

Detecting Threats of Acoustic Information Leakage through Fiber Optic Communications

Vladimir V. Grishachev

Russian State Geological Prospecting University (RSGPU), Moscow, Russia
Email: grishachev@mail.ru

Received November 27, 2011; revised December 30, 2011; accepted January 29, 2012

ABSTRACT

Information leaks through regular fiber optic communications is possible in the form of eavesdropping on conversations, using standard fiber optic communications as illegal measuring network. The threat of leakage of audio information can create any kind of irregular light emission, as well as regular light beams modulated at acoustic frequencies. For information protection can be used a means of sound insulation, filtration and noising. This paper discusses the technical possibilities of countering threats by monitoring the optical radiation to detect eavesdropping.

Keywords: Fiber Optic Communications; Acoustic (Speech) Information Leakage Channel; Protection of Acoustic (Speech) Information

1. Introduction

Modern technologies of remote and local cable communication systems are based on optical data transmission systems due to the advantages of fiber optic cable over electrical cable as the transport medium. One of the main directions of development is to ensure the broadband subscriber access which is based on optical networks, completely passive (PON) in the future. Technologies such as fiber to the building/home/office/desk (FTTB/FTTH/FTTO/FTTD) lead to the fact that the fiber replaces wire technology in near environment of user [1]. In addition to communications technology fiber is actively used in measuring and security systems. Fiber optic distributed measuring network can control all the basic physical fields in real time with high sensitivity and accuracy [2,3]. One of the most active trends of fibers in the security systems is the application of optical interfaces for extension of special lines in Closed Circuit Television (CCTV), perimeter security system object.

Advancement of optical structured cable systems (SCS) closer to the man create new threats to information security circulating in building, office, workplace. One of the risks associated with possibility eavesdropping on confidential conversations, using influence of acoustic fields on transmission of light in the fiber. Optical fiber is successfully used to create sensors and distributed measuring networks. Hence regular optic structured cabling system in building is nothing short of a distributed measurement network, which can be used to measure various physical fields, including acoustic field.

Thus, in commercial and government buildings is necessary to protect confidential negotiations in office manager, office space, meeting rooms and other allocated areas of acoustic (speech) information leakage through the optic structured cabling systems. This problem is new, understudied in connection with what is very dangerous.

2. Physical Principles Eavesdropping

Covert obtain of acoustic (speech) information by using regular fiber optic communications for various purposes is one of the new methods of acoustic intelligence, which is called an acousto-optic (fiber) information leakage channel [4,5]. Forming leakage channel due to the fact that acoustic field from holder information affects the fiber of regular cable systems and causes a modulation of light passing through optical fiber, passive or active elements of optical equipment by acoustic frequencies, as well as reflection from a heterogeneities in them (**Figure 1**). Modulation of light in the optical fiber can take place in amplitude, phase, polarization and frequency of emission due to exposure on optical fiber of acoustic field. Light which has been modulated by sound can come out far beyond the protected premises through regular fiber optic communications. Then, attacker can gain access to functioning in the establishment of confidential information by demodulating.

On the principles of acousto-optic modulation implemented fiber optic sensor of acoustic field in sonar [6,7], vibration sensors [8,9], and other devices [2,3]. For example, in fiber optic perimeter security systems by vibration

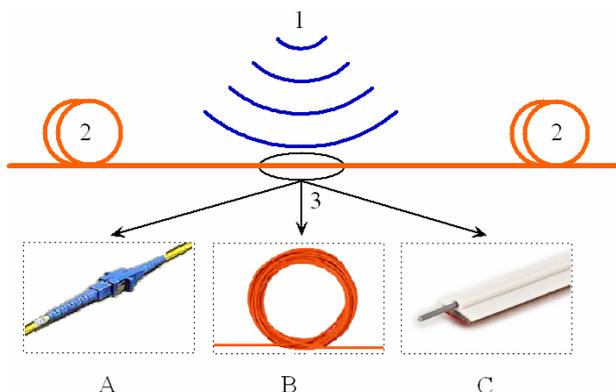


Figure 1. Model of acousto-optic (fiber) information leakage channels. 1: sound source, 2: optical cable, 3: element of optic cable system is subject to sound influence including optical plug contact (A), free optical cable (B), cable with vibro-acoustic contact with designs building (C).

acoustic effects of the intruder on fiber is registered penetration of object. Also, for a long time being developed fiber optic hydrophones, whose operation is similar to vibration sensors with various types of optical schemes. Thus, our research are supported by numerous practical work in neighboring areas. The intruder using various schemes to connect to fiber optic communications is able to conduct tapping conversations on securable.

