Combined Multi-Level Information Protection With Probability Reliability

Borys Zhurylenko[1][0000-0003-2980-5630], Kirill Nikolaev[2][0000-0002-2633-6907]

[1]National Aviation University, Fish str., 24a, Kiev, 03118, Ukraine
zhurylenko@gmail.com
[2]N.Uzhviy str. 8/140, Kiev, 04108, Ukraine
kyrylo.nikolaiev@gmail.com

Annotation. In this work, theoretical studies of the physical hacking process for combined multi-level technical information protection (TIP) with probabilistic reliability are carried out. The research uses an approach related to the reliability of various equipment, technical devices and systems, which have been studied in sufficient details and have delivered good practical results with quantitative probabilistic assessment. To calculate and evaluate the capabilities of combined multi-level technical information protection, there were used single-level TIP with probabilistic reliability which were proposed and considered in the works of B. Zhurylenko (B. Zhurilenko). A method for constructing a combined multi-level technical protection of information with probabilistic reliability and the possibility of comparing it with equivalent single-level protection is proposed. Studies of the combined information protection scheme for the selected parameters of single protection showed some improvement in information protection compared to single-level protection. Possibilities for increasing the effectiveness of protection require additional research. This approach will allow us to explore more complex information protection schemes. Studies have shown that the calculated surface of the distribution of the maxima of the probabilities of hacking equivalent single-level TIP does not coincide with the distribution of the maximum probability of hacking the combined TIP. Therefore, protection comparisons are only possible in the hacking direction selected for analysis. The paper proposes a method for determining the real probability of hacking a combined defense not by the maximum value of the probability of hacking, but by the distribution of the probability of combined multi-level TIP hacking, since hacking of a TIP may not necessarily occur at the maximum values of hacking probability. In this case, based on the constructed surfaces of hacking probabilities, the real reliability of the TIP can be determined for any direction of hacking.

Keywords: technical information protection, equivalent single-level protection, combined multi-level information protection with probabilistic hacking, distribution of the maximum probability of hacking, distribution of hacking probability, the real process of hacking.

1 Introduction

The security of the circulating information in software-controlled technical systems, and its leak will be determined by the physical, technical and software interactions of these systems and it is reflected in the works [1-6]. For example, in a computer system, information security will depend on the access of various devices to device where this information is stored. Access to stored information can be carried out through parallel and serial devices. Such a scheme of operating devices complicates the assessment of stored information leak. Parallel and serial devices can significantly change the probability of access to protected information. From information security point of view, the work of parallel and serial devices can be represented as a combined multilevel technical information protection (TIP). To determine the overall probability of hacking into such a complex multi-level TIP, you can determine the probability of hacking through an equivalent single-level protection. Such an approach will make it possible to evaluate and compare various combined multi-level information access systems with probabilistic reliability. B. Zhurilenko’s works addressed in sufficient detail the issues of hacking single-level information protection, but paid almost no attention to design issues and analyzing the state of functioning combined multi-level protection. Known methods for calculating the reliability of various equipment [7], technical devices and systems that have been studied in sufficient detail and have provided good practical results with quantitative probabilistic assessment. These methods deliver good results in ensuring the reliability of various technical systems and devices; therefore, it is advisable to use these methods for calculating the reliability of the design and analysis of the state of multilevel information protection systems, especially since the one-level protection systems considered in B. Zhurilenko’s works give a quantitative probabilistic assessment and may be applicable for calculating the total probability of combined TIP hacking.

In practice, the main difficulty in assessing and analyzing the state of combined multi-level technical protection of information using the single-level protections is that it is not known which of the single-level protections has already been hacked (for different protection efficiency factors) and what is the probability of this multi-level protection hacking. It is possible to assess the state of combined multi-level protection if the general distribution of the maximum probability of TIP hacking is known.

From the whole variety of technical interaction and rather complex technical systems in which information circulates, we consider the combined protection of information with probabilistic reliability, consisting of two parallel and then one serial protection.

