DOI: 10.24412/2470-1262-2022-3 -133-141
УДК (UDC) 004.05

Ibraim Didmanidze,
Batumi Shota Rustaveli State University,
Batumi, Georgia
Mikheil Donadze,
Batumi Shota Rustaveli State University,
Batumi, Georgia

For citation: Didmanidze Ibraim, Donadze Mikheil, (2022).
Information Security System Evaluation Criteria in
Educational Computer Networks.
Cross-Cultural Studies: Education and Science,
Vol. 7, Issue 3 (2022), pp. 133-141 (in USA)

Manuscript received: 11/10/2022
Accepted for publication: 20 /11/2022
The author has read and approved the final manuscript.

INFORMATION SECURITY SYSTEM EVALUATION CRITERIA IN EDUCATIONAL COMPUTER NETWORKS

КРИТЕРИИ ОЦЕНКИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Abstract:

The paper discusses the security issues of corporate information systems and network resources. Corporate networks, the main types of information threats and the model of attacks on information systems are described. The methods of evaluating the effectiveness of protection measures have been analyzed and criteria have been developed allowing us to obtain a quantitative assessment of the information system security condition, by taking into consideration the opinions of experts. This methodology applies the area of threats, which will allow us to develop an information security system, which, according to its characteristics, will be equal to the scale of threats. The application of this methodology will allow us to evaluate the existing systems and make a decision about their improvement and feasibility, as well as to avoid ineffective application of information security tools in the process of system design. Ensuring the security of information and network resources is a priority aspect of the enterprise and organization. Therefore, the information security criteria of the education information network developed in the paper and the results obtained as a result of the analysis will promote protection of the business enterprise information-network resources.

Keywords: information systems, computer networks, information security, criteria

Аннотация:

В статье рассматриваются вопросы безопасности корпоративных информационных систем и сетевых ресурсов. Описаны корпоративные сети, основные виды информационных угроз и модели атак на информационные системы.

Проанализированы методы оценки эффективности мер защиты и разработаны критерии, позволяющие получить количественную оценку состояния защищенности информационной системы. В данной методике используется область угроз, позволяющее разработать систему защиты информации, которая по своим характеристикам будет равна масштабу угроз. Использование данной методологии позволит оценить состояние существующей системы и принять решение об их совершенствовании и целесообразности, а также избежать неэффективного использования средств защиты информации при проектировании системы безопасности.

Обеспечение безопасности информации и сетевых ресурсов является приоритетной задачей предприятия и организации, поэтому разработанные в статье критерии информационной безопасности образовательной информационной сети и полученные в результате анализа результаты помогут защитить информацию и сетевые ресурсы коммерческого предприятия.

Ключевые слова: информационные системы, компьютерные сети, информационная безопасность, критерии безопасности

Introduction

Nowadays, the organization of information systems security regimes is a critically important strategic factor in the development of any foreign or local company. At the same time, as a rule, the main attention is paid to the findings and recommendations of the relevant regulatory and methodological framework in the field of information protection. Meanwhile, many leading companies today, in order to maintain business continuity, use additional initiatives aimed at the sustainability and stability of corporate information systems.

During the assembling of IPS (information protection system), the concept of a systematic approach is often found in information sources. The concept of systematicity is not only the creation of appropriate protection mechanisms, it is a regular process that is carried out at all stages of the information system life cycle. Simultaneusly, all means, methods and measures used to protect information are combined into a single, complete mechanism - the protection system. Unfortunately, the need for a systematic approach to information technology security issues has not yet found proper understanding among modern information system users [1].

Currently, specialists in various fields of science are forced to deal with information security issues. This is due to the fact that in the next hundred years, humanity will have to live in a society of information technologies, where the social problems of humanity, including security issues, will be transferred.

Description of corporate networks. An example of a small enterprise corporate network is shown in Figure 1. The diagram shows: central office with its own local local computer network, work with remote clients, work with remote clients - employees of the corporation, connection of territorially distributed offices to the main office and connection to partner networks. The corporate network has all the necessary services for conducting the company's business activities [4].

