Criteria for Classification of Cyber-training and Analysis of Organizational and Technical Platforms for Their Conduct

Oleksandr Puchkov, Igor Subach, Artem Zhylin, Vitaliy Tsyganok

Institute of Special Communications and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 4, Verkhnoklyuchova st., Kyiv, 03056, Ukraine

Abstract

The article deals with the levels, types and kinds of cyber-training and provides a generalized classification. Such types of cyber-training as Capture the Flag and Cyber Range (Red Team / Blue Team) are considered in detail. As a separate approach, the gamification of cyber-training in the form of board and computer games is highlighted and analyzed. Further promising areas of research in the field of organization and conduct of cyber-training are suggested.

Keywords

Cybersecurity, cyber-training, cyber polygon, classification

1. Introduction

Formulation of the problem. With the development of information technology, cybercrime and cyber terrorism are becoming the most pressing threat to the security of the state, society, and the individual. To protect information and telecommunication systems from cyber threats, various security systems are created and implemented, one of the elements of which is always the person who configures and operates these systems. As noted in [1], the lack of specialists in the field of cybersecurity prevents many organizations from implementing new cyber capabilities. To address this problem, investment is increasing every year, both in training technology in general and in the training of cybersecurity professionals in particular [1].

One of the forms of training specialists in the field of cybersecurity is cyber-training. Cyber-training is a type of training that is most often carried out on a cyber-field and conducted in real-time among cybersecurity professionals or managers of various enterprises [2].

At cyber ranges, participants can practice skills in the protection of information systems. Cyber polygon is an interactive, virtual local area network of any organization, a system, with a set of tools and programs that are connected to the virtual (simulated) Internet [2]. It provides the environment for gaining practical skills in networking devices and organizing a safe place to develop and test software. A cyber polygon can include actual hardware and software, or it can be a combination of physical and virtual components. At the Internet level, it not only simulates traffic, but also replicates network services such as web pages, browsers, e-mail, and more. At the same time, there is an understanding that cyber learning is not just about working out practical issues in cyber fields. The types of these practical exercises in different sources are explained differently, which leads to misunderstandings between different participants in the planning, organization, and conduction of these exercises. Therefore, there is an urgent task of analyzing and classifying the cyber-training and platforms that are used for their further selection in order to train cybersecurity professionals.

Analysis of recent research and publications. The analysis of recent domestic and international publications, which considered the topic of cyber-training and platforms for their conduct (cyber-

IT&I-2020 Information Technology and Interactions, December 02–03, 2020, KNU Taras Shevchenko, Kyiv, Ukraine
EMAIL: ganaga@ukr.net (O. Puchkov); igor_subach@ukr.net (I. Subach); zhylinartem@gmail.com (A. Zhylin); vitaliy.tsyganok@gmail.com (V. Tsyganok)
ORCID: 0000-0002-8585-1044 (O. Puchkov); 0000-0002-9344-713X (I. Subach); 0000-0002-4959-612X (A. Zhylin); 0000-0002-0821-4877 (V. Tsyganok)

training grounds), shows that they can be divided into those that cover the process of preparation and conduct of cyber-training, provide definitions of basic definitions and those that describe the technical component of cyber polygons. For example, [3] presents an analysis of cyber fields implemented by government agencies, special services, and US universities, and suggests a model the University of Delaware cyber field is based on. [4] describes the process of deploying and maintaining the operation of the cyber landfill through the use of Docker containerization technology, describes in detail the topology of this environment, and provides configuration files for its configuration. The theoretical substantiation of the essence, content, and goals of cyber-training, as well as the purpose, composition, and structure of the cyber polygon, is considered in [5].

In [6] the process of preparation and conduct of cyber-training from the beginning to the submission of reports is considered. The work focuses on key aspects of exercise planning and implementation, including objectives, scenarios, reporting, and evaluation procedures, network architecture, tools, and experience gained by using the scenarios outlined during the training. The reference materials presented in the document enable the training planner to understand the purpose, goals, plans and processes in the organization and conduct of cyber -training.

[7] describes an exercise that investigates the impact of cyber-offensive operations on the ability of US defense systems to perform assigned tasks. The document describes the four steps of the cyber-training process – preparation, execution, analysis of actions during execution, and submission of reports.

