UDC 621.391.052
DOI https://doi.org/10.32782/2663-5941/2024.4/07

Manko O.O.
Kyiv Professional College of Communications

Kharlai L.O.
Kyiv Professional College of Communications

Konovalov O.Yu.
Kyiv Professional College of Communications

Nikiforenko K.B.
Kyiv Professional College of Communications

Sotnichenko Yu.O.
Kyiv Professional College of Communications

Vakas V.I.
Kyiv PJS"Kyivstar"

INCREASING THE EFFICIENCY OF OPTICAL CRYPTOGRAPHY USING PASSIVE OPTICAL ELEMENTS

In the proposed article, a new method of protecting information flows transmitted over optical communication lines is investigated. It is based on the formation of special linear codes with an increased number of units. At the same time, passive optical elements are used to form linear codes and perform reverse operations, namely: fiber splitters and delay lines for a certain part of the clock interval. The use of a special line code significantly increases the level of information protection during unauthorized access to line structures, namely to an optical cable. At the same time, when using a fixed type of code, there is a danger of its interception during unauthorized access and subsequent analysis with the creation of appropriate decryption measures. Taking this into account, the paper proposes a regular change of linear codes according to a pseudo-random law. At the same time, such active devices as optical switches are used. The structural construction of the devices included in the linear optical path, and which are necessary for switching the types of codes used, with the determination of the connections between passive and active equipment, is provided. As the main codes on the basis of which linear codes are formed, the use of RZ optical codes (with a return to zero) is proposed. In order to increase the effectiveness of the protection level, the article proposes dynamic switching of the generated linear codes. Thus, the basis for the operation of the proposed method is fast switching according to the pseudo-random law of linear codes generated according to a special algorithm using optical elements that have a high switching speed. In this work, the use of three types of codes is proposed. The receiving equipment is also built on the decoding of the generated types of codes at the expense of exclusively passive elements and devices. When switching the transmitting device to another type of code, the corresponding inputs of the receiving equipment are connected to the output of the linear path. Given the high speed of switching and the pseudo-random law of switching in time, adequate perception of information when using three types of codes becomes practically impossible.

Key words: *optical fiber, unauthorized access, information protection, optical splitter, optical switch, optical delay line.*

Introduction. Currently, the amount of confidential information transmitted over optical communication networks is constantly growing. This necessitates the protection of such an important infrastructure as a computer optical communications network from unauthorized access, especially at the level of linear structures, most of which are located outdoors.

Fiber-optic communication lines, due to the characteristics of the distribution of electromagnetic energy in the optical fiber, have increased protection against access to information transmitted along the linear tract [1]. However, there are situations in which access to information becomes possible, and this leads to the need to develop measures to counter such attempts.

The protective sheath, the armor cover and other structural elements of the optical cable (OC) so strongly weaken the possible radiation outside the optical fiber (OF) that it practically does not penetrate the limits of the sheath. Consequently, information interception can only occur due to a violation of the integrity of the outer sheath and other cable sheaths in order to directly access the interception equipment to optical fibers. But even in this situation, without additional effects on the fiber, the interception of the optical signal is impossible, since there is practically no radiation outside the optical fiber.

In order to provide radiation outside the optical fiber in this situation, a bending of the OF is formed. In the place of such bending the law of full internal reflection is violated and radiation of energy of a light signal outside of OF is observed [2]. Because of this, at the point of interception of information, the fiber is characterized by an increased level of losses [1], which can be determined by optical reflectometry [3], or by increasing the error rate in the line. In this case, from the moment of removal of information to the moment of detection of unauthorized connection, some time passes, which depends on the principles of monitoring the line and equipment used for control. If specialized high-sensitivity equipment is used to record information, the radiation at the bend of the OF required for its operation may be quite insignificant. In this case, it is not easy to establish the fact and determine the place of connection with the help of line control equipment. There is a method of determining the moment and place of violation of the armor of the cable in the process of unauthorized connection to the line [4,5], but it allows you to provide supervision at relatively short distances from the point of the control.

