Efficiency of Intellectual System of Secure Access in a Phased Application of Means of Protection Considering the Intersection of the Sets of Threat Detection

Vladimir S. Kolomoitcev,
Vladimir A. Bogatyrev, Vladimir I. Polyakov
ITMO University
Saint-Petersburg, Russia
dekskornis, vladimir.bogatyrev{@gmail.com}, v_i_polyakov@mail.ru

***Abstract*—We have conducted time delays estimation induced by system of secure access in a stage-by-stage uses means of protection of information to detect and eliminate threats for intellectual information protection system. Was considered a different sequence of the stage-by-stage uses means of protection of information and intersection of the sets of threat detection and elimination. For system of secure access is shown that the best option of system protection elements consistent use is the option in which the system elements are used sequentially from the least "simple" (which having a smaller area prevent security threats) to the "complex" (which having a large activity area). At the same time, at low arrival rate, consistent use of connecting "complex" means to "simple" means gives close results to the best options. However, the difference between them begins to grow rapidly with the increase in the arrival rate, approaching the worst options – options in which "complex" means are at the center of the information security system. It shows a comprehensive estimating of the effectiveness of the system of secure access in terms of the introduced delays and information security.**

***Keywords*—information protection, information security, computer system, system of secure access, system secure assessment, intellectual protection system, information threat**

I. Introduction

Design of computer systems (CS) that can actively withstand to information security (IS) threats using intellectual system of secure access (SSA) is one of the key tasks of corporate system design [1], [2], [3], [4], [5].

An intellectual SSA have limitations to threat detection especially when they function in real time. Their capabilities are limited by the computing power of the means of protection of information (MPI) and allowable delays in detecting and eliminating IS threats (which largely depend on the configuration MPI's for the SSA and the sequence of their application.

Information security threats can be of a different nature, ranging from unauthorized access to a CS and ending with getting infected with virus data on individual nodes of a CS, in order to create conditions for the inability of the CS to work properly. An MPI's to prevent threats to IS can be firewalls of various types, anti-virus means located at different levels of the CS, means of protecting against unauthorized access, and other MPI's. Each of these means, both individually and in the complex, is able to provide one or another level of information security of the computer system as a whole and its individual nodes with various delays in processing requests received by the system.

The purpose of this work is to increase the effectiveness of the SSA based on the selection of variants of its structure on the stage-by-stage use of different MPI and likely intersection of the sets of threat detection of these MPI's.

The efficiency of designing SSA is defined in terms of providing them protection from threats of IS and delays processing of incoming requests to IS.

The calculation of delays is especially important for intelligent protection systems that require complex information processing when detecting fuzzy decision-making models under uncertainty [6], [7].

II. The object of study

The object of the study discusses the SSA "Direct connection" involving connecting several elements (means or ways) protection implemented in the form of hardware, software platforms or their combinations as part of a unified system of information protection [8], [9], [10]. Typical SSA "Direct connection" is shown in "Fig. 1".

The SSA "Direct connection" includes three key elements: terminal nodes of the CS, MPI that are outside of terminal nodes of the system and communication channel.

The objective of the SSA "Direct connection" is to ensure IS of terminal nodes of the CS. For this in its

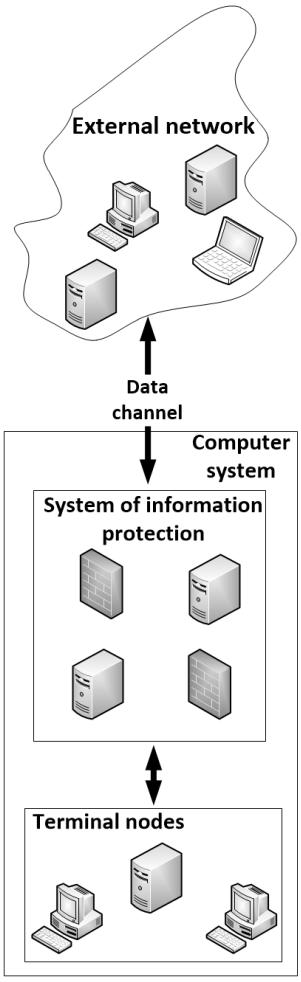

Figure 1. The system of secure access – "Direct connection".

composition used specialized hardware and software MPI aimed at solving problems of IS. MPI may also be located on the terminal nodes of the CS. First, however, the process of IS within the CS rests on external remedies to improve performance of SSA and reduce processing load on end nodes of CS.

