UDC 004.75:004.49
https://doi.org/10.31891/CSIT-2022-1-5

MYKOLA STETSIUK, ANTONINA KASHTALIAN
Khmelnytskyi National University

THE METHODS OF ENSURING FAULT TOLERANCE, SURVIVABILITY AND PROTECTION OF INFORMATION OF SPECIALIZED INFORMATION TECHNOLOGIES UNDER THE INFLUENCE OF MALICIOUS SOFTWARE

The paper examines the provision of fault tolerance, survivability and protection of IT information on the impact of malicious software and computer attacks. Each method is presented separately by its steps. The states of hardware and software on which the implemented methods are impelled in the corresponding systems are investigated. The common states are singled out and on the basis of them and together with the steps of the methods the synthesis of the method of ensuring fault tolerance, survivability and protection of IT information is carried out. It combines three developed methods. This method is represented by four generalized steps. All representations of the models are made by graphs with weight vertices, which specify either the states or steps of the methods. This representation made it possible to connect common vertices.

Some methods of ensuring resilience, survivability and protection of IT information under the influence of malicious software were compared with one integrated method. Experimental studies confirm the effectiveness of both the proposed solution to ensure fault tolerance, survivability and protection of IT information and the effectiveness of the method, which combines the provision of fault tolerance, survivability and protection of IT information.

Key words: *efficiency, method, fault tolerance, survivability, information protection, hardware and software, information technology, malware*

МИКОЛА СТЕЦЮК, АНТОНІНА КАШТАЛЬЯН
Хмельницький національний університет

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ, ЖИВУЧОСТІ ТА ЗАХИСТУ ІНФОРМАЦІЇ СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВПЛИВІВ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В роботі досліджено забезпечення відмовостійкості, живучості та захисту інформації IT щодо впливу зловмисного програмного забезпечення та компютерних атак. Окремо представлено кожен метод його кроками. Досліджено стани апаратно-програмних засобів, на яких реалізовані методи імпентовано у відповідні системи. Спільні стани виокремлено і на основі них та разом з кроками методів здійснено синтез методу забезпечення відмовостійкості, живучості та захисту інформації IT. В ньому поєднано розроблені три методи. Цей метод представлено чотирма узагальненими кроками. Всі представлення моделей здійснені графами з ваговими вершинами, в яких задано або стани або кроки методів. Таке представлення надало змогу поєднати спільні вершини.

Окремі методи забезпечення відмовостійкості, живучості та захисту інформації IT в умовах впливів зловмисного прогармного забезпечення було порівняно з одним інтегрованим методом. Проведені експериментальні дослідження підтверджують ефективність як запропонованого рішення щодо забезпечення забезпечення відмовостійкості, живучості та захисту інформації IT так і ефективність методу, в якому поєднано забезпечення відмовостійкості, живучості та захисту інформації IT.

Ключові слова: *ефективність, метод, відмовостійкість, живучість, захист інформації, апаратно-програмні засоби, інформаційні технології, зловмисне програмне забезпечення*

Introduction

The continued spread of malware and various computer attacks confirms that the problem of combating malicious software and computer attacks will remain relevant, and its relevance will only increase. Creating an information system to avoid malware threats and computer attacks is possible using scientific approaches based on threat models and methods based on them.

When designing information systems, you need to take into account the peculiarities of the tasks assigned to them, which can be performed under the influence of malicious software and computer attacks. In this regard, the necessary scientific task is to develop specialized IT that will provide opportunities to combat malicious software and computer attacks, which will allow to develop on their basis resistant to such influences information systems.

Subject area analysis and related decisions

Many researchers and organizations working on the development of anti-virus tools pay attention to combating malicious software. Leading developers of anti-virus tools [1] - [13] are focused on creating separate specialized tools to combat malicious software. The installation of such tools in computer systems significantly helps users to save information and detect malicious software. The developers point to the high reliability of detecting malicious software by their means. But independent organizations testing antivirus and intrusion detection systems [14] - [17] confirm incomplete detection. That is, there is a small percentage of malware that can penetrate the detection tools. This creates problems with the reliability of information storage. Therefore, researchers continue to develop a variety of detection methods and systems [18] - [25], which would detect malicious software at

different stages of penetration into computer systems. This direction is actively developing and will continue to develop, because criminals benefit and therefore it motivates them. In addition, most countries in the world, paying considerable attention in recent decades to the problem of information protection, have created appropriate means of another type, including counter-protection. It also allowed them to take part in countering cyber threats and thus increased the number of participants in detecting and combating malicious software in cyberspace, putting this direction on a systemic basis. Thus, the space for research into the detection of malicious software by special methods and systems is growing.

