Resilient Computer Systems Development for Cyberattacks Resistance

Sergii Lysenko[a], Kira Bobrovnikova[a], Piotr Gaj[b], Tomas Sochor[c], and Iryna Forkun[a]

[a] *Khmelnitsky National University, Khmelnitsky, Ukraine*
[b] *Silesian University of Technology, Gliwice, Poland*
[c] *Prigo University, Havirov, Czech Republic*

Abstract

The dynamic growth of cyberattacks amount makes the antivirus developers to construct and involve new approaches to not only detect, but mitigate the impact of the attacks. One of new direct to ensure such possibility is the concept of construction of a resilient computer system, that will be able to resist the attacks. This paper presents some principles concerning the computer systems' resilience for cyberattacks resistance. In particular, we describe the concept of resilience as the set of requirements to the computer system. Thus, to ensure the resilient functioning of the computer system in the conditions of cyberattacks, it must be prepared for possible cyberattacks, protected, able to detect cyberattacks, able to respond cyberattacks and to adsorb the cyberattacks' impact, be adaptive, be recoverable. In addition, paper presents experimental issues concerning the techniques are to be used to ensure computer system's resilience under the cyberattacks.

Keywords

Resilience, Cyberattack, Computer Network, Cybersecurity, Computer system, Malware, Malicious traffic, Cyberattacks Detection

1. Introduction

Today we are observers of the dynamic growth of the cyberattacks amount. Attacks impact every sphere where the computer systems are used. Thus, the very strong challenge is to develop new techniques not only to detect the attacks, but also to mitigate, adsorb and resist the attacks. The very new approach to do this is to develop resilient computer systems, able to resist the known and unknown attacks [1-5]. The concept of resilience has been widely used in many contexts, and some of these researches are already applied to critical infrastructures. For example, in the ecological context [6-10] resilience is a property of the population, which can be considered in terms of the properties of equilibrium and oscillations caused by the disturbances of the system. Also, resilience interpretation is applied in economics [11-16]. The construction of buildings includes the property of resisting disasters [17-18]. In the context of protection of critical infrastructure, system resistance is presented in [19]. From the point of view of cybersecurity, computer system resilience is the ability to anticipate, resist, restore and adapt under the influences caused by cyberattacks [20-21]. So, it is very important to develop the concept of resilient computer system functioning under the cyberattacks.

2. Related work

IntelITSIS'2021: 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 24–26, 2021, Khmelnytskyi, Ukraine
EMAIL: sirogyk@ukr.net (Sergii Lysenko); bobrovnikova.kira@gmail.com (Kira Bobrovnikova); piotr.gaj@polsl.pl (Piotr Gaj); tomas.sochor@osu.cz (Tomas Sochor); ivforkun@gmail.com (Iryna Forkun);
ORCID: 0000-0001-7243-8747 (Sergii Lysenko); 0000-0002-1046-893X (Kira Bobrovnikova); 0000-0002-2291-7341 (Piotr Gaj); 0000-0002-1704-1883 (Tomas Sochor)

Nowadays, a great variety of approaches [22] and techniques [23] for identification and object classification [24] are employed. In the paper [25] a comprehensive set of current challenges of phishing attacks and literature review of different Artificial Intelligence (AI) based detection techniques: Scenario-based, Machine Learning, Deep Learning, Hybrid Learning were provided. Also the comparison of different works devoted to detection the phishing attack for these AI technique as well as their advantages and disadvantages were highlighted. In [26] the pros and cons of all aspects of the concept of moving target defense (MTD): key roles, principles of design, classifications, common attacks, basic methodologies and algorithms, metrics and evaluation methods were discussed. The goal of this work is to provide the common trends of the concept of moving target defense research in terms of critical aspects of systems defense for researchers who seek to develop adaptive, proactive mechanisms of MTD.nWith aim of insights into the aspects of proactive defense-in-depth strategies in work [27] a dynamic game framework to model an interaction between a proactive defender and a stealthy attacker was proposed. The deceptive and stealthy behaviors take place by the multi-stage game with incomplete information, where each player has his own unknown to the other information and act according to their convictions which are formed by the learning based on multi-stage observation. In [28] a solution for visual analytics and analysis the possible cyberattacks and identifying suitable mitigations was developed. This solution allows security operators to improve the network security by make decisions on the possible countermeasures. Developed system allows presenting visually the relevant information for a better understand of the attack and its probable evolution. In the paper [29] intrusion detection system (IDS) for a proactive network security monitoring for a computing infrastructure was presented. It includes an intelligent module with using deep learning modeling in order to monitoring network traffic flows in near real-time. In the work [30] a system for cyberattack detection and corrective action in the distribution system was proposed. The developed framework allows detecting abnormal behaviors and identifies them as internal failure or cyberattack. It based on two algorithms: to identify anomalies in the distribution system and provide a corrective control using smart inverters. In addition, this framework includes geographic community smart devices measurements based cyberattack detection mechanism.

