Improving the information security of modern telecommunications networks

M.V. Vasylkivsky
Vinnytsia National Technical University
Vinnytsia, Ukraine
mvasylkivskyi@gmail.com

H. L Antonyuk
Vinnytsia National Technical University
Vinnytsia, Ukraine
annaantonuik@gmail.com

O.S. Poludenko
Vinnytsia National Technical University
Vinnytsia, Ukraine
rtt.poludenko@gmail.com

Abstract —**The main characteristics of fiber-optic networks for which you can keep statistics, predict losses in signal propagation by communication lines, establish the presence of unauthorized access to the network are the power of the optical signal at the transmitter output and receiver input, respectively, and bit error rate. Its value is defined as the ratio of error-decoded bits to the total number of bits transmitted. According to the specified characteristics it is possible.**

Existing methods prevent the main methods of ND to optical fiber, but are characterized by low accuracy of establishing the location of unauthorized connection in fiber-optic communication lines. The proposed method of control of fiber-optic communication lines is based on the simultaneous use of hardware and software, which allows to increase the protection of information flows through additional processing of information signals transmitted in fiber-optic communication lines and increase the reliability and accuracy of location unauthorized access to optical channels.

This argument confirms the timeliness and relevance of the scientific and practical problem, the solution of which requires the development of methods and practical provisions for the construction of means of control of unauthorized access in fiber-optic communication lines.

Keywords — bit error rate, fiber optic transmission system, communication line, unauthorized access, tight wavelength sealing, gigabit passive optical network, optical line terminal, optical network device, passive optical network.

I. Introduction

In modern infocommunication networks based on fiber-optic communication lines (FOCL) there is a problem of unauthorized access to the linear path. The analysis of the main existing methods of unauthorized access (UA) in fiber-optic networks has identified the need to develop and implement methods to combat UIA and protect information from unauthorized interception. The research is based on the simultaneous use of hardware and software, which allows to increase the effectiveness of protection of information flows transmitted in fiber-optic communication lines and increase the reliability and accuracy of determining the location of unauthorized access to optical channels. A new method of control of fiber-optic communication lines is proposed, which reflects the relevance of the research topic [1].

Existing methods prevent the main methods of UA to fiber optics, but are characterized by low accuracy of establishing the place of unauthorized connection in the fiber-optic linear paths or the technical complexity of implementation. In works [1, 2] the general description of procedural stages is given, and the basic attention is paid to the mathematical models defining correctness of work of the offered algorithms. At the same time, little attention was paid to the software implementation of algorithms and further generalization of the principles of operation of information security protocols of telecommunication systems and networks.

The aim of the work is to increase the effectiveness of counteracting unauthorized access, development of information security control algorithm in fiber-optic transmission systems due to the proposed software, which operates as part of a combined (hardware-software) method of protection of optical information flows in VOLT.

II. The objectives of the work are: analysis of information security problems of fiber-optic lines and transmission systems; development of information security control algorithm in fiber-optic transmission systems

In [1, 2] a combined hardware and software method of protection of fiber-optic lines and communication systems was developed. Figure 1 shows a generalized structure of a fiber-optic security control device.

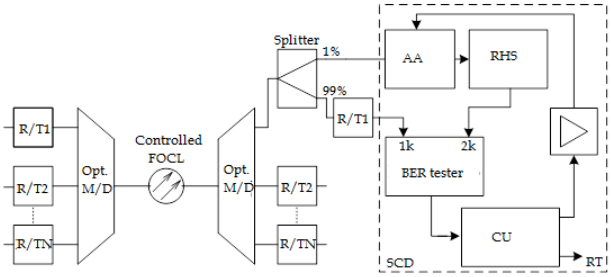


Fig. 1 Generalized structure of the security control device as part of the fiber-optic linear path

The structure uses an optical splitter (OS) in front of the receiver, which divides the input signal: 99%: 1% in order to achieve the threshold power at the input of the optical receiver. Accordingly, when the power in any part of the communication line changes, the power at the receiver's input will decrease, which will cause the receiver to stop receiving this signal, because before this change it was already operating at the sensitivity threshold. When the power level recorded by the high-sensitivity optical receiver is reduced, the result is transmitted to a two-channel BER tester, which simultaneously determines the value of the error rate for two optical channels: working (reference) and controlled. After that, the values of the error rate are sent to the unit for comparison and determination of the difference, which includes a device for comparing the reference values and a device for generating a signal to decide on the presence or absence of unauthorized access. This control device should be used in small networks because the results comparison unit

978-1-6654-0093-0/21/$31.00 ©2021 IEEE

requires periodic manual adjustment (calibration). The advantage of the proposed device is that it provides control of information security of fiber optics in real time. Schematic implementation of the control device is based on serial blocks used in VOSP. The comparison unit consists of a high-speed analog-to-digital converter (ADC), a programmable logic integrated circuit, ie a programmable IC, which are characterized by high speed, higher than a similar version of the circuit on the microcontroller, RAM, ROM and control and display unit.