[8] provides recommendations on the frequency and duration of cyber-training among cyber defense units of the security and defense sector, public authorities, critical infrastructure, etc.

However, the analysis showed that at present there are no fixed and accepted norms on the criteria for cyber-training classification as well as organizational and technical platforms on which they are conducted.

Therefore, the urgent scientific task is to develop criteria for the classification of cyber-training and scientifically based recommendations for the selection of organizational and technical platforms for their implementation.

The purpose of the article is to develop approaches to the classification of cyber-training and practical recommendations for the selection of organizational and technical platforms for their implementation during the training of specialists in cybersecurity and cyber defense.

2. Result of the research

In order to implement cyber-training in the educational process effectively, it is necessary to understand clearly the purpose, the scope, and the level of efforts and resources involved. Nowadays, there is no established generalized classification of cyber-training that would distinguish their levels, forms, types, and kinds. The analysis of the literature [2,9] allows to allocate the following criteria of cyber-training classification:

By level:

strategic level – the level at which cyber-attacks are considered, decisions are made and risks are assessed. Applied without the use of software and hardware. Usually, training is conducted for heads of various power structures or organizations;

technical level – the level at which practical skills are practiced. Training is conducted on a cyber-proving ground with the use of software and hardware. Engineers and information security specialists are trained;

operational level – a level in which, on the background of strategic level tasks, practical issues of technical level are also worked out. This approach is considered to be the most effective for cyber-training [9].

By form:

discussion – designed to familiarize participants with cybersecurity plans, policies, and procedures. In the discussion exercises, participants discuss a specific, predetermined dilemma;

practical – used to test plans, policies, and procedures, as well as employee training. Usually, a simulation is selected that correlates with the real environment.

By kind:

Desk Check – used to check cybersecurity plans, procedures, and any changes to them. Scenario-based plans and procedures are discussed gradually. This allows you to understand what steps are necessary and how they should be performed;

Walkthrough – a specific scenario, such as a cyber-attack, is discussed in detail. It is determined who does what and when, what actions are to be taken in a given situation. Specific steps to counter attacks, including detection, response, follow-up, and conclusions are considered;

Tabletop exercise – covers all aspects of attack management. All participants are previously given the same information about the attack and its impact on the system. During the exercises, players practice communication between themselves and society to disseminate information about the cyber-attack and respond to it. During Tabletop exercise, the attacked team can share relevant information, get an overview, make decisions, and work out communication activities;

Workshop – work on the scenario (step by step). Participants work out different actions and analyze the possible result. This allows you to practice the actions of teams and individual participants without time constraints, which helps to improve skills in crisis situations and scenarios;

Comms check – this type of exercise is used to check systems and infrastructure for proper operation according to specified requirements;

A distributed tabletop exercise is a role-playing game in which participants act according to their roles in the plans and procedures of the script. This exercise is similar to the Tabletop exercise but there is no discussion. Participants must act in real-time. The results are discussed later. The advantage of this exercise is that participants can practice procedures and actions in a normal environment;

Command Post Exercise – exercises are modeled without the possibility of using emergency services. Attacked teams address issues and situations in realistic and evolutionary scenarios. As a result, teams respond to the implementation of evolving scenarios in their own environment and on their own;

Simulation Exercise – in the simulation process, participants implement a realistic scenario in their own environment. Participants practice under normal circumstances, as far as possible, at the expense of their own resources in their own environment. The rest of the scenario is developed according to the results of their decisions and actions. Exercises are suitable if the purpose of training is to test and prepare participants in their own environment in conditions that are close to real. The intensity and development of the scenario depends on the number of participants and their level of experience. It is also important to decide whether only internal parties will be involved or whether external parties will also be involved. Training can last from several hours to several days;

Capture the Flag – "capture the flag". The purpose of training is to find a "flag" or other element and "capture" it by identifying and presenting it to the head of training. The exercise can be conducted in teams or individually, as well as with elements of competition or not;

Cyber Range (Red Team / Blue Team) – a type of exercise in which the red team attacks a network or other important object, and the blue team tries to weaken this attack and protect this object. This exercise raises awareness of the potential risks of cybersecurity; it provides insights into possible vulnerabilities and ways to address them, as well as strategies for detecting cyber-attacks and ways to respond to them. [2]

The classification of cyber-training according to the above criteria is shown in Table 1.