In [31] the approach for defense a cyber-physical system under various types of attacks, including actuator and sensor attacks was proposed. A novel integral Bellman-based IDS to detect and mitigate the cyberattacks by collecting data online and without knowledge of the systems physical interpretation was developed. The proposed IDS consist of proactive and reactive components. With aim to neutralize the efforts of attackers the proactive component based on the principles of moving target defense and a stochastic switching changes dynamically behavior of system. In order efficiency increasing this component uses the entropy based unpredictability metric. The reactive component blocks the compromised system components.

The presented in [32] IDS for cyber-physical systems is based on an approximate dynamic programming technique that learns the policies for optimal tracking and optimal regulation for the detection and mitigation against actuator and sensor cyberattacks in a model-free fashion. Switching rules are used to force proactive and reactive defense mechanisms and increase of the stability.

The research [33] devoted to detection, prediction, prevention and recover from cyber-attacks in the railway industry by using defensive controls called the Railway Defender Kill Chain (RDKC). With this aim the proposed approach uses an extended cyber kill chain (CKC) model and an industrial control system (ICS) cyber kill chain. The CKC model includes internal and external CKC. Early breaking of these chains allows stopping the cyber-attacks. Also, an OSA (open system architecture) with the cybersecurity OSA-CBM (open system architecture for condition-based maintenance) architecture was developed. The OSA-CBM architecture includes eight layers: collection, processing and analysis of data; detection, assessment and prognostics of incident; decision support.

In [34] a proactive defense approach for protection a group of related users against lateral spear-phishing was proposed. The proposed technique is based on frequently randomly mutation of sender email address that can only be verified by trusted users. Also corresponding algorithm, protocol and implementation for any email service providers such as Gmail, Apple iCloud, etc were presented.

3. Operational Cycle of the Resilient Computer System under cyberattacks

3.1. Requirement to the resilient computer system under cyberattacks

To ensure the resilient functioning of the computer system in the conditions of cyberattacks, the system must be:

1. prepared for possible cyberattacks.
2. protected;
3. able to detect cyberattacks;
4. able to respond cyberattacks and to adsorb the cyberattacks' impact;
5. be adaptive;
6. be recoverable.

Let us consider a set A of destructive actions a_m against the computer system C, $A = \{a_m\}_{m=1}^{N_m}$. Then operational cycle of the resilient computer system under the cyberattacks we will consider as a set of information and technical states that the system passes (Fig. 2):

$$S = \{s_{prep}, s_{prot}, s_{detect}, s_{absorb}, s_{respond}, s_{recovery}, s_{adapt}\}, \quad (1)$$

where s_{prep} – preparation for the functioning of the system under the cyberattacks; s_{prot} – system protection; s_{detect} – attack detection; s_{absorb} – attack absorption; $s_{respond}$ – attack response; $s_{recovery}$ – system recovery after the attack; s_{adapt} – system adaptation based on knowledge about previous cyberattacks.

