ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 10 , October 2020

To A Technique of Maintenance of Information Safety in Networks and Systems of Telecommunication

H.Nigmatov, A.Muhammadiyev

Professor of International Academy, Uzbekistan
Teacher, International Academy, Uzbekistan

ABSTRACT: Rapid development of information-communication technologies in Republic Uzbekistan demands special conditions to systems and networks of telecommunication on maintenance of protection of the information. On networks of telecommunications the huge quantity{amount} of volume of the diverse information, possessing is transferred by the certain value. Now, with transition to market attitudes{relations} any information becomes the goods (product) for the addressee and everyone under the semantic maintenance{contents} can have various value.

KEY WORDS: information safety, systems of telecommunication, technique of maintenance, network.

I.INTRODUCTION

As is known, information safety is understood as security of the information and a supporting infrastructure from casual or deliberate influences of natural or artificial character which can cause unacceptable damage to subjects of information attitudes{relations}, including owners and users of the information and a supporting infrastructure, and protection of the information is a complex of the actions directed on maintenance of information safety. The basic requirements of information systems is maintenance of availability, integrity and confidentiality of information resources and a supporting infrastructure.

On a network of telecommunication transfer of voice messages, video of the information, the computer data, etc., in various modes are carried out. Especially, now very roughly there is a connection to the international computer network the Internet, using both transport, and user's networks of telecommunication. For good safety information and telecommunication systems the following means of protection are used: Hardware (technical); Program; Organizational (organizational - legal and organizational - technical); Physical; Cryptographic; Legal; Special means of protection of the information by transfer on liaison channels, and also Means protection against computer viruses.

The set forth above means of protection of the information can be used in a combination as it is hardware - program or программно-technical, organizational - legal and organizational - technical, etc.

II. SIGNIFICANCE OF THE SYSTEM

In computer networks and systems it is very important to pay attention to protection of the information against various viruses and against penetration of attacks of not authorized users.

The decision of a problem of maintenance of information safety in systems and networks of telecommunication is complex and a challenge. Various electron-mechanical devices which are included in structure of means of system refer to as hardware of protection and carry out independently or in a complex with other means some functions of protection. By present{true} time the significant number of various hardware is applied, and they can practically be included in all devices of the given system: terminals of users, devices of group input-output of the data, the central processors, external memories, other peripheral equipment.

III. LITERATURE SURVEY

So, for example, in terminals of users the greatest distribution devices intended for the prevention{warning} of the non-authorized inclusion of the terminal in work (a various sort have received locks and блокираторы), maintenance of identification of the terminal (the circuit of generating of an identifying code) and identification of the user (magnetic individual cards, dactyloscopic and acoustic devices of the identification, etc.). In computer networks and systems systems of detection of attacks **Real Secure,** the analysis of security **Internet Scanner**, etc., developed by the American **company ISS (Internet Security Systems, Inc.)** are used, And also **system Secret Net,** developed in Russia scientific - engineering **enterprise " Информзащита "** for protection against the non-authorized access. Association of computers in a network breaks old axioms of protection of the information. For example, about static character of safety. In the past vulnerability of system could be found out and eliminated by the manager of system by installation of corresponding updating which could only in some weeks or months to check up functioning established "patch". However, this "patch" could be removed the user casually or during work, or other manager at installation new a component. All varies, and now information technologies vary so quickly, that static mechanisms of safety any more do not provide full security of system. Until recently the basic mechanism of protection of corporate networks were gateway screens (firewall). However the gateway screens intended for protection of information resources of the organization, frequently it appears vulnerable. It occurs because system administrators create so many simplifications in system of access, that in a result the stone wall of system of protection to become holey, as решето. Protection with the help of gateway screens (МСЭ) can appear inexpedient for corporate networks with the intense traffic as use of many МСЭ essentially influences productivity of a network. In some cases it is better “ to leave doors widely opened ”, and the basic emphasis to make on methods of detection of intrusion into a network and reactions to them. For constant (24 hours per day of days per week, 365 days in one year) monitoring of a corporate network for detection of attacks are intended systems of "active" protection - systems of detection of attacks. The given systems reveal attacks to units of a corporate network and reacts to them the set manager of safety in the image. For example, interrupt connection with the attacking unit, inform the manager or will wear out the information on an attack in registers. The system of detection of attacks RealSecureтм is developed by American **company Internet Security Systems**, Inc. Also it is intended for the decision of one of prominent aspects of management by network safety - detection of attacks. System RealSecuretm is an intellectual analyzer of packages with the expanded base of signatures of attacks which allows to find out hostile activity and to distinguish attacks to units of your corporate network. System RealSecuretm is constructed on technology of the analysis of network packages in real time (real-time paket analysis) concerns to systems of detection of the attacks focused on protection of the whole segment of a network (network-based). For protection of concrete unit (Host-based) a corporate network system RealSecuretm 3.0 earlier named by system LookOut can применятьтся.

