The Ministry of Education of the Republic of Belarus
Institution of Education
Belarusian State University of Informatics and Radio Electronics

UDC 621.391; 621.383.92

Ali Abdl Hsen Mhmd Jwad

The mathematical model of fiber-optic link protected from unauthorized access

ABSTRACT

for the degree of Master of Engineering
the specialty 1-98 80 01 - Methods and systems of information protection, information security

Supervisors: doctor of technical sciences,
Professor Lynkov L.M., Ph.D.,
Associate Professor Timofeev A.M.

Minsk, 2016

LIST OF ABBREVIATIONS

FOCL - fiber-optic communication line
APD - avalanche photo detector
MM OF - multimode optical fiber
OF - optical fiber
DTR - data transmission rate
PC - photon counter
CWDM - wavelength division multiplexing technology with sparse wavelength division
DCF - quartz optical fiber
DWDM - wavelength division multiplexing technology packed
EDF - quartz optical fiber, erbium-doped
EDFA - Erbium optical amplifiers
HDWDM - the highly wavelength division multiplexing technology
NDF - silica fiber doped with neodymium
NDFA - Neodymium optical amplifiers
OTN - technology of optical transport networks
PCF - photonic crystal fiber PDH - plesiochronous digital hierarchy technology
PMF - optical fiber, preserving the polarization state
SDH / SONET - Synchronous Digital Hierarchy technology

INTRODUCTION

The development of modern telecommunication systems is based on the use of an optical signal band having a large information capacity [1, 2]. The most important requirement for such systems is to ensure the secrecy and confidentiality of transmitted information, which provides the full cycle of organizational and technical measures for comprehensive information security fiber-optic communication lines (FOCL), including methods of cryptography. One of the methods of detecting unauthorized access to information transmitted on such communication links,is a reduction in power of the optical signal to tens of photons per one bit of information. This is due to the fact that if the information transfer is performed weak optical pulses comprising not thousands of photons and single photons, any attempt at interception will be discovered [3-5]. Fiber-optic communication system in which to encode each character uses the binary state of a photon,is called quantum cryptography. Modern quantum cryptographic communications systems have a low data transfer rate, which according to [3, 6, 7], is not more than 50 kbit / s. Low speed of transmission of information (TOI) is largely limited to the characteristics of the receiving unit a communication system [4]. As a receiver module quantum cryptographic systems used photon counter (PC) based on avalanche photodetector (FOCL) [3]. To improve channels of communication SPI their optimization is performed using the mathematical models of communication channels [8-10], but to date there are no mathematical models channel fiber-optic communications to assess the SPI communications channel in view of presence of unauthorized access. In this regard, the aim of this work was to develop a mathematical model of tamper-proof fiber-optic connection.

To achieve this goal the analysis of threats to information security of data transmission over fiber-optic lines, the basic methods and systems for detecting unauthorized access to the transmission of information via fiber optic link, a method for determining the dead time of FOCL in the photon counting mode, the mathematical Model of communication channel in which data is transmitted using individual photons with different polarization, and an expression for calculating the bandwidth of the optical fiber, and the likelihood of depolarization and absorption, performed experimental studies the impact of information leakage channel created by forming Macrobend optical fiber, the probability of loss of the optical signal in the presence of various diameters macrobend and transfer the most common in the art of fiber-optical communication wavelength of the optical radiation.

As the object of the investigation photon counter was used, built on a silicon FOCL.The subject of the research was to determine the impact of Macrobend diameter of an optical fiber produced by the formation of protected from unauthorized access fiber optic communication channel bandwidth of the communication channel .

GENERAL DESCRIPTION OF WORK

The goals and tasks of the research

The aim of this thesis is to develop a mathematical model protected from unauthorized access to fiber-optic connection.

To achieve this goal it took to solve the following interrelated problems:

1. Analyze the threats to information security of data transmission over fiber-optic lines and to define the basic methods and systems for intrusion detection in information transmission through fiber optic link.

2. On the basis of the implementation review of known methods of measuring the dead time of FOCL for registration of optical radiation in the photon counting mode to offer a method for determining the dead time of FOCL in this mode, which simplifies existing processes by eliminating an external light source of the measuring process and enhances the way active extinction.

3. Get the expression for calculating the dead time of FOCL operating in the photon counting mode and the inclusion of the passive damping circuit avalanche.

4. Develop a mathematical model of a communication channel in which data is transmitted using individual photons with different polarization, and an expression for calculating the bandwidth of the optical fiber, the likelihood of depolarization and the radiation absorption.

5. The effect of the channel leakage of information created by forming Macrobend optical fiber, the probability of loss of the optical signal in the presence of various diameters macrobend and transfer the most common in the art of fiber-optical communication wavelength of the optical radiation.

As the object of the investigation a photon counter was used, built on a silicon FOCL.