The bases of channels leakage are light beams in an optical cable lines. All light beams can be divided into regular (legal), related to the physical implementation of data transmission protocol, and irregular (illegal), specially generated by an attacker to gain unauthorized output of the speech information. Regular light beams that are formed digital transmission techniques can create a leakage channel without disrupting the entire system, since level of acoustic action on a regular light beam reduces the signal/noise is negligible. By irregular flows will be assigned any radiation, which generated by light sources with unauthorized connections to fiber optic communications.

Research on the effectiveness of speech leakage carried by the articulator method, which defines speech intelligibility W (%) as the number of words correctly understood at channel output to the number of words spoken at entrance channels leakage. They showed a high risk of new method of eavesdropping. Estimation of efficiency made for amplitude modulation of light passing flows in communication line, containing the basic elements of passive optical networks—fiber optic cable free and attached to the building design, detachable connections, attenuators, etc. This research on shared standard equipment was shown possibility eavesdropping of voice over fiber optic communications with the sound pressure level (SPL) of 60 dB in intelligibility of W up to 80%. The modulation depth of intensity of transmitted light reached saturation into 0.3% at an SPL of 90 dB in the surrounding space.

3. Script Eavesdropping Threats

We discuss the overall sequence of actions infringer to obtain acoustic information through fiber optic communications and give a general description used by special technical facilities (Figure 2). Formation of an acousto-optic

