Lesja KOZUBTSOVA[1]

Opiekun naukowy: Yuriy KHLAPONIN[2]

DOI: https://doi.org/10.53052/9788366249868.11

BADANIE EKSPERYMENTALNE DOTYCZĄCE OCENY EFEKTYWNOŚCI UDOSKONALONEJ METODY MONITOROWANIA CYBEROPORU SYSTEMÓW INFORMACYJNYCH SPECA SPECO

Streszczenie: Aby zapewnić stabilną pracę systemu informatycznego specjalnego przeznaczenia w środowisku narażonym na zagrożenia cybernetyczne, zaproponowano udoskonaloną metodę monitorowania cyberodporności. W niniejszym artykule zbadano skuteczność zaproponowanej ulepszonej metody monitorowania cyberodporności w zakresie cyberbezpieczeństwa i cyberodporności.

Słowa kluczowe: ewaluacja, efektywność, metoda, monitoring, cyberodporność, systemy informacyjne

EXPERIMENTAL RESEARCH TO EVALUATE THE EFFICIENCY OF THE IMPROVED METHOD OF MONITORING THE CYBER RESISTANCE OF INFORMATION SYSTEMS OF SPECA SPECO

Summary: To ensure the stable operation of the special purpose information system in an environment vulnerable to cyber threats, an improved method for monitoring cyber resilience has been proposed. In this paper, the effectiveness of the proposed improved method of monitoring cyber resilience in terms of cybersecurity and cyber resilience is investigated.

Keywords: evaluation, efficiency, method, monitoring, cyber resilience, information systems

1. Setting objectives

The COVID 19 pandemic has created an unprecedented challenge for the world. While everyone is quarantined, the load on the Internet is growing. Many

[1] Technical Sciences, Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty, Faculty Of Information Technologies, l.kozubtsov@i.ua

[2] Doctor of Technical Sciences., Kyiv National University of Construction and Architecture, Faculty Of Automation And Information Technology, y.khlaponin@gmail.com

enterprises, companies, non-governmental and governmental organizations have been forced to send their employees to remote work and increased use of information systems. It should be noted that some users were unaware of the threats and risks to which they are exposed when working from home. Therefore, online work has increased the number of potential victims of cybercrime. Employees are at great risk, thereby endangering enterprise software, making it more vulnerable to cybercriminals.

According to scientists, RV Grishchuk and VO Well, "cyber confrontation" is nothing more than a kind of armed struggle, as a result of which with the help of cyber destructive information influences (IRS) is targeted intervention and disruption of normal operation of a certain algorithm of automated control systems, information systems and information and telecommunications networks [1; 2].

In Ukraine, global trends in cyber threats are exacerbated by hybrid warfare, in which critical infrastructure and special-purpose information systems become targets for new cyber-attack technologies [3].

This follows a high level of requirements for the reliability of the information system (IS): adequacy, optimality, efficiency, stability, continuity, secrecy.

“Cyber resilience of IP” should be understood as the state of its security, which ensures stable operation in the conditions of accidental actions of cyber IRS [4].

"Cyber resilience" includes [5-7]:

cyber survivability – the ability to maintain IS performance (survival) in the event of failure of technical means of information processing;

cybersecurity is the state of ensuring the implementation of the target function of IP with a given quality in terms of the use of "common" and targeted IRS [8];

cyber reliability is the ability to ensure the performance of the target function of the IP for a certain period of time in the event of software errors, technical failures and unintentional erroneous actions of technical staff and officials.

If the cyber security system of the IP is in a state without changes in the settings for some time enough to create malicious intrusion software by the attacker, the cyber vulnerability increases accordingly. In this case, the factor of accumulation of the latest cyber threats such as zero-day works.

Based on the existence of IRS on special purpose information systems (ISSP), there is an urgent scientific and applied problem of dissertation research, which aims to increase the cyber resilience of IRS in cyberspace in the event of accidental action of external IRS [5]. To this end, the author proposed an improved method for monitoring the cyber resilience of ISSP [6; 7]. Therefore, it is necessary to evaluate the effectiveness of the proposed method of monitoring the cyber resilience of ISSP.

2. Purpose of the work

Investigate the effectiveness of an improved method of cyber resilience monitoring for special purpose information systems in terms of cybersecurity and cyber resilience.

3. Research methodology

The initial data is an improved method for monitoring the cyber stability of the ISSP developed in the context of [6; 7]. It is necessary to investigate the effectiveness of the improved method of monitoring the cyber stability of the ISSP. To assess the effectiveness of the improved method of monitoring cyber stability, the ISSP is proposed to be based on the generalized indicator $P_{(IRS)}$ – The probability of conducting a cyber attack of the IRS on the IP SP. to do this, we will use the following experiment, the description of which is presented in [6].

The research experiment involved two information systems of the same structure and content of the tools: control ISSP №1 and experimental ISSP №2. The following assumption is made:

1) at the control ISSP №1 – we conditionally assume that the system is operated without using an improved method of monitoring cyber security. In fact, this method was also used on it, but its purpose was only to control changes in the value of the probability of cyber security (R_{KZ}). At the same time, in the event of a significant deterioration in the R_{KZ} probability value, the security administrator does not apply drastic measures to restore (increase) cyber security.
2) experimental ISSP №2 used an improved method for monitoring the cybersecurity of ISSP for timely monitoring and detection of changes in the probability value of R_{KZ}. But unlike ISSP №1, based on the results of the R_{KZ} analysis, the security administrator necessarily applied a set of measures to restore cyber security on this system.
3) at the initial (zero) stage, due to setting up measures of cybersecurity procedures, R_{KZ1} ISSP №1 and R_{KZ2} ISSP №2 have the same values, i.e. $R_{KZ1} = R_{KZ2}$.

4. Research result

At Stage 1 (time T1), the cyber security of R_{KZ1} ISSP №1 and R_{KZ2} ISSP №2 was monitored, according to the results of which it was established that $R_{KZ1} = R_{KZ2} = 0.9$ (fig.1). This value corresponds to the probability of conducting a cyberattack $P_{(IRS)}$ on ISSP systems №1 and, accordingly, on ISSP №2 is $P_{(IRS)} = 0.1$.

At stage 2 of the experiment (time T2), a controlled test IRS was performed simultaneously on ISSP №1 and ISSP №2. Using an advanced method of monitoring cybersecurity, security administrators simultaneously recorded the fact of decreasing cybersecurity ISSP №1 and ISSP №2 $R_{KZ1} = R_{KZ2} = 0.78$, which corresponds to the estimated increase in $P_{(IRS)} = 0.22$. Taking into account the obtained results on reduction of R_{KZ1} and R_{KZ2} the head of the experiment made an unambiguous decision to implement the stage of cybersecurity adjustment on the experimental ISSP №2 by choosing adequate measures and procedures of cybersecurity, and on the control ISSP №1 to leave unchanged the value of cybersecurity.

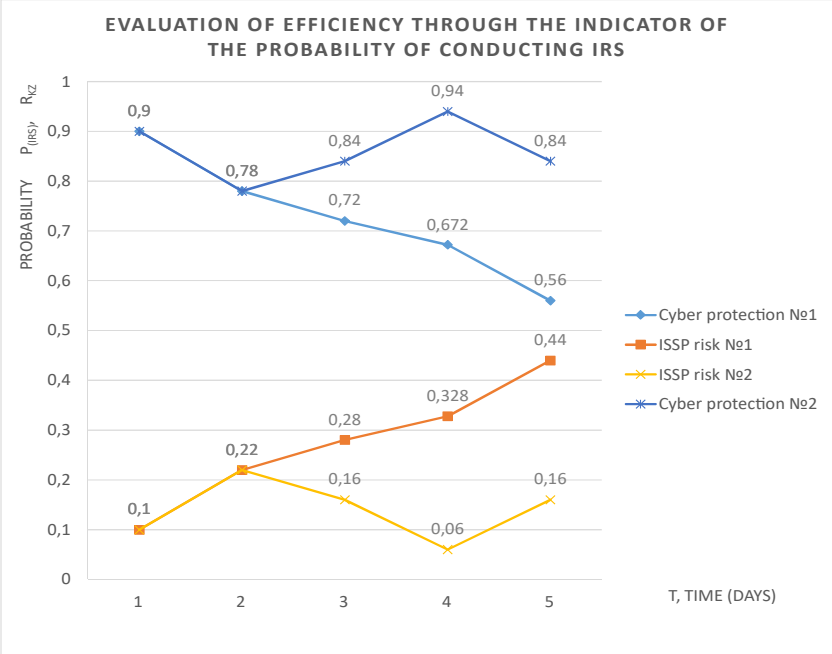

Figure 1. Evaluation of effectiveness using the probability indicator of IRS action

At stage 3 (time T3) the cyber security of these systems was re-monitored. The following values of $R_{KZ1} = 0.72$ and $R_{KZ2} = 0.84$ were set. According to these values, the probability of a cyberattack, respectively, is for ISSP №1 $P_{(IRS)} = 0.28$, and ISSP №2 $P_{(IRS)} = 0.16$. As can be seen from the graphs (Fig.1) cybersecurity R_{KZ1} ISSP №1, which did not apply the stage of timely adjustment of cybersecurity, continues to decline, and the probability of a cyber attack on it in accordance with table.1 is growing.

Table 1. Qualitative scale for estimating the probability of conducting IRS $P_{(IRS)}$

№	Criterion	$P_{(IRS)}$	Description
1	$0 \leq P_{(IRS)} \leq 0,25$	Very low	The IRS it will almost never be held
2	$0,25 \leq P_{(IRS)} \leq 0,5$	Low	The probability of holding the IRS is quite low
3	$0,5 \leq P_{(IRS)} \leq 0,75$	Average	The probability of holding an IRS is average
4	$0,75 \leq P_{(IRS)} \leq 0,9$	High	The IRS most likely it will be conducted
5	$0,9 \leq P_{(IRS)} \leq 1$	Very high	The IRS will be conducted

The research experiment was completed in step 5 (time T5) with the following values of ISSP №1 $R_{KZ1} = 0.56$, $P_{(IRS)} = 0.44$, and ISSP №2 $R_{KZ2} = 0.84$, $P_{(IRS)} = 0.16$, that in accordance with the criteria of the quality scale for estimating the probability of conducting IRS $P_{(IRS)}$ given in table.1.

Then it can be confirmed that on the basis of the decrease in the cybersecurity of ISSP №1 there is an increase in the probability of conducting IRS, despite the fact that we measured it on ISSP №1 for self-monitoring.
In the graph shown in fig.2 shows the recalculation of the probability of cybersecurity of R_{KZ} ISSP according to the formulas given in [5-7] in the value of cyberstability of these systems, obtained by applying the improved method of calculating the components of cyberresistance.

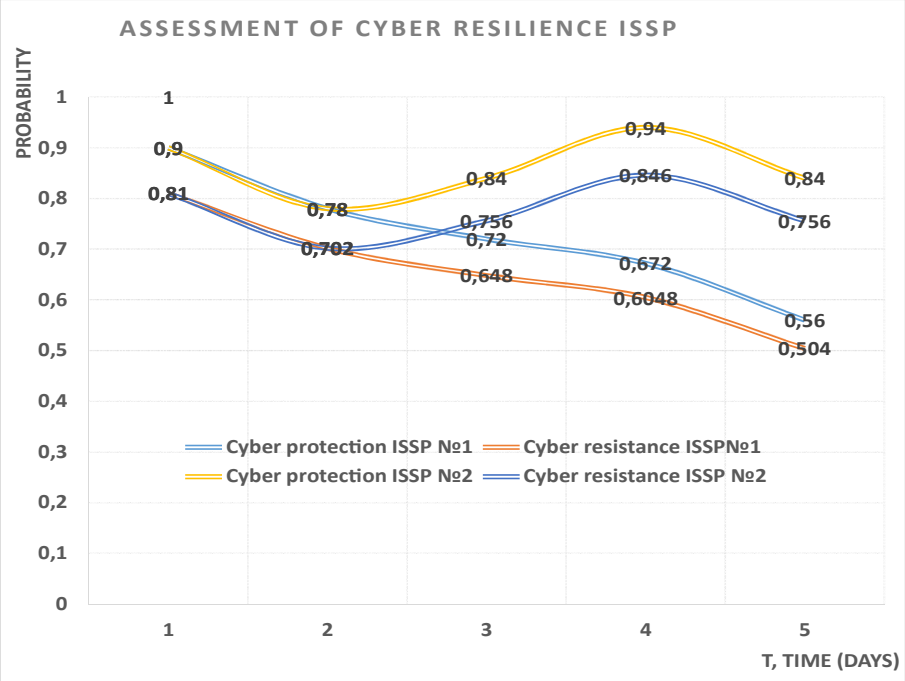

Figure 2. Assessment of the cyber resistance of IP SP

5. Conclusions

Thus, based on the need to function special-purpose information systems in an environment vulnerable to cyber threats, there is an actual scientific and applied task of the dissertation research, on operational tracking of the real value of the probability of cyber security of the system, which the author solved by developing an improved method for monitoring cyber stability.
The obtained results of evaluating the effectiveness of the proposed improved method of monitoring cyber resilience of the special purpose information system can be argued that in case of non-application of the developed advanced method of cyber resilience monitoring, we remain able to assess the probabilities of IRS.

LITERATURA

1. ГРИЩУК Р.В.: Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї. Сучасна спеціальна техніка, 2016, 3(46), 94 – 101.
2. ХОРОШКО В.О., ГРИЩУК Р.В.: Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї. Сучасна спеціальна техніка, 2016, 4(47), 30 – 36.
3. КОЗУБЦОВА Л.М., КІТ Г.В., ЛІЩИНА В.О., КОЗУБЦОВ І.М.: Аналіз змісту поняття інформаційна системи спеціального призначення. Materials of the XVI International scientific and practical Conference Cutting-edge science – 2020, April 30 – May 7, 2020 Construction and architecture. Mathematics. Modern information technology. Technical science: Sheffield. Science and education LTD, 2020, 8, 56 – 58.
4. ЗАБАРА С.С., ХЛАПОНИН Ю.И., КОЗУБЦОВА Л.М.: Анализ понятия кибернетической стойкости информационной системы специального назначения. Materials of the XVI International scientific and practical Conference Science without borders - 2020, March 30 - April 7, 2020: Sheffield. Science and education LTD, 2020, 20 – 23, ISBN 978-966-8736-05-6.
5. КОЗУБЦОВА Л.М.: Удосконалення методів моніторингу кіберстійкості інформаційної системи спеціального призначення: дисертація кандидата технічних наук: 05.13.05 – "Комп'ютерні системи та компоненти": – Захищена 22.09.2020: Затв. 26.11.2020. К.: Відкритий міжнародний університет розвитку людини «Україна», 2020, 222.
6. ZABARA S., KHLAPONIN Yu., KOZUBTSOVA L.: Methods for diagnosing cybernetic stability of a special purpose information system. Scientific and Practical Cyber Security Journal (SPCSJ), Scientific Cyber Security Association (SCSA), 2020, 4(1), 80 – 86, ISSN 2587-4667.
7. ZABARA S., KOZUBTSOVA L., KOZUBTSOV I:. Method for calculating the components of the cybernetic stability indicator for the functioning of a special purpose information system in cybernetic space. Journal «Scientific discussion». Praha, Czech Republic, 2020, 42(1), 29 – 38, ISSN 3041-4245.
8. ZABARA S., KOZUBTSOVA L., KOZUBTSOV I.: Improved method of diagnostics of cyber security of the information system taking into account disruptive cyber impacts. «Danish Scientific Journal» (DSJ). Kobenhavn. Denmark, 2020, 35(1), 68 – 74, ISSN 3375-2389.