The subject of the research was to determine the impact of Macrobend diameter of an optical fiber produced by the formation protected from unauthorized access fiber optic communication channel bandwidth of the communication channel.

Personal contribution of the applicant

The content of the thesis reflects the contribution of the applicant. The work is carried out in co-authorship, the author participated in the definition of objectives, targets research as well as in the conduct of the studies and the processing of the results.

Testing and publication of results

Main results of the thesis are reported and discussed at the XIII Belarusian-Russian Scientific
Technical Conference "Information Security Means" (Minsk, Belarus, 2015) and XX International scientific-technical conference "Modern means of communication" (Minsk, Belarus, 2015). Two theses of reports are published.

The structure and scope of the thesis

The dissertation work consists of a list of abbreviations used, an introduction, the general characteristics of the work, three chapters, conclusion and bibliography. The thesis consists of
50 typewritten pages. The thesis contains 10 drawings on pages 7,4 tables on page 1. Bibliographic list covers 6 pages and consists of 58 names of references and a list of publications of the applicant's own two titles on one page.

CHAPTER 1
FIBER-OPTIC COMMUNICATION SYSTEMS FOR PRIVATE DATA TRANSMISSION

1.1 Analysis of the threats to information security of data transmission over fiber-optic lines

In the development of systems of fiber-optic communication it's quite important to ensure their information security. To do this, you need to install the main types of threats that can occur when transmitting data over fiber optic links.

In works [11-14] the basic kinds of threats to information security of data transmission over fiber optic links are discussed, which are usually classified as well as security threats and automated information processing systems [15-19], - the impact on the target. Thus, we can identify threatened breach of confidentiality, authenticity and integrity of information transmitted over fiber optic links.

Violation of privacy of information transmitted via fiber optic links, may be due to unauthorized access to optical fibers when using special funds of the optical power output.

Violation of reliability of the transmitted information is most often in communication networks constructed based on optical fibers, for example in passive optical fiber networks PON, the implementation of which is defined in the [20-29] with high-speed versions of [23-29]. At the same violation of the reliability of the transmitted information occurs when an unauthorized user sends a PON network of information on behalf of the authorized user. Table 1.1 shows the comparative analysis of the basic characteristics of network PON. As can be seen from Table 1.1, the protection of information on a possible violation of its accuracy is provided for networks PON, built on the basis of technologies APON (BPON) and GPON. It uses the principles of cryptographic protection of information, which are sufficiently detailed in [17-19].

Cryptography is a set of methods for data transformation, aimed at making the data useless to the unauthorized user [17-19].

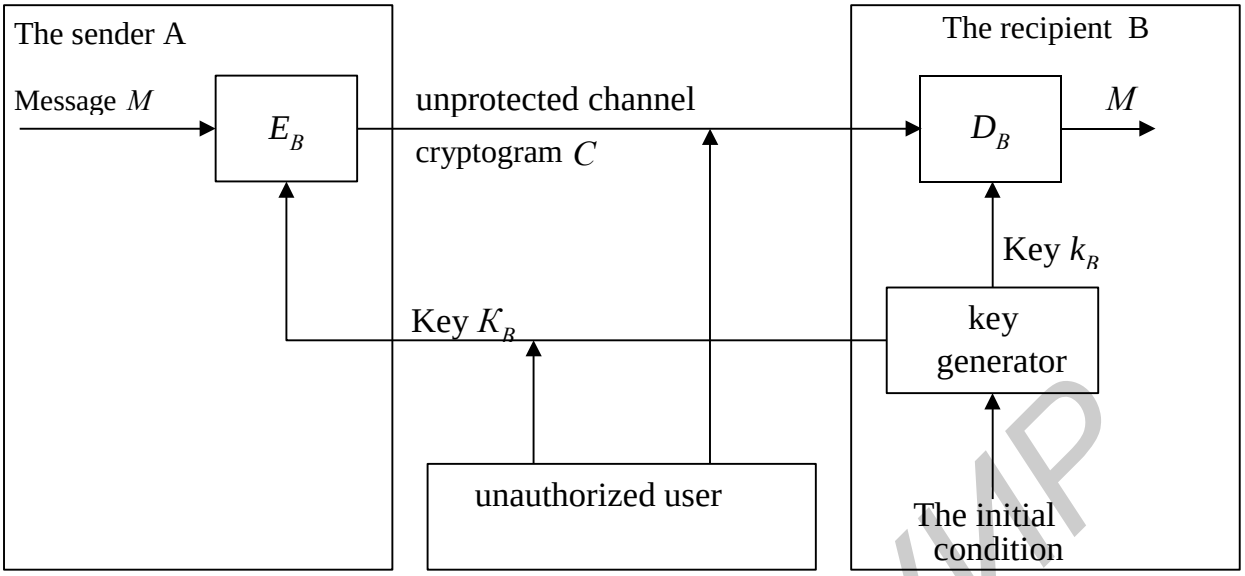
Table 1.1 - Comparative information of technologies APON, EPON and GPON