Figure 2 shows a generalized structure of an adaptive security control device

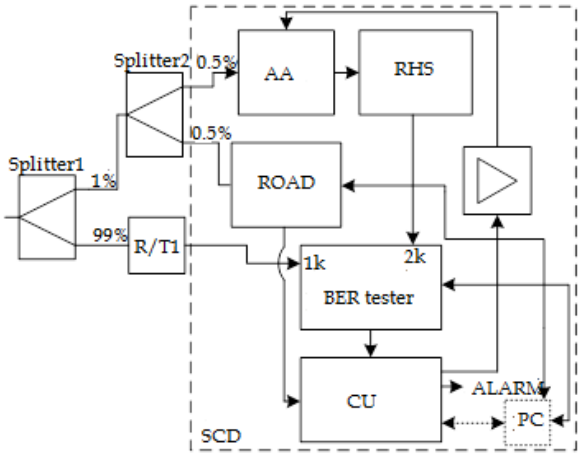


Fig. 2 Generalized structure of the adaptive security control device

For networks that are gradually expanding, or have the prospect of expansion, the use of such a method is irrational, so for such networks with adaptive configuration of the comparison unit, it is necessary to use in the structure (Fig. 2) SCD another OS and power meter optical signals. The use of PC as part of PKZ makes it possible to build an adaptive means of security control (SCD) [1].

As a result, we see that the embodiment shown in Figure 1 is hardware, and the variant shown in Figure 2 is hardware and software. To simplify the hardware, additional software is used, which will operate according to the algorithm, the block diagram of which is shown in Figure 3.

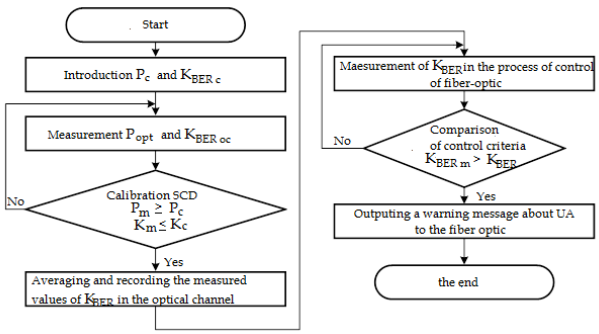


Fig. 3 Block diagram of the algorithm of the program for monitoring the security of fiber-optic communication lines

At the first stage the required threshold power and the corresponding error rate at such power are set. Next, the unit that checks the correctness of the received data by measuring the actual signal strength and error rate, in case of incorrect calibration causes the repetition of the cycle of actions. Then the results are recorded in the program, and cyclic measurement of the error rate through the power parameter and verification with the recorded average data begins. In case of discrepancies, a notification is generated and the transmission is stopped. In [4] the part of the program code of the fiber optic simulator with the establishment of the presence of unauthorized access, which is implemented in this algorithm, is given.

There are also similar options to those listed above, for example, the use of complex codes, armored cables or other types of cables that do not provide full protection [1, 3].

The research is of scientific novelty, as the problem of information security today, at a time when globalization is developing rapidly and information is becoming one of the most important aspects of modern life, when countries can wage hybrid wars in which information becomes a weapon whose use can have devastating consequences. It is obvious that the protection of structurally complex information and communication technologies should come to the fore before the introduction of such systems into operation, along with increasing the protection of information and its confidentiality for existing systems.

The software is universal, so it can be used by both ordinary users and large enterprises on an industrial scale. The main competitive advantage of this product is: high sensitivity due to the use of arsenide-indium-gallium photodiodes, which allows to ensure high reliability and low cost; high speed due to the use of packages of short length. According to other indicators, the development will not lose to analogues in the market [3-5].