In addition to the development of certain detection methods to detect malicious software at different stages of penetration into computer systems, promising is to ensure the stability of hardware and software in the face of malicious software and computer attacks [15]. In particular, when designing specialized IT, such mechanisms could ensure resilience to impacts.

The methods of ensuring fault tolerance, survivability and protection of information of specialized information technologies under the influence of malicious software

To ensure the resilience of IP to the effects of SDRs and computer attacks in the process of their operation, synthesize in IT in conjunction with specialized functionality of its purpose, as well as components whose purpose will be to maintain the ability of IS to perform specialized functionality to perform the main task. and computer attacks. Let's set the constituent elements of specialized IT M_{IT} as follows:

$$M_{IT} = \{F_0, F_1, F_2, \dots, F_{N_{IT}}, A_{IT}\}, \quad (1)$$

where F_0 is the functional of the main IT task and must be present in M_{IT}; F_i - i - the component in IT that provides additional functionality; i = 1,2,…, N_{IT}; N_{IT} - the number of additional components in IT; A_{IT} is a component element in IT that activates elements $F_1, F_2, \dots, F_{N_{IT}}$ in IT when certain events or requests from element F_0 occur and it does not contain additional functionality to perform other actions.

The components of IT will be synthesized as follows: fault tolerance, survivability, information security. These components will be implemented as separate completed modules, but with the possibility of activation in terms of signaling the impacts and needs that will require the functionality of the main task. That is, for $N_{IT} = 3$, then the generalized structure of specialized IT will have the representation shown in Fig. 1.

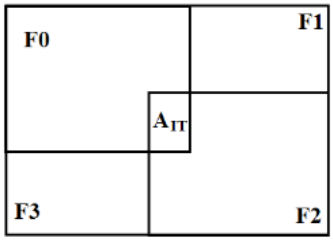

Fig. 1. Generalized structure of specialized IT with elements

Method of ensuring fault tolerance of specialized IT.

The essence of the first step of the method is to use block labels. The second step in the IT fault tolerance method is to use functional redundancy. The third step in IT resilience is cross-redundancy. The fourth step of the IT fault tolerance method focuses on the application in the server part and, therefore, in the client part will not be used, except in cases of combination of tasks and capabilities of both parts of the IS.

The steps of the developed method combined two ways to ensure the sustainability of IT: attracting redundancy; attracting excesses. This integration is combined with IP adaptability.

Method of ensuring the viability of specialized IT.

To ensure the operability of the method, its model includes a software bank that contains software modules of all client workstations and their reference parameters. The survivability method of specialized IT is based on the use of markers, which indicate the boundaries of software modules included in such files. This allows you to separate the software part from the overall file structure and thus calculate the checksum only for the constant part of the file.

The main steps of the method of ensuring the viability of specialized IT:

1. Inclusion of markers in the software at the preparatory stage of ensuring the viability of specialized IT.
2. Calculation of checksums marked in accordance with paragraph 1 of the executable module of the client workstation software. Their number can be a set from 1 to n.
3. Executable software modules of the client workstation are placed in the database of the reference software of the relevance control service.
4. Preservation of the list of values of markers and checksums of the modules marked by them.

5. If the background process is started, then in a certain iteration the software of some workstation will be checked and if its list of markers and values of checksums that correspond to them do not match, or the required markers are not found at all, the software update procedure will be performed. ARM.

6. The fact of updating the software of some workstation is entered in the log-file for further analysis of the reasons that caused its replacement.

The developed method of ensuring the viability of specialized IT is based on the analysis of markers and the preservation of key information needed for research in the process of IP operation.

Method of ensuring information protection of specialized information technologies.

The steps of the method of ensuring the protection of information in specialized IT according to the two-factor verification of the legality of user software:

1. We create a base of reference software for client workstations.

2. Create a database of reference parameters of client workstation software modules and a registration list of the physical location of the workstation with startup parameters and binding to the IP address.

3. The workstation software is installed on the computer without startup parameters.

4. When you try to run the workstation software from the client station, a request is made to the bootloader, which is on the server, to run with the registration code of the workstation.