Characteristics	Technology of building a network PON		
	APON (BPON)	EPON	GPON
The data rate forward / reverse flow Mbit / s	155/155; 622/155; 622/622	1000/1000	1244/155,622,1244 2488/622,1244,2488
Base protocol	ATM	Ethernet	SDH
Line Code	NRZ	8B/10B	NRZ
The maximum radius of the network,	20	20÷30	20
The maximum number of subscriber units on one optical fiber	32	16	64÷128
The wavelengths of the forward / reverse flow, Nm	1550/1310; 1480/1310	1550/1310; 1310/1310	1550/1310; 1480/1310
data protection	Public-key encryption	No	Public-key encryption
Reservation	Yes	No	Yes

Such transformations allow to solve two major problems of data protection: privacy concerns (by denying unauthorized user the possibility to extract information from the communication channel) and the issue of integrity (by denying unauthorized user the possibility to change the message so that its meaning is changed, or enter false information in the link) .

Asymmetric cryptosystem, also called public-key cryptosystem is used in networks PON (see Table 1.1), involves the use of two keys. The first key is open and can be published for use by all users on the network, which encrypts the data. Decrypting data using a public key is impossible. To decrypt the data recipient of encrypted data use a second key, which is secret. A decryption of a key can not be determined from the encryption key.

The generalized scheme of asymmetric public key cryptosystems is shown in Figure 1.1 [19].



K_B – The sender's A public key; k_B – The recipient's B private key;
C – cryptogram; E_B – encryption algorithm; D_B – decryption algorithm

Figure 1.1 - Generalized scheme of asymmetric cryptosystem

The cryptosystem shown in Figure 1.1 can use two different keys: the public key KB of the sender A and a secret key kB of the recipient B.

It's useful to have key generator at the receiver in order not to send the secret key kB over an insecure channel. Key values of KB and kB depend on the initial state of the generator key.

Disclosure of the secret key kB with the help of the known public key of KB should be computationally impossible task.

Characteristic features of asymmetric cryptosystems are as follows:

1. The public key KB and a cryptogram C may be sent over insecure channels, i.e.,the enemy knows KB and C (see Figure 1.1).

2. Algorithms for encryption and decryption

$$\begin{aligned} Å_{Â} &: Ì \rightarrow Ñ, \\ D_{Â} &: Ñ \rightarrow Ì \end{aligned} \qquad (0.1)$$

are open.

Thus, the protection of information in an asymmetric cryptosystem is based on secret key kB.

An important requirement is to ensure the authenticity of the sender of the message. This is achieved by the mutual authentication information exchange of participants. Procedures for user identification and authentication can be based not only on the secret information possessed by the user (password, secret key, a personal identifier etc.). In recent years, increasingly common biometric identification and authentication of the user, allowing confidently identify potential user by measuring

physiological parameters and characteristics of the person, especially his behavior [15-19]. The main advantages of biometric methods of user identification and authentication, as compared to traditional, are a high degree of reliability of biometric identification features because of their uniqueness, the inseparability of biometric features of a capable person and the difficulty of falsification of biometric features. As biometric traits that may be used to identify the potential user may perform pattern of the iris and the retina, fingerprints, geometry hand shape, form and dimensions, particulars of voice biomechanical characteristics of the handwritten signature, the biomechanical characteristics of the "keyboard handwriting." When registering, the user must demonstrate one or more times its typical biometric features. These symptoms (known as the original) are registered by the system as a controlling "image" of a legitimate user. This way the user is stored electronically and is used to check the identity of everyone who pretends to be the appropriate legal user. Depending on the match or mismatch presented together with signs registered in the reference image the one who showed them is recognized their legitimate user (in coincidence) or not (a mismatch) [15-19].

The main advantage of public-key cryptosystems is their potentially high security: there is no need to transfer or to report someone else the values of secret keys, not to make sure in their authenticity. However algorithms underlying into the cryptosystems with public-key have two major drawbacks. Firstly, the generation of new secret and public key based on the new generation of large prime numbers and primality testing takes a lot of CPU time. Secondly, this procedure is used to encrypt and decrypt the related exponentiation multivalued number, rather cumbersome.

Violation of the integrity of information is its unauthorized modification or removal, which are more susceptible to a system where data is stored [13]. However, this kind of information security threats takes place during data transmission on the fiber optic link, as an unauthorized user from intercepting information optical fibers may change it as entering again into the optical fiber, and remove.

