Conducting Cyber Exercises Based on the Information Security Threat Model

Aleksandr V. Dorofeev[1] and Alexey S. Markov[1,2]

[1] *NPO Echelon, 24 2nd Electrozavodskaya ul., Moscow, 107023, Russia*
[2] *Bauman Moscow State Technical University, 5/1 2nd Baymanskay ul., Moscow, 105005, Russia*

Abstract

The purpose of this study is to demonstrate the use of Russian guidelines for computer threat assessment to organize information security exercises. The study deals with the cyber exercises as a relevant class of online learning in information security. The authors analyzed the definitions and shown specific features as well as classifications of cyber exercises. They reviewed the codes, regulations, and guidelines applicable to cyber exercises, described systematics underlying the cyber exercise scenarios. MITRE ATT&CK and FSTEC guidelines on information security threat assessment are compared in brief. It is concluded that Russian guidelines can be used to develop cyber exercises scenarios. We provided an example of a Russian CTF competition and presented a CTF competition scenario compliant with the Russian guideline.

Keywords 1

Education, game-based learning, information security exercises, training, awareness, table-top exercise, cyber-defense exercises, drill, cyber range, cyber security polygon, ATT&CK

1. Introduction

It is commonly believed that the basics of learning by simulation of real crises (which can include targeted cyber-attacks) were determined by John Dewey in 1938. [1, 2]. In the military field this approach, called exercises, was used much earlier: Few people do not know the saying of the great military leader Aleksandr Suvorov "What is difficult in training will become easy in a battle", as stated in the regulation on military training of troops in 1794.

Currently, the applied capabilities for simulation of real-life situations for training purposes have changed fundamentally with the general computerization, testing of online work, and introduction of computer simulation packages for thematic media (e.g. critical information infrastructure facilities), etc. The transfer of crisis simulation into the field of information security has given the rise of a new discipline, that is, cyber competitions and exercises. In creating and implementing cyber exercises, methodologists usually rely on information security systematics of American origin, in particular those developed by NIST and MITRE. In this publication, the authors give an example of cyber exercises based on the Russian FSTEC threat assessment procedure [3, 4].

2. Introduction to Definitions

At present, the definitions of cyber exercises are still in their infancy and originate, of course, from the military field. For example, MITRE [5] refers to exercises to simulated military cyber operations (involving planning, preparation, and execution) aimed to train and evaluate the organization with a

Proceedings of VI International Scientific and Practical Conference Distance Learning Technologies (DLT–2021), September 20-22, 2021, Yalta, Crimea
EMAIL: av@cnpo.ru (A. 1); a.markov@bmstu.ru (A. 2)
ORCID: 0000-0003-0111-7377 (A. 2)

focus on an information security program. NIST [6] notes that exercises should be a simulation of an emergency designed to test the IT plan, primarily the roles and responsibilities of personnel. The ITU interprets the goals of cyber exercises as improving the coordinated response to cyber incidents in dealing with cyber threats [7]. According to ISO 22398, exercises can be used to verify documents, train, clarify and educate personnel on roles and responsibilities, improve coordination and communication, improve individual performance, etc. [8]. The term is elaborated in ECSO [9], which defines cyber exercises as a planned activity in which an organization simulates cyber-attacks, information security incidents, or other types of breaches to test the cyber capabilities of the organization, starting from the ability to detect a security incident to the ability to respond adequately and minimize any associated consequences (Fig. 1).

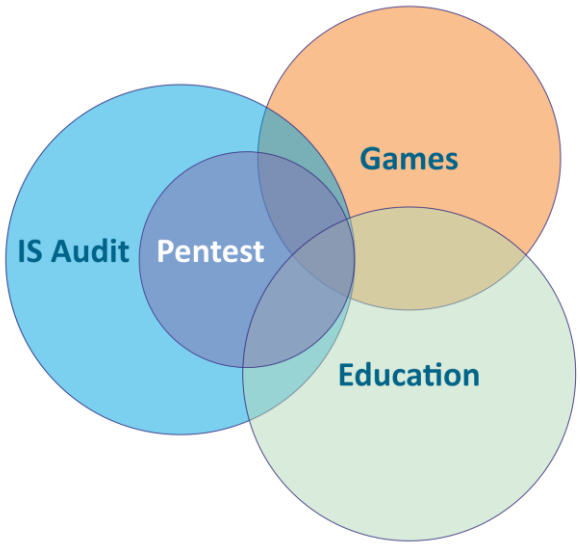


Figure 1: Cyber Exercises as an Interdisciplinary Activity

Based on the descriptions of cyber security exercises [2, 10-13], cyber exercises should include the following specific activities:

- Simulate an information security emergency;
- Evaluate actual and real (rather than hypothetical) threats, vulnerabilities, and computer security attacks,
- Use a comprehensive training program, including a game scenario that can be developed during the game,
- Improve both staff awareness, roles and responsibilities, coordination, and ability to make decisions in abnormal situations.

