ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

Approach to assessing the security of information from unauthorized access

KadirovMir-khusanMirpulatovich

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

ABSTRACT: The purpose of this article is to propose a methodology for assessing the security of information from maliciously studying technical means of protecting information for further unauthorized access to protected information. The linear theory of algorithms in solving the problem of estimating the time required for an attacker to study the information security system is considered.

KEYWORDS: computer systems,access, unauthorized access, realization of threats, vulnerability, intruder, degree of security, signature stamp

I. INTRODUCTION

Of particular importance in the world is the improvement of effective methods and means of information protection, the organization of controlled information applications, and the development of models and algorithms for protecting information from unauthorized access[1-3].

Statistics of unauthorized access to information show that most modern information systems are quite vulnerable from a security point of view. The solution to 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[4].

II. THE LINEAR THEORY OF ALGORITHMS IN SOLVING THE PROBLEM OF ESTIMATING THE TIME REQUIRED FOR AN ATTACKER TO STUDY THE INFORMATION SECURITY SYSTEM

Assuming that the task of studying (decrypting) a program of length N written in some algorithmic language is commensurate with the complexity of writing a program of length N bits in the same language, we use the approximation of the time equation necessary to write a program if only the length of the program is known - N bits [5]. In this case, the average time of studying (decoding) the program - T can be found as:

$$T = \frac{N_2^2 \times log_2 \eta}{4 \times S} [c] \quad (1)$$

where: $\eta -$ program language language alphabet;

$S -$the Stroud number ($S = 4 \div 20$ operations per second), characterizes the number of objects that an attacker can operate simultaneously (a kind of performance characteristic of an attacker studying a program text);

$N -$program text length (instructions + operands) in bits.

$$T \approx N^2, [c]$$

Since information protection programs are characterized by a long length, and the work of an attacker is characterized by fatigue, we introduce a correction for the fatigue of an attacker, then the expression for T will look like:

$$T \approx 3N^2, [c] \quad (2)$$

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

III. CATASTROPHE THEORY IN SOLVING THE PROBLEM OF ASSESSING THE PROBABILITY OF DECODING A PROGRAM TEXT ON A TIME INTERVAL

Information security theory requires that an attacker be considered as a subject of high qualification, which makes it possible to put the malicious distribution process of the information protection system into the distribution function of a smart attacker. exponential distribution with parameter.

$$S = \frac{1}{T}[c]$$

Here $T -$ average time for decoding (studying) the text of a program.

In this case, the probability (P_u) of undecoding the program text for a certain time interval (no disaster occurs), distributed in turn according to the exponential law with parameter β, can be represented according to [6] as the Laplace-Stieltjes transform of the distribution function of the time interval over which the probability is estimated decryption (study) of the text $B(t)$:

$$P_u = \int_0^\infty e^{-st} dB(t) = \frac{\beta}{\beta+s} \quad (3)$$

Thus, we managed to "smoothly" switch from the length of the text of program N written in some algorithmic language, which the developer of the information protection system "provided" for the attacker, to the probability of undeciphering the text of the protection program for a certain time interval, which in turn is distributed exponentially[7]. It is assumed that the hardware of the information protection system allows for "unfolding" into the text of the program of finite length and the "text of the protection program" is the sum of the texts of the software and hardware.

IV. INFORMATION SECURITY FROM UNAUTHORIZED ACCESS

It is known that for the implementation of unauthorized access to information, leading to disruption of the normal functioning of computer systems, confidentiality, integrity and accessibility of information, the violator will always spend the time T_{una} necessary to form a channel for realizing a threat to the security of information, that is, the specified time characterizes the time interval:

$$T_{una} = \sum_{i=1}^{4} T_i$$

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

Based on this, by increasing $T_i 1$ it would always be possible to control the security of information in secure computer systems (SCS). That is, T_i could be taken as a criterion for assessing the security of information in secure computer systems. Then, by setting the threshold value of $T_{add\ una}$ during the design of the SCS and ensuring the fulfillment of condition $T_i \leq T_{add\ una}$, it would be possible to implement acceptable protection of limited access information in the SCS.