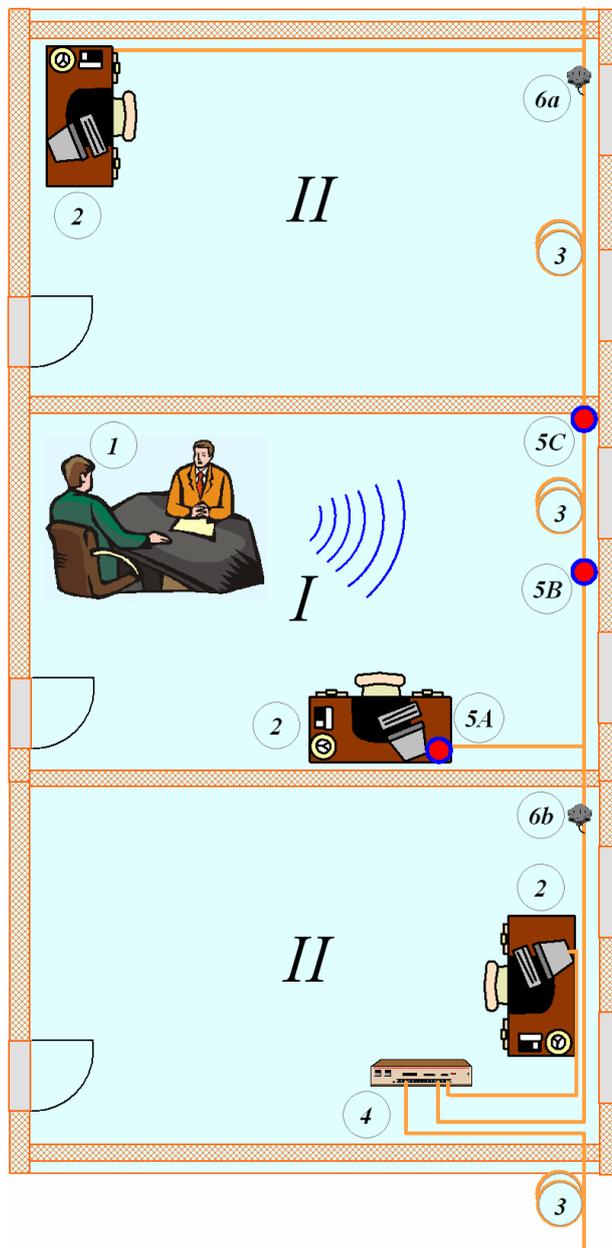


Figure 2. Generalized script of acoustic (speech) information leakage through fiber optic communications (the model of acousto-optic (fiber) leakage channel). I: allocated room; II: secondary rooms. 1: location of confidential negotiations; 2: workplace (workstation); 3: fiber optic communications; 4: regular active optical network equipment; 5: location of leakage channels such as A, B, C; 6: technical means of acoustic intelligence: a (source) and b (receiver) for leakage channel on passing of light; a or b (source and receiver in one location) for leakage channel in reflected light.

(fiber) information leakage channel is virtually impossible without physical access to optic cable that passes through selected rooms. Cabling must be free of active optical equipment on site between the infringer and the source of acoustical information, which is associated with recovery of regular shape signal and suppressing noise components of radiation in active equipment. Between the infringer and the source of acoustical information must be placed only passive optical elements, which do not change significantly modulation of light. To passive optical elements, except the optical cable relate sockets, adapters, splitters, couplers, attenuators. It should be noted that such a structure of the optical cable network is the most promising for subscriber access and rapidly developing as technology of passive optical networks.

Implementation of leakage channel requires applying technical facilities to connect to the cable and recording optical emission. Connection is implemented through regular plug connections, which are used to connect parts of network among themselves and to attach to optical line (OLT) and optical network (ONT) terminals. Connection is dropped and into gap is inserted insertion with input of probing radiation and outlet of part. Another method of connection is to apply coupler radiation on macrobends optic cable. All the proposed methods do not require special technical facilities, distribution of which is regulated by normative documents, such devices are used for installation the optical network. Another method is using cable break to insert the coupler by welding fibers.

Optical scheme of eavesdropping can be accomplished in several ways (Figure 3). First, it can be applied the special probe light sources which are not provided regular

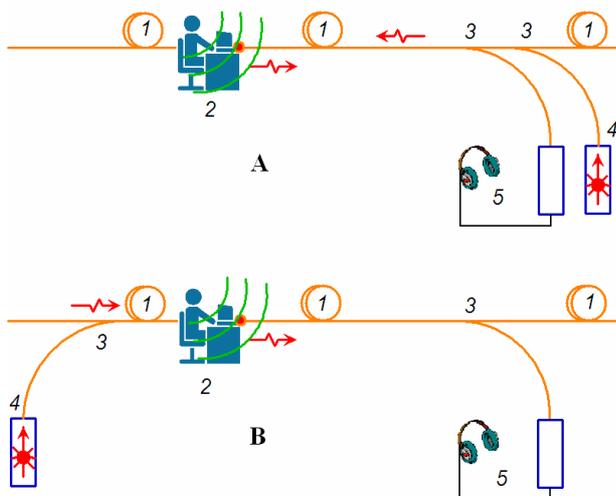


Figure 3. Structure of acousto-optic (fiber) leakage channel in scheme at reflection (A) and scheme for passage (B). 1: optical cable network; 2: confidential source (speech) information with sensitive to vibro-acoustic influence of optical cable; 3: optical coupler; 4: light source (laser); 5: analog optical detector with acoustic demodulator and headphones.

network. Probing by light can be produced by reflection or by passing from place of modulation. In this case it is possible to combine transmitting and receiving radiation. Second, for eavesdropping can be used regular radiation which applies for traffic within the network.