As for the last item, it should be noted that exercises require practicing decision-making based on the knowledge obtained [14], for example in any situation that is not described in the incident management and computer attack response manuals [15-19].

It is well known that cyber exercises personnel is represented by some teams, usually the following: Red team - attackers, Blue team - defenders, Green team - administrators, White team - organizers, Yellow team - researchers, etc. (Fig. 2).

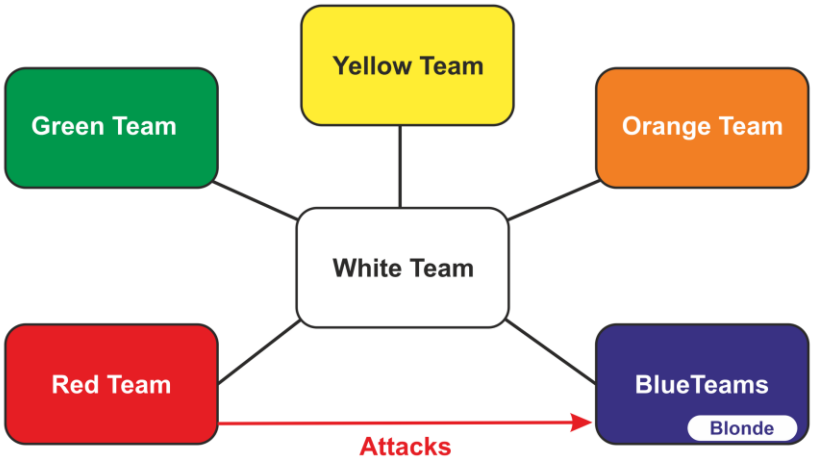


Figure 2: Cyber Teamwork

The objectives and expectations of cyber exercises are determined by specific goals and capabilities, and may, for example, include the following:

- Train technical personnel in the use of information security tools,
- Increase cyber security awareness,
- Practice the management of decision-making while responding to incidents,
- Practice communication processes within the team of defenders,
- Check the adequacy of the organization's incident response regulations, etc.

A cyber range normally includes the following segments [9-20]:

- Base segment: high-performance servers that can run dozens or hundreds of virtual servers simultaneously, as well as a virtualization system;
- Virtual infrastructure for protection and attack: network equipment, servers, and workstations, information security tools;
- Supporting infrastructure;
- Scoring system (refereeing system).

3. Regulations and Guidelines

Regulations provide answers to the following questions:

- When are cyber exercises necessary?
- How should they be conducted?

As far as the first question is concerned, it should be pointed out that the staff of organizations shall be trained and information security audits recommended (primarily a penetration test by simulating real attacks). As we know, in most countries of the world these matters are regulated by the state. In Russia, information security audit requirements (including penetration tests) are explicitly defined by the security regulators in the banking sector (Bank of Russia standard) and critical information infrastructure (Orders of FSTEC of Russia). Necessity and frequency of personnel retraining and advanced training are determined by Resolutions of the Russian Government (Resolution of the Government of the RF No. 79, Resolution of the Government of the RF No. 171, Resolution of the Government of the RF No. 313) and specified in recommendations and regulations of information security regulators.

Cyber exercises matters are most specifically described in the MITRE document [5]. In addition, ISO 22390 regarding general IT exercises [8] and French publications dealing with business continuity exercises [21].

It should be noted that these documents imply the classification of cyber exercises to form tasks, expectations, teams, etc.

4. Classifications

Based on the literature (e.g. [2, 20, 22]), the authors propose the following classification (Fig. 3):

- Types of exercises and degree of abstraction (theoretical, real),
- Level of publicity (closed, opened),
- Target (business continuity, CIA),
- Target audience (management, administrators, users),
- Types of scenarios (CTF competition, multi-tasking, role-based)
- Classes of attacks (techniques and tactics),
- Scale (organization, industry, etc.).