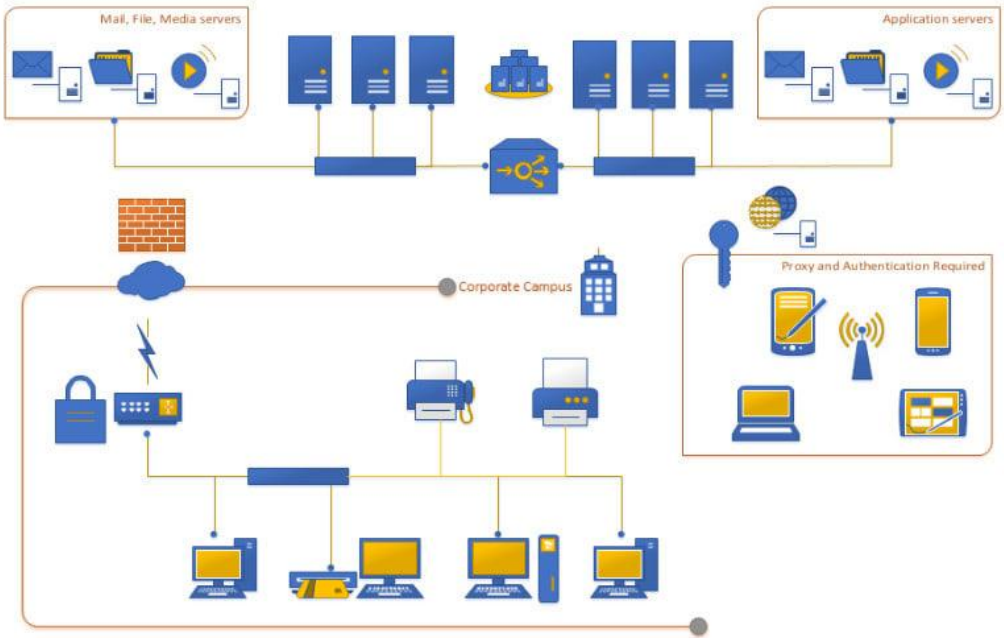

Figure 1. Corporate network diagram of a medium-sized enterprise

Along with the advantages of the corporate network, there are a number of disadvantages that can threaten the normal functioning of the company. The basic and main problem of corporate networks was and still is information security. Nowadays, in the age of information, the loss of information resources can lead to the bankruptcy of a business enterprise. As a result, large companies have to spend money to keep their networks at an adequate level of security. Despite this, this does not make the technology of corporate networks less attractive for business arrangements, on the contrary, today the majority of large companies carry out their activities at the expense of information systems [1].

Threat model. As we mentioned above, one of the main tasks of the normal functioning of the corporate information system and the support of business success is the security of the information circulation that is distributed in it.

In general, in this case, there are the following main types of threats to information resources:

- Violation of privacy
- Violation of integrity
- Access violation
- Violation of monitoring
- Violation of authentication

Model of attack on information systems. Depending on the planned operation conditions of the information protection means and, accordingly, the value of the protected information, there are four levels of the infringer's capabilities:

Zero level - accidental exposure of information (accidental listening to the channel);

The first level - the intruder has limited capabilities. It independently creates methods of attack on means of the defense system, as well as on information and telecommunication systems, using common software tools;

The second level - a corporate-type violator has the ability to create special technical means, the cost of which is related to the possible financial loss in case of loss, alteration or destruction of protected information.

Third level - the violator has a scientific-technical resource equal to the scientific-technical resource of a special service of an economically developed country.

In the corporate networks of organizations, you may encounter criminals of all levels. It can be company employees who pose a threat due to their incompetence or deliberately harm the

company, and also the hacker community trying to harm the company on behalf of competing firms.

Setting the security assessment problem. Maintaining the required level of security is an urgent issue for many organizations, both public and private. Therefore, a lot of money is spent on solving this issue. The challenge is to create an effective security system that not only provides a guaranteed level of protection, but also meets the needs of the company as much as possible. At the same time, as a rule, attention is paid to the description of various technical solutions, the analysis of advantages and disadvantages of known hardware and software tools [2].

Effectiveness is the key in information protection design, efficiency is directly related to other system characteristics, including quality, reliability, controllability, stability.