The danger leakage channel is determined by efficiency of acoustic modulation of light in location of sound source. Acoustic field causes various kinds of modulating light in optical fiber, by choosing parameters demodulation (amplitude, phase, polarization and frequency) is always possible to achieve very high efficiency of leakage channel acoustic (speech) information. Another danger associated with availability of installation equipment that can be used as special technical facilities of acoustic intelligence. For example, for voice communication between installers network uses fiber optic phone, which allows for direct connection to fiber carry voice communications over a distance of 200 km. Fiber optic phone can connect to fiber optic cable without it breaking through macrobend fiber. On the same principle joining works detection of optical signal in fiber, which allows establishing direction of optical signals in coated with 250 micron, 900 microns, as well as in standard optical cords up to 3 mm without gap. Level meters backscatter is designed for monitoring quality of polishing of single-mode fiber optic connectors and measure level of backscatter from other components of communication lines can be used for eavesdropping, also. Still has great potential optical time domain reflectometer (OTDR)—basic device condition monitoring optical. The above instruments are widely available commonly used for installation of optical cable systems, which increases their use in the channel leakage [10].

4. Preventing Eavesdropping Threats

All of the major ways to counter of speech information leakage through waveguide channels can be divided into the following types:

- Soundproofing channel environment, the passive method is to reduce influence of acoustic field on channel environment;
- Filtration of data carrier in transmission channel, the method consists in not passing through channel of irregular signals and modulations with confidential speech information;
- Masking data carrier in transmission channel, the method consists in concealment by addition of a special mask signal and modulations;
- Moisy channel environment, the active method consisting in creating synthetic interference and noise on acoustic frequencies [11,12].

Each method has its advantages and disadvantages, but the overall effectiveness of any security depends largely on the technical capabilities of detecting threats to information security [13]. Technical means to detect the fact

of eavesdropping or preparing equipment to implement it will undoubtedly increase the reliability of the protection system. In the case of fiber optic communications should take into account physical characteristics of fiber optic communication channel, such as small size, direction of radiation and absence of side light beams that go beyond the channel.

Features fiber optic channel allows us to offer a simple and effective way to detect unauthorized output of information (eavesdropping) by monitoring the current in channel of light beams. Any attack on the security system via fiber optic channel for accessing acoustic (speech) information associated with light beams in fiber. Monitoring parameters of light beams in the channel allows identifying any possibility of unauthorized output. This will require registration of radiations pass through fiber optic elements, the allocation authorized by the data carriers (regular radiation), to identify unauthorized flows (irregular radiation) and modulation of acoustic frequencies in any of them. Irregular emission (from external sources) may have a spectral composition as the crossover with regular radiation and does not intersect with it, which is modulated by an external acoustic signal contains confidential information.

Preventing eavesdropping is achieved by performing the following rules. First, regular light beams should not be modulated on audio frequencies. Second, irregular flows that are not provided by the physical implementation of data transmission protocol of network must be absent, and when available, they should not be modulated sound. These simple rules make it possible to detect an attack on a security system and neutralize it. Thus, the degree of risk of acoustic (speech) information leakage is determined by the following features:

- 1) Irregular light beams is detected in the channel information transmission;
- 2) Regular light beams is modulated by one of the parameters of optical radiation (amplitude, phase, polarization, frequency) and/or simultaneously on several parameters by external acoustic signal;
- 3) Abnormal light beams which are separated from spectrum are modulated by one of the parameters of optical radiation (amplitude, phase, polarization, frequency) and/or simultaneously on several parameters by external acoustic signal on a given optical wavelength.

That at least one of these conditions is sufficient for the formation of acoustic (speech) information leakage and can be used to estimate threats to information security.

5. Practical Implementation Protection

The problem of detecting possibility of speech information leakage through regular fiber optic communication is solved by installing special equipment, registering light beams in transmission channel information. Implementation

can be carried out based on standard or specially created items, which include photodetector, connected to the fiber optic link, also, optical, electronic and optoelectronic analytical element for allocation of acoustic oscillations parameters detected optical radiation. Protection device can be done in two structural decisions: as a separate unit, which has its own alarm system threats, or block the built-in active equipment, which has informational link with the main equipment. Let us discuss possible implementation of devices and their features function.