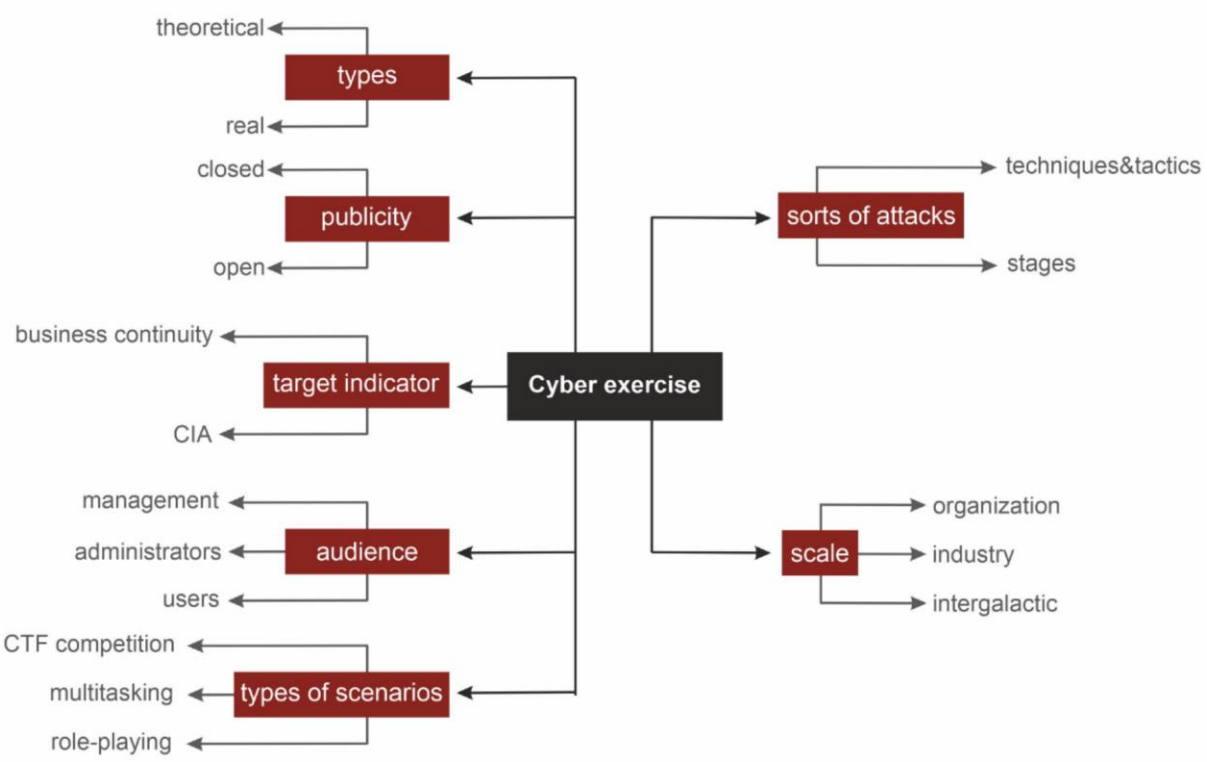


Figure 3: Cyber Exercise Classification

The above classification covers fundamental exercises which may include the following [6, 23]:

1. Discussion based:

- Table Top (TTX),
- Games,
- Workshop,

Seminars;

2. Operations based:

- Checking management, control, and coordination,
- Drill,
- Full-field exercises,

3. Mixed.

In terms of scope and themes, most open exercises focus on critical information infrastructure (CII) or cyber warfare [24, 25].

Figure 4 shows statistics of European cyber exercises in the field of CII [2].