III. EVALUATION OF INFORMATION PROTECTION OF FIBER-OPTICAL COMMUNICATION LINES ACCORDING TO ERROR COEFFICIENT CRITERIA

To ensure the set BER value at the output of the optical receiver, it is necessary that the input power of the optical signal at its input is greater than the minimum optical power, ie the sensitivity of the receiver. Recommendations ITU-T G.691, G.692, G.659.1, indicate that the calculated rate of bit error rate (BAC) for the area of optical amplification is not more This coefficient depends on the Q-factor and is calculated by the formula:

$$BER = \frac{1}{2} erfc\left(\frac{Q}{\sqrt{2}}\right), \quad (1)$$

where the additional error function is defined as:

$$erfc(x) = \frac{2}{\sqrt{\pi}} \cdot \int_{x}^{\infty} e^{-x^2} dx. \quad (2)$$

OPC $BER = 10^{-12}$ corresponds to the value $Q \approx 7$. [4], formula (3) was given, which associates the threshold value Q_{tv} with the minimum (threshold) power P_{tp} at the input of the optical receiver, at which you can provide the required OPC:

$$P_{tp} = \left(Q_{tv} / S_i\right) \cdot \left(4kT \cdot F_a \cdot f_s / R_f\right), \quad (3)$$

Where S_i – current (monochromatic) sensitivity of the optoelectronic converter (photodiode); ;

$k = 1,38 \cdot 10^{-23}$ (Дж/град) – became Boltzmann;

T – absolute temperature, K;

F_a – amplifier noise figure ;

$f_s = f_m$ – signal clock frequency ;

$R_f \approx \left(2\pi \cdot f_в \cdot C_{зз}\right)^{-1}$ – resistance of the resistor in the feedback circuit

$$20 \lg Q_{tv} = 4,63 + 11,42 \lg\left[\lg\left(BER^{-1}\right)\right], \qquad (4)$$

From expression (3) it is seen that the OPC is directly related to the sensitivity of the receiver through the parameter of the Q-factor. Thus, a change in input power leads to a change in the Q-factor and vice versa, which in turn changes the OPU. To find the threshold value of the Q-factor, ie the required value of the signal / noise, the expression [4] is used:

$20 \lg Q_{tv}$ – signal/noise value, dB

Expression (4) does not take into account the margin of noise protection In the future, replace the notation with (1…4dB). Since the OPC is the output characteristic of the receiver, and the ratio S/N of the input and output characteristics of the fiber optic, then to estimate the change in the OPC it is necessary to obtain the appropriate expression that will link the change of the output parameter according to the input change:

$$BER = \frac{1}{10^{\frac{S/N - 4,63}{11,42}}}. \qquad (5)$$

Introducing $10^{\frac{S/N-4,63}{11,42}}$ as A, expression (5) can be written as:

$$BER = \frac{1}{10^{A}}.$$

In [5] the algorithm of control of information security of fiber-optic line by cyclic measurement of BKP is offered. This analysis can be performed on the basis of the obtained expression. We construct a graph of the dependence of the BKP on the value of the signal / noise at the input of the optical receiver, taking into account (5) and a graph of the dependence of the BKP on the Q-factor.

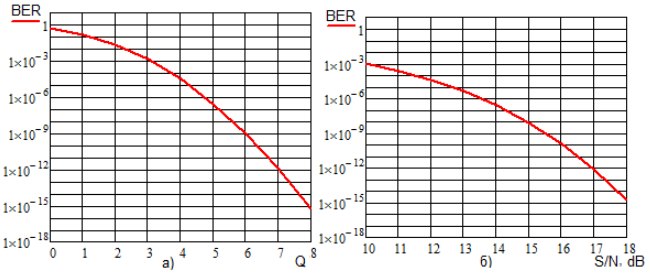


Fig. 1 Dependence of OPC: a) on the Q-factor; b) from the S / N ratio

From expression (3) we see that the threshold sensitivity of the receiver depends on the specified OPC, current sensitivity of the receiver, the natural noise of the amplifier and frequency. Comparing the graphs in Fig. 1, it can be concluded that the proposed formula correctly reflects the dependence of the change in the OPC on the change in the signal-to-noise ratio at the input of the optical receiver. Therefore, the obtained graphs can be used to determine the dynamic range of signal power in the fiber-optic linear path (VOLT).

To evaluate the change in the energy parameters of the receiver, we assume that the amplifier's own noise is absent and a photodiode *p-i-n* with the value [6] is used.