However, this approach will not reflect the real picture, since time 1 is a random variable whose distribution law is difficult to calculate, since it will vary depending on the capabilities of the violator. In addition, the main factors of operation are not taken into account here, such as: various threats to information security in the SCS, the operating time of the SCS, the characteristics of the information protection tools used, which can also affect unauthorized access to information.

Therefore, to increase the objectivity of monitoring the timeliness, reliability, completeness and continuity of information security designed by the SCS, 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 the complex of information protection tools. On the basis of the found model, formulate qualitative and quantitative criteria for increasing information security in the design of computer systems.

It is known that the classic statement of the problem is the development of information security systems to ensure maximum efficiency of the functioning of computer systems under unauthorized access will look like:

$$\begin{gathered} U_\Sigma \to min \\ C = C_{opt} \end{gathered} \quad (1)$$

where U_Σ is the total damage caused; $C -$ the cost of designing a complex of information protection tools or

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

$$E_3 \to max, \quad \delta_3 \to max, \\ C = C_{opt} \qquad C = C_{opt} \tag{2}$$

where E_3 – the effectiveness of the functioning of computer systems; δ_3 – relative efficiency of functioning of computer systems.

Despite the apparent simplicity of the classical formulation of the problem, in practice it is rarely possible to use the results presented. This is due to the complexity of the mathematical description of the reduction of possible unauthorized access from the cost of designing a complex of information protection tools. If the dependence of security on the cost of remedies can be obtained with the technical and cost characteristics of the remedies available on the market, it is extremely difficult to assess the real damage from unauthorized access [14], since this damage also depends on many factors affecting the likelihood of damage.

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

$$U_\Sigma = \frac{U}{f(C)} \tag{3}$$

In this case (1) and (2) take the form:

$$U_\Sigma \to min \\ C = C_{add} \tag{4}$$

Or

$$E_3 \to max, \quad \delta_3 \to max, \\ C = C_{add} \qquad C = C_{add} \tag{5}$$

where C_{add} is the allowable cost of protection.

Thus, unauthorized access to information in the SCS will depend on the information security tools used, the number of threats to information security, the degree of security and the operating time of the SCS.

Let the SCS be designed, containing k units, each of which may implement $N_i, i = 1, 2, \ldots, k$information security threats. In total, the SCS contains S possible security risks, and $S = N_1 + N_2 + \ldots + N_k = \sum_{i=1}^{k} N_i$. Security threats are countered by means of information security included in the complex of information security tools. Information protection tools have various functionalities for providing protection, depending on the characteristics implemented by the protection mechanisms, technical requirements, compatibility with other protection means, economic and ergonomic characteristics.

To distinguish between a set of information protection tools, it is advisable to introduce weight coefficients $M_i, i = 1, 2, \ldots, k$. The higher the security stamp of the processed information, the more stringent the requirements for protection are 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 during the implementation of at least one security threat occurs with a probability of P_x, and the probability of unauthorized access to information when all security threats are realized is P_y.

The considered SCS contains S possible security threats. Suppose 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 a relative place for its implementation and the security of a set of means of protecting information from unauthorized access is determined as follows:

$$P_S = \frac{1}{S} \tag{6}$$

In order to take into account the vulnerabilities of the SCS unit, the presence of which is a prerequisite for the formation of a channel for implementing security threats [17], it is necessary to introduce the weight coefficient $M_i$in (6), taking into account the characteristics of the used information protection tools for this i-th unit. If M_i is introduced into the denominator of expression (6), then the resulting expression will reflect the physics of the process of unauthorized access to information when one of the security threats of the i-th unit is realized, i.e. we get:

$$P_{iS} = \frac{1}{M_i + S} \tag{7}$$

Indeed, if $M_i = 0$, which corresponds to the absence of protection, then (7) turns into (6). And if M_i increases, then the probability of unauthorized access to information will decrease, which correctly reflects the physics of the phenomenon.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

Recall that the SCS of the arbitrary i-th unit contains N_i possible security threats. Therefore, for the probability of unauthorized access to information U_i when realizing at least one security threat from N_i possible threats of the ith unit, the following expression will be true:

$$U_i = 1(1 - P_{iS})^{N_i} \tag{8}$$

There are similar security threats in k units, where they can also form channels for implementing threats. Therefore, for the probability of unauthorized access to information when at least one security threat is realized, taking into account all k units, the expression defined by the formula for calculating the total probability of events will be valid:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \sum_{i=1}^{k} \frac{N_i}{S} [1 - (1 - P_{iS})^{N_i}] \tag{9}$$

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

The value P_x indicates the probability of unauthorized access to information in at least one unit when at least one security threat is realized, that is, the probability of unauthorized access to information when at least one of S threats is realized.

