UDC 621.618

V. Karlov[1], O. Lukashuk[1], S. Sholokhov[2]

[1] *Ivan Kozedub Kharkiv National Air Force University, Kharkiv*
[2] *M/U A1906*

TO QUESTION ABOUT INFORMATIVE SAFETY IN TELECOMMUNICATION SYSTEMS

In the article classification is conducted and methods and facilities of realization of informative safety are considered in the telecommunication systems. It is reasonable, that methods and backer-ups of safety are presently known in the telecommunication systems can be presented as formal and informal. To the formal methods and facilities it is suggested to take physical vehicle and programmatic methods and facilities. From position of practical realization the formal methods of informative safety of the telecommunication systems are considered in detail.

Keywords: *electromagnetic compatibility, computer safety, telecommunication system, network attacks, local networks.*

Introduction

At consideration of questions, related to safety of telecommunication networks take into account threat, vulnerability and attack. As is generally known [1], threat safety of the telecommunication system (TS) is potential possible incident which can render the undesirable affecting system, and also on information, kept in it. Vulnerability of the telecommunication system – it certain its description which does possible the origin of threat. Practically all of descriptions of electromagnetic compatibility determine vulnerability of the system. From the presence of vulnerability there are undesirable events in the system. An attack on the telecommunication system is an action, undertaken a malefactor, which consists in a search and use of one or another vulnerability. Thus, an attack is realization of threat. Often is it is impossible to distinguish intentional and casual actions, and good system sewn up must adequately react on any of them [2]. Usually select three basic types of threats safety – it threat of opening, integrity and refuse in service. In accordance with [2] the threat of opening consists that information becomes known to that, who its would not follow to know. In terms of computer safety the threat of opening takes a place every time, when access is got to some confidential information, to kept in the computer system or transferrable from one system to other. Threat integrity as follows from [2] plugs in itself any intentional change (modification or even delete) of information, kept in the computer system or transferrable from one system in other. It is usually considered that state structures are subject to the threat of opening in a greater degree, and to the threat integrity-business or commercial.

The threat of refuse in service arises [1–2] up every time, when as a result of some actions access is blocked to some resource of the computer system. Blocking is real can be permanent, so that an ascable resource never was got, or it can cause the delay of ascable resource, long enough in order that he became unavailing only. It is talked in such cases, that a resource is outspent. Descriptions electromagnetic compatibility in a greater measure correspond threats integrity and refuses. The basic feature of any network system is that its components are up-diffused in space and connection between them is physically carried out through network connections, realized as the structured cable systems (SCS) and programmatic through the mechanism of reports. Thus all of signalling messages and information, sent between the objects of the distributed telecommunication system, are passed on network connections as packages of exchange. The network systems are characteristic that, along with by volume (local) attacks, carried out within the limits of one computer system, to them will apply the specific type of attacks, conditioned state of distribution resources and information in space. It is the so-called network attacks. They are characteristic, at first, that a malefactor can be for thousands of kilometres from the attacked object, and, secondly, that a concrete not computer, but information, transmissible on network connections, can undergo an attack. With development of local and global networks exactly remote attacks become leading both on the amount of attempts and on success of their application and, accordingly, providing of safety of TS from point of opposition remote attacks acquires a primary value. The specific of up-diffused TS consists of that if in local TS most frequent were threats of opening and integrity, in the network systems into first place the threat of refuse goes out in service. If the basic types of threats safety in the telecommunication systems in detail enough are considered in the known literature, to consideration of methods and backer-ups safety, and the more so related to classification them, not sufficient attention is spared in the known literature.

Purpose of the article. A leadthrough of classification and consideration of methods and facilities of realization of informative safety is in the telecommunication systems.

Basic part

Results of analysis of process of providing of informative safety in ductings of telecommunication about

[1–2] allow to present methods and facilities of his realization in a kind block of chart.

