляции кабельной системы. Таким образом, мониторинг оптической кабельной системы не позволит выявить такие волоконно-оптические закладки, так как мониторинг на длинах волн вне областей окон прозрачности не проводится на большие расстояния из-за большого поглощения. Если на длине волны 1550 нм поглощение в аморфном кварце уменьшается до 0,125 дБ/км, то на пиках поглощения 1383 нм превышает 1 дБ/км, а в видимой области поднимается выше 3 дБ/км. Волоконно-оптическая закладка в виде брэгговской решетки позволяет создать высокочувствительный к акустическим, тепловым полям датчик информативных сигналов.
- **волоконно-оптические закладки инсталляции** – в процессе внутри объектного монтажа волоконно-оптической структурированной кабельной системы путем преднамеренного или непреднамеренного нарушения требова-

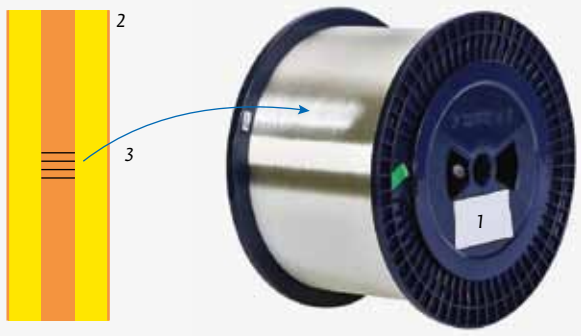


Рис. 5. *Волоконно-оптическая закладка: катушка оптоволокна (1), элемент оптоволокна (2), решетка Брэгга (3)*
Fig. 5. *Fiber optic marker: fiber coil (1), optical fiber element (2), Bragg grating (3)*

3. Fiber Optic Markers

The structural changes in the optical network passive elements can be made during manufacture, installation, operation of the optical network. Each of such network has its own specifications and capabilities that makes it possible to divide the threat into three groups:

- fiber-optical production markers – during the production of optical elements, the manufacturer can make changes to the passive element design that does not affect its functionality, but increases sensitivity to the superimposed physical fields.

  The changes made may be applied to the optical fiber, to the protective sheaths and other elements of the optical cable. One such possibility is generation of the Bragg gratings in the fiber core with a resonant reflection wavelength at the wavelengths within the fiber material absorption range (Fig. 5). Having considered the small spectral width of the grating resonant reflection, it will not affect the radiation transmission at the operating wavelengths of the communication channel in the area of the material transparency windows. Availability of such gratings every 100–200 m along the cable length makes it possible to locate them near the informative signals when the cable system is installed. Thus, monitoring of an optical cable system will not detect such fiber optic markers, since monitoring at the wavelengths beyond the fiber transparency windows is not performed over the long distances due to high absorption values. If the absorption in amorphous quartz is

ний по выполнению работ могут быть изменена восприимчивость кабельной системы к внешним воздействиям, которые могут быть, в том числе, изначально не известны.

Наиболее очевидные изменения могут связаны с нарушением нормативно-методических рекомендаций и требований, например, величина изгиба оптического кабеля превышает нормативные требования, проводка кабеля с натяжением, жесткое крепление кабеля к стенам и другое существенно повышают чувствительность к акустическим полям. С одной стороны, создаваемые отклонения могут быть не отмечены в требованиях к монтажу, так как не влияют на основную функцию кабельной системы – передавать информацию. С другой, их наличие еще не создает угроз безопасности информации, циркулирующей на объекте, если не учитывать расположение относительно защищаемых помещений.

Рис. 6. *Пример кабельного канала с пониженным акустическим контактом со стенами: гофра труба (1), пластиковая клипса (2)*

Fig. 6. *An example of a cable duct with reduced acoustic contact with the walls: corrugated pipe (1), plastic clip (2)*

Одним из таких отклонений, повышающих акустическую чувствительной кабельной системы, является место монтажа кабельных каналов. Жесткое крепление оптического кабеля к фундаментальным конструкциям здания, таким как железобетонные несущие стены, создают распределенную измерительную систему виброакустических колебаний в стенах – высокоинформативному структурному звуку, который слабо поглощается в монолитных строительных конструкциях. В качестве демонстрации снижения акустического контакта кабельного канала со стенами можно предложить использовать гофра трубу с креплением к стене с помощью клипсы, которые изготавливаются из пластика с повышенной эластичностью (рис. 6). В таких кабельных каналах можно дополнительное провести акустическую изоляцию от стен (клипса) и внутри гофры, путем специальных звукопоглощающих прокладок.