Let us consider the initial moment of computer system functioning C as t_0, in which the system functions normally, t_a – the moment when the attack A starts, t_{deg} – the moment when the system began to degrade under attack A, t_{rec} – the moment when computer system begins to recover, t_{norm} – the moment when the system has reached a normal state after the recovery. Then let us determine the set of time intervals that characterize the resilience of system C under attacks:

$$\tau = \{\tau_0, \tau_{att}, \tau_{inf}, \tau_{rec}\}, \quad (2)$$

where τ_0 is the interval of normal functioning of the system, $\tau_0(C, A) = [t_0, t_a)$; τ_{att} – the interval of resilient functioning of the system when an attack is carried out, but the degradation system is not yet affected, $\tau_{att}(C, A) = [t_a, t_{deg})$; τ_{inf} – system degradation interval under the influence of destructive actions of the attack, $\tau_{inf}(C, A) = [t_{deg}, t_{rec})$; τ_{rec} – system recovery interval after the attack, $\tau_{rec}(C, A) = [t_{rec}, t_{norm})$.

Each state of computer system is characterized by a set of values of parameters

$$\forall s_j \in S : s_j = \{X_j, Z_j, F_j\} \quad (3)$$

where $X_j = \{X_{sys}, X_{env}, X_{req}, X_{fail}\}$; X_{sys} – system parameters, $X_{sys} = \{x_j\}_{j=1}^{N_{X_{sys}}}$, $N_{X_{sys}}$ – number of system parameters; X_{req} – system requirements, $X_{req} = \{x_j\}_{j=1}^{N_{X_{req}}}$; $N_{X_{req}}$ - number of system requirements; X_{env} – environment parameters, $X_{env} = \{x_j\}_{j=1}^{N_{X_{env}}}$; $N_{X_{env}}$ – the number of parameters of the environment; X_{fail} – fail parameters, $X_{fail} = \{x_j\}_{j=1}^{N_{X_{fail}}}$; $N_{X_{fail}}$ – number of failure parameters; $F_j = \{F_{prep}, F_{prot}, F_{detect}, F_{absorb}, F_{respond}, F_{recovery}, F_{adapt}\}$ – set of mechanisms F_j, which have to be applied depending on the state of the system C and in the conditions of attack A_k, $C_i \times A_k \to F_j$; $Z_j = \{Z_{prep}, Z_{prot}, Z_{detect}, Z_{absorb}, Z_{respond}, Z_{recovery}, Z_{adapt}\}$ – a set of system parameters obtained as a result of the use of mechanisms F_j.

From the point of view of the operating cycle, the resilience of computer system C will be influenced by a set of indicators w, which reflect different aspects of the uncertainty of states S $W = (w_1; w_2; \ldots)$, $w_i (i = 1, 2, \ldots)$.

Since the information and technical states S are independent, the probability P of successful implementation of operational cycle of the functioning of the computer system C will be presented as:

$$P(W) = P(W_{prep}) \cup P(W_{detect}) \cup P(W_{absorb}) \cup \quad (4)$$

$$\cup P(W_{respond}) \cup P(W_{recovery}) \cup P(W_{adapt}), P(W) = \sum_{w_i \in W} P_i,$$

where $P(w_{prep})$ is the probability that the system is timely prepared and protected; $P(w_{detect})$ is the probability that the system is capable of detecting threats; $P(w_{absorb})$ is the probability that the system is capable of absorbing threats; $P(w_{respond})$ is the probability that the system is capable of responding to a threat; P(w) is the probability that the system is capable to recover after the attack.

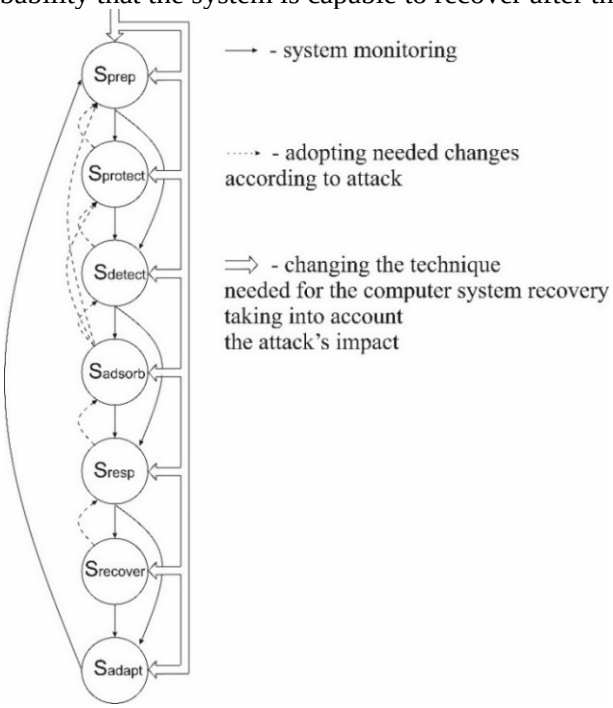

Figure 1: Operational cycle of the resilient computer system in conditions of cyberattacks

3.2. Stages of the resilient computer system functioning under the cyberattacks

Let us consider the stages of the resilient computer system functioning under the cyberattacks.