As follows from [2] the methods of providing of safety in ductings of telecommunications will be realized in practice application of different facilities of defence, such as technical, programmatic, organizational, legislative and mental and ethical. We will consider them more detailed. In accordance with hardwares – realized as electric, electromechanics and electronic devices. All of aggregate of hardwares is divided on:

• vehicle are devices, built directly in a telecommunication apparatus or devices which are attended with a similar apparatus on a general-purpose interface. From the most known vehicle facilities it is possible to mark the charts of control of information on evenness, charts of defence of the fields of memory on the key;

• physical – realized as off-line units and systems. For example, locks on doors, where an apparatus, grates, is placed on windows, electronic-mechanical equipment of the guard signaling;

• technical is creation of obstacles for electromagnetic or conductive losses or violations of integrity of information. Programmatic facilities are software, specially intended for implementation of functions of priv. Facilities indicated higher and made basis of mechanisms of defence on the first phase of development of technology of providing of safety of connection in ductings of telecommunications. Comparison of existent methods and facilities of defence and evolution of technology of providing of safety of connection shows in ductings of telecommunications, that on the first phase of development of this technology programmatic facilities had primary development, the second phase was characterized intensive development of all of basic methods and facilities of defence, on the third phase of development the followings tendencies appear all more certain:

• hardware representation of basic functions of defence;

• creation of complex facilities of defence, executing a few protective functions;

• standardization and standardization of algorithms and hardwares.

Quite obviously, that for successful defence of the information an user must have an absolutely clear picture about the possible ductings of loss of information, properly to accept counter-measures on suppression of unauthorized division (to strengthen programmatic defence, utillize the anti-virus programs, strengthen passwords, apply screening of apartment. To that end we will transfer basic unauthorized electromagnetic access paths to the closed information:

it is an intercept of electronic radiations; renewal of text of printer;

• connecting to the apparatus and flow lines;

• ill-intentioned outcommissioning mechanisms of defence by electromagnetic influence (electromagnetic terrorism). The special place among facilities of defence is occupied by vehicle facilities. Thus under vehicle facilities of defence the special facilities, directly entering in the complement of the technical providing of TS and executing functions of defence both independently, are understood and in a complex with other facilities. Vehicle facilities of protection of data can be de bene esse divided into groups in obedience to types apparatuses which they are utillized in. As such groups will consider the followings: are facilities of defence of processor; are facilities of boundary protection; are facilities of defence of terminals; are facilities of defence of input-outputs; are facilities of defence of ductings of connection.

Not deciding on technical details, briefly will consider maintenance of facilities of defence of the transferred groups of apparatus. We will consider facilities of defence of processor of the operative system. We will mark that one of main terms of providing of safety of the processed information is providing of impossibility of one program to influence on the process of implementation of other program and, especially, on implementation of the programs of the operating system (OS). Usually it will be realized introduction of the so-called privileged processor (in some systems – supervisor mode), characterized the special privileged commands state. Attempts to execute these commands which are utillized for process of treatment of tasks control and for implementation of separate functions of defence, the "task of user" is able cause breaking, processed OS. For implementation of functions of defence in the complement of processor included:

• programmatic-read clock;

• commands of cleaning of blocks of memory;

• programmatic-read identifiers of processor and other technical devices;

• the special bats of secrecy are in every computer word;

• controls registers, their scopes of memory set.

We will mark that many computers and devices, entering in the complement of TS, contain the different mechanisms of boundary protection for prevention of reading and modification of information by different users. For a boundary protection the followings facilities and mechanisms are usually utillized:

• are registers of scopes of memory, settings the lower and overhead addresses of main memory for the program, executable presently to time;

• there are protection of blocks of memory of the fixed size "locks" in-memory. The executable program adds the "key" to the special register. Every selection and record in main memory is controlled vehicle facilities on confirmation that the key corresponds a lock;

• segmentation of memory, presenting the use of descriptors for description of units of information in-memory. Every descriptor is contained by the leading

address of segment, his length and pointers, determining the type of access to information of this segment;

• page organization of memory in which a table is put in accordance every program of user – pages, representing virtual addresses in physical one. Usually defence of page organization of memory will be realized through segmentation;

• hierarchical rings of safety, which provide the vehicle isolation of information and programs, related to the different rings.