There is a method for determining the moment of unauthorized access to optical linear closures along the entire length of the regeneration section [5]. This allows you to accurately determine the location of the optical closure and the moment of access, but the linear structures between the optical closures go unnoticed. Thus, in order to prevent unauthorized access to information flows on optical lines, it is necessary, along with methods for determining the presence of access, to apply additional methods that make it impossible to adequately interpret the information during the fact of access. For this, the use of continuous additional coding (masking) of optical linear codes of the RZ type using passive optical devices was proposed in [6].

Formation of linear codes using passive elements. At this time on optical communication networks there is a use of a linear code type RZ (return to zero) [6, 7]. The main difference of this code is that the value of the signal corresponding to the transmission of a single symbol is returned to zero before the end of the clock interval. The code type with a return to zero on half of the clock interval T is denoted as RZ-0.50, and on the quarter of the clock interval is denoted as RZ-0.25. The type of code, the duration of a single character of which is the full clock interval T, is denoted as NRZ (without returning to zero).

Studies show that when using the optical transmission system of the linear code RZ-0.25, it is possible, using only passive optical elements such as optical delay lines and optical splitters (dividers), to perform additional coding (masking) of the signal at the input of the tract to protect the information that is transmitted along a linear tract.

Fig.1 shows the method of masking the optical signal in order to protect it from unauthorized access to the linear tract and its subsequent decoding at the receiving end. The figure shows the time diagrams of the code combination during the passage of certain points of the optical linear tract. Here as I the designation of the intensity of the optical signal is given. Fig. 2 shows the construction of a linear tract using this principle. As can be seen from the figure, the output signal of the transmission system, which is also the input signal for the linear tract, based on the code RZ-0.25, and denoted as $I_{\text{in RZ-0.25}}$, is connected to the optical splitter (OD_1). The optical splitter (divider) works as an optical power divider in half. Then, to the inputs of the second divider (OD_2), operating in the adder mode, connects the part of the signal that has passed through the optical delay line (ODL_1) with a delay time T/2 ($I_{\text{out ODL (T/2)}}$) and the undelayed part of the signal. As a result, at the output of the second divider code combinations are formed that differ from the original by twice the number of units (I_Σ), which are transmitted on a linear tract. At the output of the linear tract, the optical power divider (OD_3) is turned on as an optical power divider in half. In this case, to the second divider (OD_4), operating in the adder mode, is fed an undelayed part of the signal I_Σ, and part of the signal that has passed through the delay line (ODL_2) with a delay time T/4 ($I_{\text{out ODL (T/4)}}$). After assembling these parts, an optical signal corresponding to the original is formed in the NRZ code ($I_{\Sigma\text{out NRZ}}$).

The double number of units in the optical linear tract during transmission makes it impossible to adequately recover the signal when trying to gain unauthorized access to information. This ensures the protection of the transmitted information.

The proposed method can be developed and improved, and extended to other types of RZ code. For example, Fig. 3 shows a method of masking linear code combinations of an optical signal in order to protect it from unauthorized access to the linear tract and its subsequent decoding at the receiving end using the optical code RZ-0.125 [6]. Fig. 4 shows the construction of a linear tract using this principle. The construction of the linear tract in this case contains one degree of optical delay more than in the previous case.

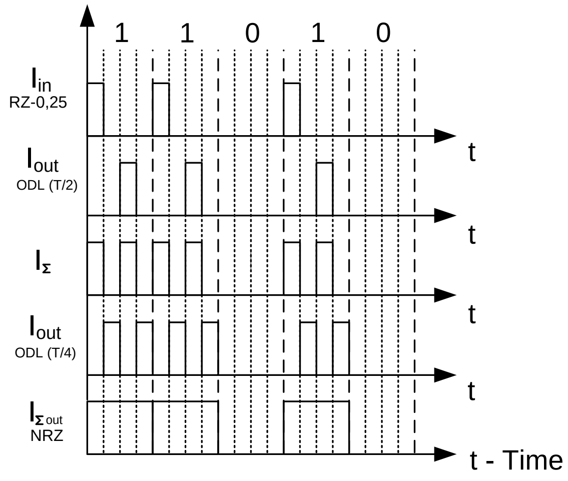
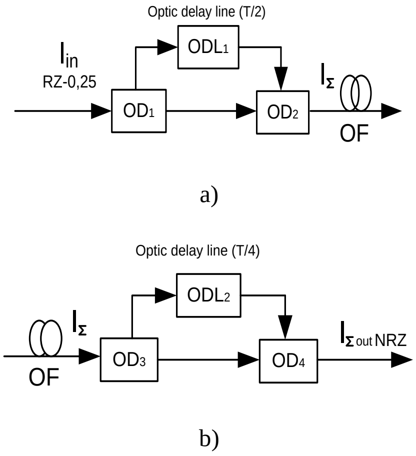