Preparation. To build a resilient system C that is under cyberattack A and we are to apply a set of preparatory measures G_{prep} to predict the prevention of possible cyberattacks:

$$G_{prep} = \{Ar, Com, Seg, Mon, SS, Res\}, \quad (5)$$

where Ar is a set of measures for customizing the architectural components of the system, $Ar = \{ar_j\}_{j=1}^{N_{Ar}}$, N_{Ar} – the number of measures; Com – a set of measures to configure the connection between the computer system components, $Com = \{com_j\}_{j=1}^{N_{Com}}$, N_{Com} – the number of measures; Seg – a set of measures to adjust the segmentation of the computer system, $Seg = \{seg_j\}_{j=1}^{N_{Seg}}$, N_{Seg} – the number of segmentation measures; Mon – a set of measures to ensure monitoring of the computer system, $Mon = \{mon_j\}_{j=1}^{N_{Mon}}$, N_{Mon} – the number of monitoring measures; SS – a set of security scenarios, which are to be applied to attacked system, $SS = \{ss_j\}_{j=1}^{N_{SS}}$, N_{SS} – number of scenarios; Res – a set of measures to ensure the critical data and system information backup execution, $Res = \{res_j\}_{j=1}^{N_{Res}}$, N_{Res} – the number of backup measures.

Other aspects of the resilient computer system functioning are the preparedness, that is the implementation of actions:

1. understanding and evaluating cyber risk by analyzing and simulating cyberattacks;
2. identifying and eliminating known vulnerabilities in computer systems by which cybercriminals carry out cyberattacks;
3. raising awareness of the signs of known cyber threats and understanding how to recognize them;
4. appropriate backup and restore strategies.

Protection. The protection stage involves the development and implementation of a set of methods and measures of G_{prot} for the computer system security C in order to limit or determine the of cyberattacks impact.

The goal of this stage is to protect the computer system' infrastructure and minimize the likelihood that an attack can be successful and, if that happens, the ability to respond quickly to reduce the damage.

The assessment of the security of the system should reveal any vulnerabilities in existing protection methods.

Detection. The purpose of detection stage is to develop and implement a set of methods G_{Detect}, $G_{Detect} = \left\{G_{Detect}^{host}, G_{Detect}^{lan}\right\}$ to quickly detect attack A, to evaluate the affected system, and to ensure timely response, where G_{Detect}^{host} – a set of methods for detecting host type cyberattacks, G_{Detect}^{lan} – a set of methods for detecting network type cyberattacks.

Absorption. Continued functioning of computer system under cyberattacks may require unpredictable changes in the basic architecture of the system, depending on what exactly is degraded by means of a cyberattack.

To describe the process of system degradation under the of cyberattacks, let us consider a function ξ that will reflect the current performance of the computer system. Any destructive action a_m of attack A will affect the computer system, then $\xi(t \mid a_m)$ will indicate the value of the computer system performance at the time t when it performs the action a_m. Given the impact of destructive actions of attack A on system C, which functioned in the time interval from t_0 to t_{norm}, let us consider the set of actions of attack A as $A = \{a_m : \xi(t \mid a_m) \neq \xi(t_0)\}$, $t \in [t_0, t_{norm})$.

Respond. The respond stage of the resilient computer system has to contain a set of G_{resp} methods for activities that can speed up the time to mitigate the impact of attack after it was detected.

Recovery. The final and most important stage of ensuring the resilience computer system under the attack is recovery stage.

Adaptation. To increase the system's resistance, adaptation involves a set of methods G_{adapt}, $G_{adapt} = \{R_{str}, R_{cnf}\}$, where R_{str} is a set of restructuring methods, R_{cnf} is a set of methods for reconfiguring system components based on knowledge about previous cyberattacks.