The external indicating device threat (**Figure 4**) includes in an optical channel with standard optical connectors and closes the communication link without a significant impact on passing traffic. The main risk associated with probing (illegal) radiation, which is separated from regular light by beamsplitters. Incident radiation at regular wavelength is reflected, and irregular radiation at otherwise wavelengths passes through it and is registered a photodetector. Part passing through beamsplitters of regular radiation is allocated and is recorded by another photodetector. Received at photodetector output signals are analyzed on existence of probing (illegal) radiation and on possible amplitude modulation. The decision about danger is taken from obtained data, which consists in answer to questions—what is the danger level? And on which side of indicator is a threat comes? The highest danger level corresponds to existence of irregular radiation or amplitude modulation of regular radiation. The average level corresponds to existence of amplitude modulation of regular radiation at the level noise in optical channel. Absence of irregular emissions and any irregular modulation corresponds to the safe mode.

Although the device registers only amplitude modulation of optical radiation and does not register other modulation types, but given that other types of modulation can be effectively observed only when using probing (illegal) radiation, we can assert control of all types of modulation by detecting irregular radiation. Another possibility inherent in this device is that it acts as a filter irregular optical radiation since the regular radiation passes indicator threats and irregular do not pass. Such property greatly limits the application optical design on the passage, which is more effective scheme for reflection. Reflected signal is always weaker than direct probing radiation. Scheme on reflection to the infringer demands more intense radiation to reach an acceptable echo. However for threat indicator any probe signal is a direct that goes either left or right of him so its check will be much safer than the infringer, recording only reflected signal.

The internal indicating device threat (**Figure 5**) can be integrated directly into the active optical network equipment. It can be integrated into equipment or join a removable modules—transceivers. In the last case, the physical changes to basic equipment may be required and

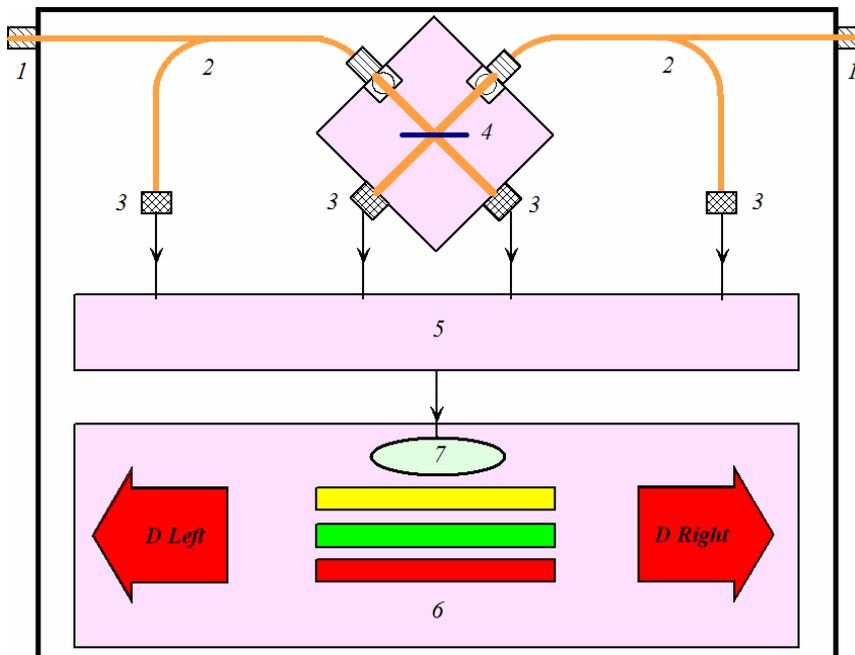


Figure 4. External indicator attacks. 1: optical inputs; 2: optic couplers; 3: photodetectors; 4: beamsplitters; 5: spectrum analyzer; 6: display unit; 7: sound indicator attacks. *D Left*—LED attack on the left, *D Right*—LED attack on the right, the color risk indicators.

