Development of the information security system effective structure for the distributed computer networks

V A Gasimov1, Y A Amashov2, F P Aliyeva3, E A Mustafayeva3, D I Mutin4 and V E Bolnokin4

1 Computer systems and networks department, Azerbaijan Technical University, H.Cavid ave., 25, Baku, Azerbaijan
2 Academy of the Armed Forces of the Republic of Azerbaijan, Parliament ave., 3, Baku, Azerbaijan
3 Institute of Control Systems of Azerbaijan National Academy of Sciences, B.Vagabzade str. 9, Baku, Azerbaijan
4 Mechanical Engineering Research Institute of the Russian Academy of Sciences, Small Kharitonyevsky lane, 4, Moscow, Russia

E-mail: gasumov@yahoo.com

Abstract. The work is devoted to the study of the problems of creating an integrated information security system for distributed computer networks. The task of determining the effective structure of the information security system is set. The solution of such a task allows minimize the probability of threats, as well as material, moral damage and time loss as a result of the implementation of such threats. The methods of synthesis of the effective structure of the information security system are described below.

1. Introduction

It is known that solving information security problems in distributed computer networks is provided by performing functions such as controlling user access to individual computers and information resources (files, disks, databases, information systems and servers), administration, event registration, ensuring confidentiality, integrity and availability of data, the health (efficiency) of the system as a whole, the identification and authentication of users, the system and protected resources, the protection of information during repair and maintenance work in emergency situations, data encryption when stored on storage media and transmitted via communication channels, etc. [1-3].

Studies show that by now many individual methods and means of protecting information from various threats have been developed. Such methods are designed to at least protect one object from a single threat or to confront a single threat. Note that even sufficiently reliable methods and tools developed and used autonomously, are not able to properly protect objects from threats and eliminate weak (easily vulnerable) places in the data protection system.

Considering the above, it can be concluded that data security can be ensured and supported by a set of software, hardware, and organizational methods and protections that perform their functions in close cooperation with the main components of the network. In other words, a reliable solution to the information security problem requires the development of a well-organized, efficiently information security system (ISS) whose main tasks are to select an effective system structure, streamline the
functions of system-wide information security tools, synthesize the structure of components, evaluate the reliability of information protection, etc.

It follows that in the development of the architecture of the ISS, special attention should be paid to the design of system-wide protection tools. Such characteristics as customizable, reliability and fault tolerance of the system, mobility and software feasibility, cost and ease of use, costs of implementing protection, as well as material and time-related damages from security breaches largely depend on the successful design of system-wide protection tools. Each of these characteristics sets its own requirements for the system-wide architecture of the ISS and, therefore, the degree of submitting these requirements determines its complexity [2-4].

The most effective ISS are those in which all possible and available methods and means, both engineering and non-technical, are implemented. However, the implementation of such a complex cannot always lead to the desired result. It should be borne in mind that the damage from the violation of the security of the protected information or from various unauthorized actions may be much less than the cost of the ISS (that is, the cost of creating such a system). Therefore, it is an urgent task of research and development of economically optimal ISS, providing the as less as possible risk to the owner and users of information from damage and loss as a result of unauthorized actions. Here, the expected total losses and costs in the process of protecting information during a certain period of time can be considered as the main parameter for creating an optimal ISS [5].

This paper aims to address the issues related to the creation of an effective ISS structure designed to perform the functions of managing a set of tools to ensure data security, risk analysis and system status, identify and evaluate types of threats, and use means to counter identified threats in distributed computer networks (DCN).

2. Functional description of ISS
The main tasks to be addressed in the organization of information security are [1,2,6,7]: Assessment of potential damage from breach of information security; Formation of a more complete list of threats to information security and determination of their characteristics; Development of a methodology for determining and predicting the values of characteristic indicators of information security; Definition of security policy; Research and development of a system of solutions that ensure information security continuously; Research and development of tools, methods and means of effective implementation of solutions; Formation of a system of conditions necessary for the effective implementation of decisions or contributing to the improvement of their effectiveness.