- **волоконно-оптические закладки эксплуатации** – вносятся внутренним нарушителем путем локального механического, теплового, магнитного, электрического другого физического воздействия на кабельные каналы, оптический кабель структурированных кабельных систем защищаемого объекта на стадии эксплуатации оптической сети.

При функционировании волоконно-оптических подсистем структурированных кабельных систем объекта всегда есть возмож-

decreased to 0.125 dB/km at a wavelength of 1550 nm, then it exceeds 1 dB/km at the absorption peaks of 1383 nm, and it exceeds 3 dB/km in the visible range. The fiber-optic marker in the form of a Bragg grating makes it possible to manufacture an informative signal sensor that is highly sensitive to the acoustic and thermal fields.

- fiber-optic installation markers – during the process of intrafacility installation of a fiber-optic structured cable system, by intentional or unintentional violation of the work performance requirements, the cable system susceptibility to the external influences that may not be initially know (among other things) can be changed.

The most evident changes may be related to non-observance of the regulatory and methodological recommendations and requirements, for example, the optical cable bending value exceeds the regulatory requirements, the cable wiring is made with tension, the cable is rigidly fastened to the walls, etc. Such facts significantly increase sensitivity to the acoustic fields. On the one part, the deviations made may not be noted in the installation requirements, since they do not affect the main function of the cable system, namely the data transmission. On the other part, their availability does not yet pose a threat to the security of information circulating at the facility, if their location relative to the protected premises is not considered.

ность повысить эффективность несанкционированного сбора информации путем воздействия на нее. Вид воздействия зависит от задач и возможностей нарушителя, но основная цель такого воздействия – создать локальные оптические неоднородности кабельной системы вблизи защищаемого помещения, вблизи опасных элементов строительных конструкций. Например, угроза конфиденциальности переговоров может определяться не только близостью к защищаемому помещению, но и к акустическим волноводам в виде монолитных стен, воздуховодов, водных и другим хозяйственных коммуникаций здания. Соблюдение требований по нейтрализации угрозы на этапах инсталляции можно свести угрозы к минимум, но внутренний нарушитель может механическим воздействием на кабельную систему, размещением источников полей вблизи нее в наиболее чувствительных местах вызвать повышение уровня угроз.

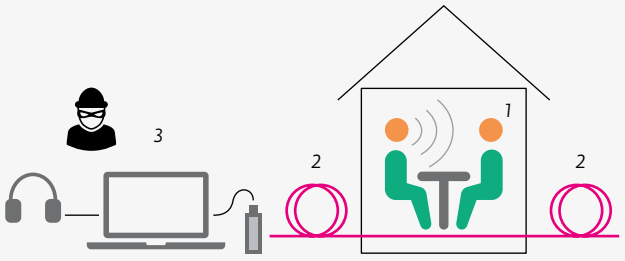


Рис. 7. *Принципиальная структура канала утечки конфиденциальной речевой информации через волоконно-оптические коммуникации: защищаемое помещение (1), волоконно-оптическая линия связи (2), нарушитель с средствами технической разведки (3)*

Fig. 7. *Basic structure of the confidential verbal information leakage channel through the fiber-optic communications: protected premises (1), fiber-optic communication line (2), an intruder with the technical intelligence tools (3)*

Модель угроз волоконно-оптического канала утечки речевой информации [12]

Отдельным направлением технической разведки являются волоконно-оптический канал утечки акустической (речевой) информации, который определяется паразитной акустической модуляцией параметров светового потока в оптоволокне (рис. 7). В этом случае, оптический кабель и его волокна являются нештатным распределенным волоконно-оптическим преобразователем (микрофоном) акустических колебаний воздуха или вибраций конструкций зданий с высокой чувствительностью. Выбор параметров зондирующего сигнала, повышение акустического или виброакустического контакта с оптоволокном, топология и другие обычно не учитываемые характеристики кабельной инфраструктуры позволяет создать угрозу подслушивания конфиденциальных переговоров. Как показывают экспериментальные исследования, наибольшую опасность несут модуляции света на неоднородных участках оптического кабеля, связанные с виброакустическим воздействием (структурным звуком), а также возможность применения в качестве средств технической разведки стандартного волоконно-оптического оборудования, например, волоконно-оптического тестера-телефона с амплитудной модуляцией типа Рубин-021.