Fig. 1. Method of forming a linear code for the optical signal in the code RZ-0.25 when transmitting it on a linear tract and restoring the output signal in the NRZ code. I – is the designation of the intensity of the optical signal



a)

b)

Fig. 2. Construction of a linear tract using linear encoding and decoding of the optical signal in the code RZ-0.25 using passive elements. Here a – is the transmitting part; b – is the receiving part

An optical signal (code combination) using the code RZ-0.125 and denoted as $I_{\text{in RZ-0.125}}$, is fed to the divider (OD_1). The optical divider works as an optical power divider in half. After that one part of signal is fed to the delay line ODL_1 with a delay time of a quarter of the clock interval T/4 ($I_{\text{out ODL1 (T/4)}}$). The second part of the signal propagates without delay. Then the both components of the signal are added, and at the output of the optical splitter in the adder mode (OD_2) a code signal with twice the number of units ($I_{\Sigma 1}$) is formed. This signal is fed to the splitter OD_3. One of the components after leaving the divider passes through the optical delay line ODL_2 (delay time T/2, and on the output of the line ODL_2 signal is denoted as $I_{\text{out ODL2 (T/2)}}$) and adds with the undelayed part in the adder OD_4. The number of units after such a forming process in the linear code combination will be four times greater than in the original. The generated and protected signal $I_{\Sigma 2}$ from the output OD_4 is fed to the linear tract. At the output of the linear tract, the signal is fed to the optical splitter OD_5 which divides it into two components.

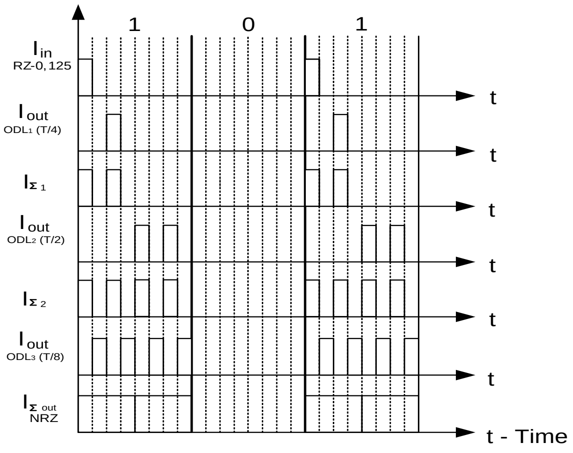


Fig. 3. Method of forming a linear code for the optical signal in the code RZ-0.125 when transmitting it on a linear tract and restoring the output signal in the NRZ code. I – is the designation of the intensity of the optical signal

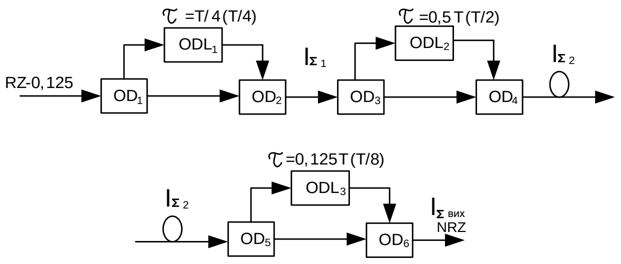


Fig. 4. Construction of a linear tract using linear encoding and decoding of the optical signal in the code RZ-0.125 using passive elements

One of these parts passes through the optical delay line ODL_3 (delay time T/8, and on the output of the line ODL_3 signal is denoted as $I_{\text{out ODL3 (T/8)}}$) and is added to the undelayed part of the code combination in the optical adder OD_6. In this case, an optical signal is generated at the output of OD_6, with code combinations that are adequate to the initial code combinations, only in the NRZ code ($I_{\Sigma out\ NRZ}$). This method can be generalized for the code RZ-($1/2^{n+1}$), where n is a positive integer. Cases when n = 1 and n = 2 were discussed above. Construction of a linear tract with increasing number n will be performed at the receiving end as the connection of a number of elements that perform the division of the signal in half, the delay of one of the components to the corresponding part of the clock interval and their subsequent assembly. At the receiving end, the function of translating the linear code into the NRZ code will be performed by the same elements using the optical delay line for time $T/2^{n+1}$. The number of units in the code combinations of the optical linear tract will be 2^n times greater than in the original combinations.