The aim of the work is to obtain surfaces of the distribution of the maximum probability and probability distribution of hacks for a combined multilevel information protection system and its comparison with the equivalent distribution of single-level protection, which will allow us to study and compare different types of combined multilevel information protections during their work, design and modernization.

The relevance of study is proved by fact that, in contrast to regulatory documents, a new approach to the development of a multilevel TIP based on real physical processes of hacking information is considered.

Scientific novelty of study is represented by development of a new methodology for the approach to the design, modernization and analysis of the working condition of a combined multilevel TIP in order to save financial costs invested in protection.

2 Description of the problem

It is known [7] that the probability of complex technical systems failure will be determined by the reliability probabilities of these systems' components. For TIP, the presentation of complex technical systems will correspond to penetration through a combined multilevel defense, for which an attacker needs to hack specific protections that have access to information.

Figure 1 shows the structural diagram of the combined multi-level information protection. Access to information (output 3) is possible from inputs *1* and *2*. Information is protected by devices with hacking probabilities ***P1***, ***P2***, ***P3***. If inputs 1 and 2 are interconnected (dotted connection **a-b**), then we will have parallel protection with the probabilities of hacking ***P1, P2*** and a series of protection with a probability of hacking ***P3***. If inputs *1* and *2* are not interconnected, then we get two separate inputs with access to information through sequential protections with hacking probabilities ***P1, P3*** and ***P2***, ***P3***. Studies of the probability distributions and the maximum probability of hacking for a sequential two-level information protection system and its comparison with the equivalent distribution of single-level protection were considered earlier.

In this paper, we will carry out theoretical studies of the hacking process of the combined multi-level data protection shown in Fig. 1, with connection a-b between inputs *1* and *2*. If attempts to crack the protection will be carried out simultaneously through inputs *1* and *2*, then we will calculate probability distributions using different intensities and directions of hacks.

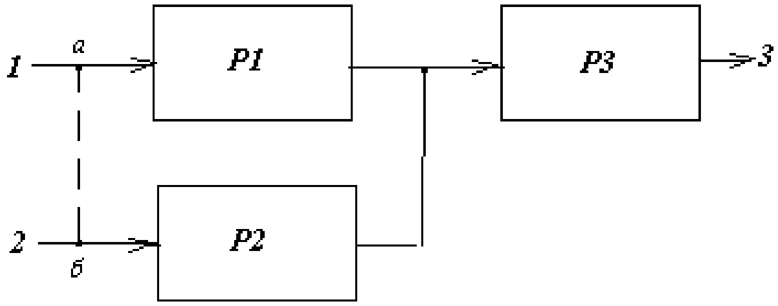

Fig. 1. The structural diagram of the considered combined information security; *1, 2* - inputs from information access devices; *3* - output to the information storage device; **a-b** - a possible connection between inputs *1, 2*; ***P1, P2, P3*** - probabilities of hacking protection with unauthorized access to information.

3 Theoretical construction and study of a combined multi-level information protection system and its comparison with the effective distribution of single-level protection

There are publications [8-10] for single-level information protection, in which the probability distribution of hacking is obtained depending on the funding invested in protection, the coefficient of protection efficiency and the direction of the hacking process, that is, on the attempt m and the time of this hacking attempt t. The surface of the distribution of the hacking probability maxima will be described by the expression

$$
\begin{aligned}
P_{взлі}(m,t) &= \{ P(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m,t)}{t}} \cdot [\frac{t}{f(m,t)+t}]\}^{\gamma} = \\
&= \{ P(X) \cdot [\frac{f(m)}{f(m)+t}]^{\frac{f(m)}{t}} \cdot [\frac{t}{f(m)+t}]\}^{\gamma}
\end{aligned}
\qquad (1)
$$

where *m, t* are the current coordinates of the attempt and the time of hacking; the function *f(m, t)* determines the probabilistic reliability of protection and the direction of hacking; *γ* - takes into account the effectiveness of security and is determined by the ratio of the risks of invested financing in protection to total financial losses [11]; *P(X)* - the probability of TIP hacking from the investment in its construction [11].
The function *f(m, t),* depending on the change in one of the coordinates, can be represented as an attempt to hack into *m* and the direction or intensity of hacking

$$
f(m) = [t_1 + \frac{1}{\omega} \cdot (m - m_1)] \cdot (m - 1) \qquad (2)
$$

where $\omega = \frac{m_2 - m_1}{t_2 - t_1}$ is the direction or intensity of hacking [11].

