ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 3, March 2019

A Model for Assessing the Security of Information from Unauthorized Access when Designing Computer Systems in a Protected Version

KadirovMirhusanMirpulatovich, Karimova NazimakhanAybekovna, DjurayevaShokhistaTagirovna, NosirjonovaMunisaMuzaffarqizi

Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Student, Tashkent State Technical University, Tashkent, Uzbekistan.

ABSTRACT: The article describes ways to increase the level of information security based on a probabilistic method of analysis. And also considered the issue of increasing the security of information in the design of computer systems in a protected version in the conditions of the development of information space and the growth of information security threats. An assessment of the security of information for the design of computer systems in a protected version is given.

KEYWORDS: information security, unauthorized access, automated systems, protected version, CSPV.

I. INTRODUCTION

The solution of the problem of protecting information from unauthorized access in any information system is based on the implementation of control and delimitation of access rights of subjects to protected resources, first of all, to file objects, since they are intended to store the processed data. In this case, the subjects of access in the demarcation policy are the users identified by the accounts[1].

In periods of the need to choose a complex of security solutions, the following requirements for the methods of organizing information security are taken into account as limitations:

- the existence of certificates on information security issues in accordance with the classification of the information being processed and the order of functioning of automated systems;
- the invariance of the functioning of protective equipment;
- provision of a protection mode for protected information, including the preservation of such information security properties as confidentiality, availability, integrity and authenticity;
- guaranteed preservation of the target functions of the protected automated system - no restrictions associated with the use of protective equipment that impede the implementation of the technological cycle of information processing.

The main function of the security system is countering threats with the help of people and technology. Each threat entails damage, and counteraction is designed to reduce its magnitude, ideally - completely. This is not always possible.

II. INCREASE THE LEVEL OF INFORMATION SECURITY BASED ON A PROBABILISTIC METHOD OF ANALYSIS

The ability of the security system to perform its primary function should always be quantified. The relative damage prevented in Figure 1.1 can be measured.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 3, March 2019

MagnitudeQ_0 - measure of the overall effectiveness of protection. The more Q_0, the less damage will create threats. Thus, the measure of risk is (1-Q_0). The quest for high performance protection whenQ_0close to 1 (or 100%), quite natural, but it will require significant expenditure on resources. That is, the higher the cumulative allocations (B_0) resources, the greater the effectiveness of protection can be counted on. Theresultingdependenceisvisibleinthefigure. 1.1.

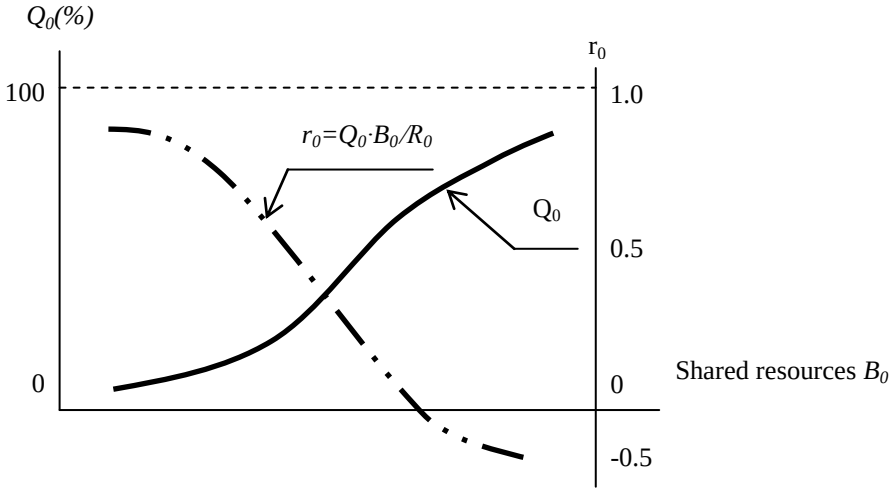

Figure 1.1 Typical dependence of the efficiency Q_0 and the profitability of protection r_0 from shared resources

However, excessive expenditures on their own security are not always economically justified. You may encounter a situation where the cost of protection (B_0) will exceed the level (R_0) maximum damage from the realization of threats. In this case, there is a danger of the threat of "self-dilution" from protection. Its level can also be estimated, for example, by*r*the difference of relative "protected" damage$Q_0$and relative costs B_0/P_0on resources. Let's call this value the profitability of protection. If it is positive (i.e.$B_0<=P_0Q_0$), then protection is cost effective. Unlike efficiency, the greater the cost(B_0), the lower the profitability [2]. This contrast creates an ambiguous situation in the choice of protection strategy.