Реализация канала утечки речевой информации возможна методом на прохождение оптиче-

One of such deviations that increase the acoustic sensitivity of the cable system, is the installation point of cable channels. Rigid fastening of the optical cable to the fundamental building structures, such as reinforced concrete load-bearing walls, leads to the distributed measuring system of vibroacoustic oscillations in the walls. It is a highly informative structural sound that is poorly absorbed by the monolithic building structures. To demonstrate the reduced acoustic contact of the cable channel with the walls, we can suggest using a corrugated pipe fastened to the wall using the clips that are made of plastic with increased elasticity (Fig. 6). In such cable conduits, it is possible to make the additional acoustic insulation in relation to the walls (clip) and inside the corrugated pipes using the special mineral fiber pads.

- fiber-optic operation markers – they are made by an insider using the local mechanical, thermal, magnetic, electrical and other physical impact on the cable conduits, optical cable of the structured cable systems of the protected facility at the optical network operating stage.

When the fiber-optic subsystems of the structured cabling systems at the facility are functioning, it is always possible to increase the efficiency of unauthorized data collection by having an impact on it. The type of impact depends on the intruder's aims and capabilities, however, the main purpose of such impact is to create local optical inhomogeneities of the

ского излучения или оптической рефлектометрии, путем использования параметров (интенсивности, фазы, поляризации и длины волны) штатного или нештатного оптического излучения. Фактически любой участок кабельной системы выступает источником информативных сигналов и использование оптической рефлектометрии позволяет создать распределенную волоконно-оптическую измерительную систему акустических колебаний.

Методы защиты акустической информации от утечки по акустооптическому (волоконному) каналу делятся на пассивные (звукоизоляция оптического кабеля, «правильный» монтаж сети и т. д.) и активные (фильтрация, маскировка, зашумление информационного сигнала и т. д.). Можно выделить еще один способ, заключающийся во включении в каждый оптический трансивер функции непрерывного мониторинга световых потоков на возможность применения технических средств акустической разведки. Уменьшение опасности подслушивания возможно путем разработки новых рекомендаций по монтажу и эксплуатации оптических кабельных систем.

4. УГРОЗЫ ПРИМЕНЕНИЯ СРЕДСТВ ТЕХНИЧЕСКОЙ РАЗВЕДКИ НА ОСНОВЕ ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЙ

Волоконно-оптические средства технической разведки – волоконно-оптические технические устройства

cable system near the protected premises or near dangerous elements of building structures. For example, the threat to the negotiations confidentiality can be determined not only by proximity to the protected premises, but also to the acoustic waveguides in the form of cast-in-place walls, air ducts, water and other utility pipelines in the building. Compliance with the requirements for threat manageability at the installation stages can minimize the threats. However, the insider can mechanically affect the cable system, place the field sources near it in the most sensitive places, cause an increase in the threat level.

Threat Model of a Fiber-Optic Channel of Verbal Information Leakage [12]

A separate technical intelligence area is the fiber-optic channel for the acoustic (verbal) information leakage that is determined by the spurious acoustic modulation of the light flux parameters in the optical fiber (Fig. 7). In this case, the optical cable and its fibers represent a non-regular distributed fiber-optic converter (microphone) of the air acoustic vibrations or vibrations of the building structures with high sensitivity. Selection of the probing signal parameters, increased acoustic or vibroacoustic contact with the optical fiber, topology and other cable infrastructure specifications that are usually not considered can create a threat of interception of the confidential conversations. As the experimental studies show, the greatest danger is posed by the light modulations in the inhomogeneous sections of an optical cable related to the vibroacoustic effects (structural sound), as well as the possible use of the regular fiber-optic equipment as the technical reconnaissance equipment, for example, a Rubin-021 fiber-optic testing telephone with an amplitude modulation.