Table 1

Classification of cyber-training by level and form

Strategic level	Technical level	Operational level
Desk Check	Workshop	Command Post Exercise
Walkthroug	Comms check	Simulation Exercise
Tabletop exercise	Distributed tabletop exercise	Capture the Flag
		Cyber Range (Red Team/Blue Team)

By type:

- desktop;

- hybrid;
- close to reality.

The type of cyber-training determines the complexity of cyber-training, how long it will take and what resources are needed [9].

Table 2

Classification of cyber-training by type.

Type	Description	Complexity	Duration	Resources
Desktop	Exercises with tasks presented on paper.	Can be planed and executed quickly, depending on the number of organizations involved.	Planning: 1-2 months. Execution: 1-3 days.	Limited resources are involved, the number of which depends on the number of organizations
Hybrid	Conducted on the basis of scenarios (scanning, e-mail, spoofing, etc.).	Requires more time for planning and execution	Planning: 3-6 months. Execution: 3-5 days.	It takes time and people to organize training according to the script.
Close to reality	Include realistic scenarios with problems for more detailed training of specialists.	Requires detailed coordination and planning.	Planning: 6-12 months. Preparation: 2-3 months. Execution: 7-14 days	A large number of organizations and participants. Requires significant information resources and expenses for the implementation of the scenario.

Before the start of cyber-training, their planning is carried out: the type, shape, kind, and level at which it will be conducted are determined. This stage usually takes from one to two months. First, the problem that needs to be solved is identified – the problem of communication between members of the governing body or other levels of management, inefficient procedures and processes, the implementation of which leads to additional expenses and losses, lack of knowledge in management, and so on. After identifying the problem, the management of cyber-training develops a scenario for its implementation and determines its subject. Currently, the following topics are usually used:

- leakage of important information;
- infraction of contractual obligations;
- initiation by competitors of inspection of the regulator;
- blackmail by fraudsters / hackers;
- publication of information about the incident in the media;
- mass infection with the encryptor, etc.

At the stage of cyber-training and assessment of acquired knowledge and skills, the data obtained at the preparatory stage are taken into account:

- purpose and planned results;
- assessment of the necessity to involve outsiders and, if such necessity exists, arrangements with them;
- list of required resources;
- the final scenario, which should remain secret, but participants should understand the training conditions, rules, and their roles;
- final and approved rules for conducting cyber-training;
- list of participants indicating their roles;
- final materials for training;

- action plan, dates, deadlines, responsibilities, etc. [10].

Thus, the analysis allows us to formulate a generalized scheme for the classification of cyber-training (Table 3):

Table 3

Generalized scheme of cyber-training classification

Level	Kind	Type
Strategic	Desk Check Walkthroug Tabletop exercise	Desktop
Technical	Workshop Comms check Distributed tabletop exercise	Hybrid Close to reality
Operational	Command Post Exercise Simulation Exercise Capture the Flag Cyber Range (Red Team/Blue Team)	Hybrid Close to reality

Practical experience in training specialists with a bachelor's and master's degree in 125 Cybersecurity shows that the most interesting of these classifications are such kinds of training as Capture the Flag and Cyber Range (Red Team / Blue Team).

Cyber Range training (Red Team / Blue Team), their concept and tactics were suggested by the NATO Cooperative Cyber Defense Center of Excellence (CCD COE) [11].

Training scenarios are different each year, but the structure and infrastructure for practical exercises are relatively the same. A typical organizational structure of the exercises is shown in Fig. 1. It includes five teams: White, Green, Yellow, Red and Blue teams.