Figure 1.2 shows the characteristic dependence of the effectiveness of protection on the relative response time of the system.(T_p/T_y) forallthreecountermeasures.

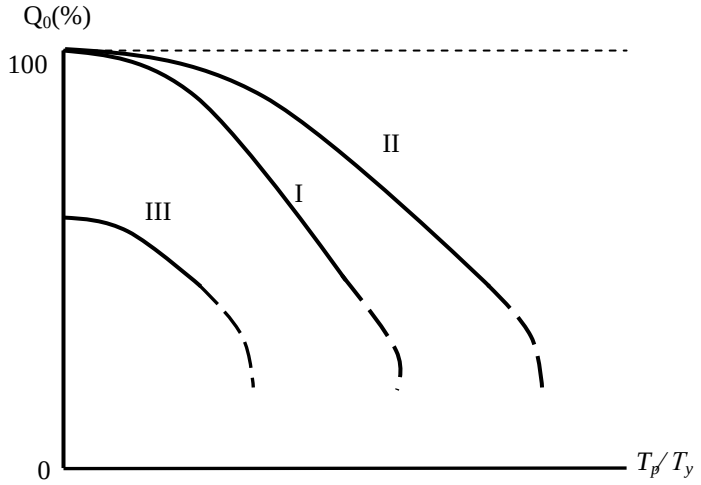

Figure 1.2 Dependence of the effectiveness of protection Q_0relative time T_p/T_yreactions of the system with simultaneous (I), leading (II) and delayed (III) counteraction

Simultaneous counteraction will be sufficient for highly effective protection against the threat if the reaction to it is quick. This task is very real for objects of big business [3].

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 3, March 2019

Speaking about the tactical issues of the business security system in terms of technical communication channels, first of all they mean the speed of its reaction, the reliability of decisions, the blocking of the development of threats and their elimination. It is especially important to ensure stringent requirements for the reliability of all protection systems, which depends on the time of their operation and the frequency of resource updates.

III. MODEL FOR ASSESSING THE SECURITY OF INFORMATION FROM UNAUTHORIZED ACCESS

It is known that the violator will always spend time on the implementation of unauthorized access to information leading to disruption of the normal functioning of computer systems, confidentiality, integrity and availability of information T_{und}, necessary for the formation of a channel for the realization of an information security threat, that is, the indicated time characterizes the time interval:

$$\mathrm{T}_{und} = \sum_{i=1}^{4} T_i.$$

where T_1 - identifying software hardware vulnerabilities; T_2 - assessment of the possibility of exploiting the vulnerability, taking into account the existing information protection system of the intended object of impact (information carrier) T_3 - choosing a method for implementing unauthorized access; T_4 - unauthorized access.

Based on this, by increasing T_i one could always manage the security of information in computer systems in a protected version (CSPV). I.e T_i could be taken as a criterion for assessing the security of information in the CSPV. Then by setting the threshold for the CSPV $T_{add\ \ und}$ and enforcing the condition $T_{und} \le T_{add\ \ und}$, It would be possible to implement the permissible protection of restricted access information in the CSPV [4].

However, this approach will not reflect the real picture, since time T_i - this is a random variable, the distribution law of which is difficult to calculate, since it will change depending on the abuser's capabilities. In addition, it does not take into account the main factors of operation, such as: various threats to the security of information in the APSI, the operating time of the APSI, the characteristics of the information security tools used, on which unauthorized access to information may also depend.