A communication channel carries out switching of the CS from the external network or to other areas of the corporate network which uses other methods to ensure IS.

We consider a system of information protection implemented in the compute node with a certain set of software MPI. MPI that are used in the SSA are activated step-by-step (sequentially), in this regard, consider the protection system as a queueing system with a step-by-step executing queries [11], [12]. Service process of request in the system of information protection, including the R-stages, is shown in "Fig. 2".

A request immediately leaves the system with probability P_i (the MPI found and removed the threat of

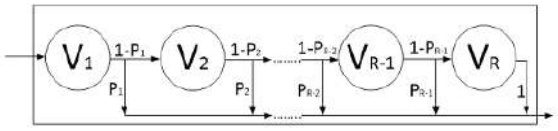

Figure 2. Service process of request in the system of information protection, including the R-stages: $V_1, \ldots, V_R$ – the processing time on the stages of the system of information protection; $P_1, \ldots, P_{R-1}$ – the probability of passing the request to the $i-th$ stage of the system of information protection, i = 1,. . . , R.

IS) or arrives at the next $(i+1)$-th stage of service with probability $(1 - \breve{}P_i)$, after the completion of the i-th stage. The request leaves the system and begins phased implementation of the next request from the queue after service completion at stage R. We assume that the service time of these stages has an exponential distribution.

III. Estimation of average residence time of the request in the system

Queuing system with stage-by-stage service "Fig. 2" is a special case of a queuing system of type $M/G/1$ [12], [13], [14], [15], [16], [17]. The average residence time of the request in the system T can be defined by the Pollaczek–Khinchine equation, as shown in "(1)":

$$T = \overline{x} + \rho\overline{x}\frac{1+C_v^2}{2(1-\rho)} \tag{1}$$

where $\overline{x}$ — the average time of service request; $\rho = \lambda\overline{x}$ — the coefficient of exploitation ($\rho < 1$), here λ — arrival rate; $C_v^2 = \sigma_v^2/(\overline{x})^2$ — the square of the coefficient of variation, and σ_v^2 -– the dispersion of the service time of the request.

One way to improve the reliability and performance of the SSA is the integration of MPI in clusters with a distribution of requests between nodes [19], [20], [21]. Then, the arrival rate of requests that arrive in each of M-systems will be divisible by M if the SSA includes M-systems, which serve incoming requests. In the result, the equation to calculate the average residence time of the request in the system shown in "(2)":

$$T = \overline{x} + \rho\overline{x}\frac{1+\sigma_v^2/(\overline{x})^2}{2(M-\rho)}. \tag{2}$$

We assume that the service time of these stages has an exponential distribution. Then, using the distribution of Cox (in accordance with "Fig. 2"), we obtain the Laplace transform for the density of probability distribution of service time in the form "(3)" [13], [14]:

$$B(s) = \frac{\mu_1}{s+\mu_1}P_1 + (\sum_{i=2}^{R-1} P_i(\prod_{j=1}^{i-1}(1-P_j))\cdot \cdot \prod_{j=1}^{i-1}(\frac{\mu_j}{s+\mu_j}) + \prod_{i=1}^{R}(\frac{\mu_i}{s+\mu_i})\prod_{j=1}^{R-1}(1-P_j) \tag{3}$$

where μ_i – the intensity of service; P_i – the probability of removing the threat of IS on the $i-th$ stage of the service; R – the number of stages in SSA.

We can obtain the mathematical expectation and dispersion of the average service time for the system, including the R-stages of service after the definition of the Laplace transform for the density of probability distribution of time. We will use the following equation to calculate the $n-th$ initial moment of the random variable [13]:

$$\overline{X^n} = (-1)^n A^{*(n)}(0) \tag{4}$$

The first derivative of $B(s)$ corresponds to the first initial moment, and the mathematical expectation:

$$x = \frac{dB(s)}{ds}|s = 0 \tag{5}$$

The second derivative of $B(s)$ corresponds to the second initial moment:

$$x^{(2)} = \frac{d^2B(s)}{ds^2}|s = 0 \tag{6}$$

Given the Laplace transform, receiving the first (x) and second ($x^{(2)}$) initial moment, it is possible to find the dispersion:

$$\sigma_v^2 = x^{(2)} - x^2 \tag{7}$$

For example the calculation, suppose a system of information protection of CS includes three MPI ($R = 3$). Thus, the average time R-stage service defined as:

$$\begin{aligned} B`(s) = &\frac{P_1\mu_1}{(s+\mu_1)^2} + \frac{\mu_1\mu_2P_2(1-P_1)}{(s+\mu_1)(s+\mu_2)^2} + \\ &+ \frac{\mu_1\mu_2\mu_3(1-P_2)(1-P_1)}{(s+\mu_1)(s+\mu_2)(s+\mu_3)^2} + \\ &+ \frac{\mu_1\mu_2P_2(1-P_1)}{(s+\mu_1)^2(s+\mu_2)} + \frac{\mu_3}{s+\mu_3} \times \\ &\times \left(\frac{\mu_1\mu_2(1-P_1)(1-P_2)}{(s+\mu_1)(s+\mu_2)^2} + \right. \\ &\left. + \frac{\mu_1\mu_2(1-P_1)(1-P_2)}{(s+\mu_1)^2(s+\mu_2)}\right) \end{aligned} \tag{8}$$

Knowing that $\mu_i = V_i^{-1}$ and having $s = 0$, we get the average service time, as shown in "(9)":

$$\begin{aligned} \overline{x} = &V_1P_1 + (V_1+V_2)(1-P_1)P_2 + \\ &+ (V_1+V_2+V_3)(1-P_1)(1-P_2) \end{aligned} \tag{9}$$

where V_i – service time $i-th$ MPI.

The second initial moment for SSA that includes 3-step defined as:

$$\begin{aligned} B``(s) = &\frac{\mu_1}{(s+\mu_1)}\left(\frac{\mu_2\mu_3(1-P_1)(1-P_2)}{(s+\mu_2)^2(s+\mu_3)^2}\right) + \\ &+ \frac{\mu_1\mu_2\left(\frac{1}{\mu_2+s} + \frac{1}{\mu_3+s}\right)(1-P_1)(1-P_2)}{(s+\mu_2)(s+\mu_3)^2} + \\ &+ \frac{2\mu_2(P_2)(1-P_1)}{(s+\mu_1)^2(s+\mu_2)} + \\ &+ \frac{2\mu_2\mu_3(1-P_1)(1-P_2)}{(s+\mu_2)(s+\mu_3)} \times \\ &\times \left(\frac{1}{(s+\mu_1)^2} + \frac{1}{(s+\mu_2)^2} + \right. \\ &\left. + \frac{1}{(s+\mu_1)(s+\mu_2)}\right) + \\ &+ \frac{2\mu_1(1-P_1)P_2}{(s+\mu_2)^3} + \frac{2\mu_1(1-P_1)P_2}{(s+\mu_1)(s+\mu_2)^2} + \\ &+ \frac{2P_1}{(s+\mu_1)^2} + \frac{2\mu_2\mu_3(1-P_1)(1-P_2)}{(s+\mu_2)(s+\mu_3)^3} + \\ &+ \frac{\mu_2\mu_3(1-P_1)(1-P_2)}{(s+\mu_1)(s+\mu_2)(s+\mu_3)} \end{aligned} \tag{10}$$

Knowing that $\mu_i = V_i^{-1}$ and having $s = 0$, we get the dispersion of the service time, as shown in "(11)":

$$\begin{aligned} \sigma_v^2 = &2(V_1(P_1 + (1-P_1)(P_2)) + V_2^2P_2(1-P_1) \\ &+ (V_1^2 + V_1V_2 + V_2^2)(1-P_1)(1-P_2) + \\ &+ V_3^2(1-P_1)(1-P_2)) + V_1V_2P_2(1-P_1) + \\ &+ 2V_3(V_1+V_2)(1-P_1)(1-P_2) - \overline{x}^2 \end{aligned} \tag{11}$$

IV. Determining the probability of detecting threats in a stage-by-stage uses means of protection of information

The probability of detection of threat after applying r MPI's can be defined as:

$$P_r = 1 - \prod_{i=1}^{r}(1-p_i) \tag{12}$$

There are some sets:

- H -- the set of threat of IS which need to be addressed in the context of a specific CS;
- E – the set of threat of IS which is capable of detecting (and with some probability, eliminate) the set of R means (or ways) used in the system of information protection;
- A_i – the set of threat of IS which is capable of detecting and eliminate $i-th$ MPI of the system of information protection.