4. Experiments

In order to determine the efficiency of the proposed technique a set of experiments were carried out. To do this the framework named BotGRABBER was employed [35].

In this article we present as a case the process of resilient functioning of the computer system under the Man-in-the-middle (MitM) attack [36]. This type of attack may occur when an attacker performs the communications insertion between a client and a server. In our case, attack involved the hijacking of the communication session between a trusted client and network server. The computer system infected by MitM substitutes its IP address for the trusted client. At this moment the infrastructural server continues its session and does not know about intrusion.

Consider the operating cycle of the computer system under the MitM attack let it present as $A_{MitM} : s_{prep} \rightarrow s_{detect}$ $C \times A_{MitM} \rightarrow F_{MitM}$, $\tau_{att}(C, A_{MitM}) = [t_a, t_{deg})$.

MitM attack mitigation relies on performing of a set of mechanisms and measures:

1. Strong WEP/WAP Encryption on Access Points.

2. Strong Router Login Credentials.
3. Virtual Private Network.
4. Force HTTPS.
5. Public Key Pair Based Authentication.

The usage of the mitigation mechanisms $F_{MitM}\ \tau_{inf}(C, A_{MitM}) = [t_{deg}, t_{rec})$ at the moment t_{deg} will transfer the computer system to the response and recovery stages: $s_{detect} \rightarrow s_{resp} \rightarrow s_{req}$. Depending on the intensity of the attack and the effectiveness of the mitigation measures at the time of $t_{req,}$ the system goes into a state of recovery $s_{req} \rightarrow s_{norm}$, $\tau_{rec}(C, A_{MitM}) = [t_{rec}, t_{norm})$.

In order to assess the assurance of the network' s resilience, the integrated resilience metric presented in [37] was used:

$$R = f(R, SRAP_{DP}, SRAP_{RP}, TMPL, RCAB) = R \times \left(\frac{SRAP_{RP}}{SRAP_{DP}}\right) \times \frac{1}{TMPL} \times RCAB \quad (6)$$

where R – computer system resistance, which indicates a value of the compute system performance value between some period of time and is normalized between 0 and 1 (where 0 - a total compute system operation's degradation under attacks and 1 – value for the normal network functioning); $SRAP_{DP}$ - the attack's rapidity; $SRAP_{RP}$ – the computer system reconfiguration stage rapidity; TMPL – averaged value of the computer system performance degradation; RCAB – the reconfiguration ability to apply the security scenario in order to recover after the attack.

We will consider that the computer system recover was successful if GR> δ, where δ - the predefined threshold.

Based on the above-described concept of resistance and its attributes, we have involved the set of techniques able to perform needed action for preparation [38-39], detection [40-42], respond [43-46] and recovery [47-48]. During the experiments, the 357 attacks of different types against the hosts, server and routers were performed [49-52]. The rates of the successful computer system reconfigurations that leads to the mitigation of the attacks are presented in a table 1. Thus, the involvement of the proposed approach has demonstrated the ability to ensure the computer system resilient functioning under the cyberattacks at the rate of 73%.

Table 1

Results of the experiments

Attack's target	Number of attacks	Number of the successful computer system recovery	Resilience value
Network hosts	143	41	0.69
Server	111	38	0.74
routers	103	36	0.76
total	357	105	0.73

5. Conclusion

This article gives an approach concerning the construction of the computer systems' resilience for cyberattacks resistance. It presents the main principles to assure resilience as the set of needed requirements to construct such computer system. Thus, to ensure the resilient functioning for the computer system under the cyberattacks, it has to be prepared for possible cyberattacks, protected, able to detect cyberattacks, able to respond cyberattacks and to adsorb the cyberattacks' impact, be adaptive, be recoverable. Article also paper presents experimental section with the analysis of possible computer system resistance under attacks. Thus, approach involves the set of techniques to not only detect the attacks, but to mitigate it performing the computer system reconfiguration scenarios according to the cyberattacks. Experimental results showed that the implemented principals ensured the resilient functioning under the cyberattacks by botnets at the rate at about 73%.

The further work may be devoted to the development of the techniques that involve machine learning algorithms for increasing the efficiency of the computer system resilience.