The theoretical possibility of breaches of confidentiality, authenticity and integrity of the information, in addition to the above networks PON, exists for networks built on the basis of other techniques, which as a transmission medium using optical fibers. These technologies may include those described in [30-32] technology plesiochronous digital hierarchy (Plesiochronous Digital Hierarchy, PDH), Synchronous Digital Hierarchy (Synchronous Digital Hierarchy, SDH / SONET), wavelength division multiplexing with sparse wavelength division (Coarse Wavelength Division Multiplexing, CWDM) compacted wavelength division multiplexing (Dense Wave Division Multiplexing, DWDM), the highly wavelength division multiplexing (High-Dense Wave Division Multiplexing, HDWDM), as well as the technology of optical transport networks (Optical Transport Network, OTN), which determines how the data from the wave channel DWDM.

It should be noted that for the above techniques can be used various types of optical fibers (OB), which are basically classified according to the number of traveling waves or modes (multi-mode and single-mode), the profile of the refractive index of the core

RH (stepwise, parabolic / gradient and special) type characteristics dispersion parameter D (standard s-shifted / zero-dispersion non-zero dispersion shifted, with zero water peak), sign D (OM with positive and negative sign D). In addition to these options, there are also special features peculiar only to certain types of agents and defined in the core areas of their practical application [1, 2, 4, 20-29], which can be seen from Table 1.2.

Table 1.2 - The main kinds of special types of OM

Type OM	The practical application
Quartz OB DCF	Creating a dispersion compensation module for DCM
Quartz RH doped with erbium (Erbium-Dopped Fiber, EDF)	Erbium optical amplifiers
Quartz RH doped with neodymium (Neodim-Dopped Fiber, NDF)	type EDFA (Erbium-Dopped Fiber Amplifier)
Fused fiber Bragg with a large (300 ÷ 800 micron) core diameter	Neodymium optical amplifiers (Neodim-Dopped Fiber Amplifier, NDFA)
Quartz OB UV spectrum	Making light streams high brightness and power used in various dimensions and for transporting the laser beams
Fiber, preserving the state of polarization (Polarization Maintaining Fiber, PMF)	It is used in the range of 190 ÷ 250 nm for various applications (has a much greater chemical stability and mechanical strength, in comparison with other types of OS)
Photonic crystal OB (Photonic Crystal Fiber, PCF)	Applied quantum cryptographic systems, transmission of confidential information, as well as the creation of different types of fiber sensors

Classes multimode (MM) explained OB tables 1.3 and 1.4 [33].

Table 1.3 - Classes of MM OB

class	Materials core / shell	The diameters of the core / shell microns
class A1	glass / glass	50/125, 62.5 / 125, 85/125 and 100/140
class A2	glass / glass	200/240
class A3	glass / plastics	200/280
class A4	plastic / plastic	980/1000

Table 1.4 - Categories of MM OB

Category	The maximum transmission distance, km	The total attenuation value of all components of the longest side, dB			
		single-mode		multimode action	
		λ = 1310 нм	λ = 1550 нм	λ = 850 нм	λ = 1310 нм
OF 300	0,3	-1,80	-1,80	-2,55	-1,95
OF 500	0,5	-2,00	-2,00	-3,25	-2,25
OF 2000	2,0	-3,50	-3,50	-8,50	-4,50

Note: multimode attenuation is given for 1 communication channel.

As shown in Tables 1.3 and 1.4 MM OB are mainly classified by the core refractive index profile (stepwise, PAR) and depending on the material of OB and its structural features (classes A1 ÷ A4). However, OM OB are mainly classified by core refractive index profile (stepwise, with a profile of a special type), the type of characteristic dispersion parameter D (standard s shift of zero dispersion, OB with

clipping offset, non-zero dispersion-shifted RH with nonzero dispersion broadband, insensitive to bending loss of OB) [33, 34].

In order to implement one of the above types of threats to information security of data transmission over fiber optic links, as noted above, an unauthorized user organizes the channel leakage of information, for which in the fiber-optic line a device of unauthorized connections can be integrated [11, 35, 36] . For unauthorized connection to the fiber optic link at the beginning it's better to break the optical fiber, the installation of unauthorized devices to connect and then connect optical fibers by mechanical connection by means of optical couplers / connectors, by a welded (thermal) connection or by adhesive bonding. RH Connection using mechanical connectors allows you to quickly (within minutes) provide a single-mode or multimode dock OB, but low in absolute value interface return loss limit the application of this method for high-speed fiber optic link. Method of welded (thermal) compound is currently the most used during the construction and installation work on the installer, because the parameters of interface are close to the most stringent requirements on the amount of insertion and return loss and the mechanical strength of the joint. The method of adhesive bonding practice in the construction and operation of fiber-optic line is rarely used. This is due to the fact that nowadays there are no established adhesive formulations suitable for short time to provide a rigid fixation of OB connector design. So used adhesives based on epoxy compounds, have a good optical performance, durability and the polymerization of 2 ÷ 24 hours. When moisture in the field bonding the process slows down even more. In this regard, the most common method nowadays is the method based on compound RH welding. However, to detect unauthorized access, implemented by retraction of the optical power with breaking the fiber-optic is quite simple, so to hide this access abduction of optical power can be carried out without breaking the fiber-optic [35-38].

Abduction of optical power without rupture of fiber optic links may be based on the change in the angle of total internal reflection at the mechanical exposure (macrobend, torsion, tension, etc.), to change the attitude of refractive indices under the influence of acoustic and electromagnetic fields, as well as the method of optical tunneling, in which the output of optical radiation outside the main optical fiber is carried out by means of another optical fiber having a higher coefficient refractive index than the main [11, 13, 14, 36]. Optical method of tunneling is the most dangerous, since it is not making a reverse scattered and reflected radiation (that's why it is difficult to detect) and allows you to adjust the power leakage [14].

It is also important to note that in addition to the above, there are other kinds of information security threats of fiber-optic communications systems, for example, the threat of malfunction or accessibility [13]. However, as a rule, the implementation of such threats is detected quickly enough by legitimate users.

CONCLUSION

On the basis of applying analytical review of the literature, the main types of threats to information security of data transmission over fiber optic links were set. Breach of confidentiality, authenticity and integrity of information transmitted over fiber optic links, may be due to unauthorized access to optical fibers when using special funds of the optical power output. Such threats have a place for communication systems and networks built on the basis of technology PDH, SDH / SONET, CWDM, DWDM, HDWDM, OTN and PON.

It was found that the cryptographic methods of information protection help to ensure confidentiality and integrity of the transmitted information. This public-key encryption, used in passive optical fiber network provides a high enough security, but it requires the formation of new private and public keys to generate new large prime numbers and primality testing takes a long duration of the CPU time. Furthermore, the procedures, used to encrypt and decrypt the related exponentiation multivalued number are rather cumbersome.

The main ways to detect unauthorized access to the transmission of information on the installer, based on the measurement of optical power level, the spectrum of the optical signal, and the level of the reflected optical power were determined. For implementation of these methods unauthorized user arranges channel information leakage or due to the rupture of the optical fiber with its subsequent reduction, without any discontinuity. Leading optical power without breaking the fiber optic links can be based on the angle of total internal reflection at mechanical influence (bending, torsion, tension, etc.), on changing the attitude of refractive indices under the influence of an acoustic or electromagnetic fields and optical tunneling method; the last is the most dangerous since it does not introduce backscattered and reflected radiation, so it is difficult to detect.

The systems that detect unauthorized access when transmitting information over a fiber-optic communication lines, based on the measurement of the level of the reflected optical power and using information and control signals were considered. Systems that detect unauthorized user in the fiber optic data transmission in automatic mode, in comparison with others, are more preferred, because they provide better information security through continuous testing of fiber optic links.

A mathematical model of a communication channel in which data is transmitted using individual photons with different polarization, and an expression for calculating the bandwidth of the optical fiber, the likelihood of depolarization and the radiation absorption was built.

An experimental device for transmitting and receiving information, the creation and detection of information leakage from fiber-optic link by Macrobend agents was suggested. The investigations have shown that the probability of loss of the optical signal increases with decreasing the diameter of Macrobend OB for all the studied wavelength of the optical radiation. Moreover, for a given diameter of Macrobend probability of loss of the optical signal is higher, the longer the wavelength of the optical radiation. The lowest probability of loss of the optical signal was observed at a wavelength of 850 nm, which is closest to the maximum sensitivity of silicon APD.

The possibility of the use of silicon avalanche photodetectors in the photon counting mode for systems transmitting confidential information macrobends detecting optical fiber was shown. The experimental dependence of the probability of loss of the optical signal of the diameter of Macrobend optical fiber allowed to justify such systems a choice of two wavelengths of optical radiation transmitted through a single optical fiber: $\lambda 1 = 1625$ nm for the transmission of high-power clock and control macrobend optical fiber and $\lambda 2 = 850$ nm for transmission the data by weak optical signals.

A method for determination of the dead time of the detector running in single photon counting mode, and the device implements it was created. This method simplifies the measurement of the dead time of APD in the mode of operation by eliminating an external light source of the measuring process and to extend the capabilities of the active quenching method.

REFERENCES

List of references

1 Dmitriev, S.A. Fiber-optic technology: current status and new perspectives / S.A.Dmitriev, N.N. Slepov. - 3rd ed., Rev. and add. - M .: Technosphere, 2010. - 608 p.

2 Kokhanenko, A.P. Fiber-optic communication lines. Physical basics of optical fibers: a tutorial / A.P. Kokhanenko, Y. Maslov. - Tomsk: TSU, 2013. - 64 p.

3 Killeen, S.J. Quantum cryptography: the idea and practice / S.Y. Killeen; ed. S.Y .Killeen, D.B. Khoroshko, A.P. Nizovtsev. - Minsk: Belorus.science, 2007. - 391 p.

4 Gulakov, I.R. Photodetectors quantum systems: monograph / I.R. Gulakov, A.O. Zenevich. - Minsk: UO VGKS, 2012. - 276 p.

5 Olifer, V.G. Computer Network Security / V.G. Olifer, N.A. Olifer. - M .: Hotline Telecom, 2014. - 644 p.

6 Experimental setup for quantum cryptography with single photons polarized / V.L. Kurochkin [et al.] // Technical Physics. - 2005 - m. 75, no. 6. - P. 54-58.

7 The use of single photon detector for quantum key generation in the experimental fiber-optic communication system / V.L. Kurochkin [et al.] // Avtometriya. - 2009 - m. 45, № 4. - pp 110-119.

8 Introduction to the mathematical modeling: Tutorial / V.N. Ashihmin [et al.]; ed. P.V. Trusov. - M .: Logos, 2005. - 440 p.

9 Binder, K. Simulation Monte Carlo method in statistical physics: an introduction / K. Binder, D.V. Heermann; tr. from English. V.N. Zadkova. - M .: Nauka. FIZMATLIT, 1995. - 144 p.

10 Bezruchko, B.P. Mathematical modeling and chaotic time series / B.P. Bezruchko, D.A. Smirnov. - Saratov: GosUNTs"College", 2005. - 320 p.

11 Bulavkin, I.A. Macrobend detection in PON networks without the use

of OTDR / I.A. Bulavkin // Herald of communication. - 2008 -№ 3. - p. 54-58.

12 Matthijsse, R. Influence of bending of the optical fibers on their characteristics / R. Matthijsse, G. Kuyt // Science and Technology. - 2005. - № 4 (293). - p. 17-22.

13 Kirillov, V.I. Investigation of the generalized model script attacks on the information transmitted by the passive optical fiber networks PON / V.I. Kirillov, E.A. Kovriga // Herald of communication. - 2014. - № 2 (124). - p. 38-43.

14 Grishachev, V.V. Identify threats of voice over fiber optic communications / V.V. Grishachev // Photonics. - 2011. -№ 4. - P. 32-39.

15 Shangin, V.F. Information security of computer systems and networks: Proc. Benefit / V.F. Shangin. - M .: Publishing House "FORUM" INFRA-M, 2008. - 416 p.

16 Information Security Audit / AP Kuril [et al.]. - M .: Publishing Group "BDC-press", 2006. - 304 p.

17 Zavgorodniy, V.I. Comprehensive protection of information in computer systems: Textbook / V.I. Zavgorodniy. - M .: Logos, 2001. - 264 p.

18 Yarochkin, V.I. Information security: a textbook for high schools / V.I. Yarochkin. - M .: Academic Prospect: Triksta, 2005. - 544 p.

19 Melnikov, V.P. Information security and protection of information: a textbook for university students / V.P. Melnikov S.A. Kleimenov, A.M. Petrakov; ed. S.A .Kleimenova. - 3rd Ed. - M .: Publishing center "Academy", 2008. - 336 p.

20 G.983.1 // Broadband optical access systems based on Passive Optical Networks (PON). [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.983.1/en. - Date of access: 01.04.2015.

21 G.983.2 // ONT management and control interface specification for B-PON. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.983.2 / en. - Date of access: 01.04.2015.

22 G.983.3 // A broadband optical access system with increased service

capability by wavelength allocation. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.983.3/en. - Date of access: 01.04.2015.

23 G.984.1 // Gigabit-capable passive optical networks (GPON): General characteristics. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.984.1 / en. - Date of access: 01.04.2015.

24 G.984.2 // Gigabit-capable Passive Optical Networks (G-PON): Physical Media Dependent (PMD) layer specification. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.984.2/en. - Date of access: 01.04.2015.

25 G.984.3 // Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.984.3/en. - Date of access: 01.04.2015.

26 G.984.4 // Gigabit-capable passive optical networks (G-PON): ONT management and control interface specification. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.984.4/en. - Date of access: 01.04.2015.

27 G.984.5 // Gigabit-capable passive optical networks (G-PON): Enhancement band. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.984.5/en. - Date of access: 01.04.2015.

28 G.984.6 // Gigabit-capable passive optical networks (GPON): Reach extension. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.984.6 / en. - Date of access: 01.04.2015.

29 G.984.7 // Gigabit-capable passive optical networks (GPON): Long reach. [Electronic resource]. - Access: http://www.itu.int/rec/T-REC-G.984.7 / en. - Date of access: 01.04.2015.

30 Portnow, E.L. Principles of construction of the primary network and optical cable lines: a textbook for high schools / E.L. Portnov. - M .: Hotline - Telecom, 2009. - 550 p.

31 Nikolaenko, S.V. Methods for increasing the resistance of quantum communication security protocols: Author. Dis. cand. tehn. Sciences: 05.13.21 / S.V. Nikolaenko; Odessa National Academy of Telecommunications A.S. Popov. " - Odessa, 2013. - 23 p.

32 A method for protecting the information signal against unauthorized access to the fiber-optic communication lines: U.S. Pat. 2254683 Ros. Federation IGC 10/02 H 04V / J.V. Borodakiy, A.Y. Dobrodeev, N.I. Klimov, A.V. Korol'kov, S.V. Dmitriev, A.V. Anoshkin, M.I. Ermokhin, A.A. Osvetimsky; Fed applicant. state. the company "Concern"Systemprom» - № and 2002134015/09; appl. 18.12.2002; publ. 10.07.2004 //Official Bulletin. / Federal Service for Intellectual Property, Patents and Trademarks. - 2005. - №17. - 11 p.

33 A method of protecting information from unauthorized access to the fiber-optic communication lines: US Pat. 2234194 Ros. Federation IPC 04V 10/00 H / S.N. Popov, V.V. Shubin; Ros applicant. Fed. Nuclear Center- All-Russia. sc.-Inst. Institute of Experimental Physics - № 4525936/09; appl. 29.12.1989; publ. 10.08.2004 // Official Bulletin. / Federal Service for Intellectual Property, Patents and Trademarks. - 2004. - №22.- 5p.

34 A method for detecting portions of the optical fiber transmission line with an increased lateral radiation: Pat. 2252405 Ros. Federation IPC G 01M 11/00 / V.V. Shubin; Fed applicant. state. UNITA. Enterprise Ros. Fed. Nuclear Center - All-Russia. sc.-Inst. Institute of Experimental Physics - VNIIEF - № 2003110558/28; appl. 14.04.2003; publ. 20.05.2005 // Official Bulletin. / Federal Service for Intellectual Property, Patents and Trademarks. - 2005. - №14. - 6p.

35 A method of protecting information from unauthorized access to the fiber-optic communication lines: US Pat. 2110894 Ros. Federation IPC 04V 10/00 H / SN Ivchenko, VV Shubin; Ros applicant. Fed. Nuclear Center All-Russian. sc.-Inst. Institute of Experimental Physics, Department Ros. Federation of Atomic Energy - № 95103579/09; appl. 14.03.1995; publ. 05/10/1998 // Official Bulletin. / Federal Service for Intellectual Property, Patents and Trademarks. - 1998. - №13. - 11p.

36 A method for detecting slow extraction of optical radiation through a side surface of the fiber-optic communication lines: US Pat. 2251810 Ros. Federation IPC 04V 10/08 H / V.V. Shubin, S.I. Ovechkin, S.N. Ivchenko; Ros applicant. Fed. Nuclear Center - All-Russia. sc.-Inst. Institute of Experimental Physics - VNIIEF - № 2003101467/09; appl. 20.01.2003; publ. 10.05.2005 // Official Bulletin. / Federal Service for Intellectual Property, Patents and Trademarks. - 2005. - №13.- 7p.

37 Fiber optic transmission system with wavelength-division: a stalemate. 2456748 Ros. Federation, IPC H 04J 14/00 (2006.01) / A.I. Zemlyansky,

V.I. Maslov, A.V. Popov, G.N. Tolstikhin; the applicant State. sc.-Inst. Testing Institute of problems of information protection Fed. service tech. and Export Control - № 2011110404/07; appl. 18.03.2011; publ. 20.07.2012 // Official Bulletin. / Federal Service for Intellectual Property, Patents and Trademarks. - 2012. - №20.

38 Slepov, N.N. Modern technologies of digital fiber-optic networks (ATM, PDH, SDH, SONET and WDM) / NN Blind. - 2nd revised ed. - M .: Radio and Communications, 2003. - 468 p.

39 Information technologies - Generic cabling for customer premises // Individual Recommendations (Direct download or purchase): G Transmission systems and media, digital systems and networks. [Electronic resource]. - Access: http://www.itu.int/pub/T-REC. - Date of access: 04.06.2015.

40 ITU-T Recommendations // ISO / IEC 11801: 2002. [Electronic resource]. - Access: http://www.iso.org/iso/ru/catalogue_detail?csnumber=36491. - Date of access: 04.06.2015.

41 Bulavkin, I.A. Information security networks PON / I.A. Bulavkin // Technology and communications. - 2006. - № 2. - S. 104-108.

42 Bulavkin, I.A. Research and development of the system detect unauthorized connections in passive optical access networks: dis. cand. tehn. Sciences: 05.12.13 / I.A. Bulavkin; Fed. state. UNITA. Enterprise Central sc.-Inst. Inst connection. - Moscow, 2008. - 135 p.