The surface of the probability distribution of hacking will be described by the expression

$$
\begin{aligned}
P1_{взлі}(m,t) &= \{ P(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m_c,t_c)}{t_c}} \cdot [\frac{f(m,t)}{f(m,t)+t}]\}^{\gamma} = \\
&= \{ P(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m_c)}{t_c}} \cdot [\frac{f(m,t)}{f(m,t)+t}]\}^{\gamma}
\end{aligned}
\qquad (3)
$$

where the function $f(m_c, t_c)$, which determines the direction of hacking, depending on the change in one of the coordinates, can be represented as the maximum value of a hacking attempt with coordinates m_c and t_c.

$$f(m_c, t_c) = f(m_c) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m_c - m_1)] \cdot (m_c - 1). \qquad (4)$$

Equations (1), (2), (3), and (4) allow us to calculate the probabilities of hacking of a combined multilevel defense, which is a complex of single defenses. This approach to calculating the probability of hacking into multilevel protection is one of the ways to assess the probabilistic reliability of a multilevel complex of technical information protection (TIP).

Let us consider the case of TIP presented in Fig. 1, which consists of three single-level information protection systems with distributions of maximum hacking probabilities for one or the first protection ***P1*** = *P1$_{max}$*, the other or the second - ***P2*** = *P2$_{max}$*, and the third - ***P3*** = *P2$_{max}$*, whose surfaces are determined by the expression (1), that is, the distributions of the maximum probabilities of hacking for the second and third defenses are the same. To calculate and plot surfaces of the maximum probabilities of hacking, we will assume that the parameters of the first defense ***P1*** will be: *X1=x/H=0,5*, *x* - financing invested in the first defense, *H* - financial losses if no protection used; *γ1=X1/ (1 + X1) = 0.333* - coefficient of effectiveness of the first defense; *P1 (X1)=X1^{X1}/ (1 + X1)* $^{(1\ +\ X1)}$ =0.385 - the maximum probability of hacking from the given invested financing in defense of *X1*; *ω1 = (m21-m11) / (t21-t11) = 1* - direction or intensity of hacking; *m11 = 1, t11 = 0* - initial conditions of the hacking process for the first defense (first hacking attempt and its time); *m12 = 3, t12 = 2* - subsequent hacking attempt and its time in the direction of hacking for the first single-level defense. Similarly, we determine the parameters for the second ***P2*** and third ***P3*** information protection: *X2 = 0,4* - reduced investment in the second and third protection; *γ2 = 0,286* - coefficient of effectiveness of the second and third protection; *P2(X2)=0,433* - the maximum probability of hacking from the reduced invested funding in the second and third protection *X2*; *ω2=(m22-m21)/(t22-t21)=0,429* - direction or intensity of hacking in the second and third protection; *m21 = 1, t21 = 0* - initial conditions of the hacking process for the second and third defense (the first hacking attempt and its time); *m22 = 7, t22 = 14* - subsequent hacking attempt and its time in the direction of hacking for the second and third single-level protection.

Figure 2 shows the surfaces of TIP hacking maximum probabilities distribution depending on the attempts and their hacking time (dark surfaces): for the first defense, Fig.2a along the line of hacking 1; for the second and third protection along hacking line 2 - Fig.2b. Line 1 indicates the hacking direction for the first single-level defense, and line 2 - for the second and third. The light surface gives the real probability of hacking into each of the defenses and is determined by the expression ***P$_{real}$=1/m***, where m is the current hacking attempt. It can be seen from Fig. 2 that there's no big difference in calculated surfaces for TIP hacking, although the calculated directions for hacking in these defenses are different.