The implementation of the verbal information leakage channel is possible by the optical radiation transmission method or optical reflectometry, by using the parameters (intensity, phase, polarization and wavelength) of the regular or non-regular optical radiation. In fact, any section of the cable system is used as

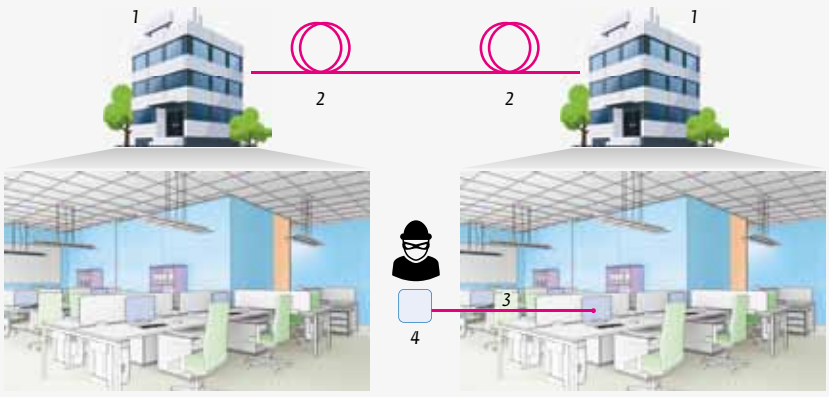


Рис. 8. *Принципиальная схема применения волоконно-оптических средств технической разведки: защищаемые объекты (1), волоконно-оптическая линии связи (2), волоконно-оптические средства разведки (3), нарушитель со средствами технической разведки (4)*

Fig. 8. *Circuit diagram of the use of fiber-optic technical intelligence tools: protected facilities (1), fiber-optic communication lines (2), fiber-optic intelligence tools (3), an intruder with the technical intelligence tools (4)*

(датчики), предназначенные для приема, регистрации и обработки информативных сигналов (рис. 8), при этом объектом угрозы является информация, циркулирующая на защищаемом объекте в виде различных физических полей – акустические, электромагнитные, оптические поля.

Преимущества волоконно-оптических технологий может быть использовано для создания волоконно-оптических средств технической разведки в виде волоконно-оптических датчиков и измерительных систем, адаптированных для выполнения специальных функций [2,3]. Изначально волоконно-оптические датчики и измерительные системы обладают свойствами, требуемыми для этих целей. Они обладают высокой чувствительностью к широкому кругу физических полей; многофункциональны, т.е. позволяют проводить измерения различных физических величин одним оптоволокном; обладают возможностью как точечных, так и распределенных измерений; не обнаруживаются стандартными электромагнитными способами, так как не содержат проводящих элементов; пассивны и нечувствительны к внешним электромагнитным полям; пожара-безопасны; миниатюрны и т.д. Все эти преимущества делают их очень эффективным средством технической разведки. В частности, волоконно-оптические микрофоны могут быть использованы в оперативной работе по скрытному подслушиванию переговоров.

В качестве примера одного из направлений применения волоконно-оптических средств технической разведки является возможность повышения эффективности лазерных микрофонов по скрытному дистанционному подслушиванию конфиденциальных переговоров. Одной из трудностей реализации лазерного зондирования вибрирующих поверхностей состоит в диффузном отражении от неподготовленной поверхности лазерного излучения или наоборот узкой направленности отраженного излучения подготовленной поверхности (зеркала). Снятие подобных ограничений можно произвести путем внедрения в стены здания с выделенным помещением сенсорного оптоволокна без защитных оболочек с микролинзами на концах, которые имеют оптический контакт с окружающей средой. Тогда освещение инфракрасным лазерным излучением одного конца на другом конце можно получить модулированное структурным звуком оптическое излучение, которое легко регистрируется как направленное в известном направле-

a source of informative signals, and application of optical reflectometry makes it possible to create a distributed fiber-optic measuring system for acoustic vibrations.