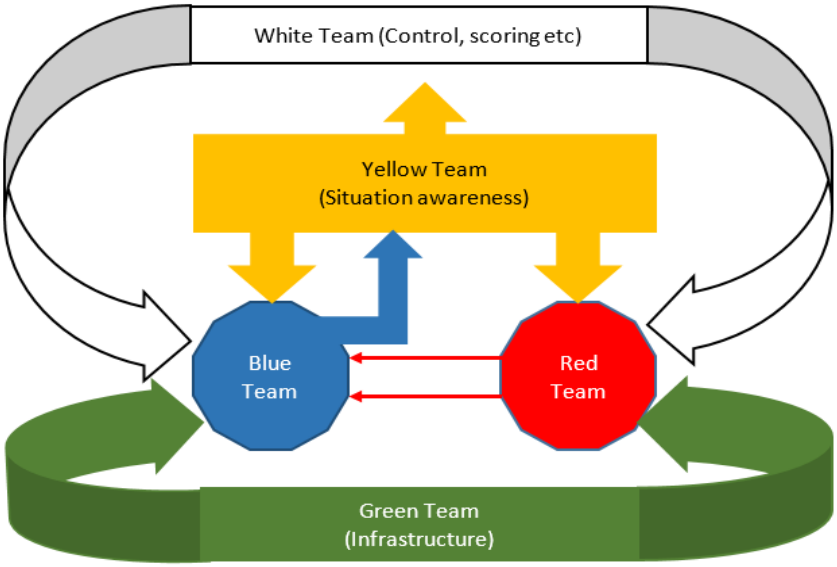

Figure 1: Organizational structure of Cyber Range training (Red Team / Blue Team)

All teams are in one information and telecommunications network (ITM) but they can be geographically separated. Each team member has different skills, roles, and responsibilities. The team usually consists of 6-10 specialists in the field of information technology and cybersecurity.

The purpose of the blue team is to protect its virtual network and maintain the normal mode of its operation. The Blue Team must report to the White Team on the detection and disposal of cyber-attacks. The task of the Red Team is to carry out cyber-attacks on the information infrastructure of the Blue Team in order to compromise it. The red team may have other subordinate teams whose actions

are aimed at overcoming certain defense systems. The white team monitors the progress of training. It sets the rules for both the Red and the Blue teams. The White team performs the functions of the control cell in the process of performing practical exercises. It announces the stages and manages the score of the Blue and the Red teams. The main goal of the Yellow Team is to ensure situational awareness of the White Team, as well as of other teams. Situational awareness is formed from the submitted reports of the Blue Team. The Green team creates an information infrastructure for cyber-training by using the typical components of the platform chosen for it. In addition, the activities of this team are aimed at maintaining the functioning of the information infrastructure of cyber-training. The Green team consists of network administrators and software developers.

Since Cyber Range-type cyber-training is focused on practical exercises and operation of hardware and software complexes. Their effectiveness depends on such parameters as the number of places for students; the complexity of the infrastructure, scenarios, and environment that was modeled; tools used (to model the operation of system services and generate network traffic); categories of people involved; completeness of automation, implementation, and virtualization of the network (The Virtual Clone Network (VCN)); virtual private networks (VPN); use of public cloud infrastructure and intellectual property rights on the platform on which Cyber Range training is conducted, etc.

Hardware and software systems for Cyber Range training (hereinafter – Cyber Range Platforms) are also aimed at:

- development and use of own training programs;
- testing students and providing an environment for research in the field of cybersecurity;
- support and integration of several groups of students in one environment;
- gamification and additional implementation of exercises such as Capture The Flag (CTF);

The analysis shows that the current Cyber Range Platforms are heterogeneous and can be used to perform various practical tasks (scenarios) – from testing the response to errors in the work of web services to learning the latest methods of cyber intelligence:

- scanning of hosts, ports, and operating systems;
- scanning hosts for vulnerabilities;
- scanning for vulnerabilities in web resources;
- use of frameworks;
- response to incidents;
- network forensics;
- digital data forensics;
- conducting penetration tests (pentests);
- Open Source Intelligence;
- reverse engineering
- conducting social engineering;
- training in response in teams of specialists of the Security Operations Center (SOC);
- analysis of log files, etc.

Since Cyber Range Platforms are complex hardware and software systems that simulate the environment of the corporate network, its means of protection and attack, malicious and normal traffic, the main components of these platforms should be routers (statistical and dynamic); switches; wireless access points; DNS servers; firewalls (Host Based Firewalls, Network Based Firewalls, Packet filtering firewall, Stateful Inspection firewall, Proxy firewall, Next Generation firewall); intrusion detection systems (Host Intrusion Detection System, Network Intrusion Detection System); Deep Packet Inspection (DPI), Load Balancers; Email; spam filters, virtual private networks, DHCP servers; SCADA components; elements of physical security and alarm (doors, alarms, fire alarm and fire extinguishing systems, access control systems); web servers, databases (relational, distributed, non-relational); control systems (SIEM, Nagios, Zabbix); personal computers; cloud environment; other hosts (with anti-virus protection systems); security analysis tools, etc.