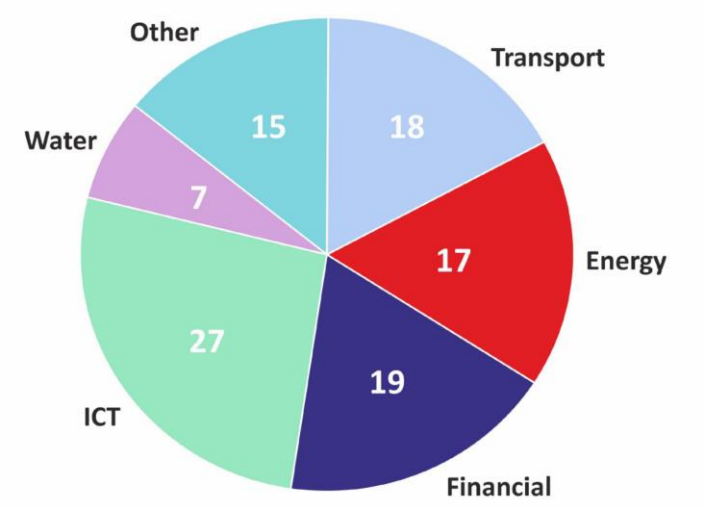


Figure 4: European CII Cyber Exercises

Based on the publications of National Cyber Range (created by Rostelecom as part of the Digital Economy of Russia program), large-scale CII security exercises have already been performed in energy and banking industries, and studies of the oil and gas, telecommunications, transport, and metallurgy industries have been announced (Fig. 5).

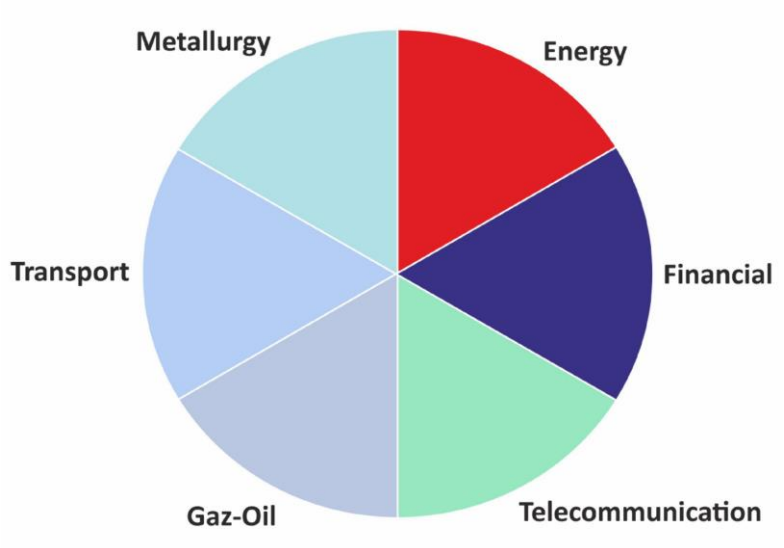


Figure 5: Russian CII Cyber Exercises

Below is an example of a typical scenario for cyber exercises in an organization [26]:

- Connecting the organization's employees to the community,
- Phishing with remote administration software,
- Planting USB with remote administration software,
- Network attacks on externally accessed IT infrastructure,
- Hidden transmission of data from the network using standard protocols, such as DNS,
- Attempts to physically obtain confidential information from employees using social engineering techniques.

Industry exercises could be organized to repulse some kind of cyber-attack, such as APT Tonto and TA428 if the objective is to protect intellectual property, or Cobalt and Carbanak hacker groups in case of banking exercises. In this regard, it is convenient to use the attribute characteristics of APT attacks presented by MITRE to create a cyber exercises scenario.

In this paper, the authors present a full-scale exercise integrated with qualification tests, Capture the Flag (CTF). It should be noted that the origins of such exercises were formed back in 1996 at the Defcon conference.