The acoustic data protection methods against leakage through an acoustic and optical (fiber) channel are divided into the passive (soundproofing of an optical cable, «correct» network installation, etc.) and active ones (filtering, masking, noise contamination of an information signal, etc.). It is possible to emphasize an additional method that consists in inclusion of the light flux continuous monitoring function in each optical transceiver for the possible use of technical acoustic reconnaissance means. The interception danger level can be lowered by developing new recommendations for the installation and operation of optical cable systems.

4. THREATS OF USING TECHNICAL INTELLIGENCE TOOLS BASED ON THE FIBER-OPTIC TECHNOLOGIES

The fiber-optic technical intelligence tools mean the fiber-optic technical devices (sensors) designed to receive, record and process the informative signals (Fig. 8), while the object of the threat is information circulating at the protected facility in the form of various physical fields, such as acoustic, electromagnetic, optical fields.

The advantages of fiber optic technologies can be used to produce the fiber optic technical intelligence tools in the form of fiber optic sensors and measuring systems adapted to perform special functions [2, 3]. Initially, the fiber optic sensors and measurement systems have the properties required for these purposes. They are highly sensitive to a wide range of physical fields; they are multifunctional, i.e. allow the measurements of various physical valies using one optical fiber; they can perform both point-by-point and distributed measurements; they are not detected by the regular electromagnetic methods, since they do not contain any conductive elements; they are passive and insensitive to the superimposed electromagnetic fields; they are fire-safe; very small, etc. All these advantages make them a very effective technical intelligence tool. In particular, the fiber-optic microphones can be used in operational activity for surreptitious conversation listening.

Possible increase in the laser microphone efficiency for surreptitious remote listening of confidential conversation can be used as an example of one of the applications of fiber-optic technical intelligence tools. One of the difficulties in the laser probing of vibrating surfaces is diffuse reflection of laser radiation from an unprepared surface or, vice versa, a narrow

нии и имеющее известную длину волны лазерное излучение.

Противодействие волоконно-оптическим средствам технической разведки требуют специальных исследований по обнаружению оптического волокна и кабеля, воздействию на его преобразовательные возможностью для нейтрализации и др.

ЗАКЛЮЧЕНИЕ

Представленный анализ модели угроз информационной безопасности объектов с волоконно-оптическими технологиями показывает широкий спектр и высокий уровень возможных угроз, которые необходимо исследовать, разрабатывать возможные модели угроз, проводить обучение и переподготовку специалистов в данном направлении.

СПИСОК ЛИТЕРАТУРЫ

1. **Скляров О. К.** *Волоконно-оптические сети и системы связи.* – СПб.: Лань, 2010. 272 с. ISBN 978–5–8114–1028–6.
2. **Дмитриев С. А., Слепов Н. Н.** *Волоконно-оптические системы мониторинга состояния инфраструктурных объектов.* – М.: Экслибрис-пресс, 2015. 304 с. ISBN 978–5–88161–388–4.
3. **Листвин А. В., Листвин В. Н.** *Рефлектометрия оптических волокон* – М.: ЛЕСАРарт, 2005. – 208 с. ISBN 5-902367-03-4.
4. **Гришачев В. В.** Фотоника в системах безопасности и защиты информации. – *Фотоника.* 2011;№ 6:58–64.
5. **Денисов В. И., Гришачев В. В., Косенко О. А.** Волоконно-оптические технологии в системах безопасности и защиты информации. *Специальная техника.* 2010;47–61.
6. **Зеневич А. О.** *Обнаружители утечки информации из оптического волокна: монография.* – Минск: Белорусская государственная академия связи, 2017. 142 с. ISBN 978-985-585-020-6.
7. **Шубин В. В.** *Информационная безопасность волоконно-оптических систем.* – Саров: РФЯЦ-ВНИИЭФ. 2015. 257 с. ISBN 978-5-9515-0242-1.
8. **Алексеев Е. Б., Булавкин И. А., Попов А. Г., Попов В. И.** *Пассивные волоконно-оптические сети. Проектирование, оптимизация и обнаружение несанкционированного доступа.* – М: Медиа Паблишер, 2014. 206 с. ISBN 978-5-903650-21-7.
9. **Гришачев В. В., Кабашкин В. Н., Фролов А. Д.** Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения. – *Информационное противодействие угрозам терроризма.* 2005; 4: 194–204. http://www.contrterror.tsure.ru/.
10. **Гришачев В. В.** Перехвата трафика в оптических сетях: метод оптического туннелирования. *Фотоника.* 2020;14(8):680–695. DOI: 10.22184/1993-7296.FRos.2020.14.8.680.695.
11. **Гришачев В. В.** Перехвата трафика в оптических сетях: информативные паразитные электромагнитные излучения. *Фотоника.* 2019;13(3):280–294. DOI: 10.22184/FRos.2019.13.3.280.294.
12. **Гришачев В. В., Казарин О. В., Калинина Ю. Д.** Физическая модель угрозы утечки акустической (речевой) информации через волоконно-оптические коммуникации. – *Вопросы защиты информации.* 2018;3: 35–51.