The modern market of Cyber Range platforms is developing very actively and is represented by the following solutions (Table 4). Their description is given on the corresponding sites, which are

specified to each platform. The purpose and architecture, in general, correspond to the above information.

Table 4

Cyber Range platforms

Name of the platform	Type of use	Owner	Country
BreakingPoint [12]	Commercial	Ixia	USA
CdeX [13]	Commercial	Vector Synergy	Poland
Cisco Cyber Range [14]	Commercial	Cisco	USA
Cyberbit Range [15]	Commercial	Cyberbit	Israel
RGSE [16]	Commercial	JYVSECTEC	Finland
NCRC [17]	Military	DAPRA	USA
OCCP [18]	Academic	University of Rhode Island	Iceland

However, despite the significant benefits of Cyber Range training, CTF training has gained widespread popularity in the cybersecurity professionals training, mainly due to its ease of implementation compared to discussed above and support during its carrying out. Its popularity is based on the popularity of the Quake and Team Fortress computer game competitions, which became its prototype, but at some point transformed into cybersecurity. Although CTF cybersecurity competitions are built on the rules of the classic Capture the Flag, they have changed greatly over the years. Experience and experiments with such competitions have led to the creation of varieties of CTF. The main ones are Attack-Defense, Jeopardy, Mixed. and others.

Attack-Defense. This type of CTF is considered a classic because it uses the rules of Capture the Flag in its purest form. The organizers give the teams virtual images (or maybe a laptop, server, or remote access to something) of operating systems with multiple services in which there are certain vulnerabilities. Teams usually have administrator rights on the virtual machine, although there are some cases where access is restricted. Images need to be exactly the same, and, accordingly, the same for vulnerabilities in services. The main idea of CTF is to look for vulnerabilities in your system and attack others. In most cases, a virtual image is a Linux distribution.

Testing machines (bots) help to check the performance of tasks. They mimic the actions of a legitimate user who uses the service as intended. Each round bot, in some special way for each service, sends it some confidential information. This information is the flag. In the next round, the bot comes and checks whether the previous flag is available and whether it is correct, and then puts a new one. The organizers thus learn that the service works correctly. The duration and number of rounds are described in the rules and may vary from game to game.

A successful attack is detection of vulnerabilities that could allow, for example, to read other people's messages on the mail server. If the team finds such a vulnerability, it will be able to read the bot's message and thus capture the flag. Sometimes the bot cannot pick up the flag from the previous round. For example, a virtual machine does not respond, or a team makes incorrect service fixes, or another team uses a vulnerability to remove or change this flag. Then the organizers believe that the service is not available to the protection team. As long as the service works correctly, the protection team receives points for protection. If not, the team does not receive anything in the rounds of its unavailability.

In addition to points for defense, there is a second type of points – for the attack. They are charged for the delivery of flags stored in the services of other teams. The formulas for calculating these points vary greatly from competition to competition. The formula, for example, may or may not include the number of teams that captured the flag. The place in the ranking of the team in which the flag was captured is often taken into account.

The competition regulations always state very clearly what the flags should look like. It is necessary for participants to understand well what they need to protect and capture. Most flags look something like this: 322d4e510659dc1e3a9d5b6d6df6c3e0

Jeopardy. This is the most popular type of CTF training because it is easier to implement than others. Instead of "breaking" each other, teams perform certain tasks. A flag is awarded for solving

the tasks and upon passing it, the team receives points. Usually, in such CTF training, there are several branches of tasks – each of its own discipline. The mechanisms of training jeopardy CTF are different. For example, more complex tasks may open up as simpler ones are solved. Alternatively, it happens that the team that solved the problem first gets extra points. However, in general, the idea remains the same – whoever solved more tasks, he scored more points and he eventually wins.

Mixed. There are CTF exercises that combine the features of attack-defense and jeopardy: teams need not only to defend their services and attack others but also to solve problems. In this case, the rules can be any and are limited only by the imagination of the organizers.