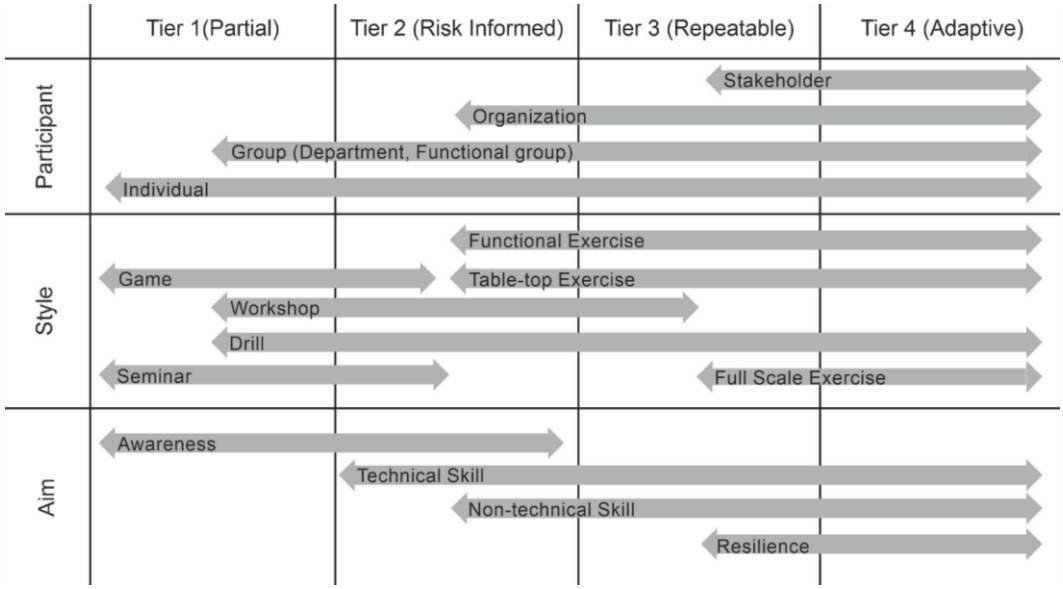
We will note the characteristic features of CTF exercises:

- Teams are offered a set of tasks on information system security testing, forensics, information search and analysis, password selection and exploitation of combinations of vulnerabilities, cryptography, steganography, etc;
- Successful completion of a task is a set of symbols (flag). For example, a flag can be an administrator's password, contents of a file accessible only by a certain user, decrypted value, etc;
- Flags are recorded in a special refereeing system, which automatically calculates points for each team.

These tasks - the scenario - are either expertly generated (based on the organizers' experience) or are linked to computer attack systematics, which, according to the authors, include the following:

- NIST Framework (company maturity and/or milestones),
- Lockheed Martin Cyber Kill Chain (cyber-attack phases),
- MITRE ATT&CK (attackers' post-behavior),
- FSTEC of Russia: procedure for assessing threats to information security (list of threats).

For example, [18] discusses in detail the formation of various kinds of cyber exercises in relation to the NIST Cyber Framework. The highlight of the project is the consideration of the maturity of companies involved in exercises. The table developed in the said study is presented in Fig. 6.



Source: Aoyama, etc. [18, fig. 2]

Figure 6: Cyber Exercise on Preparedness

Until recently, the most cited model in the literature was the 7-stage Cyber Kill Chain model. In this case, cyber exercises are organized about the phases of cyber operations [27-29]. For example, similar systematization is shown in [30].

Current studies related to scenario identification and demonstration focus on the use of behavioral methods of attacks (post-incident is considered). In this case, the scenario is related to the MITRE ATT&CK taxonomy. This taxonomy currently includes 14 tactics (target stages) and 144 techniques (attack execution methods) [27, 31, 32].

The authors propose a similar approach to developing a scenario based on the threat model adopted in Russia. The current threat assessment procedure of the Russian FSTEC includes 10 targeted attack stages used to develop scenarios for information security threats [3]:

- T1. Information collection [33],

- T2. Initial access,
- T3. Introduction and execution of malware,
- T4. Access securing,
- T5. Malware management,
- T6. Privilege increase,
- T7. Activities hiding,
- T8. Provision of access to related systems,
- T9. Collection and withdrawal of information from the system,
- T10. Unauthorized impact or access (target impact).

There are 145 ways of implementing the specified target stages.

In principle, it is not difficult to compare the above approach with ATT&CK systematics. Due to the limited scope of publication, the authors compared only one target stage T4.

Table 1

Examples of Russian normative legal acts comparison of ATT&CK and FSTEC systematics

T4. Access securing	
FSTEC	MITRE ATT@CK
T4.1. Unauthorized creation of accounts	T1136, T1212
T4.2. Using in-built OS remote access tools	T1133, T1021
T4.3. Covertly installing and running OS remote access tools	T1133, T1021, T1219
T4.4. Masking connected devices as legitimate devices	Close to T1036
T4.5. Making appropriate entrieš in the auto start components	T1542, T1053, T1547, T1037
T4.6. Compromising device firmware	T1542.001, T1495
T4.7. Backing up malicious code to hidden areas	none

The following is an example from the Russian cyber exercises.