6. References

[1] R. Leizerovych, G. Kondratenko, I. Sidenko and Y. Kondratenko, "IoT-complex for Monitoring and Analysis of Motor Highway Condition Using Articial Neural Networks," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, pp. 207-212 (2020), doi:10.1109/DESSERT50317.2020.9125004.

[2] Sokol P., Zuzcak M., Sochor T. Denition of attack in the context of low-level interaction server honeypots. Lecture Notes in Electrical Engineering 330, pp. 499-504 (2015).

[3] Potii O., Illiashenko O., Komin D. Advanced Security Assurance Case Based on ISO/IEC 15408. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds) Theory and Engineering of Complex Systems and Dependability. DepCoS-RELCOMEX. Advances in Intelligent Systems and Computing, Springer, Cham, Vol. 365, pp. 391-401 (2015).

[4] Drozd O., Kharchenko V., Rucinski A., Kochanski T., Garbos R., Maevsky D. Development of Models in Resilient Computing, Proc. of 10th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT' 2019), Leeds, UK, June 5-7 2019, pp. 2-7 (2019), doi: 10.1109/DESSERT.2019.8770035.

[5] Zuzcak, M., Sochor, T. Behavioral analysis of bot activity in infected systems using honeypots. Communications in Computer and Information Science: Springer, 2017, Vol.718, pp. 118-133.

[6] Cimellaro G. P., Dueñas-Osorio L., Reinhorn A.M. Introduction to special issue on resilience-based analysis and design of structures and infrastructure systems. Structural Engineering, 2016, No. 142(8), pp.1-5.

[7] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A. Resilience metrics for cyber systems. Environment Systems and Decisions, 2013, No. 33(4), pp. 471-476.

[8] Bodeau, D.J., Graubart, R. D. Cyber resiliency design principles: selective use throughout the lifecycle and in conjunction with related disciplines. MITRE Corp., Tech. Rep., 2017, p.98.

[9] Zashcholkin, K., Drozd, O., Sulima, Y., Ivanova, O., & Perebeinos, I. Detection method of the probable integrity violation areas in FPGA-based safety-critical systems. International Journal of Computing, 2020.19(2), 282-289. https://doi.org/10.47839/ijc.19.2.1772.

[10] Strigini, L. Resilience: What is it, and how much do we want? In: IEEE Security & Privacy, 2012, No. 10(3), pp. 72-75.

[11] Alexeev, A., Henshel, D. S., Levitt, K., McDaniel, P., Rivera, B., Templeton, S., Weisman, M. Constructing a science of cyber-resilience for military systems. In: NATO IST-153 Workshop on Cyber Resilience, 2017, p.13.

[12] Leslie, N. O., Harang, R. E., Knachel, L. P., Kott, A. Statistical models for the number of successful cyber intrusions. Defense Modeling and Simulation, 2017, No. 15(1), pp. 49-63. doi: 10.1177/1548512917715342.

[13] Bostick, T. P., Connelly, E. B., Lambert, J. H., & Linkov, I. (2018). Resilience Science, Policy and Investment for Civil Infrastructure. Reliability Engineering & System Safety 175:19–23.

[14] Colbert, E. J., Kott, A., Knachel III, L., & Sullivan, D. T. (2017). Modeling Cyber Physical War Gaming (Technical Report No. ARL-TR-8079). US Army Research Laboratory, Aberdeen Proving Ground, United States.

[15] Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M. V., Lambert, J. H., Nielsen, K., Nogal, M., & Todorovic, B. (2017). Bridging the gap from cyber security to resilience. In I. Linkov & J. M. Palma-Oliveira (Eds.), Resilience and risk: Methods and application in environment, cyber, and social domains (pp. 383–414). Dordrecht: Springer.

[16] Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M. V., Lambert, J. H., Nielsen, K., Nogal, M., & Todorovic, B. (2017). Bridging the gap from cyber security to resilience. In I. Linkov & J. M. Palma-Oliveira (Eds.), Resilience and risk: Methods and application in environment, cyber, and social domains (pp. 383–414). Dordrecht: Springer.