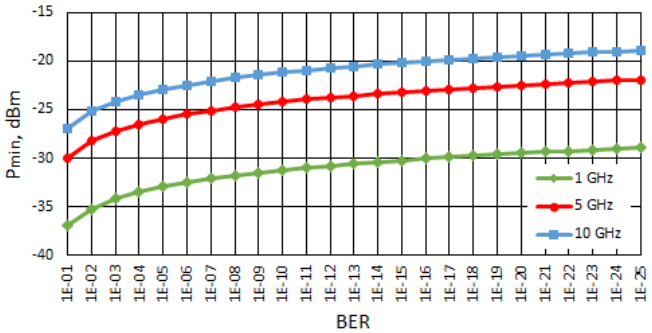


Fig. 2. Dependence of the minimum power of the receiver on the OPC at different frequencies

In SONET / SDH infocommunication protocols, it is necessary that when using a long pseudo-random sequence of binary characters (bits) the number of errors was not more than 1×10^{-10} bits. In digital data protocols such as Ethernet when using short packets, the bit *BER* should be greater 10^{-12}.

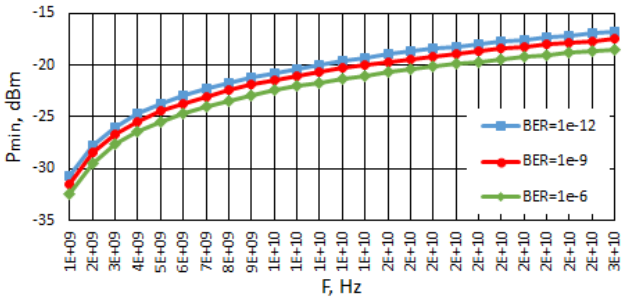


Fig. 3 Dependence of the minimum power of the receiver on the frequency at different values of the OPC

The data transfer rate is related to the frequency band (Δf), so in the real conditions of the DSP operation, it is necessary to determine the required testing time of the system, which works flawlessly. Statistical methods have shown that to achieve a level of 95% test reliability, you need to form a sequence of symbols that will be three times the inverse of the BER, that is $1/BER^n$

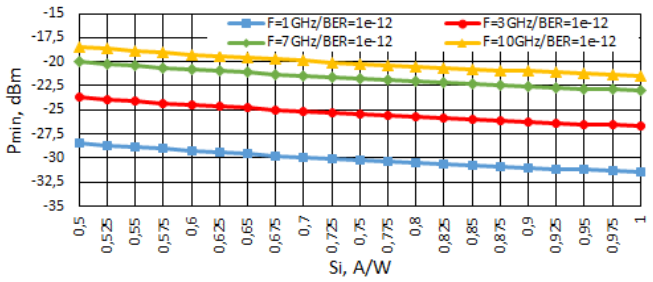


Fig. 4 The dependence of the minimum power of the receiver on the current sensitivity at different frequencies at the OP = 10^{-12}

High efficiency of BCP assessment tools is based on a number of the following principles of construction: functionality, integration into the system, increasing functional complexity, system approach and optimization. System approach and optimization are the main principles of construction of BCP assessment tools. The system approach involves the construction of the device at the highest level of the structural hierarchy, taking into account the results of construction at lower levels. The optimal synthesis of the BKP estimation device consists in the developed schemes that provide the maximum dynamic range and resolution, as well as high stability of the BKP estimates in a given frequency band.

The results of an experimental study of the means of estimating the OP in telecommunication systems, which confirmed the correctness of the obtained expressions for determining the energy characteristics of fiber optics.

IV. CONCLUSIONS

After analyzing the state of development and the pace of implementation of fiber-optic transmission systems to create Internet coverage, one of the issues is information security, namely the security of data of end users of telecommunications services.

The review of the main types of hardware and software protection of fiber optics showed a number of objective shortcomings of the existing methods and created the preconditions for the use of combined means of information protection in VOSP. An analysis of the parameters that affect the protection of OB and OS, and found that their protection against ND is the use of such methods of modulation and / or coding, which should differ from the main methods in order to complicate the process of decoding signals by an attacker. allow the latter to perform actions that would allow him to obtain the transmitted information. Accordingly, it is concluded that all of them do not provide a 100% security guarantee, but only slightly complicate the process of direct access to OB and information transmitted through it, so it is necessary to develop means of protection of local fiber-optic communication lines and means for detection and exclusion of unauthorized access.