Therefore, to improve the objectivity of monitoring the timeliness, reliability, completeness and continuity of information security designed by CSPV, it is advisable to develop a mathematical model of the probability of unauthorized access to circulating information, taking into account operating conditions and the composition of a complex of information protection tools. On the basis of the model found, formulate qualitative and quantitative criteria for enhancing the security of information when designing computer systems.

Description of the approach. It is known that the classical formulation of the task of developing sets of information protection tools to ensure maximum efficiency of computer systems in the conditions of unauthorized access will be:

$$\begin{matrix} U_{\sum} \to \min \\ C = C_{opt} \end{matrix}, \qquad (1.1)$$

where $U_{\sum}$ – total damage; C – the cost of designing a set of information security tools or

$$\begin{matrix} E_3 \to \max, & \delta_3 \to \max, \\ C = C_{opt} & C = C_{opt}. \end{matrix} \qquad (1.2)$$

where E_3 – efficiency of computer systems; δ_3 – relative performance of computer systems.

Despite the seeming simplicity of the classical formulation of the problem, in practice it is rarely possible to use the above results. This is due to the complexity of the mathematical description of reducing the possible unauthorized access from the cost of designing a complex of information protection tools. If the dependence of

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 3, March 2019

protection on the cost of protective equipment can be obtained with the technical and cost characteristics of protective equipment available on the market, but it is extremely difficult to estimate the actual damage from unauthorized access [5], since this damage also depends on many factors affecting the probability of damage.

The choice of information protection means is carried out with the best indicators and therefore, the influence of the cost of protection means on efficiency can be neglected, that is, if $C << U$, that:

$$U_{\Sigma} = \frac{U}{f(C)}. \tag{1.3}$$

In this case (1.1) and (1.2) take the form:

$$\begin{aligned} U_{\Sigma} &\to \min \\ C &= C_{alw} \end{aligned} \tag{1.4}$$

Or

$$\begin{aligned} E_3 &\to \max, \qquad \delta_3 \to \max, \\ C &= C_{alw} \qquad C = C_{alw}. \end{aligned} \tag{1.5}$$

where C_{add} - allowable protection costs.

Thus, unauthorized access to information in the CSPV will depend on the information security tools used, on the number of information security threats, the degree of security and the operation time of the CSPV [5].

Let designed CSPV containing k units, each of which is possible implementationN_i, *i* = 1,2,...,*k*information security threats. All in all, CSPV contains *S* possible to implement security threats, and $S = N_1 + N_2 + ... + N_k = \sum_{i=1}^{k} N_i$, Parry security threats are carried out by means of information protection included in the set of information protection tools. Information security tools have various security functionalities, depending on the characteristics of the protection mechanisms, technical requirements, compatibility with other protection tools, economic and ergonomic characteristics.

To distinguish between a set of information security tools, it is advisable to enter weights.M_i, *i* = 1,2,...,*k*. The higher the security classification of the information processed, the stricter the protection requirements, the higher the technical requirements and characteristics, the greater the value should be assigned to the coefficient$M_i$and vice versa.

It is assumed that a possible unauthorized access to information when at least one security threat is implemented occurs with probability P_x , and the probability of unauthorized access to information in the implementation of all security threatsP_y.

Recall that the considered CSPV contains *S* possible to implement security threats. Suppose that all threats are random with an equiprobable distribution law. Then, the probability of unauthorized access to information during the implementation of one specific security threat without the relative location of its implementation and the security of a set of information security tools against unauthorized access is determined as follows:

$$P_S = \frac{1}{S}. \tag{1.6}$$

In order to take into account the vulnerabilities of the CSPV of the unit, the presence of which is a prerequisite for the formation of a channel for the realization of security threats [6], it is necessary to enter a weighting factor in (1.6)M_i, taking into account the characteristics of the information security tools used for this *i*-th unit. If a$M_i$enter the denominator of expression (1.6), then the resulting expression will reflect the physics of the process of unauthorized access to information when implementing one of the security threats of the i-th unit, i.e. we will receive:

$$P_{iS} = \frac{1}{M_i + S}. \tag{1.7}$$

Indeed, if $M_i = 0$, which corresponds to the absence of protection, then (1.7) turns into (1.6). What if$M_i$will increase, the probability of unauthorized access to information will decrease, which correctly reflects the physics of the phenomenon.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 3, March 2019