[17] Marchese, D., Reynolds, E., Bates, M. E., Morgan, H., Clark, S. S., & Linkov, I. (2018). Resilience and sustainability: Similarities and differences in environmental management applications. Science of the Total Environment, 613, 1275–1283.

[18] Larkin, S., Fox-Lent, C., Eisenberg, D. A., Trump, B. D., Wallace, S., Chadderton, C., & Linkov, I. (2015). Benchmarking agency and organizational practices in resilience decision making. Environment Systems and Decisions, 35(2), 185–195.
[19] Kott., et al. A Reference Architecture of an Autonomous Intelligent Agent for Cyber Defense (Tech.l Rep.). US Army Research Laboratory, Aberdeen Proving Ground, United States(2018).
[20] Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I.. Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis. (2017).
[21] Gao, J., Barzel, B., & Barabási, A. L. Universal resilience patterns in complex networks. Nature, (2016).530(7590), 307–312.
[22] Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., and Vasylkiv, N. Botnet detection approach based on the distributed systems. International Journal of Computing, 2020.19(2), 190-198. https://doi.org/10.47839/ijc.19.2.1761.
[23] A. V. Barmak et al.: Information technology of separating hyperplanes synthesis for linear classifiers. J. Autom. Inf. Sci. 51(5), 54–64 (2019). doi:10.1615/JAutomatInfScien.v51.i5.50.
[24] Krak, Iu.V. Barmak, O.V., Romanyshyn, S.O. The method of generalized grammar structures for text to gestures computer-aided translation. Cybern. Syst. Anal. 50(1), 116–123 (2014). doi:10.1007/s10559-014-9598-4.
[25] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, pp. 1-16 (2020).
[26] Cho, J. H., Sharma, D. P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T. J., & Nelson, F. F. Toward proactive, adaptive defense: A survey on moving target defense. IEEE Communications Surveys & Tutorials, 22(1), 709-745 (2020).
[27] Huang, L., & Zhu, Q. A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. Computers & Security, 89, 101660 (2020).
[28] Angelini, M., Bonomi, S., Lenti, S., Santucci, G., & Taggi, S. MAD: A visual analytics solution for Multi-step cyber Attacks Detection. Journal of Computer Languages, 52, pp. 10-24 (2019).
[29] Nguyen, G., Dlugolinsky, S., Tran, V., & García, Á. L. Deep learning for proactive network monitoring and security protection. IEEE Access, 8, 19696-19716 (2020).
[30] Fard, A. Y., Easley, M., Amariucai, G. T., Shadmand, M. B., & Abu-Rub, H. Cybersecurity analytics using smart inverters in power distribution system: Proactive intrusion detection and corrective control framework. In 2019 IEEE International Symposium on Technologies for Homeland Security (HST) (pp. 1-6). IEEE (2019).
[31] Kanellopoulos, A., & Vamvoudakis, K. G. Entropy-based proactive and reactive cyber-physical security. In Proactive and Dynamic Network Defense, pp. 59-83. Springer, Cham (2019).
[32] Zhai, L., & Vamvoudakis, K. G. Data-based and secure switched cyber–physical systems. Systems & Control Letters, 148, 104826 (2021).
[33] Kour, R., Thaduri, A., & Karim, R. Railway defender kill chain to predict and detect cyber-attacks. Journal of Cyber Security and Mobility, pp. 47-90 (2020).
[34] Islam, M. M., Al-Shaer, E., & Rahim, M. A. B. U. Email address mutation for proactive deterrence against lateral spear-phishing attacks. In International Conference on Security and Privacy in Communication Systems, pp. 1-22. Springer, Cham (2020).
[35] Lysenko S., Bobrovnikova K., Savenko O., Kryshchuk A. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks. In: Gaj P., Sawicki M., Kwiecien A. (eds) Computer Networks. CN 2019. Communications in Computer and Information Science, vol 1039, p. 127-143. Springer, Cham (2019), doi: 10.1007/978-3-030-21952-9 10.
[36] Jeff Melnick. Top 10 Most Common Types of Cyber Attacks Updated: October 8, 2020 URL: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Man-in-the-middle%20(MitM)%20attack.
[37] Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A.: Self-adaptive System for the Corporate Area Network Resilience in the Presence of Botnet Cyberattacks. In: International Conference on Computer Networks, pp. 385-401. Springer, Cham (2018).