5. Example of Using an Information Security Threat Model

Regarding the Russian cyber exercises market, it is arguable that cyber exercises can already be presented as a service, e.g.:

1. Cyber exercises as infrastructure. Here, the national cyber exercises ground could be given as an example.

2. Cyber exercises as a platform. An example would be the Ampire boxed product developed by the Infotex group of companies.

3. Cyber exercises as a product. Products of dozens of Russian companies, producing a wide range of data protection tools, involved in the exercises, can be referred to this class. We are talking about SIEM, IDS/IPS, VA tools, and firewalls.

The latter includes the CTF cyber exercise Echeloned Defence (Defence in Depth exercise), initiated by the Patriotic Youth Movement of Russia. Thus, the competition included 3 levels of participants: juniors, students, and undergraduate students. In 2019 there were 147 participants in 25 teams and in 2020 the competition included more than 100 teams. Scenarios were created by the threat model recommended by the FSTEC of Russia [3]. An example of a scenario for the above exercises is shown in the matrix (Fig. 7).

T1. Information collection	T2. Initial access	T3. Introduction and execution of malware	T4. Access securing	T6. Privilege increase	T7. Activities hiding	T8. Provision of access to related systems	T10. Target impact
T1.1	T2.3	T3.1	T4.1	T6.1	T7.1	T8.1	T1.1
T1.4	T2.4		T4.2	T6.2	T7.17	T8.2	T1.4
T1.5				T6.3			T1.5

Figure 7: CTF Cyber Exercise Scenarios within the FSTEC Methodology

6. Conclusion

This overview allows for making some brief conclusions.

1. Cyber exercises are a relevant form of incident-based training. An important feature of cyber exercises is full alignment with online learning, which became usual during the pandemic. At the same time, CTF competitions are currently the most popular in universities.

2. There is global awareness of the formation of cyber exercises scenarios that are currently based on evolving attack systematics, most notably ATT&CK. However, the paper shows that scenarios can be created based on threat models, including the Russian procedure.

3. It may be argued that a market for cyber exercises has developed globally and in Russia, including cyber exercises as a service (cyber exercises as infrastructure, cyber exercises as platform, and cyber exercises as product). There are a wide range of proprietary (paid) and open source products for conducting or organizing exercises. Many companies producing security products (SIEM, IDS/IPS, VA, FW) have free software for universities.

7. References

[1] J. Dewey. Education and Experience. Kappa Delta Pi, 1938. 91 p.

[2] E.G. Díez, D.F. Pereira, M. A. L. Merino, H. R. Suárez and D.B. Juan. Cyber Exercises Taxonomy, Spanish National Institute for Cyber-security, 2015, 56.

[3] Methodology for assessing threats to information security. Methodological document. FSTEC of Russia, 2021. 87 c. (In Russ.)

[4] S. V. Solovev, Y. K. Yazov. Information support of the activity for technical protection of information. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2021. N 1 (41). P. 69-79. DOI: 10.21681/2311-3456-2021-1-69-79. (In Russ.)

[5] J. Kick. Cyber Exercise Playbook. MP140714. Wiesbaden, Germany. MITRE, 2014. 50 p.

[6] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White and T. Good. NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, 2006. 97 p.

[7] ITU-D Study on Potential Development Trends in the CIS Region 2022-2025 - Cybersecurity. RPM-CIS21/INF/5-R. ITU WTDC, 2021. - Version 1.0 - 52 p. (In Russ.)

[8] ISO 22390: 2013 – SS. Guidelines for exercises and testing, 40 p.

[9] Understanding Cyber Ranges: From Hype to Reality. WG5 PAPER. SWG 5.1. I Cyber Range Environments and Technical Exercises. European Cyber Security Organisation, 2020. 31 p.

[10] G. Angafor, I. Yevseyeva, Y. He. Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and Privacy vol 3 No 6, 1-19 (2020). DOI: 10.1002/spy2.126.