As soon as attack is distinguished, there is a notification of the manager through the console of management or e-mail. Besides attack can be registered in a database, and also all operations at realization of attack can be written down for the further reproduction and the analysis. In a case realization of attack which can lead to to deducing{removing} out of operation units of your corporate network, probably automatic end of connection with the attacking unit or реконфигурация gateway screens and routers so that further connections with the attacking unit have been forbidden. The distributed{allocated} architecture of system RealSecure allows to establish components of system so that to find out and prevent attacks to your network both from within, and outside.

At construction of any modern information system it is practically impossible to do without development and realization of some mechanisms of protection. It can be as simple mechanisms (for example, a filtration of packages), and complex{difficult} enough (for example, application in gateway screens of technology Stateful Inspection). Such mechanisms can and to not be. In this case maintenance of information safety of projected system is assigned to operational system or any additional means of protection. However in all these cases before departments of protection of the information and managements of automation there is a problem{task} of check as far as the realized or used mechanisms of protection of the information corresponds{meets}, to positions of the policy{politics} of safety accepted in the organization. And such problem{task} will periodically arise at change updating of components of information system, change of a configuration of operational system, etc.

IV. METHODOLOGY

However, managers of networks have no enough time for such carrying out of checks for all units of a corporate network. Hence, experts of departments of protection of the information and managements of automation require the means facilitating the analysis of security of used mechanisms of maintenance of information safety. To automate this process means of the analysis the securities named also the scanning software (scanniq software) or scanners of safety (security scanner) will help. Use of these means will help to define{determine} vulnerability on units of a corporate network and to remove them until malefactors will take advantage of them. *Network*

System of the analysis of security Internet Sßá»»Ñú*153; it is developed by the American company 1п1егпе1 Security System, 1nc. and it is intended for the decision of one of prominent aspects of management by network safety - detection уязвимостей. By means of the given system it is possible to carry out{spend} regular all-round or selective tests of network services, the operational systems, the widespread applied software, routers, gateway screens, Web-servers, etc. On the basis of the lead{carried out} tests system Internet Ssanneg*153; develops the reports containing the detailed description of each found out vulnerability, its{her} arrangement on units of your corporate network and the recommendation on their correction or elimination. System IternetSsanneg*153; can be used for the analysis of security of any systems based on a stack of reports TCP/1P. It can be as the computers connected to a local or global network (Internet), and independent computers with established support *TC*

The constant confidence that in your network are absent known vulnerability, is reached{achieved} by periodic scanning functioning network devices and the used software. These preventive measures will help you to find out in due time potential vulnerability and to remove them until as malefactors will take advantage of them. *A*

On all above-stated means of protection of the information now there are many development, to the devoted program-technical, legal, organizational - technical and cryptographic means of protection.