As for terminals, they usually contain locks for prevention of the unauthorized including, and also block. Block can contain the devices of establishment of authenticity of user on a counter, finger-prints. For the systems with rigorisms to providing of safety of information terminals are provided with the built-in charts of encipherement of information, authentications of terminal.

Input-outputs for a decision tasks of defence can contain: are registers of addresses and identifiers; are registers of scopes selected the device of memory, charts of verification of input-output-conclusion channel; are registers of control of level of secrecy of communication channel; are charts of control of number of channel.

Ductings of connection, as follows from [2], are on the defensive, mainly, by cryptographic facilities.

Vehicle facilities of defence include the associated units which provide functioning of TS. Such devices devices of elimination of information are, for example, on magnetic transmitters, devices of signaling about violation of registers of scopes of memory.

In same queue physical safety means maintenance of computer and information in him out of harm's way from physical dangers by locks on included in an apartment, where h e is, buildings of protection round buildings and placing of guard round an apartment. But physical safety now changed from a modern computer environment – environment which often is an office with the large number of the personal computers or terminals. Physical safety is related to introduction of measures of defence, which protect from natural calamities (fires, floods, and earthquakes), and also every casual incidents. Physical safety measures determine, what surroundings of computer, entered information, and results of treatment of information, will be.

Conclusion

Thus, presently basic methods and backer-ups safety of TS can part on formal and informal. Most widespread presently among formal methods and facilities there are physical, vehicle and programmatic.

References

1. Петраков А.В. Основы практической защиты информации: учеб. пособ. 2-е изд. / А.В. Петраков. – М.: Радио и связь, 2000. – 368 с.

2. Ярочкин В.И. Информационная безопасность. учеб. пособ. для студентов непрофильных вузов / В.И. Ярочкин. – М.: Междунар. отношения, 2000. – 400 с.

3. Karlov V.D. Essence and types of informative weapon in modern informative conflicts / V.D. Karlov , O.V. Lukashuk, S.M. Sholokhov // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2016. – Вип. 2(47). – С. 42-44.

Надійшла до редколегії 24.05.2017

Рецензент: д-р техн. наук проф. Л.Ф. Купченко, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.

ДО ПИТАННЯ ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В.Д. Карлов, О.В. Лукашук, С.М. Шолохов

У статті проведена класифікація і розглянуті методи і засоби реалізації інформаційної безпеки в телекомунікаційних системах. Обґрунтовано, що нині відомі методи і засоби забезпечення безпеки в телекомунікаційних системах можуть бути представлені у вигляді формальних і неформальних. До формальних методів і засобів запропоновано віднести фізичні апаратні і програмні методи і засоби. З позиції практичної реалізації детально розглянуті формальні методи інформаційної безпеки телекомунікаційних систем.

Ключові слова: *електромагнітна сумісність, комп'ютерна безпека, телекомунікаційна система, мережеві атаки, локальні мережі.*

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОМУНИКАЦИОННЫХ СИСТЕМАХ

В.Д. Карлов, Е.В. Лукашук, С.Н. Шолохов

В статье проведена классификация и рассмотрены методы и средства реализации информационной безопасности в телекоммуникационных системах. Обосновано, что в настоящее время известны методы и средства обеспечения безопасности в телекоммуникационных системах могут быть представлены в виде формальных и неформальных. К формальным методам и средствам предложено отнести физические аппаратные и программные методы и средства. С позиции практической реализации детально рассмотрены формальные методы информационной безопасности телекоммуникационных систем.

Ключевые слова: *электромагнитная совместимость, компьютерная безопасность, телекоммуникационная система, сетевые атаки, локальные сети.*