The use of fairly inexpensive passive optical elements to mask optical linear codes significantly increases the reliability of the information protection process, compared with the use of active equipment.

Dynamic protection of information on computers optical networks. Given the fact that unauthorized access systems can be adapted to a certain fixed variant of linear codes, the paper proposes a dynamic system for switching variants of linear codes under a pseudo-random law. The block diagram of such a device is shown in Fig. 5. In this case, two systems of forming linear code combinations are used, which are switched according under pseudo-random law. To this end, the paper proposes to use two systems for generating linear codes based on input codes (e.g. RZ-0.25, RZ-0.125), as shown in Fig. 5. In this case, two types of linear code generator (LCG) operate on the transmitting end, forming code combinations based on signals from the transmission system in the codes RZ-0.25 and RZ-0.125, respectively.

The linear tract receives signals in the selected code in accordance with the control signals from the generator of pseudo-random time intervals (PRTG).

The signal from the outputs 1, 2 of the PRTG generator is fed to the control input of the optical switches OS_1 and OS_2, operating in key mode. In this case, a linear code generator is selected for forming linear code combinations. The output signal PRTG from output 3 is supplied to the transmission system to generate a pilot signal when the linear code changes. Considering the fact that the signals at the outputs of the LCG generators must be mutually inverted – the corresponding information signal is received at the input of only one of the linear code generators (LCG_1 or LCG_2). After the formation of the linear code combination, it enters the optical divider OD_1, which operates in the mode of combining signals, and then enters the optical linear tract. At the receiving end, a linear code combination is supplied to the optical divider OD_2 and to the inputs of the optical switches OS_3 and OS_4 operating in key mode.

The control inputs of the switches receive a signal from the control device (CD), which is formed at the receiving end according to the pilot signal from the transmitting end. The signal from the CD provides the passage of a linear signal to the corresponding code generator NRZ ($CGNRZ_{1,2}$) and the subsequent passage of the code in NRZ format through the optical splitter OD_3, operating in the mode of combining signals, to the input of the optical receiver. Thus, the proposed solution further protects information flows from unauthorized access at the level of linear optical computer communication structures.

The construction of protection is complicated by the appearance of additional elements. The switching speed of linear code variants is determined by the switching time of optical switches, among which should be noted switches based on the Mach-Zender interferometer (MZI) and electro-optical switches (EOS) [8].

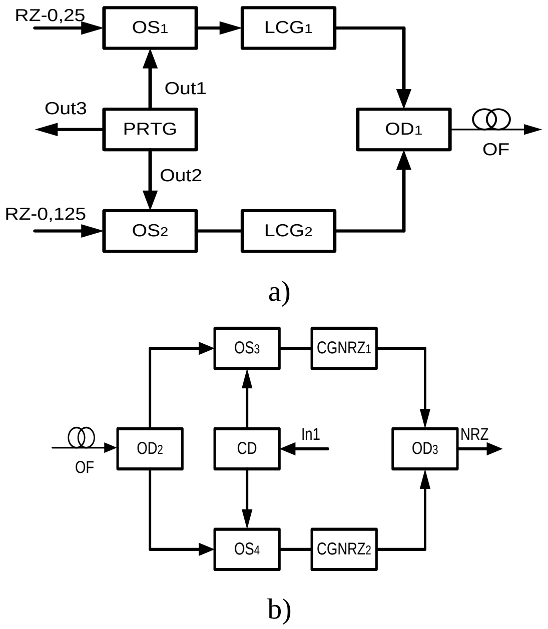


Fig. 5. Construction of a linear tract that uses dynamic information protection. Here a – is the transmitting part; b – is the receiving part

The switch based on the MZI is built on the basis of two series-connected optical splitters (branch factor 3 dB), which are interconnected by two optical waveguides of different optical lengths to create a phase difference at the output of II by changing the voltage U applied to one of shoulders of the interferometer Fig. 6.