Therefore, the quantitative assessment of efficiency allows to measure and objectively analyze the main properties of systems at all stages of their life cycle, starting from the stage of requirements formation and preliminary design.

Thus, using the modern methodological framework, the evaluation of the effectiveness of the information security system is mostly uncertain and subjective. There are practically no standardized quantitative indicators taking into account possible accidental or intentional effects. As a result, it is complicated and often impossible to evaluate the quality of the functioning of the information system in the presence of unauthorized influence on its elements and, therefore, to determine why one version of the created model is better than another. It seems that the solution to the problem of complex assessment of the effectiveness of information security systems is the use of a systematic approach, which allows to assess the level of security at the design stage and create a risk management mechanism. However, this way is realized if there is a corresponding system of indicators and criteria [3].

The methodology of information security systems described in the article is based on the idea that the level of risks in a protected system should be minimal compared to the level of risks in an unprotected system. In this situation, you can get a quantitative assessment of the level of information security. The level of accuracy of the assessment largely depends on the completeness of the list of information security requirements, in accordance with the requirements of the list of threats.

The problem of selecting an efficient solution. Any purposeful human activity, starting from everyday life and ending with professional activity, is a continuous sequence of implemented decisions. The ability to make effective decisions distinguishes qualified specialists from standard users.

In general, the decisions made differ in the importance of the results, the peculiarity of the situation, and the completeness and accuracy of the initial information, but from a formal point of view, they have a common methodology and implementation tools. From a formal point of view, they can be represented as a single generalized model that is invariant to the specific content of the decision-making problem. The analysis allows us to outline the following main tasks of the generalized decision-making procedure:

- Formation of the goal, its analysis and formalization;
- Determination of different possible ways to achieve the goal (set of solutions);
- Assessment formation that will allow us to compare (sort) possible solutions according to quality;
- Choosing the extreme one from the possible set, i.e. The only best decision by quality; [3]

In decision-making theory, the set of listed tasks forms a common decision problem, the third is called the evaluation problem, and the fourth is called the optimization problem.

The ultimate goal of solving a general decision-making problem is to select the only best solution from the set of possible solutions x, that is, the extreme decision selected according to specific criteria.

$$x^o = \arg \underset{x \in X}{extr} \{k_i(x)\}, i = \overline{1,n} \quad (1)$$

If the task is single-criteria, it means that the process is evaluated according to the only indicator of efficiency, that is, we have the only objective function, and the solution method depends on the form of the corresponding mathematical model, the solution method, which is used only in a specific case.

Since, in most practical tasks, we have to make the best decision not according to the only indicator of efficiency (the only criterion), but according to several indicators, we are interested in the case when n>1 and, accordingly, we have a multi-criteria optimization task. On the other hand, the solution of any multi-criteria optimization problem will ultimately be reduced to a single criterion, but there are different methods, which differ from each other, and the use of one of them more often depends on the specific field where we have to solve the multi-criteria problem. If n> 1, in our case the problem is multi-criteria, its unique solution is possible only in special cases, and in general, the problem does not have a unique solution.

The multi-criteria optimization problem (1) does not allow determining the only optimal solution from the admissible set x. This inaccuracy can be eliminated by regularizing the task, i.e. By introducing additional information (mathematical relationships or rules that ensure the selection of the only solution). When implementing a non-constructive approach, the decision-maker decides on an intuitive level from regulated (selected) information.

A general approach to solving this problem is to transform the multi-criteria problem into a single-criteria problem with a scalar criterion. This is due to the following two reasons. First, the value of a scalar quantitative criterion can be defined as a point on the numerical axis, and it is not difficult to rank such points, since the relations of superiority and equivalence turn into inequality (>) and equality (=), respectively. Second, all extremum-finding methods are focused on a scalar function.

There are several ways to transform a multi-criteria optimization problem into a single-criteria one. One of these methods is the "main criterion method", which we will use later to evaluate the effectiveness of the protection system for solving the optimization problem [5].