Small differences in the surfaces of the maxima of the hack probabilities are explained by close values of the initial parameters. By the intersection of the dark, light surfaces of the maximum probabilities and the direction of the cracking line (Fig. 2), it is possible to determine the parameters of the maximum values of the probability of attempt and the time of this cracking attempt for single-level defenses with different hacking directions. It is possible that different hacking directions will allow designing multilevel complexes with greater information protection efficiency and comparing these multilevel TIP using their equivalent parameters for single-level protection by protective properties.

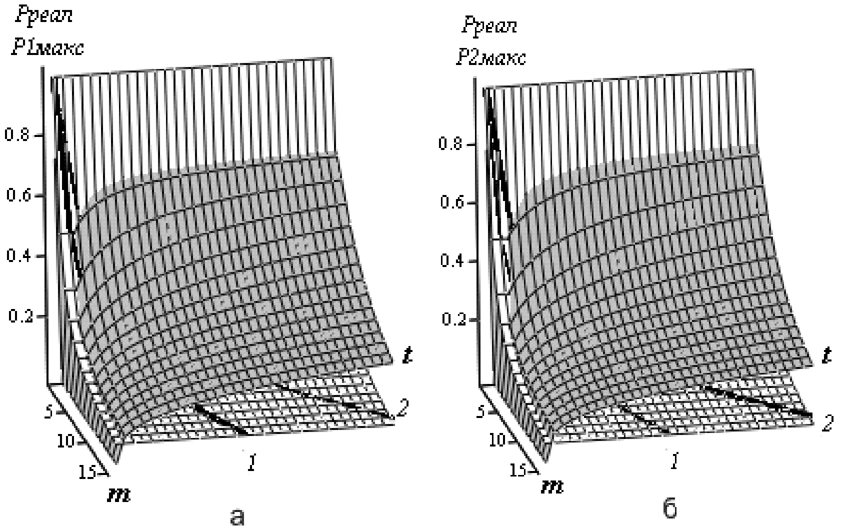

Fig. 2. The surface of the distributions of the maximum probabilities of hacking TIP depending on the attempts and their hacking time (dark surface); P1max - for the first protection of P1; P2max - for the second P2 and third P3; Rreal - probability distribution of real hacking (light surface)

For line 1 and the corresponding calculated surface, the coordinate of the hacking point for the first defense will be $m1_{взл} = 3$ and $t1_{взл} = 2$, and for the second, third protection and line 2, $m2_{взл} = 2$ and $t2_{взл} = 2$.

As a result, considered structural scheme (Fig. 1) of combined information protection and the probability of access to a device or information system will be determined by the expression

$$P_{макс0} = (P1_{макс} + P2_{макс} - P1_{макс} \cdot P2_{макс}) \cdot P2_{макс} \tag{5}$$

Let us determine the parameters of the attempt and its time of the maximum probability of hacking in the direction of line 2, for the selected block diagram of the combined multilevel TIP. Using these parameters of the maximum probability of hacking, we determine all the necessary parameters for the equivalent single-level protection.

Using the given initial data by formulas (1) and (5), we calculate the maximum probabilities of hacking the combined multilevel information protection. The calculation results are presented in Fig.3. It is seen that the maximum probability of hacking in the direction of line 2 will be at the intersection of the light (real) and dark (calculated) hacking surfaces at $m_{max}=7{,}5$ and $t_{max}= 5$. In the direction of line 1, the value of the maximum probability of hacking will be at large values of m_{max} and t_{max} and is not displayed in the calculated area shown in Fig. 3, since the intensity of hacking along line 1 is greater than along line 2.

To represent the parameters of a multilevel TIP through equivalent single-level protection, we use the formulas in [8-11]. In [8], an equation is presented for determining the coefficient of information protection efficiency of a single-level information protection.

