



"RESEARCH ON THE POSSIBILITIES OF INFORMATION SECURITY IN OPTICAL ABONENT ACCESS NETWORKS"

Buvajonov Hamidjon Halimjon o'g'li

Fergana branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, master of 2 stages

ANNOTATION: In today's world, we are exposed to too many threats to the information through software. The following article looks into the methods of data protection.

Key words: produce a large number of products, variety of processes and phenomena, information society, information

INTRODUCTION

In the information society, information is the main resource. It is on the basis of possession of information about a variety of processes and phenomena that any activity can be efficiently and optimally built.

It is important not only to produce a large number of products, but to produce the right products at a specific time. With a certain cost and so on. Therefore, in the information society, not only the quality of consumption increases, but also the quality of production; a person using information technology has better working conditions, work becomes creative, intellectual, and so on.

Information is expensive today and needs to be protected. The massive use of personal computers, unfortunately, turned out to be associated with the emergence of self-replicating viruses that interfere with the normal operation of the computer, destroy the file structure of disks and damage the information stored in the computer.

1. Features of optical communication systems

Fiber optic communication lines are a form of communication in which information is transmitted over optical dielectric waveguides known as optical fiber.

Recently, one of the most promising and developing areas of building communication networks in the world is fiber-optic communication lines (hereinafter - FOCL). In the field of information transmission systems with a large information capacity and high reliability of operation, FOCLs have no competitors. This is due to the fact that they significantly surpass wired ones in terms of such indicators as throughput, length of the regeneration section, and also noise immunity.

It is believed that FOCLs, due to the peculiarities of the propagation of electromagnetic energy in an optical fiber (hereinafter - OF), have increased secrecy. This is due to the fact that optical radiation, which is a carrier of information, propagates in the OF according to the law of total internal reflection, and behind the OF, electromagnetic radiation exponentially decreases.

The concept of FOCL is collective. It includes receivers, transmitters of an optical signal, an optical path, regenerators and other equipment. In this regard, the fiber-optic line can be divided into local and distributed sections. Local areas, including modulators, optical transmitters and receivers, regenerators, are most protected from unauthorized removal due to the localized area of their location. Distributed sections (fiber-optic paths) have the greatest length and, accordingly, the least protection against unauthorized removal. Unlike all other media for information transmission, for the formation of leakage channels in sections



of the optical path, as a rule, they require direct access to the optical fiber and special measures to remove part of the radiation from the optical fiber or to register the passage of radiation.

Information is owned and used by all people, without exception. Each person decides for himself what information he needs to receive, what information should not be available to others, etc. It is easy for a person to store the information that is in his head, but what if the information is entered into the "brain of the machine" to which many people have access.

To prevent the loss of information, various mechanisms for its protection are being developed, which are used at all stages of working with it. It is necessary to protect from damage and external influences both devices that store secret and important information, and communication channels.

Damage can be caused by breakdown of equipment or communication channel, counterfeiting or disclosure of classified information. External influences arise both from natural disasters and from equipment failures or theft.

Various protection methods are used to save information:

- security of buildings where classified information is stored;
- control of access to classified information;
- access control;
- duplication of communication channels and connection of backup devices;
- cryptographic transformations of information;

At present, optical fiber is considered the most advanced physical medium for transmitting information, as well as the most promising medium for transmitting large flows of information over long distances.

In connection with the extremely widespread use of optical fiber as a transmission medium, the problem of its protection from unauthorized information retrieval is quite urgent.

METHODS OF PROTECTING INFORMATION TRANSMITTED BY SOFTWARE

FOCL PHYSICAL PROTECTION

1. Development of technical means of protection from ND to information signals transmitted over OV.

This group of works is associated with the development of structural, mechanical and electrical means of protection against low pressure to optical cables (OC), couplings and optical fiber. Some of the types of protective equipment of this group are constructed in such a way as to impede the mechanical splitting of the cable and to prevent access to the OF. Similar protection means are widely used in traditional wired ad-hoc communication networks. It also seems promising to use a pair of longitudinal power elements OK, which are two steel wires placed symmetrically in a polyethylene sheath, and used for remote power supply and monitoring of sensors installed in couplings, and control of LP. It is also advisable to use a welding site protection kit, which fills the welding site with an opaque hardening gel. One of the proposed protection methods is the use of a multilayer optical fiber with a special structure of reflective and protective cladding. The construction of such a fiber is a multilayer structure with a single-mode core. The selected ratio of the refractive indices of the layers makes it possible to transmit a multimode control noise optical signal along the annular guide layer. There is no connection between the control and information optical signals in the normal state. Ring protection also makes it possible to reduce the level of radiation of the information



optical signal through the side surface of the optical fiber (by means of leakage modes arising at the bends of the fiber of different sections of the communication line). Attempts to penetrate to the core are detected by a change in the level of the control (noise) signal or by mixing it with an information signal. The ND location is determined with high accuracy using an OTDR.

MATERIALS AND METHODS

CRYPTOGRAPHIC

PROTECTION METHODS

A Brief Overview of Cryptographic Security Techniques

1. A method based on the use of code noise in transmitted signals. When implementing this method, specially selected error-propagating codes are used in accordance with the required transmission rate. Even with a slight decrease in the optical power caused by the connection of the information pickup device to the optical fiber, the error rate in the digital signal at the output of the fiber-optic communication line sharply increases, which is quite simple to register by means of control of the fiber-optic communication line.

2. A method based on the use of a pair of uneven-sign dispersion compensators on FOCL. The first compensator injects the dispersed signal into the line, and at the receiving end, the second compensator reconstructs the transmitted signal.

3. Using the mode of dynamic (deterministic) chaos, which allows the transmission of information with pseudo chaotically changing frequency and amplitude of the carrier. As a result, the output signal is externally noise-like, which makes it difficult to decipher.

4. Methods of quantum cryptography - combine the achievements of cryptographic science with quantum mechanics and quantum statistics. They

potentially provide a high degree of protection against interception of information on the communication line due to the transmission of data in the form of individual photons, since a non-destructive measurement of their quantum states in the communication channel by an interceptor is impossible, and the fact of intercepting photons from the channel can be detected by changing the probabilistic characteristics of the photon sequence.

REFERENCE

1. https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=QJZFznsAAAAJ&citation_for_view=QJZFznsAAAAJ:TQgYirikUcIC

2. https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=QJZFznsAAAAJ&citation_for_view=QJZFznsAAAAJ:mB3voiENLucC

3. https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=QJZFznsAAAAJ&citation_for_view=QJZFznsAAAAJ:IWHjjKOFINEC