It should be noted that when organizing information protection work, it is recommended to observe the following basic principles [2-4]:

- ensuring information security in data processing and transmission networks should be a continuous process consisting in systematically monitoring security, identifying bottlenecks and weaknesses, justifying and implementing the most rational ways to improve and develop the security system;
- information security in data processing and transmission networks can be ensured only with the integrated use and interaction of the entire arsenal of available protection tools;
- no security system can ensure the security of information without proper training of users and their compliance with all protection rules;
- no protection system can be considered absolutely reliable, in other words, it should be borne in mind that there might be such a skilled attacker who will find a loophole for access to information.

ISS in DCN is the highest component in the system hierarchy and performs mainly the following functions [1,2,7]: User login management (ULM); Access control to the system and its resources (ACSR); Registration of entries and appeals to the system (REAS); Authentication of the user and the system (AUS); Control of powers and privileges of users (CPPU); Protection of confidentiality of
information (PCI); User keys (passwords) management (UKM); Ensuring the integrity and authentication of data (EIAD); Analysis of the state and control of threats (ASCT); Prevention of violations in the system (PVS); Reconfiguration of the security system (RSS).

The listed functions have different degrees of complexity of implementation and interaction with each other. Let’s consider the procedure for performing these functions in a general sequence.

Before working with the system, each user must enter it through the ULM, which gives general information about the system. Then the user is given the opportunity to enter his name (user ID - ID) and password (user password - PSWD). After that, control is transferred to the ACSR, which takes the parameters of the ID and PSWD and checks the authorization of the access to the system and the required resources. In case of detection of the fact of unauthorized access (UAA), it gives the user a message of refusal. ACSR transfers control to the REAS, which registers all inputs and system calls (applications to the system). In the case of authorization, the input is recorded in the log of entries, and in the opposite case, the unauthorized treatment is recorded in the violation log. In both cases, the parameters ID, PSWD, date, time and name of the required resource are recorded in the log (log file).

AUS authenticates the user who successfully passes the identification. In other words, with the help of an additional procedure, the AUS establishes whether the user is who he claims to be. In addition, this module allows the user to determine whether he is dealing with the system he needs, since an attacker can formulate a corresponding message on behalf of the system in order to obtain the authorized user details. If the authenticity of the user and the system is not established, then control is transferred to the PBOC, otherwise it is transferred to the CPPU checkpoint. Having received control, the CPPU module monitors the work of users. To determine the powers and privileges, a previously formed two-dimensional matrix $A = \{a_{ij}\}, i = 1,2,\ldots,n, j = 1,2,\ldots,m$ is used, where $n$ is the number of users, $m$ is the number of network resources. The value of the element found at the intersection of row $i$ and column $j$ determines the access category of the user $i$ to the resource $j$.

The next module operating in the security system is the PCI, which protects against unauthorized use of data during storage on the media, and during transmission over the network. For this purpose cryptographic and stenographic methods, methods of code noise and special protocols for secure data transmission are used. Each time a network is transmitted or any cryptographic information hiding is performed, control is transferred to the PCI. The transfer of information is made by a special security protocol. According to this protocol, each user has two keys - one is open, while another is secret. The public (open) key is printed openly and used by other users to encrypt information that is intended for that user. The secret key is known only to the user, the owner, and is used for decryption. Keys are generated and stored in a key distribution centre (KDC).

The KDC is managed by the UKM. In addition to generating and saving keys, the UKM performs functions such as changing obsolete keys, exchanging keys between users, handing over keys to users from the KDC. Key management is performed based on key exchange protocols.

EIAD receives control from the PCI and the UKM. To ensure the integrity and authenticity of the transmitted information, a digital signature module is used. In the positive case, a satisfactory message is sent to PCI and the UKM, and they continue their work, otherwise, a violation is reported.