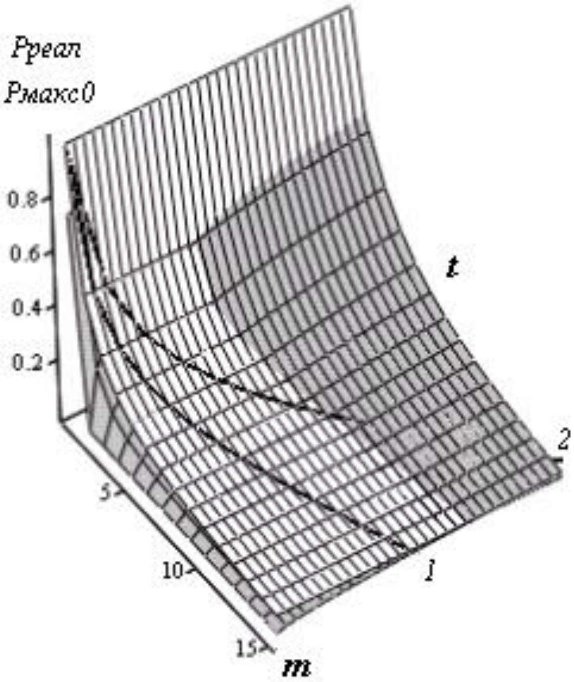

Fig. 3. Distribution of the maximum probability of hacking for combined multilevel information protection

$$\gamma = \frac{-ln(m_{max})}{ln[\frac{(m_{max}-1)^{(m_{max}-1)}}{(m_{max})^{m_{max}}}] + ln[\frac{(X_i)^{X_i}}{(1+X_i)^{(1+X_i)}}]} = \frac{X_i}{1+X_i}. \qquad (6)$$

Solving equation (6) regarding the effective reduced investment in two-level protection X_i by the point of maximum hacking, it is possible to determine all the necessary equivalent parameters of a single-level TIP.

Figure 4 shows a graphical solution to equation (6). Where $P(X_i)$ is the maximum probability of hacking from the effective reduced invested financing in defense of X_i; $f1(X_i)$ is the functional dependence of the middle part of equation (6) on X_i; $f2(X_i)$ is the functional dependence of the right side of equation (6) on X_i. The intersection of $f1(X_i)$ and $f2(X_i)$ gives a solution to equation (6) $X_i=0,9$. Given that the effective coefficient of single-level protection will be at $X_i=0,9$, we obtain $\gamma=f2(X_i)=0,47$.

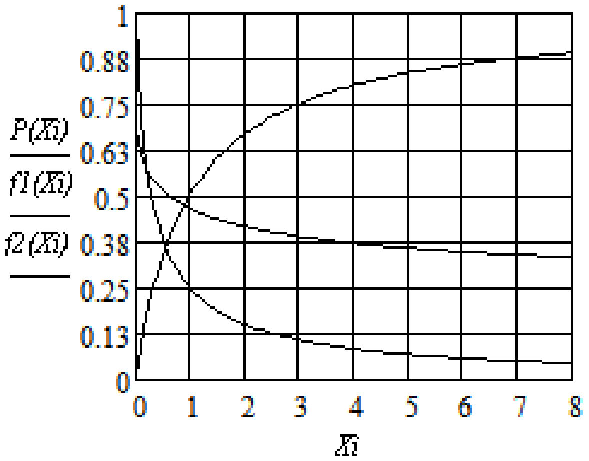

Fig. 4. Graphic solution of equation (6)

The graphical solution of equation (6) gives the following parameters for the equivalent single-level protection $P(X_i)=0{,}27$; $\gamma=0{,}47$. Using the obtained parameters and the direction of hacking along line 2 in formula (1), we obtain the surface of the maximum probabilities of hacks of single-level protection equivalent to the combined multi-level TIP shown in Fig.5. If it is necessary to determine the equivalent multi-level protection for combined protection in another hacking direction, it is necessary to construct this other direction in Fig.3 and determine the parameters of the maximum probability of hacking in this direction. And then, just as on line 2 and the parameters of hacking, determine all the necessary parameters for the equivalent single-level protection.