[38] Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., Savenko, B.: Information Technology for Botnets Detection Based on Their Behaviour in the Corporate Area Network. In: International Conference on Computer Networks, pp. 166-181. Springer, Cham (2017).
[39] O. Savenko, S. Lysenko, A. Kryschuk, Multi-agent based approach of botnet detection in computer systems Communications in Computer and Information Science, 291 (2012) 171-180
[40] Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A., Bobrovnikova, K.: Antievasion technique for the botnets detection based on the passive DNS monitoring and active DNS probing. In: International Conference on Computer Networks: Springer International Publishing, pp. 83-95. Springer, Cham (2016).
[41] Lysenko, S., Pomorova, O., Savenko, O., Kryshchuk, A. and Bobrovnikova, K. DNS-based anti-evasion technique for botnets detection. 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Warsaw, 2015, pp. 453-458 (2015), doi: 10.1109/IDAACS.2015.7340777.
[42] Savenko, O., A. Nicheporuk, Ivan Hurman and S. Lysenko. “Dynamic Signature-based Malware Detection Technique Based on API Call Tracing.” ICTERI Workshops (2019).
[43] Melnyk, A., Melnyk, V. Remote Synthesis of Computer Devices for FPGA-Based IoT Nodes. 2020 10th International Conference on Advanced Computer Information Technologies, ACIT 2020 – Proceedings 9208882, pp. 254-259.
[44] Melnyk, A., Melnyk, V. Specialized Processors Automatic Design Tools-the Basis of Self-Configurable Computer and Cyber-Physical Systems. 2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 - Proceedings, pp. 326-335. DOI:10.1109/ATIT49449.2019.9030481.
[45] C. Shu, D. Dosyn, V. Lytvyn, V. Vysotska, A. Sachenko and S. Jun, "Building of the Predicate Recognition System for the NLP Ontology Learning Module," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 802-808, doi: 10.1109/IDAACS.2019.8924410.
[46] Ivasiev S., Kasyanchuk M., Yakymenko I., Gomotiuk O., Shylinska I., Bilovus L. Algorithmic Support for Rabin Cryptosystem Implementation Based on Addition. Advanced Computer Information Technology (ACIT–2020): Proceedings of the International Conference. Deggendorf (Germany). 2020. P. 779-782 (Scopus).
[47] Yakymenko I., Kasianchuk M., Gomotiuk, O., Ivasiev S., Basistyi P. Elgamal cryptoalgorithm on the basis of the vector-module method of modular exponentiation and multiplication Proceedings - 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2020, 2020, pp. 926–929.
[48] O. Drozd, K. Zashcholkin, O. Martynyuk, O. Ivanova, J. Drozd. Development of Checkability in FPGA Components of Safety-Related Systems. CEUR Workshop Proceedings, vol. 2762, pp. 30-42 (2020). Online http://ceur-ws.org/Vol-2762/paper1.pdf.
[49] O. Drozd, V. Antoniuk, V. Nikul, M. Drozd, “Hidden faults in FPGA-built digital components of safety-related systems,” Proc. of the 14th International Conference “TCSET’2018 Conference “Modern problems of radio engineering, telecommunications and computer science”, Lviv-Slavsko, Ukraine, 2018, pp. 805-809. DOI: 10.1109/TCSET.2018.8336320.
[50] Drozd O., Perebeinos I., Martynyuk O., Zashcholkin K., Ivanova O., Drozd M.: Hidden fault analysis of FPGA projects for critical applications. In: IEEE International Conference TCSET. Paper 142, Lviv-Slavsko, Ukraine, (2020) doi: 10.1109/TCSET49122.2020.235591.
[51] S. Lysenko, K. Bobrovnikova & O. Savenko, A botnet detection approach based on the clonal selection algorithm. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE (2018) 424-428.
[52] S. Lysenko, K. Bobrovnikova, S. Matiukh, I. Hurman & O. Savenko, Detection of the botnets' low-rate DDoS attacks based on self-similarity. International Journal of Electrical & Computer Engineering, 2020, 10, 2088-8708. DOI: http://doi.org/10.11591/ijece.v10i4.pp3651-3659.