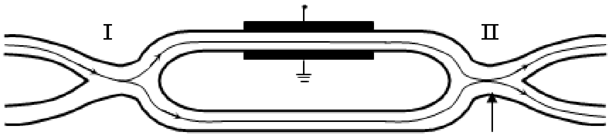


Fig. 6. Switch based on the Mach – Zender interferometer

Due to the fact that the optical waveguide to which the electric field is applied is made of an electro-optical material, such as lithium niobate ($LiNbO_3$), its refractive index changes with voltage. This changes the phase difference between the signals coming to the output II and there is a redistribution of signal power between the outputs of the interferometer so that it can be directed completely to one of the two outputs of the interferometer. When using only one output, the switch can operate in key mode.

Electro-optical switches also use directional couplers to generate light flux at one of the output ports. But this is done by changing the coupling factor between the optical waveguides. The coupling factor is changed by changing the refractive index of the splitter material in the optical coupling zone.

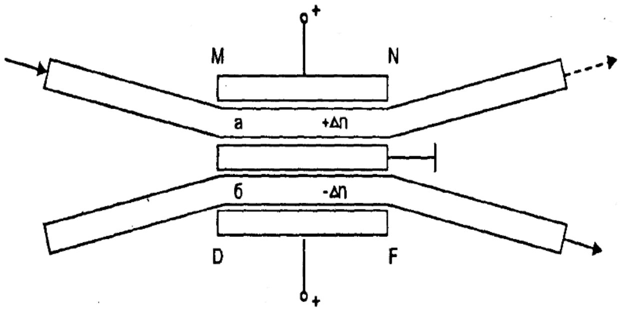


Fig. 7. Switch based on a directional splitter X – type.

Optical waveguides a and b in sections MN and DF are made of electro-optical material. Transparent electrodes are available on the outside between the optical waveguides. Due to the applied voltage, the refractive indices of optical waveguides can be changed. The division factor of the splitter also changes as a result. Electro-optical switches have a great advantage, which is manifested in the switching time, which reaches a value of the order of 10–100 ps, and it is manifested in small values of control voltages – 2.5–3 V. The advantage of electro-optical switches is also the ability to be made in integral-optical form.

Thus, the use of passive (splitters and delay lines) and active elements (switches) allows to create effective principles of dynamic protection of information on the linear structures of computer optical networks. These principles combine both the formation of a number of types of protected linear codes and their regular rapid switching at random times. This significantly increases the level of protection, as it makes it virtually impossible to adequately and timely track and identify a specific type of code in real time.

If it is necessary to increase the level of protection, you can use the code RZ-0.0625 and the corresponding line code generator in addition to the input codes RZ-0.25 and RZ-0.125.

Increasing the level of protection of optical computer networks. Protection of optical paths based on codes RZ-0.25, RZ-0.125 was discussed above [9]. The work also considered a way to improve the level of security of optical computer networks based on the codes RZ-0.25 and RZ-0.125 mentioned above, by adding an additional channel using the code RZ-0.0625.

The diagram for constructing a code converter RZ-0.0625 into a linear code is shown in Fig. 8. It contains 4 optical splitters/combiners – $OD_{1\text{-}4}$ and 4 optical delay lines – $ODL_{1\text{-}4}$.

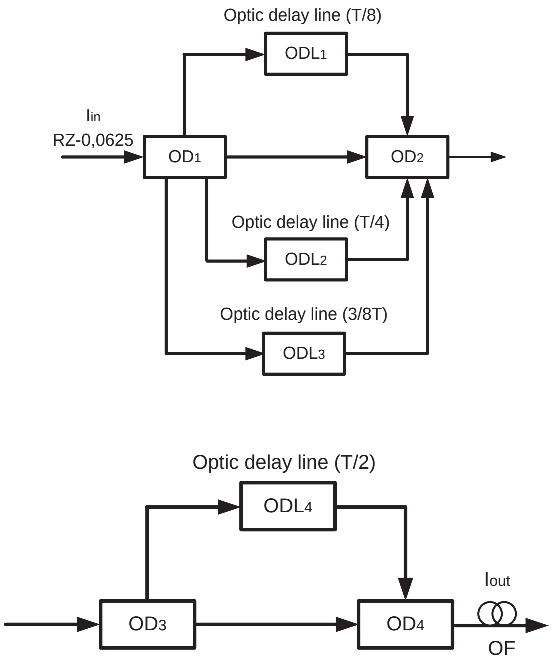


Fig. 8. Building RZ-0.0625 code converter to linear code

The type of signal at the output of the converter (input to the line) is shown in Fig. 9.