The principle is based on identifying the main criterion and converting all other criteria into constraints. Therefore, the analysis of the specific characteristics of the multi-criteria task is carried out. One of the private criteria is selected - the most important one and it is accepted as the only optimization criterion. For each other specific criterion, a threshold value is allocated below which it cannot fall. Thus, all but one of the specific criteria become constraints that further narrow the range of possible solutions x. Then the multi-criteria problem (1) turns into a single-criteria problem.

$$\begin{aligned} x^o &= \arg \underset{x \in X}{extr}\, k^*(x), \\ k_i(x) &\geq (\leq) k_i^c(x), i = \overline{1, n-1}, \end{aligned} \quad (2)$$

Where $k^*(x)$ - is the optimization scalar criterion; $k_i^c(x)$ – worst admissible values of private criteria constraints; The ">" sign is used for criteria to be incremented and the "<" sign is used for decrement.

Extracting the main (optimization) criterion and $k_i^c(x)$ level of constraints for all other criteria is a subjective operation performed by experts or decision makers. It should be noted that it is possible to consider several different options and compare the results.

When implementing the considered method, special attention should be paid to the fact that the set of admissible solutions given by private criteria is not empty [5].

Information security system evaluation criteria. In order to choose an effective information system in any field of activity, it should be considered that the system meets certain criteria, on the basis of which the choice is made. Such parameters for information security systems are: performance, management, compatibility, cost, security, etc. As mentioned above, choosing the

optimal system for such a set of features is a classic optimization problem and may not always have an efficient solution. Moreover, many parameters are contradictory: as the level of security increases, for example, the cost increases, the complexity of administration increases, while performance decreases. Thus, in our methodology, the efficiency of the system will be evaluated according to the security parameter as the main indicator of the ensured level of the information security system, and restrictions will be set for the rest of the characteristics:

$$Z = f(C_{inf}, P_{SeR}, M_{ius}, K),$$

Where C_{inf}- value of information security (indicative);

P_{SeR}- possibility of penetration (intrusion into the system);

M_{ius}- cost of information protection system (price);

K - system performance.

Taking into account the presented concept of the security system, the task of optimization is to ensure the maximum level of security (as a function of the value of the protected information and the probability of penetration) with the minimum cost of the security system and its minimum impact on the effective operation of the system:

$$Z^{opt} = \max Z\,(C_{inf}, P_{SeR}, M_{ius}, K),$$

Considering the above, it is possible to make an important conclusion about the multi-criteria nature of the task of developing a protection system. In this case, in addition to the ensured level of security, a number of the most important features of the system should be taken into account. For example, the impact of the protection system on the computing resource load of the protected object should be taken into account, which is the number of applied problems solved by the object per unit of time [5].

The initial parameters of the security system development task, as well as the possibility of reducing the task to one criterion, are shown in Figure 2 [6].

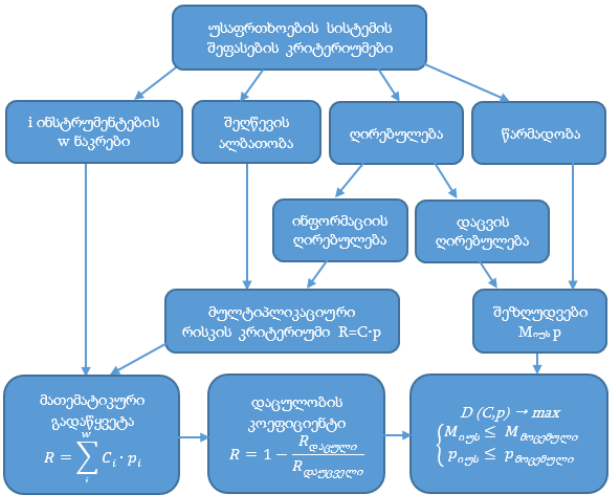

Figure 2. Security assessment criteria

Network security assessment considering risks. We should discuss system security in terms of risks. Consider that the use of risk theory to assess the level of security is the most commonly used in practice today. Risk (R) is the potential loss from security threats: $R(p) = F_{inf} * A_{SeR}$.

Apparently, the risk parameter comes in here as a multiplicative combination of the two main safety parameters. Where:

C_{inf} - cost of protected information

P_{SeR} - penetration probability;

K_{ius} - cost of information protection system; M - system performance.