The ASCT module has a wider range of functions than the others. The functions of the ASCT fall into several directions: diagnostics, ensuring reliable functioning, identifying threats and violations. The first part is launched in case of appearance of any message about unauthorized actions in relation to the system or its resources. Diagnostics of user logins, competences and privileges tables are being diagnosed. The subsystem of ensuring reliable functioning controls the work of all modules and procedures of the ISS. In the event of a failure of any element of the ISS, a message is issued to the administrator and, if necessary, control is transferred to the RSS module. The third part holds events to identify threats and violations. It runs periodically and performs a test procedure that checks all the ISS nodes, the key exchange protocol, and the KDC. If a threat of unauthorized access to system resources is detected, a violation of user rights and authorities is detected, the ISS administrator is warned and control is transferred to the PVS.
PVS receives control in identifying violations of any kind. The function of the PVS is to shut down the system, restore the system after the violation in the event of damage to it, repair the damage, and clear the memory of "garbage". When vulnerabilities are identified in the system, control is transferred to the RSS. An RSS, receiving control in man-machine mode under the control of the ISS administrator, begins to change its configuration. RSS can exclude any failed module or change to another, add a new one, etc.

Depending on the structure of the ISS, the functions it performs may have the following relationships with each other: Functions can be performed independently of each other; Functions can be performed in strict sequence; The performance of one function can be coordinated with other functions, even with all; The execution of one function may cause the execution of others; Execution of one function may prohibit the execution of others, and even require cancellation of the performed ones.

3. Model of ISS for DCN
DCN can be considered as a set of subscriber systems, which are user computers and many other types of computing equipment that perform the functions of processing, storing and transmitting information resources. Subscriber systems are united by a data transmission network and can be represented as a set of information resources and a set of application processes that use DCN resources to perform their functions. A DCN resource can be any service function, a database or a file in a computer, information located on a storage medium, a device connected to a subscriber system, a process running on a subscriber system, etc. At the same time, all resources can be divided into active, which use other resources of the DCN to perform their own functions, and passive, which participate in the performance of any functions under the control of active resources. It should be noted that a resource can be passive at one time and active at another. All the resources of the system will be called DCN objects in the future.

Data security tools can be divided into two main classes: local and network security tools. Local information security tools belong to the subscriber systems or local networks and perform verification of the subscriber’s and other access to the requested resources. Network information security tools provide control of protected data flows in the DCN and perform their functions in close cooperation with the control protocols for data processing and transmission.

The ISS should have at least one mean of ensuring security on every possible path of entry into the system or access to the facilities. In the ISS model, each area requiring protection is precisely identified, security measures are assessed in terms of their effectiveness and their contribution to security throughout the DCN. It is assumed that the unauthorized access to each of the sets of protected objects is associated with a certain amount of damage to its owner.

Each object that requires protection is associated with a number of actions that an attacker can perform. To form a set of threats \( R = \{ r_j \}, j = 1, J \) aimed at violating security, you can list all potential malicious actions against all objects \( O = \{ o_i \}, i = 1, I \) of security. The main characteristic of a set of threats is \( P = \| p_{ij} \|_{i,j} \) - the probability or frequency of occurrence of the threat \( r_j \) relative to the object \( o_i \) [7-9].

A set of relations between objects and threats can be represented as a graph, in which an edge \((r_j, o_i)\) exists if and only if the threat \( r_j \) can directly affect the object \( o_i \). As can be seen from the picture, the relationship between threats and objects is not of the type of “one to one”. In other words, a threat can affect any number of objects, and more than one threat can affect any object. The essence of information security is to exclude all edges of the graph of the type \((r_j, o_i)\), indicating the path of access of the threat \( r_j \) to the object \( o_i \).
The third set of nodes $M = \{m_1, m_2, ..., m_k\}$ entered into the graph includes all existing methods and means of ensuring the security of objects in the PKC. Each tool $m_k$ should prevent at least one threat, i.e. remove at least one edge $(r_j, o_i)$ from the given graph.

Thus, the set of methods and security tools $M = \{m_1, m_2, ..., m_k\}$ converts a two-part graph into a three-part graph (figure 1), i.e. in the protected system, all edges of type $(r_j, o_i)$ all edges are represented in the form $(r_j, m_k)$ and $(m_k, o_i)$. It is clear that the existence of an edge of the type $(r_j, o_i)$ indicates the vulnerability of the object $o_i$. It should be noted that the absence of an edge $(r_j, o_i)$ does not guarantee full security assurance, although the presence of such an edge gives the potential probability of a threat, except for the case when the probability of its appearance is zero.