Define:

- $L_i = |A_i|/|E|$ -- the proportion of threats of total set of threats of IS detected and eliminated by the $i-th$ element;
- $l_{i...m} = |A_i \cap A_j \cap ... \cap A_m|/|E|$ – the proportion of threats of total set of threats of IS detected and

eliminated elements i, j to m (using different from each other methods and/or algorithms) used in the system consisting of several elements;

- $I = |E|/|H|$ the coefficient of "coverage" of threats of IS (which can be susceptible to the CS) detected by the elements used in the system ($E \subseteq H$);
- $|E|$, $|H|$, $|A_i|$ a cardinal number (number of threats) of sets, respectively E, H, A_i.

We assume that all threats are not equivalent among themselves, that is, the losses that they can cause the CS are different.

In the system highlight areas to detect and eliminate threats of IS: an area where work can be conducted only one element that is part of the system of information protection of CS and the area where you can work several elements of the system of information protection.

In general the intersection of the sets of threats of IS to the system of information protection, which includes three elements (with the proportion of the threats addressed by each element or group of elements) is shown by Venn diagram in "Fig. 3".

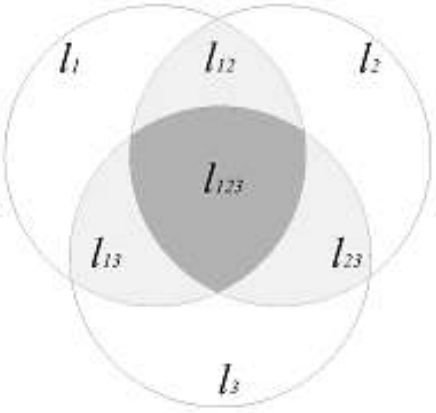

Figure 3. The proportion of the threats eliminate by each element or group of elements included in the system.

Given that the system of information protection uses MPI have the intersection of the sets of detected threats of IS, then get that the probability of eliminating the threat P_i for the $i-th$ service stage "(13)":

$$P_i = I \cdot W \cdot (l_i p_i + \sum_{i=1}^{j<i}(l_{ji}(p_i\overline{p_j}) + \sum_{q=1}^{q<i} l_{qji}(p_i\overline{p_j p_q})+ + ... + \sum_{m=1}^{m<i} l_{mt...i}(p_i\overline{p_j}...\overline{p_m}))...) \quad (13)$$

where $W = \lambda_T/\lambda$ – the proportion of threats of IS in the channel of communication, here λ_T and λ – arrival rate of threats of IS and total arrival rate (including threats of IS), accordingly; l_i – the proportion threats of total set of threats of IS detected and eliminated by the $i-th$ element of the system of information protection that consists of R-elements; $li...m$ – the proportion of threats of total set of threats of IS detected and eliminated elements i, j to m used in the system consisting of several elements; p_i – the probability a threat is detected by the $i-th$ MPI; $\overline{p_j}$ – the probability defined as $\overline{p_j} = 1 - p_j$; $i, j, \ldots, t$ – the ordinal numbers of the elements of the system of information protection. Thus, using "(13)" we get P_1 and P_2, as shown in "(14)" and "(15)":

$$P_1 = I \cdot W \cdot l_1 p_1 \quad (14)$$

$$P_2 = I \cdot W \cdot (p_1(L_2 - l_{12}) + l_{12}\overline{p_1}p_2)) \quad (15)$$

Here $L_1 = |A_1|/|E|$ and $l_{12} = |A_1 \cap A_2|/|E|$.

V. Comprehensive assessment of the effectiveness of the secure access system

We can use a comprehensive indicator of effectiveness expressing the normalized average time savings before detecting and eliminating a threat relative to the maximum allowable delay time introduced by the SSA for a comprehensive assessment of the effectiveness of the SSA "Direct Connection". The comprehensive indicator of effectiveness is shown in "(16)":

$$Q_S = \frac{T_o - T}{T_0} \cdot P_S \quad (16)$$

Here T_0 - maximum allowable time of the request in the SSA; T - average time the request in the SSA; P_S - information security of the system. The information security of the system can be found using the equation for estimating the probability of detecting a threat of information protection by the information protection system consisting of R-elements (equation extension "(13)" for the case of estimating the probability of detecting a threat to the entire system, rather than individual stages of its operation) – "(17)" [22].

$$P_S = I \cdot W \cdot \sum_{i=1}^{R}((l_i p_i + \sum_{i=1}^{j<i}(l_{ji}(1 - \overline{p_i p_j})+ + \sum_{q=1}^{q<i} l_{qji}(1 - \overline{p_i p_j p_q})+ + ... + \sum_{m=1}^{m<i} l_{mt...i}(1 - \overline{p_i p_j}...\overline{p_m}))...) \quad (17)$$

VI. Example of calculation of the average time of detecting threats in different sequences of application of means of protection of information and system effectiveness index

Let the tenth part in the incoming to CS data is malicious (threat to CS) and can be detected used in its elements of information protection ($W = 0.1$), and, also, we assume that $I = 1$ (all MPI's used as part of

a system of information protection cover all the existing threats against the CS). The service time of elements of the system of information protection m_1, m_2, m_3 : $V_1 = 0.0025$ c, $V_2 = 0.004$ c, $V_3 = 0.0075$ c. The probability of eliminating the threat of IS of each of the elements of the system of information protection: $p_1 = 0.9$, $p_1 = 0.95$, $p_1 = 0.925$. The proportion of threats of total set of threats of IS detected and eliminated elements of system of information protection: $L_1 = 35\%$, $L_1 = 50\%$, $l_{12} = 15\%$.

When completing the system with three means of protection, there are the following options for their consistent application:

- $b1 : (m_1, m_2, m_3)$;
- $b2 : (m_1, m_3, m_2)$;
- $b3 : (m_2, m_1, m_3)$;
- $b4 : (m_2, m_3, m_1)$;
- $b5 : (m_3, m_1, m_2)$;
- $b6 : (m_3, m_2, m_1)$.

Substituting in the equation “(2)”, of equations “(9)”, “(11)”, “(14)” and “(15)”, we get, the average service time of request of the SSA – corresponding to the average time a threat is detected. The dependence of the average time of request in the system on the arrival rate for different options of placing of elements of the system of information protection shown in “Fig. 4”.

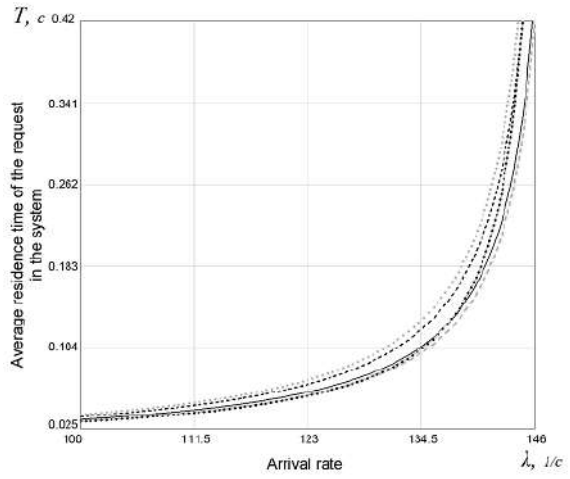

Figure 4. The dependence of the average time of request in the system on the arrival rate. Option $b1$ and $b5$ – black and grey lines, accordingly; option $b3$ and $b4$ – grey and black the dash-dotted line, accordingly; option $b2$ and $b6$ – grey and black the dotted line, accordingly.

From “Fig. 4” we can see that option $b3$ sequence of application of various MPI in the system of information protection the best. It involves a sequential arrangement of the elements of the system of information protection from “simple” (with a smaller area of detection and elimination of threats of IS, but with greater speed) to a more “complex” (a larger area of detection and elimination of threats of IS, but slower). Option b1 has, close to this embodiment the result of the placement of the elements of the system of information protection. At the same time, the difference between options b1 and b3 increases with increase in the intensity of the arrival rate. A similar pattern is observed when comparing options $b2$ and $b4$, and options $b5$ and $b6$. The options $b2$ and $b4$, the sequence of application of various MPI have significantly worse performance of the average time of request in the SSA (threats detection). This is because in the center (in this case, second) stage of work the system of information protection is the most “complex” MPI (thus, it is necessary to work with almost partially unfiltered arrival rate) in each of these accommodation options elements. At the same time, at low arrival rate, consistent use of connecting “complex” means to “simple” means (option b5 and option b6) gives close results to the best options. However, the difference between them begins to grow rapidly with the increase in the arrival rate, approaching the worst options – options in which “complex” means are at the center of the information security system (option $b2$ and option $b4$).

For the option of building a SSA "Direct connection" (b1) we get the following graph of the effectiveness of using SSA from 1 to 3 MPI‘s. “Fig. 5”.

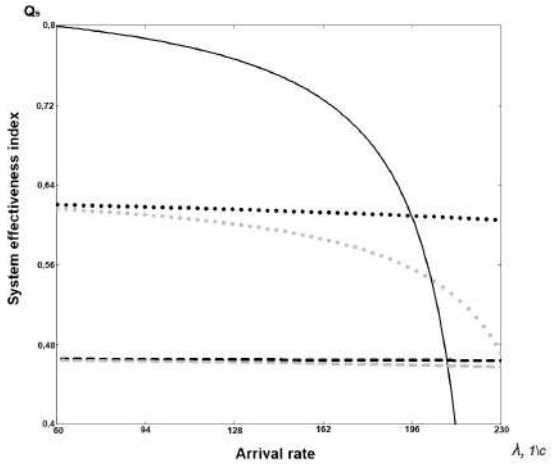

Figure 5. The dependence of the system effectiveness index on the arrival rate. Three MPI‘s option – black lines; two MPI‘s option (m_2, m_1 and m_3, m_1) – grey and black the dotted line, accordingly; one MPI option (m_2, m_3) – grey and black the dash-dotted line, accordingly.

As can be seen from the graph (“Fig. 5”) with increasing arrival rate the efficiency of the SSA using a three MPI‘s becomes lower than the use of two MPI‘s. Similarly, with a further increase in the arrival rate, it will be more efficient to use one MPI.

CONCLUSION

It was determined the average time of detecting threats in different sequences of a stage-by-stage uses of various

means of protection information in the system of secure access. We raised the assumption that the service time of each step is a random variable that has exponential distribution.

It is shown that a variant of a sequential arrangement of the elements of the system of information protection from “simple” (with a smaller area of detection and elimination of threats of information security, but with greater speed) to a more “complex” (a larger area of detection and elimination of threats of information security, but slower) is preferable in terms of providing the least values for average time of threat detection.

The effectiveness of the system of secure access using a different number of information security tools is shown.

REFERENCES

[1] Koren, I.Fault tolerant systems. Morgan Kaufmann publications, visit our San Francisco 2009 378 p

[2] Aysan H. Fault-tolerance strategies and probabilistic guarantees for real-time systems Mälardalen University, Västerås, Sweden. 2012. 190 p

[3] Aliev T.I. The synthesis of service discipline in systems with limits // Communications in Computer and Information Science. 2016. V. 601. P. 151–156. doi: 10.1007/978-3-319-30843-2_16

[4] Sorin D. Fault Tolerant Computer Architecture. Morgan & Claypool 2009 . 103 p

[5] A.G., Fedosovsky M.E., Maltseva N.K., Baranova O.V., Zharinov I.O., Gurjanov A.V., Zharinov O.O. Use of Information Technologies in Design and Production Activities of Instrument-Making Plants//Indian Journal of Science and Technology, IET - 2016, Vol. 9, No. 44, pp. 104708

[6] Survivable Network Systems: An Emerging Discipline / R. J. Ellison et al. Software Engineering Institute. 1997 URL: http://www.cert.org .

[7] Kozachok A. V., Kochetkov E. V., Tatarinov A. M. CONSTRUCTION HEURISTIC MALWARE DETECTION MECHANISM BASED ON STATIC EXECUTABLE FILE ANALYSIS POSSIBILITY PROOF // Herald of computer and information technologies - 2017. - No 3 (153). - pp. 50 – 56. DOI: 10.14489/vkit.2017.03.pp.050-056

[8] Domarev V.V. The security of information technology. Systems approach.K: DiaSoft, 2004, 992 pp

[9] Schumacher M. Security Engeneering with Patterns, LNSC 2754.Springer-Verlang Berlin Heidelberg, 2003, 87-96 pp

[10] Kolomoitcev V. S., Bogatyrev V. A. The Fault-Tolerant Structure of Multilevel Secure Access to the Resources of the Public Network // Communications in Computer and Information Science. 2016. V. 678. P. 302 – 313

[11] L. Kleinrock. Communication Nets: Stochastic Message Flow and Design. — McGraw-Hill, 1964. — 220 p. — ISBN 978-0486611051.

[12] L. Kleinrock. Queueing Systems: Volume I – Theory. — New York: Wiley Interscience, 1975. — 417 p. — ISBN 978-0471491101.

[13] L. Kleinrock. Queueing Systems: Volume II – Computer Applications. — New York: Wiley Interscience, 1976. — 576 p. — ISBN 978-0471491118.

[14] L. Kleinrock, Farok Kamoun. Hierarchical Routing for Large Networks, Performance Evaluation and Optimization. — Computer Networks 1 (3): 155–174. — 1977.

[15] L. Kleinrock, Richard Gail. Queueing Systems: Problems and Solutions. Wiley-Interscience. — 1996. — 240 p. — ISBN 978-0471555681.

[16] Harchol-Balter, M. (2012). "Scheduling: Non-Preemptive, Size-Based Policies". Performance Modeling and Design of Computer Systems. p. 499. doi:10.1017/CBO9781139226424.039. ISBN 9781139226424.

[17] Harchol-Balter, M. (2012). "Scheduling: Preemptive, Size-Based Policies". Performance Modeling and Design of Computer Systems. p. 508. doi:10.1017/CBO9781139226424.040. ISBN 978113922642.

[18] Manuel, Laguna (2011). Business Process Modeling, Simulation and Design. Pearson Education India. p. 178. ISBN 9788131761359. Retrieved 6 October 2017.

[19] V.A. Bogatyrev, S.A. Parshutina, “Efficiency of redundant multipathtransmission of requests through the network to destination servers”,Communications in Computer and Information Science, vol. 678, 2016, pp. 290-301.

[20] V.A. Bogatyrev, S.A. Parshutina, N.A. Poptcova, A.V. Bogatyrev,“Efficiency of redundant service with destruction of expired and irrelevant request copies in real-time clusters”, Communications in Computer and Information Science, vol. 678, 2016, pp. 337-348.

[21] Bogatyrev V.A., Vinokurova M.S. Control and Safety of Operation of Duplicated Computer Systems//Communications in Computer and Information Science, IET - 2017, Vol. 700, pp. 331-342.

[22] Kolomoitcev V.S., Bogatyrev V.A. A Fault-tolerant Two-tier Pattern Of Secure Access ’Connecting Node’ // ACSR-Advances in Computer Science Research - 2017, Vol. 72, pp. 271-274.

ЭФФЕКТИВНОСТЬ ИНТЕЛЕКТУАЛЬНОЙ СИСТЕМЫ БЕЗОПАСНОГО ДОСТУПА ПРИ ПОСЛЕДОВАТЕЛЬНОМ ПРИМЕНЕНИИ СРЕДСТВ ЗАЩИТЫ С УЧЕТОМ ПЕРЕСЕКАЕМОСТИ МНОЖЕСТВ ОБНАРУЖЕНИЯ УГРОЗ

Коломойцев В.С., Богатырев В.А., Поляков В.И.

Для интеллектуальных систем защиты информации определены временные задержки, вносимые системой безопасного доступа с учетом различной последовательности поэтапного применения средств защиты и пересекаемости множества обнаруживаемых и устраняемых ими угроз. Для системы безопасного доступа показано, что лучший вариант последовательного применения элементов системы защиты – тот, при котором элементы системы применяются последовательно от наименее "слабых"(имеющих меньшую область предотвращения угроз защиты информации) к наиболее "сильным"(имеющих большую область работы). В то же время при низкой интенсивности входного потока последовательное подключение от «сложных» средств к более «простыми» дает близкие результаты к лучшим из исследованных вариантам построения. Однако разница между ними начинает быстро расти с увеличением интенсивности входного потока, приближаясь к худшим вариантам - вариантам, в которых «сложные» средства находятся на центральных этапах работы системы защиты информации. Показана комплексная оценка эффективности системы безопасного доступа по показателям вносимых задержек и информационной защищенности.

Received 29.12.18