5. The bootloader program checks the legitimacy of this application in accordance with the registration list and, if the request data match the expected, then remotely run the workstation software at the client station. If not, the launch will not take place, and the very fact of attempting to run will be recorded in the log file of events in the IP. If an attacker submits an application with the correct parameters by changing the sender's address in the package, the workstation software will be launched, but not on his computer, but on the regular one, according to the registration list, which is under the control of a legitimate user.

These measures to ensure the protection of IP information in combination with organizational and legal measures, used as a single set, allow to obtain technology, the use of which in the development of specialized IP, guarantees a high level of protection of its resources from destructive influences.

Method of ensuring fault tolerance, survivability and protection of information of specialized IT.

Ensuring fault tolerance, survivability and protection of specialized IT information in the context of the influences of PPL and computer attacks according to the developed methods makes it possible to improve the resistance to influences in each individual case. But part of the steps of three different developed methods is convergence, so it is advisable to combine the three developed methods into one method according to the joint steps and states of the system in which it will be implemented. Then, the system will have a subsystem that will implement the method of ensuring fault tolerance, survivability and information protection of specialized IT, which will combine all three developed methods.

In Fig. 2 shows the model of ensuring fault tolerance of client ARM. Here, the vertices of column 1 - 4 are internal influences on software of all levels and the hardware platform of IP, which are aimed at reducing the fault tolerance of IP. Vertex 1 captures a situation where, due to the super-large complexity of modern software systems, client ARM software (Fig. 2, vertex 5), as well as the computer station OS (Fig. 2, vertex 6), can self-damage, making way 5 - 9 in Fig. 2 not available.

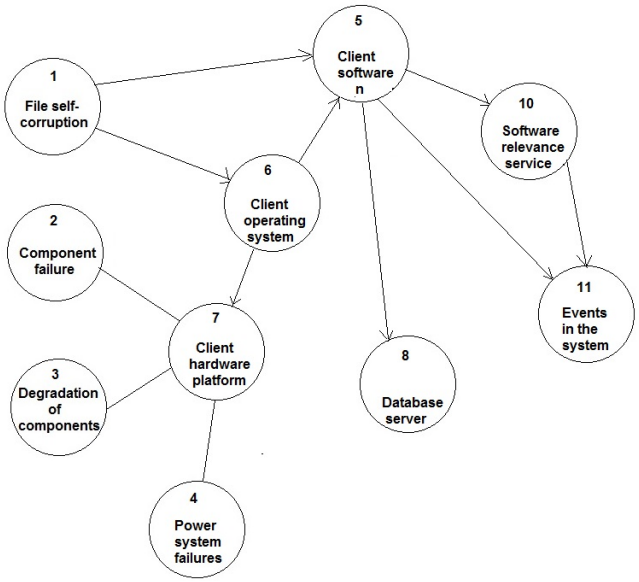

Fig. 2. Graph model of fault tolerance

The software relevance control service (Fig. 2, vertex 10) monitors the condition of the software of the client ARM and, in case of detection of its damage, replaces it with a reference one, restoring its functionality (Fig. 2, vertex 9). Thus, the automatic restoration of the availability of IP functions is ensured - path 5-9 in Fig. 2 is made available. Unavailability of client ARM functions can also occur due to external factors, namely due to the actions of malware. This situation is modeled on Fig. 3. External influences are shown in vertices 1 and 3. They take into account various methods of attacking is components. Vertex 1 simulates a situation where the impact of PPL is directed directly at the client ARM software or on the OS under which it operates.