When comparing Fig.3 and Fig.5, it can be seen that a single-level protection equivalent to a multilevel TIP does not fully correspond to the maximum probabilities of hacking into the considered multilevel TIP. However, it should be noted that in the chosen direction of hacking, equivalent single-level defenses fully correspond to the parameters of the combined TIP and, therefore, various multi-level defenses in the chosen direction of hacking can be compared.

In practice, a real hacking process is not necessarily possible with a maximum probability of hacking. Real hacking is possible with other probabilities of hacking, although theoretically it is most possible with maximum probability. To determine the likelihood of a real hacking process, it is necessary to use the expression for the distribution of the probability of hacking (3) for each of the selected hacking directions with maxima for line 1 - $m1_{взл}=3$ and $t1_{взл}=2$, and for the second line 2 - $m2_{взл}=2$ and $t2_{взл}=2$, and build a hack probability distribution surface for combined multi-level protection. Calculating the probability distribution of hacking single-level defenses in accordance with (5), we obtain the real probability distribution of hacking the combined multi-level protection.

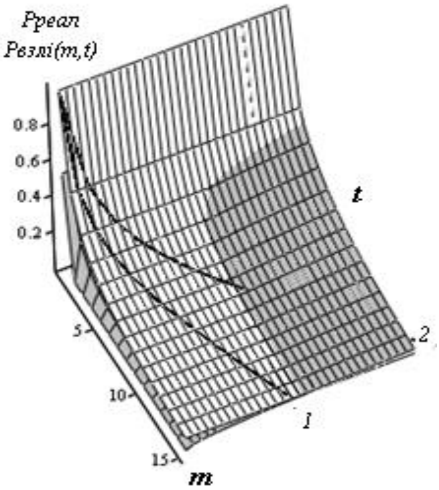

Fig. 5. Distributions of the probability surface of a real hack (light surface) and the maximum probability of a hack of a single-level protection equivalent to a combined multi-level TIP (dark surface)

Figure 6 shows the calculations of the surfaces of the distribution of the real probability of hacking (light surface) and the distribution of the probability of hacking a combined multi-level technical protection of information (dark surface), which are determined by formulas (3) and (5).

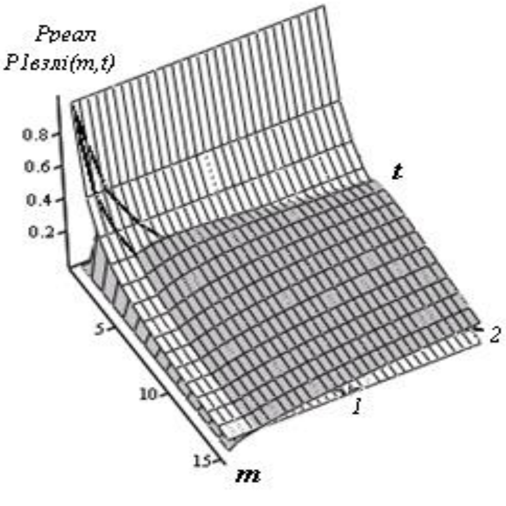

Fig. 6. Distributions of the real probability of hacking and the probability of hacking combined multilevel technical information protection

From a comparison of Fig.3 and Fig.6, it is seen that, in opposite to the distribution of the maximum probabilities of hacking (Fig.3), a real TIP hack is most likely for the direction along line 1 at the point *m1=4* and *t1=3* and for the direction along line 2 to point *m2=4* and *t2=6*. To determine the real probability of hacking in other directions, it is necessary to build these directions and find the intersection point of the surfaces of Fig.6. and other lines. The intersection point will give a possible real attempt and time for this attempt to hack into the TIP.

4 Conclusions

In this work, theoretical studies of the physical hacking process for combined multi-level technical information protection with probabilistic reliability are carried out. Single-level TIP with probabilistic reliability was used to calculate, evaluate and compare it with equivalent single-level protection. Comparison with equivalent single-level protection can be useful in evaluating and comparing combined multi-level protection devices, since this approach will allow you to evaluate the different structures of combined multi-level protection and it is quite simple to compare modernized, designed and existing functioning protection devices from a single point of view.