On the other hand, risk can be considered as losses per unit of time:

$R(\lambda)=C_{inf} *\lambda_{SeR}$,

Where λ_{SeR} - penetration flow intensity;

These two formulas are related to each other by the following ratio:

$$p_{SeR} = \frac{\lambda_{SeR}}{\Lambda}$$

Where Λ the general intensity of the flow unauthorized attempt to violate the basic properties by the malefactors.

As the main safety criterion, we will use the safety factor (D), which shows the reduction of risk in a protected system compared to an unprotected system.

$$D\% = \left(1 - \frac{R_{sec}}{R_{uns}}\right) * 100\%, \quad (3)$$

Where R_{sec} risk in the protected system;

R_{uns} - Risk in an unsecured system.

Thus, in this case, the optimization task looks like this:

$$\begin{cases} D(C_{inf}, p_{SeR}) \rightarrow max; \\ K_{ids} \rightarrow min; \\ M_{ids} \rightarrow min. \{ \end{cases}$$

To solve this problem, let's reduce it to a single criterion and set it by introducing restrictions. As a result, we get:

$$\begin{cases} D(C_{inf}, p_{SeR}) \rightarrow max; \\ K_{ids} \leq K_{moc}; \\ M_{ids} \geq M_{moc}; \end{cases}$$

Where K_{moc} and M_{moc}– are given limitations on the cost of the protection system and the performance of the system.

The target function is selected on the basis that it reflects the main functional purpose of the protection system - information security.

System performance $M_{ids}$is calculated using mass service theory methods and models. In practice, it is possible to introduce limitation of performance not directly in the form of the required performance of the system, but in the form of reducing the performance of the information system dM_{ids} . In this case, the optimization task looks like this:

$$\begin{cases} D(C_{inf}, p_{SeR}) \rightarrow max; \\ K_{ids} \rightarrow min; \\ dM_{ids} \rightarrow min, \{ \end{cases}$$

And after reducing to one criterion:

$$\begin{cases} D(C_{inf}, p_{SeR}) \rightarrow max; \\ K_{ids} \leq K_{moc}; \\ dM_{ids} \leq dM_{moc}. \end{cases}$$

Where K_{moc} and dM_{moc}- given limitations on security system cost and performance degradation. Given limitations on security system cost and performance degradation.

If the calculated value of the safety factor (D) does not meet the requirements of the protection system, then the specified limits may be changed within the acceptable limits, and the problem can be solved by the successive selection method of yielding. At the same time, an increase in costs and a decrease in performance are defined.

$K^*_{moc} = K_{moc} + \Delta K$,

$M^*_{moc} = M_{moc} - \Delta M$ ъб $dM^*_{moc} = dM_{moc} + \Delta dM$.

In this form, the problem is solved by performing an iterative procedure by selecting the options that do not meet the limiting conditions and then selecting the option with the maximum safety factor from the remaining options.

Express the safety factor in terms of hazard parameters. In general, there are many types of threats in the system. Under these conditions, we set the following values:

W –number of types of threats affecting the system;

$C_i (i = \overline{1, w})$ – i-the cost of penetration damage;

$\lambda_i (i = \overline{1, w})$ – i- intensity of penetration flow of type UR;

$Q_i (i = \overline{1, w})$ - the probability of occurrence of threats of the i- type in the general flow of attempts to realize threats, where $Q_i = \frac{\lambda_i}{\Lambda}$; $p_i (i = \overline{1, w})$ – i probability of repelling threats of type system protection. Accordingly, for the coefficient of loss from penetration of the protection system, we have:

$$R(p) = \sum R_i(p) = \sum C_i * p_{R\_i},$$

$P_{R\,i} = Q_i*(1-p_i)$.

Where $R_i(p)$ is the i-type penetration loss coefficient; The average loss from one penetration of type *i* - is shown.

For unsecured system $P_{R\,i} = Q_i$,

For protected system $P_{R\,i} = Q_i*(1-p_i)$.