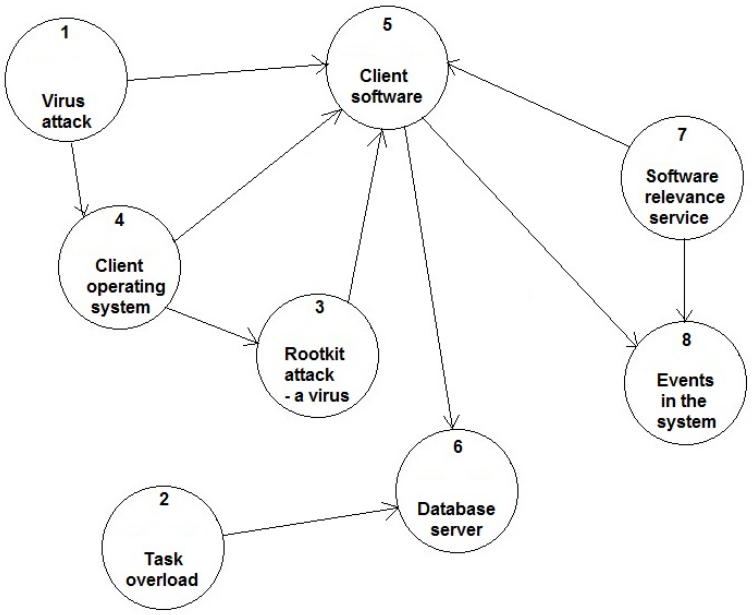

Fig. 3. Graph model of survivability

Vertex 3 simulates a situation where malicious software, in the process of attacking the OS, managed to create a disguised tunnel to further attack other components of the IP, including the software of the client ARM. Vertex 2 simulates the dos attack situation on the server part of the IS. To counteract these influences, namely their attacks on the least protected of its links - client stations, the capabilities of the advanced functionality of the software relevance office service are used (vertex 7, Fig. 3), which, in case of detection of damage to the software of some ARM (vertex 5, Fig. 3), replaces it with a standard, restoring the path of 5-6 graph model figs. 3, and thus restoring the availability of IP functions.

Presented in Fig. 4 model, demonstrates the situations in which there may be a system for ensuring the protection of IP information.

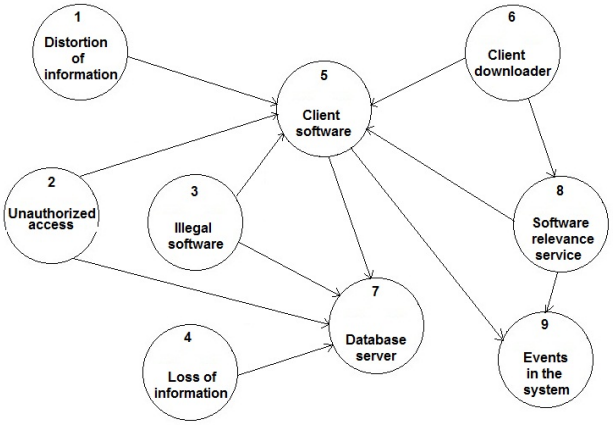

Fig. 4. Graph model of information security

It includes the main factors that in various ways threaten the information processed in the IP. This is distortion, unauthorized access and loss of information (vertices of column 1 – 4, Fig. 4). Their action is directed against client ARM and DB server (vertices 5 and 7, Fig. 4, respectively). A particularly vulnerable part of THE is client ARM, as are the least protected elements of the system. In order to strengthen their protection, a special mechanism for running ARM software is used in the IP, which is based on two factor verification of the legality of

the software, which attempts to connect to the server database. Responsible for its support are the ARM launch program (vertex 6, Fig. 4) and the software relevance control service (vertex 8, Fig. 4), which checks the compliance of the software that tries to connect to the database to the parameters stored in the registry of this service. When non-coincidences are detected in the parameters, the connection is refused, and the fact of unauthorized connection is recorded in the log file of events in the system (vertex 9 on the module graph).

Analysis of influences directed to IP and shown in Fig. 2, 3 and 4 showed that they are caused by different causes, but are aimed at almost the same components of the system. As can be seen from the presented in Fig. 5 of the resulting model, such components are client IS ARM and DB server (vertices 5 and 7, Fig. 5, respectively).

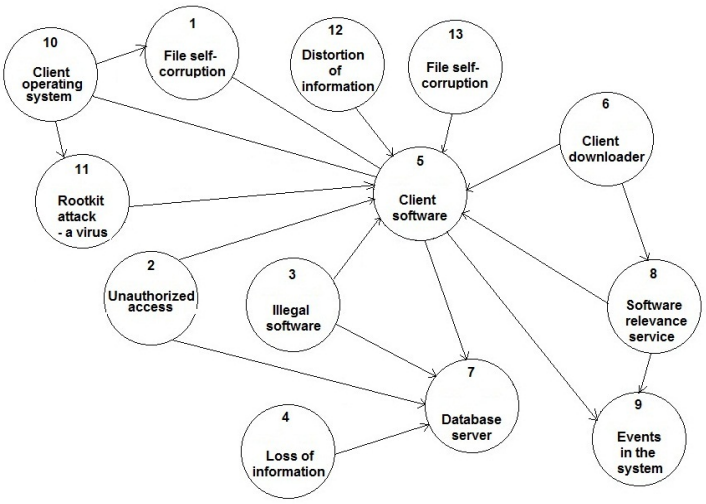

Fig. 5. The resulting graph model to ensure fault tolerance, survivability and protection of IP information