Studies have shown that the surface distribution of the maximum probabilities of hacking the equivalent single-level TIP does not coincide on the surface with the distribution of the maximums of hacking probabilities of the combined TIP. Therefore, protection comparisons are only possible in the hacking direction selected for analysis. To analyze and compare the security of information in other directions, it is necessary to calculate and construct the distribution of the maximum probabilities of hacking for these directions using the proposed methodology.

Studies of the combined information protection scheme for the selected parameters of single protection showed a slight improvement in information protection compared to single-level TIP. Possibilities for increasing the effectiveness of protection require additional research. This approach will allow you to explore and calculate more complex information protection schemes.

The paper proposes a method for determining the real probability of hacking a combined multilevel defense not by the maximum value of the probability of hacking, but by the distribution of the probability of hacking a combined TIP, since hacking of a TIP may not necessarily occur at the maximum values of the probability of hacking. In this case, from the constructed surfaces of the probabilities of hacking, it is possible to determine the real reliability of the TIP for any directions of hacking.

References

1. Tawfik Mudarri, Samer Abdo AL-RABEEI,: Security fundamentals: access control models. International journal of interdisciplinary in theory and practice,ITPB - NR.: 7, pp. 259-262. (2015)
2. Jerome H. Saltzer, Michael D. Schroeder.: The Protection of Information in Computer Systems.
https://www.google.com/search?q=3.+https%3A%2F%2Fwww.cl.cam.ac.uk%2Fteaching%2F1011%2FR01%2F75-
protec-
tion.pdf&rlz=1C1AOHY_ruUA820UA823&oq=3.+https%3A%2F%2Fwww.cl.c

am.ac.uk%2Fteaching%2F1011%2FR01%2F75-protection.pdf&aqs=chrome..69i57.3772j0j8&sourceid=chrome&ie=UTF-8

3. [Bokova O. I., Drovnikov I. G., Popov A. D., Rogozin E. A.: Model of the process of functioning of the information protection system from unauthorized access created in the software environment of imitation modeling "CPN TOOLS". https://www.researchgate.net/publication/334492982_MODEL_OF_THE_PROCESS_OF_FUNCTIONING_OF_THE_INFORMATION_PROTECTION_SYSTEM_FROM_UNAUTHORIZED_ACCESS_CREATED_IN_THE_SOFTWARE_ENVIRONMENT_OF_IMITATION_MODELING_CPN_TOOLS
4. Jerome H. Saltzer, Michael. Schroeder.: The Protection of Information in Computer Systems. https://www.cl.cam.ac.uk/teaching/1011/R01/75-protection.pdf
5. Albert Caballero.: Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. https://booksite.elsevier.com/samplechapters/9781597495332/02~Chapter_1.pdf
6. Pierangela Samarati, Sabrina de Capitani di Vimercati.: Access Control: Policies, Models, and Mechanisms. https://link.springer.com/content/pdf/10.1007%2F3-540-45608-2_3.pdf
7. Golinkovich T.A .: Reliability assessment of electronic equipment. Soviet radio, Moscow (1969)
8. Zhurilenko B.E.: Design method and evaluation of a single operational technical protection of information in the selected hacking direction. Zahist Information, vol 21, pp. 143-149. (2019) doi: 10.18372 / 2410-7840.21.13950
9. Vasyanin V., Zhurilenko B., Nikolaev N et al.: Information control systems and technologies. Problems and solutions: monograph. Ecology, Odessa (2019)
10. Zhurilenko B.E.: The method of designing a single system of technical protection of information with probabilistic reliability and specified hacking parameters. Bezpeka Information, vol 20, pp. 36-42. (2014)
11. Zhurilenko B.E.: Estimation of financial costs for building an information protection system. Zahist Information, vol 20, pp. 231-239. (2018) doi: 10.18372 / 2410-7840.20.13424