Recall that CSPV of an arbitrary *i*-th subdivision contains N_i possible to implement security threats. Therefore, for the likelihood of unauthorized access to information U_i when implementing at least one security threat from N_i possible threats of the *i*-th subdivision will be fair expression:

$$U_i = 1 - (1 - P_{iS})^{N_i}. \quad (1.8)$$

Security threats of the same type exist in k units, where they can also form channels for the realization of threats. Therefore, for the probability of unauthorized access to information when at least one security threat is implemented, taking into account all k divisions, the expression defined by the formula for calculating the total probability of events will be true:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \sum_{i=1}^{k} \frac{N_i}{S} \left[1 - (1 - P_{iS})^{N_i}\right] \quad (1.9)$$

where is the meaning η_i determined by the ratio $\eta_i = \frac{N_i}{S}$.

Value P_x denotes the probability of unauthorized access to information in at least one unit when at least one security threat is implemented, that is, the probability of unauthorized access to information when at least one of S threats is implemented.

If there is an equal number of possible security threats in the units, i.e. $N_1 = N_2 = ... = N_k$, $S = N_1 + N_2 + ... + N_k = k \cdot N_i$,

Consequently,

$$\eta_i = \frac{N_i}{S} = \frac{N_i}{k \cdot N_i} = \frac{1}{k},$$

then the formula (1.9) takes the following form:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \frac{1}{k} \sum_{i=1}^{k} \left[1 - (1 - P_{iS})^{N_i}\right] \quad (1.9.1)$$

Note that the formula (1.9 and 1.9.1) determines the probability of unauthorized access to information when implementing at least one of the possible security threats for all units in the CSPV. It is fair to assume that in this case the total damage caused will be minimally possible. On the other hand, the probability of unauthorized access of information in the implementation of at least one security threat will, as a security feature, take the maximum possible value, i.e. the upper bound estimate of the probability of unauthorized access to information in CSPV [5].

Next, we introduce the following assessment of the security of information, defined as the probability of unauthorized access to information when implementing all possible security threats at the same time.

The maximum damage occurs when, as mentioned above, when all possible security threats are realized, that is:

$$P_y = \prod_{i=1}^{k} P_{iS}^{N_i}. \quad (1.10)$$

Thus, two assessments of the protection of CSPV are given P_x and P_y give the upper and lower bounds on the likelihood of unauthorized access to information, which corresponds to the best and worst case of damage to the CSPV as a whole.

For a given interval value T_p You can determine the number of possible attempts to implement all or at least one security threat R during the exploitation of the CSPV facility T:

$$R = \frac{T}{T_p}, \quad (1.11)$$

where T - operation time, T_p - security threats implementation step.

Knowing the number of attempts, it is possible to estimate the probability of unauthorized access to the protected information when all or at least one security threat is implemented during the operation T:

$$P(t) = 1 - (1 - P_k)^R, \quad (1.12)$$

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 3, March 2019

where is the meaning $P_к$ - This is a certain estimate that characterizes the probability of one successful attempt to implement security threats, and $t = T$.

It should be emphasized that the expression (1.12) can be used throughout the entire list of security threats for a specific CSPV, and selectively, for threats that constitute a certain focus. In particular, you can identify security threats, the implementation of which violates the confidentiality of information, its integrity or availability.