At the same time, the software of client ARM is the most vulnerable from the action of all the influences given. To increase its resistance against all types of perturbations, IS includes means of automatic restoration of the robot's ability of the ARM software. And, as can be seen from the given models (Fig. 2, 3 and 4), counteraction to different types of influences is performed by the same components. They are the software relevance control service (top 8 Fig. 5) and the program that controls the launch of the ARM software (top 6, Fig. 5). The algorithm of its work is constructed in such a way that it is not important for it, which caused the violation of the ARM software, the main thing is the ability to detect the deviation of its parameters from the expected ones and its replacement with a reference one.

Such an organization to counter malign influences is quite effective in terms of costs for it, which in many projects can be a decisive argument.

According to the presented graph models of ensuring the stability of IP to various negative impacts, models of methods for ensuring fault tolerance, survivability of client ARM software (Fig. 6) and information protection (Fig. 7) have been developed.

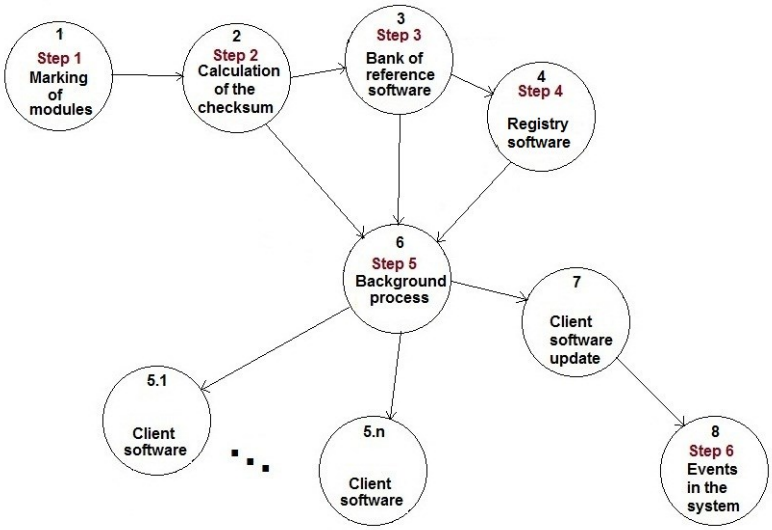

Fig. 6. Graph model of the method of ensuring the survivability and resilience of client jobs information system

Depicted in Fig. 6 the model implements the main steps of the method of ensuring the survivability of client ARM software, which include such stages as labeling software modules (step 1 - top 1, Fig.6), which are part of files without a constant checksum, counting the checksums of each module (step 2 - vertex 2, Fig.6), forming the base of the reference software of client ARM (step 3 - vertex 3, Fig.6), preparing a list of marker values and control amounts of the modules marked by them (step 4 - vertex 4, Fig.6). After performing the preparatory steps 1 - 4 method of ensuring the survivability of specialized IT, which are modeled, respectively, by the vertices of 1 - 4 graphs of Fig.6, the background process of the ARM software relevance control service (vertex 6, Fig.6) is launched, which is the fourth step of the method. If the background process detects a deviation of the parameters of some ARM (vertex graph 5.1 - 5.n, Fig.6) from the expected, then the recovery of its software will be performed (top 7, Fig.6), which will entail the implementation of another step - the last one, according to which the fact of recovery of damaged software will be recorded in the event log file in the IP (top 8, Fig.6). As a result of performing all the steps of the method of ensuring the survivability of the software of client ARM (the path along the graph of the model 1-2-3-6-7-8 or 1-2-4-6-7-8 Fig.6), the availability of IP functions will be restored. It should be noted that steps 3 and 4 can be performed sequentially, or in parallel, as shown in the model Fig.6.