If the units have the same number of possible security risks, i.e.

$$N_1 = N_2 = \ldots = N_k, \quad S = N_1 + N_2 + \ldots + N_k = k \cdot N_i$$

Consequently

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

then formula (9) takes the following form:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \frac{1}{k} \sum_{i=1}^{k} \left[1 - (1 - P_{iS})^{N_i}\right] \tag{9.1}$$

Note that the formula (9 and 9.1) determines the likelihood of unauthorized access to information when at least one of the possible security threats is realized for all units in the SCS. It is fair to assume that in this case the total damage caused will be the minimum possible. On the other hand, the probability of unauthorized access to information during the implementation of at least one security threat as a security feature will take the maximum possible value, i.e. the upper boundary estimate of the probability of unauthorized access to information in the SCS [8].

The maximum damage occurs when, as mentioned above, in the implementation of all possible threats to the implementation of security, that is:

$$P_y = \prod_{i=1}^{k} P_{iS}^{N_i} \tag{10}$$

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

For a given value of the interval 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 SCS object T:

$$R = \frac{T}{T_p}, \tag{11}$$

where T is the operating time, and T_P is the step of implementing security threats.

Knowing the number of attempts, it is possible to assess the likelihood of unauthorized access to protected information when all or at least one security risk is realized during operation T:

$$P(t) = 1 - (1 - P_k)^R, \tag{12}$$

where the value P_k is a certain assessment that characterizes the probability of one successful attempt to implement security threats, as well $t = T$.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

V. RESULT

Using the proposed approach, we present simulation modeling to assess the security and the degree of influence of operational indicators for various SCS.

It should be emphasized that expression (12) can be used both over the entire list of security threats for a specific SCS, and selectively, for threats that make up a certain orientation. In particular, it is possible to single out security threats, the implementation of which violates the confidentiality of information, its integrity or accessibility. For different SCS, the damage from the implementation of security threats of various directions may differ significantly. This is due to the variety of SCS in terms of the functions performed. For example, threats to the confidentiality of information for information-based information services are more relevant than threats, a direction to violate the availability of information. On the other hand, for the SCS, the management of a critically important object of a threat of violation of the availability and integrity of information plays a major role, in connection with the possible consequences of a disruption to the system. Such a polymorphism of expression (12) is its important advantage, since there is no need to adjust the methods for calculating the assessment of information security depending on the composition of security threats in the SCS.

The obtained quantitative results of simulation can be presented in tabular or graphical form. It should be emphasized that the expression (12) gives an upper bound on the probability of unauthorized access to information in the SCS, that is, for the worst case, which is a particularly important indicator in the design of the SCS.

Tables 1 and 2 show how the security ratings P_x and $P_y$are numerically different for SCS with different initial parameters.

Table 1. Assessment of information security for SCS.

	SCS 1	SCS 2	SCS 3	SCS 4	SCS 5
S	18	20	12	15	30
k	3	3	3	3	3
N_1	5	4	3	5	10
N_2	6	6	4	5	10
N_3	7	10	5	5	10
M_1	9	5	3	3	3
M_2	3	2	4	3	3
M_3	6	9	2	3	3
P_1	0,037037	0,04	0,066667	0,055555	0,030303
P_2	0,047619	0,045455	0,0625	0,055555	0,030303
P_3	0,04166	0,034483	0,071429	0,055555	0,030303
U_1	0,171966	0,150653	0,186963	0,248581	0,264876
U_2	0,253784	0,243551	0,227524	0,248581	0,264876
U_3	0,257637	0,295955	0,309638	0,248581	0,264876
P_x	0,232555	0,251174	0,251598	0,248581	0,264876
P_y	1,77E-25	5,37E-29	8,41E-15	1,48E-1	2,78E-46

Table 2. Assessment of information security for SCS.