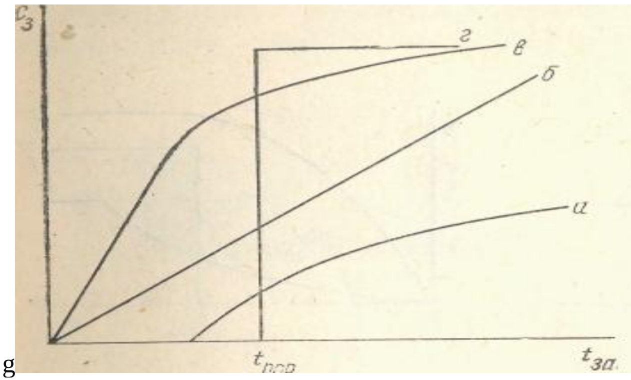
At functioning a network of telecommunication the information is delivered not instantly, during passage of signals on a path there can be the inevitable mistakes caused by handicapes or because of other factors. Besides it is possible, that the information will be delivered to the addressee with some deviations{rejections}. For immediate service of information streams in units of telecommunication interfere a number{line} of the reasons, such as: the limited quantity{amount} of channels on the set directions at the big intensity of acting loading in units of a network; low reliability of existing communication networks; the limited speed of transfer of the information, etc. and unforeseen (unintentional) or deliberate (deliberate) threats, or the non-authorized access to sources of the confidential information.

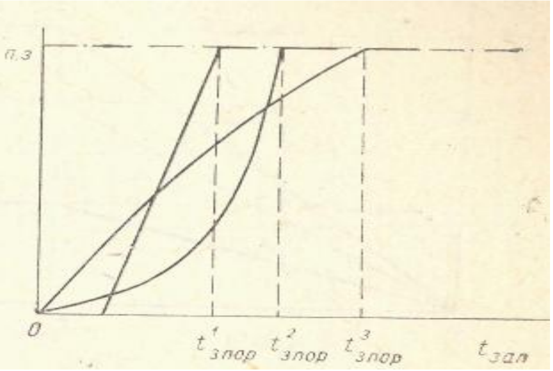
In many concrete cases delay can be odes _ ной from mistakes if true value of parameter, it is coded by the transmitted information during transfer, varies owing to change of dynamics{changes} of described object. At on _ личии mistakes in the received information in systems where she{it} ис _ Uses, the certain processes will proceed in not optimum image, i.e. with any losses$_{\text{Сош}}$, which опреде _ ляются cost estimations.

Average cost of losses$_{\text{Сзап}}$ depends on time of a delay of the information:$_{\text{Сзап}}$ = / (t back). With increase of time of a delay t back. Average cost of losses$_{\text{Сзап}}$ increases. Dependence of cost losses on time of a delay of information$_{\text{Сзап}}$ = f $_{\text{(t3ап)}}$ can have various character.

The cost losses caused by delay инфор _ мации, are defined{determined} by importance of this information managing object - the consumer of the information.

Graphic values of cost losses at$_{\text{tзап}}$ = 0 and t зап->oo characterize accordingly absence of losses from for _ паздывания by instant transfer and size of losses at non receipt of the information when$_{\text{Сзап}}$ For every portion stream reaches{achieves} the greatest value. With increase in time of a delay of the information curve$_{\text{Сзап}}$ = f (t пор.) can have various character: to row smoothly (fig. 1, a), it is rectilinear (fig. 1,) and it is sharp. Besides some portions of the information can suppose запаздыва _ ние for a while t $_{\text{П0р}}$. At a delay of the information more than on$_{\text{tпор}}$ cost losses will sharply grow.





g

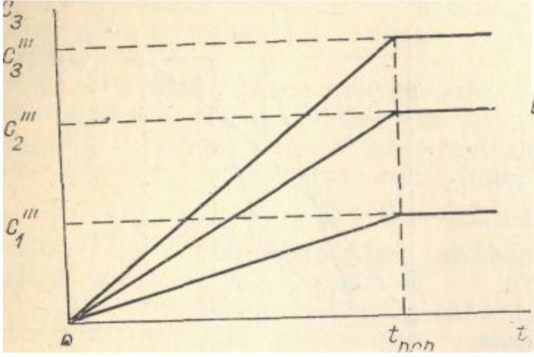
Fig. 1 Fig. 2

Threshold time of a delay$_{\text{tпор}}$ different under the maintenance{contents} of portions of the information, even at identical values$_{\text{Сзап}}$ and t>$_{\text{tпор}}$, so _ Variously. At identical time of a delay of the information max.values depend from its{her} values.