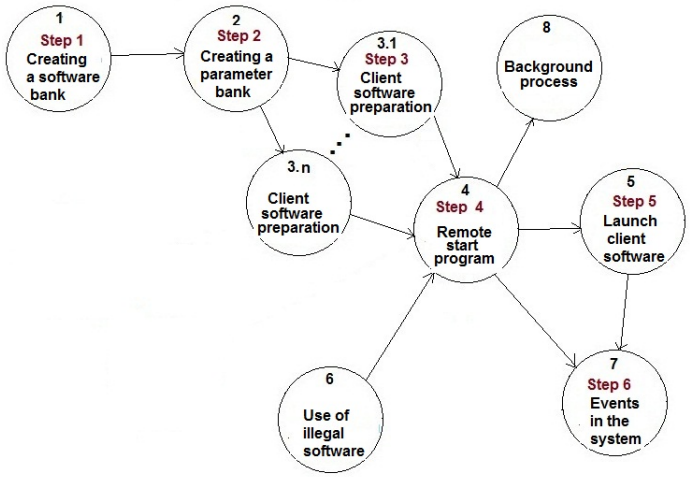

Fig. 7. Graph model of the method of information protection in the information system

The model of the process of ensuring the protection of IP information, which is based on the launch of client ARM software with two-factor verification, is shown in Fig. 7. Its main steps are modeled by the vertices of the presented graph model. In its work, the method covers three possible situations. The first provides for the mode of launching legal software. From some ARM (top 3.1 - 3.n) comes an application for launch. The program of remote launch of client programs (step 4 - vertex 4, Fig. 7) in cooperation with the background process (vertex 8, Fig. 7) checks the reliability of parameters and, if no discrepancies are detected, remotely starts the AHR software that applied with the application. The second and third situations are related to the attempt to connect illegal software to the IP (top 6, Fig. 7). In the case when the application for launch comes from an illegal copy of the software, the launch will be refused, due to the lack of information about it in the register of client software (vertices 1 and 2, Fig. 7).

In a situation where an illegal copy of the software will submit an application with parameters corresponding to one of the legal IS ARM, the software of some ARM will be launched, but not on the attacker's computer, but on the computer of a legal operator, which will become an alarm.

As can be seen from the description of all models, the IP does not contain a special mechanism for launching means of ensuring noise resistance, survivability and information protection. It serves as the detection during the background control of the ARM software discrepancies between the calculated parameters and the reference parameters stored in the bank of the ARM software relevance control service, while the reasons that caused them are not established, but only the consequence of their destructive manifestations is eliminated, and the fact of such an event is recorded in the log file for further analysis. As a result, the availability of IP functions is restored, regardless of what caused their loss.

Analysis of models presented in Fig. 2 and 3 showed that in general they are different destructive influences that are directed at them. All these influences can be divided into two groups - one include negative external influences, and the second influences that are not. This explains why the steps of methods for ensuring fault tolerance and survivability are the same – in fact, this follows from the definitions of these concepts. Their common graph model is shown in Fig. 6.

Now compare the models presented in Fig. 6 and 7, which presents the steps of methods of failure of stability and survivability on the one hand and methods of ensuring the protection of information on the other.

The analysis showed that the sequence of steps in both methods is somewhat different, but their fullness

largely coincides. This gives reason to consider the option of combining them into one generalized method. As can be seen from the graph models of methods, their preparatory steps (steps 2 – 4, Fig. 6; steps 1.2, Fig. 7) practically coincide – in fact, they are parts that cross the same process of creating reference software banks and parameter banks that are jointly used by it, understandably by each method in their own way.

Another commonality is that the executive steps of both methods (step 5, Fig. 6; steps 4.5, Fig. 7) are actually provided by the same service of monitoring the relevance of the software of client ARM IP. The difference is that the mechanism for ensuring the failure of stability and survivability is the background process (vertex 4, Fig. 6), and the remote startup program (vertex 4, Fig. 7) is responsible for ensuring information protection, which are integral interacting parts of this service.

Also, common to both methods is a step that ensures the documentation of events in the system. The commonality of all methods is also manifested in the object of influence – it is the same for all – the software of client ARM.

As a result of the operation of the composition of the graphs presented in Fig. 6 and 7 received a graph of the generalized method (Fig. 8), which combines the steps of three methods to ensure the failure of stability, survivability and protection of information.