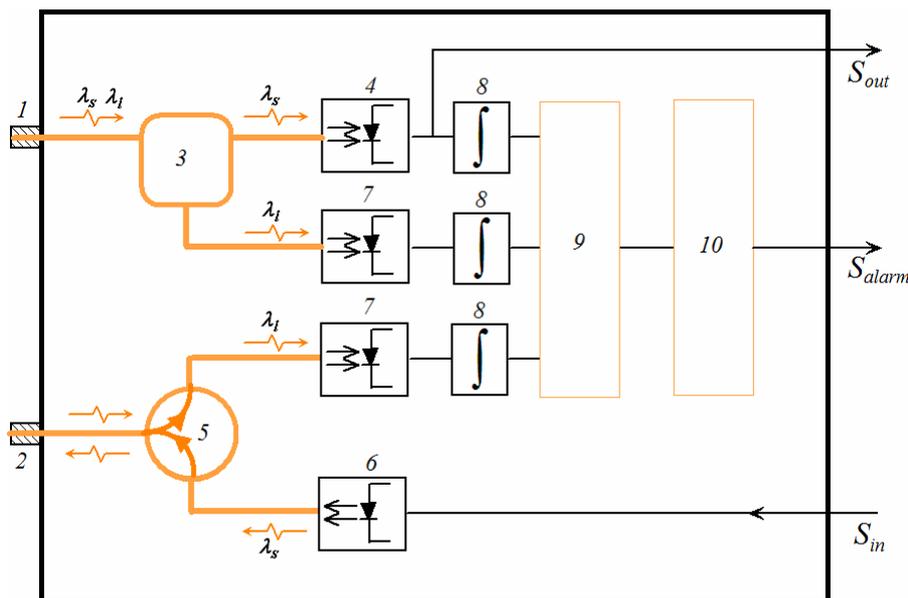


Figure 5. Integrated indicator attacks. 1: optical input; 2: optical output; 3: multiplexer which separates data signal at wavelength λ_s from probing light beam at wavelength λ_i ; 4: regular photodetector with input information signal S_{out} ; 5: coupler; 6: regular transmitter with output information signal S_{in} ; 7: additional monitoring photodetectors; 8: integrating elements; 9: spectrum analyzer; 10: analog-digital converter, generating danger signal.

to change the driver itself transceiver. The main problem of this conversion is to place additional optical elements in required form factor of transceiver. Discuss the structure and operation of indicator threats in integrated dual-port active equipment with separate fiber optic input (the channel receiver) and output (the channel transmit-

ter). Own monitoring system be put on each fiber in the form of additional sensor. In the port of receiver signal is divided into regular and irregular radiation through an optical circulator. Information signal from the regular receiver is processed by conventional means for transmission channel, and arrives at the integrator output

which generates an analog signal from the regular radiation that can be modulated by an acoustic frequencies. Selection of irregular radiation is recorded and converted to its own receiver to an analog signal. In the port of transmitter there is no incoming radiation, thus the channel is required separation of radiation on regular and irregular, they are divided by propagation direction. Photodetector is connected to transmitter through coupler and the signal from it is also integrated. Thus, the control system has three receivers with integrated units that make up three analog signals, by which concludes that existence of a threat eavesdropping. Analysis is performed on the existence of irregular radiation and the presence typical components of speech in signal spectrum. On this basis is generated danger signal.

6. Advice on Protection

At present the implementation of methods described above to identify threats to speech information leakage does not exist. As can be seen from a general description of functioning principles of protection devices, to develop working models for detection of eavesdropping by fiber-optic communications is possible based on standard equipment. The main element of protection system is optical detector with an amplifier at sound frequencies, which is present in any analog fiber-optic phone. Standard analog fiber optic phone has high sensitivity which allows recording very small fluctuations in intensity and detect attempts at eavesdropping. However, it has significant disadvantages for the systems security one of them being sensitivity shift in the infrared spectrum, which does not register with highly reliable probing emission of visible spectrum. At distances of several hundred meters, total optical loss will amount to several dB at wavelengths in the visible range in a standard quartz fiber that cannot reliably detect weak optical radiation regular photodetectors.