	SCS6	SCS7	SCS8	SCS9	SCS10
S	40	40	40	40	40
k	4	4	4	4	4
N_1	10	10	20	10	10
N_2	10	10	5	10	10
N_3	10	10	7	10	10
N_4	10	10	8	10	10
M_1	6	1	1	6	4
M_2	5	1	1	6	3
M_3	4	1	1	6	9
M_4	2	1	1	6	8

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

P_1	0,021739	0,02439	0,02439	0,02739	0,022727
P_2	0,022222	0,02439	0,02439	0,02739	0,023256
P_3	0,022727	0,02439	0,02439	0,02739	0,020408
P_4	0,02381	0,02439	0,02439	0,02739	0,020833
U_1	0,197312	0,218802	0,389729	0,197312	0,205383
U_2	0,201267	0,218802	0,116146	0,197312	0,20967
U_3	0,205383	0,218802	0,158735	0,197312	0,186324
U_4	0,214139	0,218802	0,179253	0,197312	0,189849
P_x	0,204525	0,218802	0,273012	0,197312	0,197806
P_y	1,49E-66	3,08E-65	3,08E-65	3,09E-67	3,28E-67

Let us analyze the dependence of the quantitative assessment of the probability of unauthorized access to information during the implementation of at least one P_x security risk from the operational parameters of the SCS.

So in table 1, the highest value of $P_x = 0.264876$ is taken in SCS№5 with the number of security threats $S = 30$. With lower values of S, the value of $P_x$will decrease: $P_x = 0.232555$ with the amount of $S = 18$ in SCS№1, $P_x = 0.251174$ with the amount of $S = 20$ in SCS№2, $P_x = 0.251598$ with the amount of $S = 12$ in SCS№3, $P_x = 0.248581$ with an amount of $S = 15$ in SCS№4.

VI. CONCLUSION AND FUTURE WORK

Thus, the developed analytical estimates allow us to calculate the upper and lower bounds on the probability of unauthorized access to information and the number of attempts to implement security threats at the design stages of the SCS.

Given the preference for using probabilistic-temporal indicators of security in further studies, it is planned to develop a mathematical model for assessing the temporary indicators of security of the SCS depending on the capabilities of the intruder.

REFERENCES

[1] Gulomov S.R., Kadirov M.M., Protection of information from network attacks // Monograph, “Fan vatexnologiya”, ISBN 978-9943-6155-4-0, Tashkent - 2019, P 172.

[2] Mirpulatovich K. M., Zakirovna T. N., Ismoilovna K. G. Classification of Modern Security Monitoring Systems in Computer Systems and Networks, International Journal of Advanced Research in Science, Engineering and Technology, Vol. 5, Issue 9, India 2018, p. 6764–6769.

[3]Rajaboevich G. S., Mirpulatovich K. M., Yakubdjanovich T. Z. The Methodology of the Ways for Increasing the Efficiency of Intrusion Detection Systems //International Journal of Engineering Innovations and Research, Vol. 5, Issue 5, India 2016, P. 296–301.

[4] Sagatov M., Irgasheva D., Mirhusan K. Construction Hardware Protection Infocommunication Systems from Network Attacks //Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE), 2015. – P. 271.

[5] Xolsted M. X. Nachalanauki o programmax//M.: Finansiistatistika. – 1981. – T. 128.

[6] Mizin I. A. Peredachainformatsii v setyax s kommutatsieysoobsheniy. – 1977.

[7] Ivanov V. P. Matematicheskayaotsenkazashishennostiinformatsiiotnesanktsionirovannogodostupa //Spetsialnayatexnika. – 2004. – №.1. – S. 58-64.

[8] Avramenko V. S., Kozlenko A. V. Model dlyakolichestvennoyotsenkizashishennostiinformatsiiot NSD v AS pokompleksnomupokazatelyu//TrudiSPIIrAn. – 2010. – T. 13. – №. 0. – S. 172-181.

AUTHOR’S BIOGRAPHY

Mir-khusan Kadirov assistant professor was born May 22, 1985 year in Tashkent city, Republic of Uzbekistan. In 2008 graduated «Information technology» faculty of Tashkent University of Information Technologies. Has more than 90 published scientific works in the form of articles, journals, theses and tutorials in the field Computer science and Cyber Security. Currently works in the department «Information Technology» at the Tashkent State Technical University named after Islam Karimov.