IV. RESULT

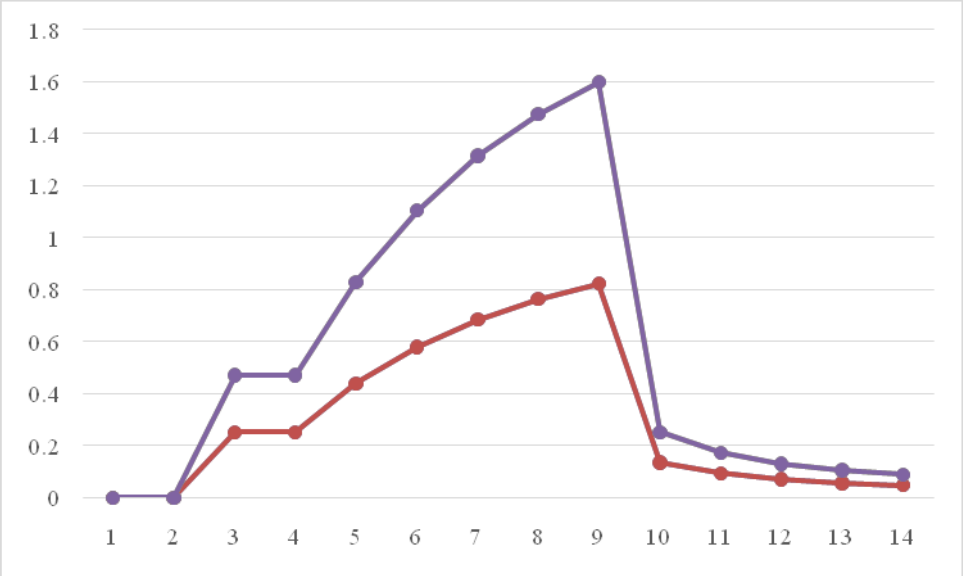

Figure 1.1. Evaluation of information security in CSPV depending on R

Having concluded, we can say that P_x increases significantly with increasing attempts to implement security threats. If the violator makes five attempts, this probability increases to 33%.

V. CONCLUSION AND FUTURE WORK

Thus, the developed analytical assessments make it possible to calculate the upper and lower bounds of the probability of unauthorized access to information and the number of attempts to implement security threats during the design stages of A CSPV.

Taking into account the preference in using probabilistic-time indicators of security in further studies, it is proposed to develop a mathematical model for evaluating the temporal indicators of security of CSPV depending on the abuser's capabilities.

REFERENCES

[1] Sheglov A. Yu. Zashitakompyuternoyinformatsiiotnesanksionirovannogodostupa. SPb: Naukaitexnika,2004. 384 s.

[2] MelyukA. A., PazizinS. V., PogojinN. S. Vvedeniyevzashituinformatsiivavtomatizirovannixsistemax. -M.: Goryachayaliniya - Telekom, 2001.- 48s.

[3] Suxoparov, I.N. Solovev, I.S. Lebedev, I.I. KomarovM.Ye. Metodikaanalizaarxitekturisistemzashitiinformatsiinaosnovetipovix elementov. Nauchno-texnicheskiyvestnikinformatsionnix texnologiy, mexanikiioptiki, 2013, № 3 (85).

[4] F.G. Xisamov, A.S. Juk, R.S. Sherstobitov, Matematicheskaya model otsenkizashishennostiinformatsiiotnesanksionirovannogodostupapriproyektirovaniiavtomatizirovannixsistem v zashishennomispolnenii. IzvestiyaSFedU. Texnicheskiyenauki. 2018, S.91-102.

[5] Gribunin V.G., Chudovskiy V.V. Kompleksnayasistemazashchityinformatsiinapredpriyatii: ucheb. posobie [A complex system of information protection at the enterprise: textbook]. Moscow: ITs Akademiya, 2009, 416p.

[6] NavikovA.A., UstinovG.N., UyazvimostIinformasionnayabezopasnosttelekommunikasionnixtexnologiy:ucheb.posobiedlyavuzov. – M.: Radioisvyaz, 2003. - №6- S.46-48.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 3, March 2019

KadirovMirhusanMirpulatovich. Assistant professor.
was born May 22, 1985 year in Tashkent city, Republic of Uzbekistan.
Has more than 85 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

Karimova NazimakhanAybekovna, Senior Lecturer.
was born 04.01.1971 year in Tashkent city, Republic of Uzbekistan. Has more than 15 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

DjurayevaShokhistaTagirovna, Senior Lecturer.
was born 05.05.1965 year in Tashkent city, Republic of Uzbekistan. Has more than 10 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

NosirjonovaMunisaMuzaffarqizi.Student.
was born 12.06.1995 year in Tashkent city, Republic of Uzbekistan.Student of the Faculty of Mining and Metallurgy, Tashkent State Technical University.