The mathematical bases of ND to fiber-optic methods were analyzed. Graphs of the dependence of the attenuation of the optical signal on the magnitude of the difference in the diameters of the cores of optical fibers, the dependence of the attenuation of the optical signal on the magnitude of the difference in the diameters of the cores of optical fibers. Next, it was found out what physical processes occur when an attacker performs unauthorized access (connection). Calculations were performed to determine the value of the threshold for registration of input optical signals by an unauthorized receiver. According to the research, an expression was obtained that characterizes the dependence of the change in the probability of error (BCP) on the change in the signal-to-noise ratio taking into account the noise, on the basis of which the plot of the BCP dependence on the signal-to-noise ratio was constructed. A graph of the dependence of the minimum power of the receiver on the OPC at different frequencies, a graph of the dependence of the minimum power on the frequency at different values of the OPC, a graph of the dependence of the minimum power on the current sensitivity at different frequencies. Next, an expression was obtained that relates the probability of false positives (which is equal to the probability of skipping the ND), the amount of optical power allocated in the ND, as well as the amount of information loss in the detection of ND. The next step was to develop generalized structures of fiber-optic security control devices. The developed version of the method minimizes the possibility of unauthorized connections to the network and allows to detect attempts to implement passive attacks, known as "sniffing", on the access network. The use of a computer makes it possible to analyze and predict possible changes in the power of optical signals and to establish the location of the sun with the help of reflectometers that can operate when controlled from a PC according to the proposed algorithm.

The developed algorithm of operation of the control means is represented according to the mathematical model. Therefore, the tasks are set, namely: to protect fiber optics it is necessary to use combined hardware and software protection; the implementation of such means must be either at the transmitting or receiving end; the operation of such equipment must not create time delays in the operation of the communication line; the designed equipment should not contain a large number of elements in its composition; safeguards should be able to monitor and provide a high level of protection - have been addressed.

The social impact of the application of this study may be to increase confidentiality, meeting the needs of a particular person. Research documentation can be developed by design engineers and managers in a short period of time.

Enterprises are interested in this development, the main direction of which is to provide the population with infocommunication services, because this tool plays a significant role in their activities.

Thus, the tasks are set, namely: analysis of information security problems of fiber-optic lines and transmission systems; development of information security control algorithms in fiber-optic transmission systems and networks; cost-effectiveness analysis was solved.

REFERENCES

[1] M.V. Vasylkivsky Protection of information in fiber-optic communication systems / M.V Vasylkivsky, R.P Palamarchuk // Visnyk of Khmelnytsky National University. "Technical Sciences" series. - 2018. - №3. - P. 202-207.

[2] M.V. Vasylkivsky Estimation of energy characteristics of fiber-optic communication lines by the criterion of error rate / M.V Vasylkivsky, R.P Palamarchuk // Visnyk of Khmelnytsky National University. "Technical Sciences" series. - 2019. - №1. - P. 216-219. DOI 10.31891 / 2307-5732-2019-269-1-209-212.

[3] M.V., Vasylkivsky, R.P. Palamarchuk Protection of information in fiber-optic communication lines: materials of the XVIII International. scientific and technical conference "Measuring and computing

equipment in technological processes", (Odessa, June 8-13, 2018) / Odessa. nat. acad. communication O.S. Popova. - Odessa, 2018. - P. 209-211.

[4] M.V. Vasylkivsky, R.P Palamarchuk Algorithm for emergency termination of transmission in optical networks with unauthorized connection: materials III Vseuk. scientific and technical conference "Computer technology: innovation, problem solving", (Zhytomyr, November 26-27, 2020) / Gos. univ. Zhytomyr Polytechnic. - Zhytomyr, 2020. - P. 200-202.

[5] M.V. Vasylkivsky., R.P Palamarchuk Algorithm for emergency stop of information transmission in optical networks with unauthorized connection: materials of the XIV International. scientific-practical Conf. undergraduate and graduate students "Theoretical and practical research of young scientists", (Kharkiv, December 1-04, 2020) / Nat. univ. Kharkiv Polytechnic Institute. - Kharkiv, 2020. - P. 150-152.

[6] H.L Antonyuk. High-speed optical access networks / M..V. Vasilkovsky, H..L. Antoniuk, O.S Poludenko, K.O. Blacksmith. - Measuring and computing equipment in technological processes. - 2017, №2. - with. 57-62.

[7] H.L Antonyuk. Methods of construction of high-speed fiber-optic tracts / M.V. Vasilkovsky, H.L. Antoniuk, O.S Poludenko // Measuring and computing equipment in technological processes (VOTTP_17_2017) XVII International Scientific and Technical Conference, June 8-13, 2017 - Materials - Odessa. - 2017 p. 187.