[11] A. A. Petrenko, S. A. Petrenko. Cyber Exercises: Methodological Recommendations of ENISA. Voprosy kiberbezopasnosti [*Cybersecurity issues*]. 2015. No 3 (11). P. 2-14. (In Russ.)
[12] M. I. Avilov. Role network monitoring system in the technical cyber defense exercise. Proceedings of Saint Petersburg Electrotechnical University. 2019. N 2. P. 43-47. (In Russ.)
[13] L. A. Wahsheh and B. Mekonnen, "Practical Cyber Security Training Exercises," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), 2019, pp. 48-53, DOI: 10.1109/CSCI49370.2019.00015.
[14] J. Rasmussen. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man, and Cybernetics, vol. SMC-13, no. 3, pp. 257-266, May-June 1983. DOI: 10.1109/TSMC.1983.6313160.
[15] A. V. Olifirov, K. A. Makoveichuk, P. Y. Zhytnyy, T. N. Filimonenkova, and S. A. Petrenko, Models of Processes for Governance of Enterprise IT and Personnel Training for Digital Economy, 2018 XVII Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES), 2018, pp. 216-219, DOI: 10.1109/PTES.2018.8604166.
[16] M. Karjalainen, T. Kokkonen and S. Puuska, "Pedagogical Aspects of Cyber Security Exercises," 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2019, pp. 103-108. DOI: 10.1109/EuroSPW.2019.00018.
[17] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, G. Witte. Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181, Rev. 1. NIST, 2020, 27 p. DOI: 10.6028/NIST.SP.800-181r1
[18] T. Aoyama, T. Nakano, I. Koshijima, Y. Hashimoto, and K. Watanabe. On the Complexity of Cybersecurity Exercises Proportional to Preparedness. Journal of Disaster Research, 2017, Vol.12 No.5, pp. 1081-1090. DOI: 10.20965/jdr.2017.p1081
[19] V.N. Taran. Quality Criteria for Professional Training of Personnel in IT Industry Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES 2018, 2019, pp. 47–50, 8604267. DOI: 10.1109/PTES.2018.8604267.
[20] M.M. Yamin, B. Katt, V. Gkioulos, Cyber ranges, and security testbeds: Scenarios, functions, tools and architecture, Computers & Security, Volume 88, 2020, 101636, DOI: 10.1016/j.cose.2019.101636.
[21] Organizing a cyber crisis management exercise, by ed. G. Poupard and V. Vallée. CCA, 2021, 128 p.
[22] E. Seker and H. H. Ozbenli, "The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation," 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2018, pp. 1-9, DOI: 10.1109/CyberSecPODS.2018.8560673.
[23] Homeland Security Exercise and Evaluation Program, FEMA, 2020, 6 p.
[24] E. Sitnikova, E. Foo, R.B. Vaughn. The power of hands-on exercises in SCADA cybersecurity education. Inform. Assurance Secure. Educ. Train. 2013. 406, pp. 83-94. DOI: 10.1007/978-3-642-39377-8_9.
[25] M. Granåsen and C. Andersson. Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study, Cognition Technology, and Work, 2016, vol. 18n, no. 1, pp. 121-143. DOI: 10.1007/s10111-015-0350-2.
[26] A.V.Dorofeev, A.S.Markov, Y.V.Rautkin. Ethical Hacking Training. CEUR Workshop Proceedings, 2019, Vol-2522, pp. 47-56.
[27] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," 2020 Resilience Week (RWS), 2020, pp. 106-112. DOI: 10.1109/RWS50334.2020.9241271.
[28] J. Straub. Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks, 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 148-153. DOI: 10.1109/SmartCloud49737.2020.00035.

[29] S. Choet al., "Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture," 2018 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2018, pp. 1-8. DOI: 10.1109/CyberSA.2018.8551383.
[30] V. Mokhor, V. Tsurkan, V. Pokrovska. Analysis of Cyber Exercises Approaches. CEUR Workshop Proceedings. 2021, Vol. 2859. P. 61-70.
[31] A. P. Golushko and V. G. Zhukov. Application of Advanced Persistent Threat Actors` Techniques aor Evaluating Defensive Countermeasures, 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2020, pp. 312-317. DOI: 10.1109/EIConRus49466.2020.9039315.
[32] R. Al-Shaer, J. M. Spring and E. Christou, "Learning the Associations of MITRE ATT & CK Adversarial Techniques," 2020 IEEE Conference on Communications and Network Security (CNS), 2020, pp. 1-9. DOI: 10.1109/CNS48642.2020.9162207.
[33] A. Dorofeev, A. Markov, V. Tsirlov. Social media in identifying threats to ensure safe life in a modern city. Communications in Computer and Information Science. 2016, N 674, pp. 441-449. DOI: 10.1007/978-3-319-49700-6_44.