Another disadvantage is need for additional fiber optic components to register modulation by polarization, frequency and phase. But in any case, a fiber optic phone is closest by principles of functioning for use in protection from eavesdropping through fiber optic communications.

Protection against eavesdropping of selected rooms through a fiber optic communications can be represented as follows (Figure 6). Optic cable passes by the selected room and connected to a computer at workplace. The whole cable with connecting elements inside the room appears as a system which is subject to acoustic effects, formed a speech of confidential information carriers. Light output is modulated a speech and exceeds the selected rooms and may be registered by an attacker. Dangerous for connecting technical reconnaissance attacker's are all parts of network in the selected room from one active equipment to another. Defining dangerous section, establish the device detecting attacks in the selected room, way optical insert.

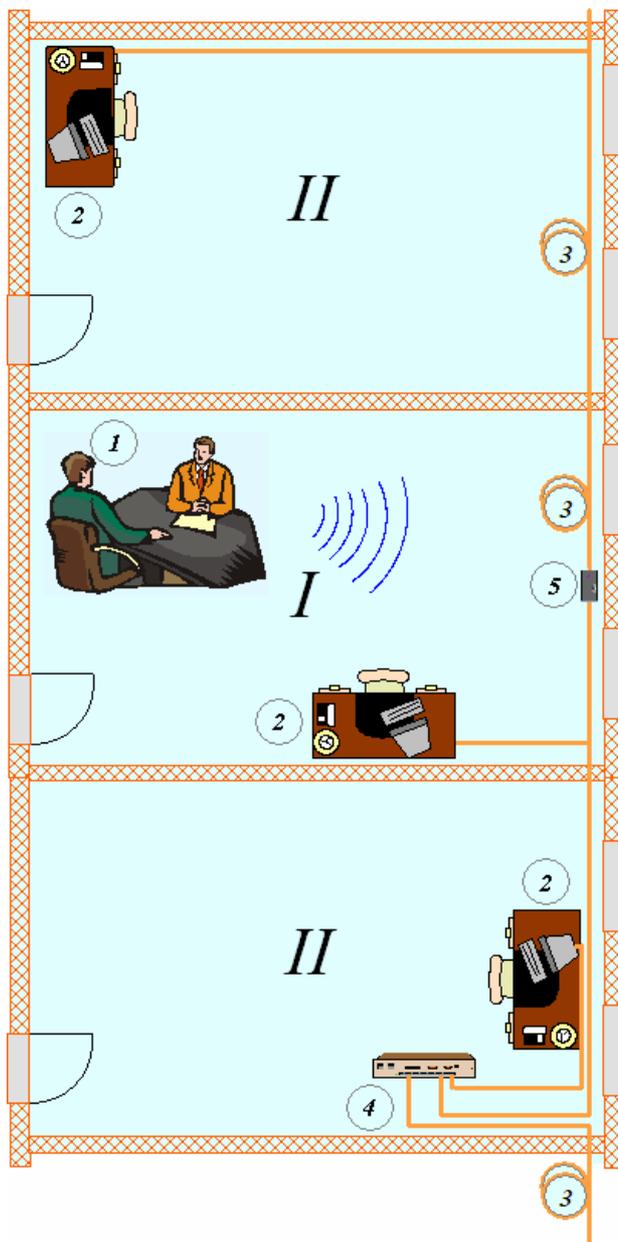


Figure 6. Schematic diagram of protection against leakage information through fiber optic communications, based on detector of attack. I: allocated room; II: secondary rooms. 1: location of confidential negotiations; 2: workplace (workstation); 3: fiber optic communications; 4: regular active optical network equipment; 5: inclusions detector attack.

We conducted a trial listening to fiber optic communication lines consisting of optical cable with dual fibers of length exceeding 25 m and a thickness of 3 mm each. Light output was formed an optical tester or a helium-neon laser and registered a fiber-optic phone with analog modulation. Acoustic effects produced locally using computer speakers, acting directly at cable and network elements. The acoustical signal was very noisy, but the words be recognized speech at the hearing.