АВТОРЫ

Владимир Васильевич Гришачев, к. ф.-м. н., доцент Института Информационных Наук и Технологий Безопасности (ИИНиТБ), Российского Государственного Гуманитарного Университета (РГГУ), Москва, Россия.
ORCID: 0000-0002-7585-7282

Анна Дмитриевна Заболотская, студент Института Информационных Наук и Технологий Безопасности (ИИНиТБ), Российского Государственного Гуманитарного Университета (РГГУ), Москва, Россия.

directivity of the reflected radiation from a prepared surface (mirror). Removal of such restrictions can be done by introducing into the building walls with a dedicated premises a sensor fiber optics without any protective shields with the microlenses at the ends that have optical contact with the environment. Then illumination with the infrared laser radiation on one end can lead to the optical radiation modulated by the structural sound that is easily detected as the laser radiation aimed at a well-known direction with a well-known wavelength.

The countermeasures against the fiber-optic technical reconnaissance tools require special studies on the detection of optical fiber and cable, impact on its conversion capabilities for neutralization, etc.

CONCLUSION

The provided analysis of the information security threat model for the facilities with the fiber optic technologies shows a wide range and a high level of possible threats that need to be investigated, with development of the possible threat models, training and retraining of the specialists in this area.

REFERENCES

1. **Sklyarov O. K.** *Fiber-optic networks and communication systems.* – St. Petersburg: Lan, 2010. 272 p.
2. **Dmitriev S. A., Slepov N. N.** *Fiber-optic systems for monitoring the condition of infrastructure facilities.* – M.: Exlibris-press. 2015. 304 p.
3. **Listvin A. V., Listvin V. N.** *Reflectometry of optical fibers.* – M.: LESARart. 2005. 208 p.
4. **Grishachev V. V.** Photonics in information security and protection systems. – *Photonics Russia.* 2011; 6: 58–64.
5. **Denisov V. I., Grishachev V. V., Kosenko O. A.** Fiber-optic technologies in information security and protection systems. *Special Equipment (Russia).* 2010;47–61.
6. **Zenevich A. O.** *Detectors of information leakage from optical fiber.* – Minsk: Belarusian State Academy of Communications. 2017. 142 p.
7. **Shubin V. V.** *Information security of fiber-optic systems.* – Sarov: RFNC–VNIIEF. 2015. 257 p.
8. **Alekseev E. B., Bulavkin I. A., Popov A. G., Popov V. I.** *Passive fiber-optic networks. Design, optimization and detection of unauthorized access.* – M: Media Publisher. 2014. 206 p.
9. **Grishachev V. V., Kabashkin V. N., Frolov A. D.** Analysis of information leakage channels in fiber-optic communication lines: violation of total internal reflection. *Information counteraction to the threats of terrorism.* 2005; 4: 194–204.
10. **Grishachev V. V.** Traffic interception in optical networks: optical tunneling method. – *Photonics Russia.* 2020;14(8):680–695.
11. **Grishachev V. V.** Traffic interception in optical networks: informative parasitic electromagnetic radiation. *Photonics Russia.* 2019;13(3): 280–294.
12. **Grishachev V. V., Kazarin O. V., Kalinina Ju. D.** Physical threat model of acoustic (speech) information leakage through fiber-optic communications. *Information security questions (Russia).*2018;3: 35–51.