43 MTP 9000A // optical measurement multifunctional device MTP 9000A. [Electronic resource]. - Access: http://www.beliit.com/products.html?id=prod&dev=mtp9000. - Date of access: 03.04.2015.

44 European publication server // Apparatus for detecting tapping of light energy from an optical fiber. [Electronic resource]. - Access: https://data.epo.org/publication- server / document? PN = EP0136271% 20EP% 200 136 271 & iDocId = 6790989 & iPosition

= 0 & iFormat = 0. - Date of access: 04.04.2015.

45 United States Patent // Secure fiber optic data transmission system. [Electronic resource]. - Access: http://patft.uspto.gov/netacgi/nph-

Parser? Sect1 = PTO2 & Sect2 = HITOFF & p = 1 & u =% 2Fnetahtml% 2FPTO% 2Fsearch- bool.html & r = 21 & f = G & l = 50 & co1 = AND & d = PTXT & s1 = 4435850 & OS = 4435850 & R S = 4,435,850. - Date of access: 04.04.2015.

46 Grehov I.V. Avalanche breakdown of the p-n-junction in semiconductors / I.V. grehov, Y.u. Serezhkin. - L .: Energy, 1980. - 152 p.

47 Klyuyev, L.L. Theory of telecommunications: the textbook / L.L. Klyuyev. - Minsk: Tekhnoperspektiva, 2008. - 423 p.

48 Dmitriev, A.L. Optical data transmission systems: the manual / A.L. Dmitriev. - SPb .: SPbGUITMO, 2007. - 96 p.

49 Panfilov, I.P. Theory of telecommunications: a textbook for high schools / I.P. Panfilov, V.E . Dyrda. - M .: Radio and Communications, 1991. - 344 p.

50 Alexeev, T.V. The manual for the course "Theory of electrical communication" / T.V. Alekseev, N.V. Dobatkin. - M .: Moscow Institute of Communications, 1991. - 58 p.

51 Trofimova T.I. The course of physics: a textbook for high schools / T.I. Trofimova. - M .: Higher School, 2003. - 541 p.

52 Gulakov, I.R. The method of counting photons in the optical and physical measurements/ I.R. Gulakov, S.V. Holondyrev. - Minsk: University, 1989. - 256 p.

53 Chen, C.-C. Effect of Detector Dead Time on the Performance of Optical Direct-Detection Communication Links / C.-C. Chen // TDA Process Report. - 1988.
- P. 146-154.

54 Photon counting for quantum key distribution with Peltier cooled InGaAs / InP APDs / D. Stucki [et al.] // Journal of modern optics. - 2001. - Vol. 48№ 13. - P. 1967-1981.

55 The method of determining the quantum efficiency of the photodetector: US Pat. 11775 Rep. Belarus, the IPC (2006) G 01R 31/00 / I.R. Gulakov, A.O. Zenevich; Bel applicant. state. Univ. - № and 20070871; appl. 11.07.07;publ. 30.04.09 // Official Bulletin. / Nat. Center

for intellectual. property. - 2009. - №2. - 6p.

56 Gol'danskii, V.I. Statistics counts for registration of nuclear particles / V.I. Gol'danskii, A.V. Kutsenko, M.I. Pidhirtsi; ed. B.L. Livshits. - M .: State Publishing House of physical and mathematical literature, 1959. - 411 p.

57 A study of single quantum avalanche photodetectors included under the scheme of the active quenching / S.A. Zenevich [et al.] // Reports BSUIR. - 2006. - № 1 (13). - p. 27-31.

58 A study of avalanche photodetectors with a large photosensitive area in the photon counting mode / I.R. Gulakov [et al.] // Instruments and Experimental Techniques. - 2007. - № 2. - p. 112-115.

List of publications of the applicant

1-A Timofeev A.M. Mathematical model of single-quantum optical fiber communication / A.M. Timofeev, Al-Mustafa Doolan Rokan Khalaf Mohammed Jawad Ali Abdulmohsen, E.I. Shulezhko // Information Security Technology: Proceedings of XIII International conference. Belarusian-Russian scientific and engineering. Conf., Minsk, 4-5 June 2015 / Belarus. state. University of Informatics and Radio Electronics; Editorial Board .: L.M. Lynkov [et al.]. - Minsk: BSUIR, 2015. - p. 20.

2-A Timofeev A.M. The bandwidth of fiber-optic communications to transmit confidential information / A.M. Timofeev, Al-Mustafa Doolan Rokan Khalaf Mohammed Jawad Ali Abdulmohsen, V.I. Chvanov, A.P. Chemerko // Modern communications: Proceedings of the XX Intern. scientific and engineering. Conf., Minsk, 14-15 October. 2015 / Executive. state. College of Communication; Editorial Board .: SA Zenevich [et al.]. - Minsk, 2015. - p. 167-168.