Accordingly, the coefficient of damage caused by breaking the protection system per unit of time will be:

$$R(\lambda) = \sum_1^w R_i(\lambda) = \sum_1^w C_i * \lambda_{R\_i},$$

Where $R_i(\lambda)$ - is the penetration loss coefficient of the i- type per time unit. For unsecured system $\lambda_{R\_i} = \lambda_i$; for protected system $\lambda_{R\_i} = \lambda_i * (1 - p_i)$. Accordingly, from (3) we have:

$$D = 1 - \frac{\sum_1^w C_i * Q_i * (1 - p_i)}{\sum_1^w C_i * Q_i} = 1 - \frac{\sum_1^w C_i * \lambda_i * (1 - p_i)}{\sum_1^w C_i * \lambda_i} \quad (4)$$

If the parameter of the initial probability of the possible occurrence of threats is Q_i, then it is convenient to calculate the safety factor in terms of the probability of occurrence of threats. If the intensity of the threat flow λ_i is given as the initial parameters, then, naturally, the safety factor is calculated according to the intensity.

When using any mathematical method of designing a protective system, it is necessary to set some initial parameters to evaluate its safety. Therefore, the main problems of formalizing the task of synthesizing the protection system, and determining the probability and intensity of threats are related to this. [6,7,8].

Thus, the entire process of security level analysis can be conditionally divided into stages of data collection and analysis and modification of protection system parameters.

The criteria developed in the paper allow us to determine the level of security of the information system with certain means of information security and, accordingly, to evaluate the effectiveness of the means of information security. Using the presented method, we will evaluate the security of the corporate information system, in the aspect of computer network protection of the system. [9]. In terms of information security, this field is very dynamic and requires special attention [9].

Conclusion

The Paper provides a discussion on security issues of corporate information systems and network resources. The main types of information threats and the model of attacks on information systems. In the paper, a methodology has been developed, through which it is possible to evaluate the security level of the corporate information system. As a result of the methodology, we obtained a quantitative assessment of security for the entire information system. The security level is defined as the ratio of the risks of a protected system to the risks of an unprotected system. The methodology is based on the systems risk assessment approach. A risk-based approach is implemented in many areas of information security, as it allows us to describe more accurately information resources, according to the information resources to the level of criticality of the organization's activity.

The developed methodology can be applied to assess the security level of the information system of the enterprise in all areas of activity. The criteria can be adapted to the specific needs of the enterprise, taking into consideration the specifics of its operation and business.

Reference:

1. Sharashenidze T., Information protection in computer networks, STU, Tbilisi 2016.
2. Malvenishvili M., Balarjishvili N., Cyber security reform in Georgia: current challenges, international practice and recommendations, 2020
3. Donadze M. Determining the performance and reliability criteria of computer networks. Proceedings of the Adjara non-regional scientific center of the National Academy of Sciences of Georgia - VI, Batumi. 2020.
4. Ghorbani A.A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention: Concepts and Techniques. Springer Science & Business Media. 2009.
5. Galitsky A., Protection of information in the network - analysis of technologies and synthesis of solutions. DMK. 2004.
6. International standard ISO 17799: 2000 "Practical rules for information security management"
7. Guide for conducting risk assessments // National Institute of Standards and Technology NIST Special Publication 800-30. - 2012. V.1. - C. E1-E8, p. 4-39.
8. Information technology - Security techniques-Information security risk management / British standards BS ISO/IEC 27005:2008. - 2008. v. 1 - C. 47-54.
9. Mukherjee A., Network Security Strategies, Packt Birmingham – Mumbai, 2020
10. https://habr.com/ru/post/344762/
11. https://www.ptsecurity.com/ru-ru/research/analytics/
12. https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/

Information about the Authors:

Ibraim Didmanidze (Batumi, Gorgia) *– Doctor of Information Technology, Associate Professor of Batumi Shota Rustavelli State University, e-mail: ibraimd@mail.ru*

Mikheil Donadze (Batumi, Gorgia) *– Doctor of Information Technology, Associate Professor of Batumi Shota Rustaveli State University, Batumi, Georgia*

Acknowledgments: *I thank colleagues for valuable advice in the process of this research and editing the article and I thank the reviewers for their valuable suggestions.*

Contribution of the authors. *The authors contributed equally to the present research.*