A general view of the linear tract that provides signal transmission using three protected channels (codes RZ-0.25, RZ-0.125, RZ-0.0625) is shown in Fig. 10.

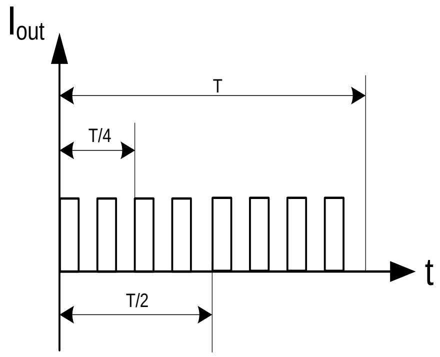
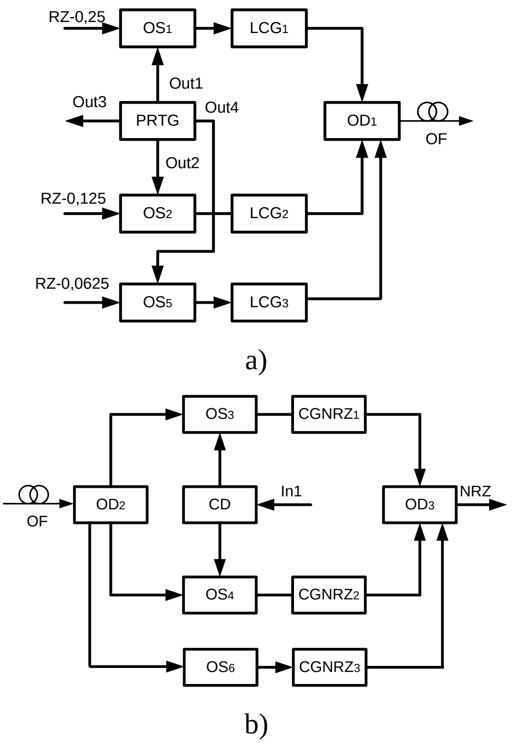


Fig. 9. Signal type at the output of the converter (input to the line)



a)

b)

Fig. 10. General view of the linear path for transmitting three secure channels (codes RZ-0.25, RZ-0.125, RZ-0.0625). Here a – is the transmitting part; b – is the receiving part

The additional advantage of a 3-channel system compared to a 2-channel system is the reduction in the probability of determining the working channel after switching.

Conclusions. The proposed new method of dynamic protection of information on the linear structures of computer optical networks, allows increasing the security of these networks from unauthorized access. The main advantage of the method is the fast switching according to the pseudo-random law of a number of linear codes generated by a special algorithm using exclusively passive optical elements. The number of units in linear code combinations can significantly exceed the number of units of the main code. Due to this, adequate perception of the main code becomes impossible. However, in the case of constant use of a certain type of linear code, it is possible, as a result of analysis, to take measures to its adequate perception. In order to prevent such a situation, the paper proposes a dynamic principle of protection, which consists in the rapid switching of types of linear codes according to the pseudo-random law. Given the high switching speed, and the pseudo-random law of switching in time, adequate perception of information becomes almost impossible.

An additional advantage of the method is the ability to perform all the elements it includes in an integral-optical form.

Bibliography:

1. Каток В.Б. Волоконно-оптичний зв’язок: [для інж.-техн. працівників, студентів-зв'язківців] /В.Б. Каток, І.Е. Руденко, Є.Г. Ранський, П.М. Однорог; ПАТ "Укртелеком". – Київ : Логос, 2015. – 380 с.