AUTHORS

Vladimir V. Grishachev, Cand.of Sc. (Phys.& Math.), docent, associate professor Institute for Information Sciences and Security Technologies (IISST) Russian State University of the Humanities (RSUH), Moscow, Russia.
ORCID: 0000-0002-7585-7282

Anna D. Zabolotskaya, student Institute for Information Sciences and Security Technologies (IISST) Russian State University of the Humanities (RSUH), Moscow, Russia.

www.prombvk.ru

РОССИЙСКИЙ ПРОМЫШЛЕННЫЙ ФОРУМ

16-18 ноября 2022

Специализированные выставки

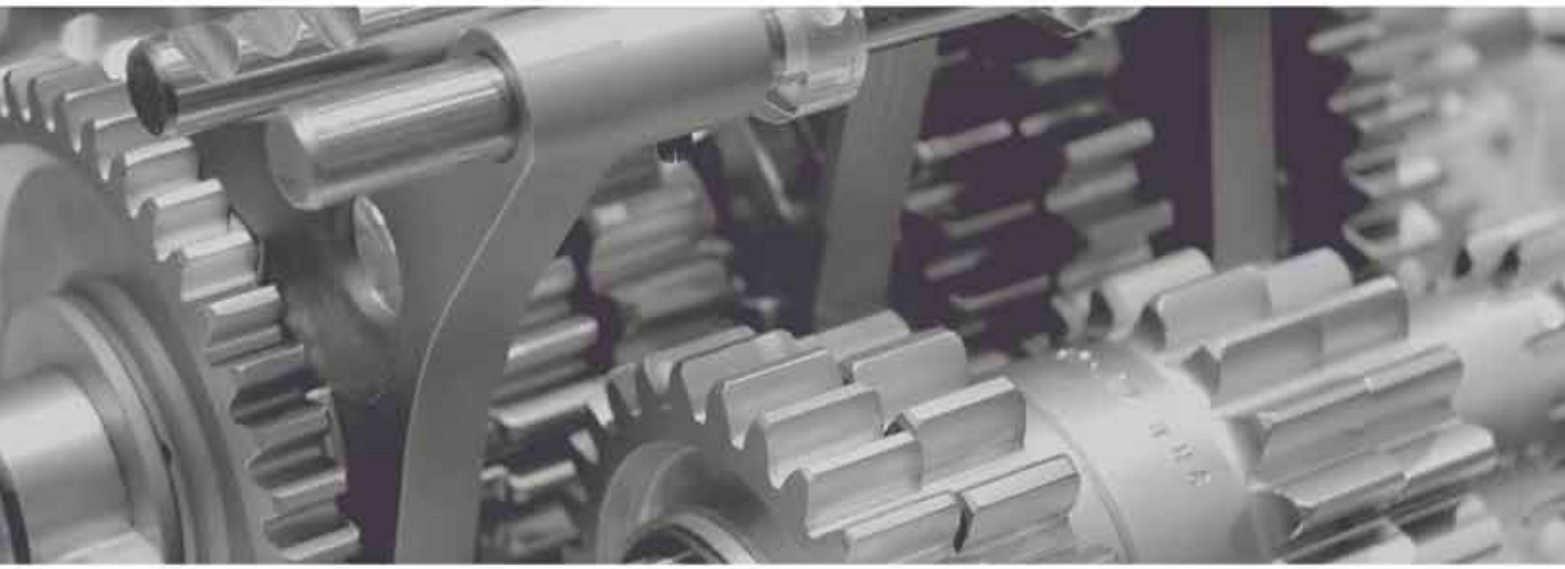
- Машиностроение
- Металлообработка
- Инновационный потенциал Уфы

ВДНХ ЭКСПО УФА

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ, ЭНЕРГЕТИКИ И ИННОВАЦИЙ РЕСПУБЛИКИ БАШКОРТОСТАН

АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА г. УФА РБ

БВК БАШКИРСКАЯ ВЫСТАВОЧНАЯ КОМПАНИЯ



ОРГКОМИТЕТ: +7 (347) 246 41 80, 246 42 37
promexpo@bvkexpo.ru

Мероприятия проводятся с учетом всех требований Роспотребнадзора