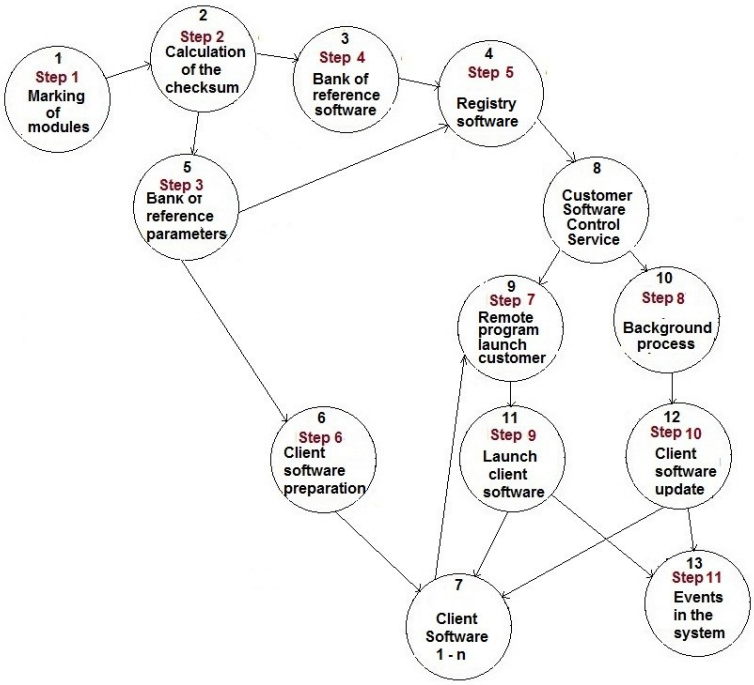

Fig. 8. Graph model of the composition of methods for ensuring the stability of information systems to destructive influences

As you can see, the model of the generalized method includes 11 steps. It should be noted that some steps (steps 2, 3, 5, Fig. 8) are shown here only for the purpose of illustrating the connection of the resulting model with the models of the previousers, and can be absorbed by a more significant step in the preparation of the ARM registry and their parameters, as it actually happens.

In general, all the steps of the generalized method are divided into four groups:

- preparatory steps 1 – 6;
- steps to ensure fault tolerance and survivability: 8.10;
- steps to ensure the protection of information: 7, 9;
- steps of documenting events in IS: 11.

The introduction of a generalized method of ensuring fault tolerance, survivability and protection of information made it possible to simplify the technology of introducing security subsystems, allowed the sharing of the same resources, which contributed to improving the efficiency of the subsystems for ensuring fault tolerance, survivability and protection of information.

Experimental research on the use of a self-organized distributed system

The developed method was implemented in the subsystem to ensure fault tolerance, survivability and information protection. An experiment was performed with the developed system. Its results are shown in Figure 9. The results confirm the improved resilience to malware.

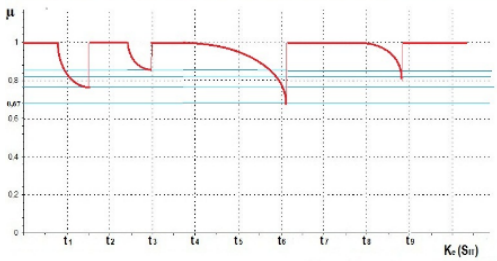

Fig. 9. Graph of reflection of simultaneous manifestations and fault tolerance and survivability

The results of the study confirm the high level of resiliency and survivability in corporate computer networks, which is more than 75%.

Conclusions

Separate methods have been developed to ensure the resilience, survivability and protection of IT information in the languages of the effects of malicious software. Subsequently, the analysis and their combination were performed.

Developed a method of ensuring resilience, survivability and protection of information of specialized IT, which, in contrast to the known, is to combine and integrate into IT mechanisms to ensure resilience, survivability and protection of information according to their coincidences in response to SDR and computer attacks made it possible to create specialized IP resistant to these influences.

References

1. Corporate Endpoint Protection Products Group Test: Socially-Engineered Malware Q2 [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.nsslabs.com/ research/ endpoint-security/ anti-malware/q2-2010-endpoint-protection-product-group-test.html (Viewed on April 3, 2021). – Title from the screen.

2. ESET Endpoint Security [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.eset.com/ (Viewed on April 3, 2021). – Title from the screen.

3. Symantec Endpoint Protection [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.anti-malware.ru/reviews/ Symantec_Endpoint_Protection (Viewed on April 3, 2021). – Title from the screen.

4. COMSS1 [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.comss.ru/page.php?id=2758 (Viewed on April 3, 2021). – Title from the screen.

5. Enterprise End Point Protection Comparative Analysis - Socially Engineered Malware: Report Overview [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: www.nsslabs.com/reports (Viewed on April 3, 2021). – Title from the screen.

6. Bakotech [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://bakotech.ua/ (Viewed on April 3, 2021). – Title from the screen.

7. ClamAV [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.clamav.net/ (Viewed on April 3, 2021). – Title from the screen.