2. Optical Fiber Telecommunications, Vol. IV A,B, ed. By I.P. Kaminov and Li Tingye, Academic Press, 2002, 1022 p.

3. Beller J., OTDRs and Backscatter Mesurement, Ch. 11, Ed. Dericson D., Prentice Hall PRT, 1998.

4. Mahlke G., Gossing P. Fiber Optic Cables, Munich: Corning Cable Systems, *MCD Corporate Publishing,* 2001. – 304 p. ISBN 3-89578-162-2

5. Манько О.О. Захист лінійних споруд ВОЛЗ від несанкціонованого доступу з використанням металевих елементів оптичного кабелю Сучасний захист інформації. – 2012. – № 3. – С. 84–86.

6. Manko O. O. Using Passive Optical Devices for the Protection of Information in the Optical Communication Lines, in Proc. Third International Scientific-Practical Conference Problems of Infocommunications. *Science and Technology* (PIC S&T`2016), October 4-6, 2016, Kharkiv, Ukraine, pp. 73–74.

7. Optical fibres, cables and systems. ITU-T Manual, 2009. – 302 p. Printed in Switzerland, Geneva, 2009.

8. Корнійчук В.І., Мосорін П.Д. Волоконно-оптичні компоненти, системи передачі та мережі. – Одеса: Друк, 2001. – 354 с.: іл.

9. Kharlai Liudmila, Kunakh Nataliya, Sotnichenko Yulia, Konovalov Oleksiy, Skubak Olexandr, Manko Oleksandr. Dynamic Information Protection Method on Computer Optical Networks, International Journal of Advanced Trends in Computer Science and Engineering. 2020/Vol. 9, #3, May – June. pp. 3666–3670.

Манько О.О., Харлай Л.О., Нікіфоренко К.Б., Коновалов О.Ю., Сотніченко Ю.О., Вакась В.І.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОПТИЧНОЇ КРИПТОГРАФІЇ З ВИКОРИСТАННЯМ ПАСИВНИХ ОПТИЧНИХ ЕЛЕМЕНТІВ

В запропонованій статті досліджено новий метод захисту інформаційних потоків, які передаються по лініям оптичного зв'язку. Він заснований на формуванні спеціальних лінійних кодів зі збільшеною кількістю одиниць. При цьому, для формування лінійних кодів та виконання зворотних операцій застосовуються пасивні оптичні елементи, а саме: волоконні розгалужувачі та лінії затримки на певну частину тактового інтервалу. Застосування спеціального лінійного коду значно підвищує рівень захисту інформації під час несанкціонованого доступу до лінійних споруд, а саме до оптичного кабелю. В той же час, при застосуванні фіксованого типу коду з'являється небезпека його перехоплення під час несанкціонованого доступу та наступного аналізу зі створенням відповідних заходів щодо дешифрування. Беручи це до уваги, в роботі запропоновано регулярну зміну лінійних кодів за псевдовипадковим законом. При цьому застосовуються такі активні пристрої, як оптичні комутатори. Надано структурну побудову пристроїв, що входять в склад лінійного оптичного тракту, і які є необхідними для переключення типів кодів, що застосовуються, з визначенням зв'язків між пасивним та активним обладнанням. В якості основних кодів, на базі яких формуються лінійні коди, запропоновано застосування оптичних кодів RZ (з поверненням до нуля). З метою підвищення ефективності рівня захисту в статті пропонуються динамічні переключення сформованих лінійних кодів. Таким чином, основою для функціонування запропонованого методу є швидке перемикання за псевдовипадковим законом лінійних кодів, що генеруються за спеціальним алгоритмом з використанням оптичних елементів, які мають високу швидкість переключення. В даній роботі запропоновано використання трьох типів кодів. Приймальне обладнання також побудоване на декодуванні сформованих типів кодів за рахунок виключно пасивних елементів та пристроїв. При перемиканні передавального пристрою на інший тип коду відбувається підключення до виходу лінійного тракту відповідних входів приймального обладнання. Враховуючи високу швидкість перемикання та псевдовипадковий закон перемикання в часі, адекватне сприйняття інформації при використанні трьох типів кодів стає практично неможливим.

Ключові слова: *оптичне волокно, несанкціонований доступ, захист інформації, оптичний розгалужувач, оптичний комутатор, оптична лінія затримки.*