![Figure 1. The graph of the object-threat-object relationship of the base model.](image)

Given the above, the basic security system can be represented as follows:

$$S = \{O, R, M\}$$

where $O = \{o_1, o_2, ..., o_I\}$ is the set of protected objects (information resources, technical and other resources) of the system, $R = \{r_1, r_2, ..., r_J\}$ is the set of malicious actions (threats) violating security, $M = \{m_1, m_2, ..., m_K\}$ - a set of methods and means to ensure the security of protected objects.

**4. Determination of effective structure of ISS**

Let’s imagine that within the framework of model (1) are given: $P = \|p_{ij}\|_{1\times J}$, where $p_{ij}$ - is the probability or frequency of the appearance of the threat $r_j$ relative to the object $o_i$; $T = \|t_{ijk}\|_{I\times J\times K}$, where $t_{ijk}$ is the time required to ensure the security of the object $o_i$ from the threat of $r_j$ using the means of protection $m_k$; $Z = \|z_{ij}\|_{I\times J}$, where $z_{ij}$ - material costs required to implement the necessary methods and means to ensure the security of the object $o_i$ from the threat of $r_j$; $Q = \|q_{ij}\|_{I\times J}$, where $q_{ij}$ - material damage caused by the violation of the security of the object $o_i$ threat of $r_j$; $X = \|x_{ijk}\|_{I\times J\times K}$, where $x_{ijk} = 1$, if the object $o_i$ is protected from the effects of the threat $r_j$ with the help of the protection $m_k$, $x_{ijk} = 0$, otherwise.
Thus, the task of ensuring the security of information resources, technical and other means of the system is reduced to finding such \( x_{ijk}, i = 1, I, j = 1, J, k = 1, K \) that would minimize functional:

\[
\sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{k=1}^{K} p_{ij} t_{ijk} (z_{ij} + q_{ij}) x_{ijk} \to \min
\]  

(2)

and satisfied the conditions:

\[
\sum_{k=1}^{K} x_{ij} \geq 1, i = 1, I
\]  

(3)

\[
\sum_{j=1}^{J} x_{ij} \geq 1, k = 1, K
\]  

(4)

Here, the functional (2) shows the weighted average damage (time and material costs) from the security breach of the system as a whole. Condition (3) shows that each object must be protected by at least one mean of protection, and condition (4) shows that each method must withstand at least one threat.

5. Conclusion

As a result of research of models and methods for creating of effective ISS for the distributed computer networks, the dependence between losses from threats and the cost of the system itself has been determined. It has been found that the development of a comprehensive ISS, the cost of which is much higher than the amount of possible losses, is not always acceptable. Therefore, it is proposed to build such ISS, the structure of which was optimal, covered all possible methods and means of ensuring security, but the cost did not exceed the total amount of possible losses. For this purpose, the optimization problem is set, the solution of which gives the weighted average amount of damage (time and material costs) from the breach of the security of the system as a whole. The following conditions are taken into account: each object must be protected by at least one means of protection and each method must resist at least one threat. Further, the methods of synthesis of the effective ISS structure by vertical (functional) and horizontal (geographical) partition are proposed.

References

[1] Azhmuhamedov I M 2012 Solving information security problems based on system analysis and fuzzy cognitive modeling (Astrakhan)
[2] Gasimov V A 2009 Basics of Information Security (Baku)
[3] Selishev V A, Cheehuga O V and Nasedkin M N 2009 Construction of information security system of the enterprise News of Tula state university. Technical science 1-2 152-9
[4] Poleshuk A V 2008 Features of construction of complex system of information security of the gas transportation enterprise Information security. ITSec.Ru-2008 Available from: http://lib.itsec.ru/articles2/bypub/itsecru-02008
[5] Bautov A H 2002 Economic view on the problems of information security Open systems. DBMS 02 Available from: https://www.osp.ru/os/2002/02/181118/
[6] Domrev V V 2002 Information technology security. Methodology of creation of protection systems (DiaSoft)
[7] Gasimov V A 1998 Construction and realization methods of effective structures of security service systems in open computer networks (Baku)
[8] Abbasov A M 1998 Information security problems in computer networks (Baku)
[9] Gasimov V A and Mamedov S Z 2007 Development of an effective information security system structure for corporate computer networks Naukovi Pratsi Odeska National Academy of Links named O.S.Popov 2 pp 70-3