8. Malwarebytes Endpoint Security [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://ru.malware bytes. com/business/endpoint security (Viewed on April 3, 2021). – Title from the screen.

9. Kaspersky Lab [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.kaspersky.ru (Viewed on April 2, 2019). – Title from the screen.

10. Avast! [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.avast.com/index (Viewed on April 21, 2020). – Title from the screen.

11. AVG [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avg.com (Viewed on April 21, 2020). – Title from the screen.

12. Avira [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avira.com (Viewed on April 21, 2020). – Title from the screen.

13. Bitdefender [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.bitdefender.com/(Viewed on April 21, 2020). – Title from the screen.

14. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks. Journal of Computational Science. 2017. ¹23. P. 145–156.

15. Stetsyuk M., Stetsyuk V., Savenko B., Savenko O., Dobrowolski M. Implementation of Control by Parameters of Client Automated Workplaces of Specialized Information Systems for Neutralization malware. CEUR-WS. 2021. Vol. 2853. P. 340-352. URL: http://ceur-ws.org/Vol-2853/paper40.pdf.Securelist. FAQ: Disabling the new Hlux / Kelihos Botnet [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://securelist.com/blog/research/32634/faq-disabling-the-new-hluxkelihos-botnet-13/ (Viewed on April 3, 2021). – Title from the screen.

16. Savenko, O., Nicheporuk, A., Hurman, I., Lysenko, S. - CEUR-WS. – 2019. – Vol. 2393. – P.633-643, ISSN: 1613-0073.

17. Savenko O. Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search / O. Savenko, S. Lysenko, A. Nicheporuk, B. Savenko // CEUR-WS, ISSN: 1613–0073. – 2017. – Vol. 1844. – Pp. 555–569.

18. Lysenko S., Bobrovnikova K., Matiukh S., Hurman I., Savenko O. Detection of the botnets' low-rate DDoS attacks based on self-similarity. *International Journal of Electrical and Computer Engineering*, Vol. 10, Issue 4, 2020, Pages 3651-3659. DOI: http://doi.org/10.11591/ijece.v10i4.pp3651-3659.

19. Pomorova O. Metamorphic Viruses Detection Technique based on the the Modified Emulators [Text] / O. Pomorova, O. Savenko, S. Lysenko, A. Nicheporuk // CEUR-WS. – 2016. – Vol. 1614. – PP.375-383, ISSN: 1613-0073

20. Sergii Lysenko, Kira Bobrovnikova and Oleg Savenko. A Botnet Detection Approach Based on The Clonal Selection Algorithm // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2018, Kyiv, Ukraine, May 24-27, 2018) – Pp. 424-428.

21. Antoniadis, K., Blanchard, P., Guerraoui, R. *et al.* The entropy of a distributed computation random number generation from memory interleaving. *Distrib. Comput.* **31,** 389–417 (2018). https://doi.org/10.1007/s00446-017-0311-5

22. Alistarh, D., Sauerwald, T., Vojnovic, M.: Lock-free algorithms under stochastic schedulers. In: Proceedings of the 2015 ACM Symposium on Principles of Distributed Computing, PODC 2015, Donostia-San Sebastián, Spain, July 21–23, 2015, pp. 251–260 (2015). doi:10.1145/2767386.2767430

23. Barker, E., Kelsley, J.: Recommendation for random bit generator (rbg) constructions. SP 800-90C (2012)

24. Zhou, H., Bruck, J.: Generalizing the Blum-Elias method for generating random bits from markov chains. In: Proceedings of IEEE International Symposium on Information Theory (ISIT) (2010)

25. Pomorova O. Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic [Text] / Oksana Pomorova, Oleg Savenko, Sergii Lysenko, and Andrii Kryshchuk // Communications in Computer and Information Science. – 2013. – Vol. 370. - PP.243-254, ISSN: 1865-0929.

Mykola Stetsiuk **Микола Стецюк**	PhD student of the Computer Engineering & Information Systems Department, Khmenlnytskyi National University https://orcid.org/0000-0003-3875-0416 e-mail: mikstt777@gmail.com	аспірант кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет
Antonina Kashtalian **Антоніна Каштальян**	PhD (Engineering), Associate Professor, Associate Professor of Physics and Electrical Engineering Department, Khmenlnytskyi National University https://orcid.org/0000-0002-4925-9713 e-mail: yantonina@ukr.net	кандидат технічних наук, професор, завідувач кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет