The Peerian Journal
Open Access | Peer Reviewed
Volume 11, October, 2022.
ISSN (E): 2788-0303
Website: www.peerianjournal.com
Email: editor@peerianjournal.com

Cyber Security Analysis of Optical Communication Networks

Ashurov Azizbek Ergash O'g'li

Abstract: In this article, internal and external protection methods, software and hardware-software against threats to the cyber security of optical communication networks, such as unauthorized use, denial of service, theft, alteration, destruction of data. tools were analyzed.

Key words: Optical communication, Internet, cyber security, threat, protection, program.

Introduction

Fiber optic communication is a communication method in which the signal is transmitted in the form of light, and optical fiber is used as a means of transmitting the light signal from one place to another. The signal transmitted in the optical fiber is converted from an electrical signal to light and again from light to an electrical signal at the receiving end. The data sent can be in the form of audio, video or telemetry data, sent over long distances or over local networks. Fiber optic communication has been used for a variety of communication purposes, with good results in high-speed data transmission over long distances.

Main Part

The proximity of fiber optic cable systems (SCS) to people creates new threats to information security around the building, office, and workplace. Eavesdropping is one of the risks associated with using the effect of acoustic fields on light transmission in fiber. It is successfully used to create optical fiber sensors and distributed measurement networks. Thus, a regular optical system cable system in a building is nothing more than a distributed measurement network that can be used to measure various physical fields, including the acoustic field.

Thus, in commercial and public buildings, it is necessary to protect confidential negotiations in the office manager, office space, meeting rooms and other isolated areas of acoustic (speech) data flow through optical system cable systems. This problem has been understudied in relation to something new and very dangerous.

Secret acquisition of acoustic (speech) information using regular optical fiber connections for various purposes is one of the new methods of acoustic intelligence, which is called acousto-optical (fiber) information leakage channel [4,5].

The role of information in modern society is increasing. It's time to pay special attention to protecting information from various threats. After all, the development of information technologies creates new and unknown information leakage channels. Technologies that use previously unknown physical principles to perform processes are especially dangerous. Some internal contradictions associated with the lack of knowledge of all the features of working in the latest technologies and techniques are manifested. On the one hand, the introduction of modern technologies creates the

The Peerian Journal
Open Access | Peer Reviewed
Volume 11, October, 2022.
ISSN (E): 2788-0303
Website: www.peerianjournal.com
Email: editor@peerianjournal.com

illusion of greater information security, which is explained by the novelty of the applied principles, for which leakage channels have not yet been developed. On the other hand, there is a risk of leakage channels operating on as yet undefined, previously unconsidered physical principles.

The same problem arises in the use of photonic technologies in information processing, transmission and storage. After all, they allow you to achieve significant advantages over other technologies. Solving the problem is possible after the physical and technical analysis of the data exit channels available in new technologies, the development of modern technical tools and information protection systems.

It is suggested to consider the existing protection systems offered on the market in engineering and technical protection of information. Most protection systems are based on optical reflectometry methods, for example, Sapphire software-hardware complex (NELC, Moscow). Traffic protection is a function of common operating systems for monitoring the condition of optical cables, such as Remote Fiber Test System (RFTS) or Optical Network Management System (ONMS) offered by various companies. There are monitoring systems for optical fiber communication lines (KBPM, Moscow) used in Russian government agencies, the essence of which is to control the passage of test signals.

The threat of implementing technical channels of information leakage [2-3]

According to the definition of the information object, not only internal and external traffic, but also the information circulating in the object in the form of speech of employees, various sounds of working equipment, physical parameters of the surrounding space, etc., have privacy. Fiber optic communication is a distributed fiber optic measurement network with non-standard measurement capabilities. Fiber optic connections located inside the information facility pass through rooms where classified information can circulate freely. Regular light flux of the network mlary or external probe radiation can be accessed by an attacker using TCP. As in the previous section, the attacker's technical capabilities are limited only by the current state of TCP.

The generalized scheme of TKUI based on the optical fiber connection of the information object repeats the traffic scheme of NSI and NSD, only it is necessary to determine and take into account the effect on the optical fiber to form the leakage signal. physical area associated with sensitive information. The effect leads to the modulation of the light flux in the optical fiber, which transmits the information outside the monitored area. The switching capacity of the optical fiber determines the risk level of the technical channel of data leakage. Network topology also plays an important role in data privacy threats. Laying fiber optic cable near or through protected buildings has a significant impact on leakage safety.

Methods of protecting acoustic information from leaking through an acousto-optical (fiber) channel are passive (soundproofing of the optical cable, "proper" installation of the network, etc.) and active (filtering, masking, noise of the information signal) divided by , etc.). Another method can be distinguished, which is to include in each optical receiver the function of continuous monitoring of light fluxes for the possibility of using the technical means of acoustic reconnaissance. The risk of eavesdropping can be reduced by developing new recommendations for the installation and use of fiber optic cable systems.

List of References

1. White. Gregory B. "Computer system and network security" CRC Press-1996

The Peerian Journal
Open Access | Peer Reviewed
Volume 11, October, 2022.
ISSN (E): 2788-0303
Website: www.peerianjournal.com
Email: editor@peerianjournal.com

2. Ben Wu, Bhavin Shastri, Paul Pruchnal. "Secure Communication in Fiber-Optic Networks", Emerging Trends in ICT Security, Pages 173-183, 2014.
3. Khillar, Sagar. "Difference between Cyber Security and Network Security." Difference Between Similar Terms and Objects, July 17, 2018
4. Singh, Kunal, "Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab" (2020). Master's Theses (2009 -). 602.
5. Collection of lectures of the republican scientific and practical conference on "Modern information, communication technologies and problems of at-education implementation", volume I. / "Security issues in the use of optical communication networks" Ghaziyev Kh.I. Samarkand-2021