It is known, that the information should be finished up to during set time with maintenance necessary достовер _ ности, i.e. with a required degree of conformity of the accepted signal transferred{handed}. However during passage of signals on трак _ That networks arise the inevitable mistakes caused by handicapes and other reasons and as a result the information is delivered to the addressee with some deviations{rejections}.

Mistakes in the received information used in systems, result in optimum control certain{determined} about _ цессами, which just as losses at delay, it can be characterized by cost losses. The account of the last фак _ тора at functioning networks allows more objectively

And really to define{determine} optimum modes of use су _ ществующих communication networks.



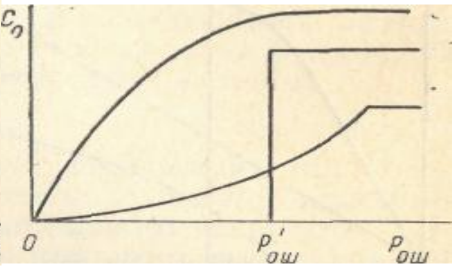


Fig. 3 Fig. 4

Apparently from fig. 4, character of losses from mistakes for each separate kind of streams depends on value of the information. A poppy _ симальные values of losses depend from economic показате _ Leu of controlled object, and also on a kind and such as the channel, on to _ торому transfer of the set requirements from unit / to unit / is carried out. For optimum use of existing communication networks it is necessary to minimize total losses from delay of the information and from mistakes:

Application of the given criterion (minimum of losses) at функцио _ нировании networks enables to take into account технико-экономиче _ ские parameters of controlled objects - consumersинфор _ мации.

V. EXPERIMENTAL RESULTS

In many concrete cases delayed reception of the necessary information or reception of the deformed or changed information, non receipt of the necessary information can be one of mistakes if true value of the parameter coded by the transmitted information during transfer, varies owing to change of dynamics{changes} of described object. At presence of a mistake in the received information in systems or objects where she{it} is used, the certain processes will proceed in not optimum image, i.e. with any losses**Сош** - which are defined{determined} by cost estimations. Cost losses from a delay of the information -**Сз** and from mistakes -**Сош** are defined{determined} by importance of this information managing object - the consumer of the information. The account of these factors at functioning networks allows more objectively and to define{determine} really modes of use of an existing network of telecommunication.

The offered{suggested} approach for maintenance of information safety in networks and systems of telecommunication consists that by development and construction of any information systems and means of protection of the information it is necessary to take into account cost losses from delay and from mistakes of the information, in view of their value, the determined addressee of this information.

Value of the information should is defined{determined} by material effect from economy of the generalized expenses of work of the object - addressee for achievement of an object in view. Generally achievement of the purpose is described by expression

VI.CONCLUSION AND FUTURE WORK

Where:**Сис**,**Сп** - accordingly resulted cost of information system and losses;**П** - the parameter describing work of incorporated system (profit, productivity, quality and quantity{amount} of production, a degree of performance of a task in view, etc.); **Оп** parameter**П** accepting the maximal values at absolutely exact and reliable functioning of information system. Advantage of this expression is that fact, that**П** synthesizes changes of cost not only creation of information system, but also losses of controlled object at functioning.

As criterion of optimization at construction of systems and means of protection of the information in networks of telecommunication it is necessary to take into account the general{common} expenses for their construction and the sums of cost losses from non receipt of the necessary information or reception of the incorrect information (cost losses from mistakes), and also losses from inopportuneness of reception of the necessary information (cost losses from a delay of the information).

REFERENCES

[1]H.Nigmatov « Models and algorithms of management of a network of data transmission with polytypic liaison channels and changing structure ». Tashkent – 1996y.220 pages.

[2]H.Nigmatov, etc. « Management of information streams of the MANAGEMENT INFORMATION SYSTEM in networks of data transmission ». Tashkent. "FAN", 1984y.96 pages.

[3]H.Nigmatov « Introduction in information safety » Tashkent. "ТАДИ", 2003y.256 pages.