The presented modeling studies confirmed possibility of implementing such schemes identify attacks even with the help not profile equipment. Production of specialized equipment can more reliably resolve the problem identification of eavesdropping and the security services to help protect speech information in modern rapid proliferation of fiber optic communications technologies.

7. Conclusion

This work is a development patent for invention [13], which proposes a solution to ensure information security talks in selected areas by identifying potential threats on formation leakage channels of acoustic (speech) information through fiber optic communication systems and proposed for use in systems to protect confidential voice communications. Detection of acoustic (speech) information leakage channel is carried out by monitoring optical emissions in regular fiber optic communications. Appearance of any irregular light emissions or modulation on acoustical frequencies of regular light streams creates a potential threat of acoustic information leakage.

REFERENCES

- [1] F. L. Cedric, "Passive Optical Networks: Principles and Practice," Elsevier, San Diego, 2007.
- [2] R. Hui and M. S. O'Sullivan, "Fiber Optic Measurement Techniques," Elsevier Academic Press, Waltham, 2009.
- [3] E. Udd and W. B. Spillman Jr., "Fiber Optic Sensors: An Introduction for Engineers and Scientists," 2nd Edition, John Wiley & Sons, Hoboken, 2011.
- [4] V. V. Grishachev, D. B. Khalyapin, N. A. Shevchenko and V. G. Merzlikin, "New Channels of Leakage of Confidential Information over the Voice of Fiber Optic Subsystems SCS," *Special'naya Tehnika*, No. 2, 2009, pp. 2-9.
- [5] V. V. Grishachev and O. A. Kosenko, "The Practical Estimation of Convert Audio (Voice) Channel Efficiency from Fiber-Optic Communications," *Voprosy Zashity Informacii*, No. 2, 2010, pp. 18-25.
- [6] J. A. Bucaro and T. R. Hickman, "Measurement of Sensitivity of Optical Fibers for Acoustic Detection," *Applied Optics*, Vol. 18, No. 6, 1979, pp. 938-940. [doi:10.1364/AO.18.000938](https://doi.org/10.1364/AO.18.000938)
- [7] B. Culshaw, D. E. N. Davies and S. A. Kingsley, "Acoustic Sensitivity of Optical Fiber Waveguides," *Electronics Letters*, Vol. 13, No. 25, 1977, pp. 760-761. [doi:10.1049/el:19770537](https://doi.org/10.1049/el:19770537)
- [8] J. C. Juarez and H. F. Taylor, "Field Test of a Distributed Fiber-Optic Intrusion Sensor System for Long Perimeters," *Applied Optics*, Vol. 46, No. 11, 2007, pp. 1968-1971. [doi:10.1364/AO.46.001968](https://doi.org/10.1364/AO.46.001968)
- [9] J. C. Juarez, E. W. Maier, K. N. Choi and H. F. Taylor, "Distributed Fiber-Optic Intrusion Sensor System," *Journal of Lightwave Technology*, Vol. 23, No. 6, 2005, pp. 2081-2087. [doi:10.1109/JLT.2005.849924](https://doi.org/10.1109/JLT.2005.849924)
- [10] Fiber Optic Devices Ltd. (FOD), "Products," <http://www.fods.com>
- [11] V. V. Grishachev, D. B. Khalyapin and N. A. Shevchenko, "Method and Device for Actively Protecting Confidential Spoken Information from Leaking over an Acousto-Optic Fibre Channel by Using External Optical Noise Masking," 2010. <http://www.wipo.int/patentscope/search/en/WO2010126400>
- [12] V. V. Grishachev, D. B. Khalyapin and N. A. Shevchenko, "Methods and Devices for Actively Protecting Spoken Information against Eavesdropping via an Acousto-Optic Fibre Leakage Channel," 2010. <http://www.wipo.int/patentscope/search/en/WO2010126401>
- [13] V. V. Grishachev, "Fiber-Optic Detector for Detecting Threats of Verbal Information Leaks," 2011. <http://www.wipo.int/patentscope/search/en/WO2011031186>