In addition, for the preparation and conduct of CTF-type training, it is necessary to know what type of task can be implemented. There is a classification of tasks by disciplines such as reverse, exploit, web, crypto, stegano, forensic, PPC, misc [19].

Reverse – usually comes down to parsing a particular compiled program. To solve the problem you need to understand the logic of its work, get some data from the body of the program, and so on.

Exploit – exploitation of various vulnerabilities. Most often, you need to find a vulnerability in binaries for Linux. Typically, this vulnerability is from series of buffer overflows, format string vulnerabilities. Security features, such as ASLR, DEP, or Canary, are often included and should be bypassed.

Web – a task for web security. It can be anything from SQL and XSS injections to finding vulnerabilities in the logic of a web server or web application.

Crypto – a task to analyze the vulnerabilities of various cryptographic algorithms and protocols, as well as services built on them.

Stegano (steganography) – in this discipline, participants try to extract hidden information from a specific stegano container (multimedia file, document, text, etc.). Very often tasks intersect with cryptographic ones.

Forensic – the task of investigating incidents and analyzing images and files. There may be tasks related to recovering deleted files and hidden partitions. Malware analysis or traffic dumping may also be possible.

PPC – Professional Programming and Coding. This is a task on the topic of sports programming but in a more applied form. There can be absolutely anything, from writing a parser or code to attack like a full search and ending with target bots.

Misc. This discipline includes any tasks that do not belong to other groups. This can be both competitive intelligence and certain entertainment tasks (for example, "a photo of the oldest IT book you can find"). That is all that the organizers have enough imagination.

Depending on the complexity of the tasks, they receive a different number of points. Very often one task may require different specialized knowledge at the same time.

For the organization and conduct of training such as CTF, as well as Cyber Range, it is possible to use special hardware and software platforms that help in this. Thus, table 5 shows the analysis of the most common CTF platforms.

Deploying Cyber Range or CTF platforms requires the purchase, configuration, and operation of hardware and software that is expensive and needs to be supported by qualified personnel. If there is a need to conduct cyber-training without purchasing and configuring the hardware and software part of the cyber range, it is possible to use online platforms for cyber-training, but their effectiveness is much lower than Cyber Range and CFT platforms. Since there are so many online platforms and they all have different scenarios and tasks, it is very difficult to compare them. But still, you can separate the most popular of them. (Table 6).

Mutillidae. Free platform for web application security testing. One of the most famous online platforms. [20] Test lab v.7. Free pentest laboratory, developed on the basis of the corporate network of a real company [21]. Hack This Site. A free, secure, and legitimate testing ground for hackers to test and expand their hacking skills. Contains many different projects, a huge forum, irc-channel. Missions are divided into types: simple, realistic, attacks on applications, forensics [22].

Hack Me. Free project created and managed by eLearnSecurity. It is possible to develop and add tasks. Tasks are broken down by specific vulnerabilities. The platform is intended mainly for beginners [23]. Hacking Lab. An online platform for learning network security and improving ethical hacking skills. Contains tasks close to CTF: forensics, cryptography, and others. It is necessary to download the image of the virtual machine and use it to connect via VPN to the laboratory [24].

Table 5
Characteristics of CTF platforms

Name of CTF platform	Type CTF	Number of participants	Type of task
DEF CON CTF	Mixed	Up to 8 participants	Reverse, exploit, web, crypto, stegano, forensic, PPC
UCSB Ictf	Attack-defence	Unlimited	Exploit, web, crypto, stegano
Mozilla CTF	Jeopardy	Unlimited	Exploit, web, crypto, stegano, forensic
PHD CTF	Mixed	Up to 7 participants	Reverse, exploit, web, crypto, stegano, forensic, PPC
RuCTFe	Attack-defence	Unlimited	Exploit, web, crypto, stegano.
Hack.lu CTF	Mixed	Up to 6 participants	Crypto, reverse, forensics, web
SECUINSIDE CTF	Jeopardy	Unlimited	Exploit, web, crypto, stegano, forensic.
rwth CTF	Attack-defence	Unlimited	Reverse, exploit, web, crypto, stegano, forensic, PPC
CSAW CTF	Mixed	Unlimited	Exploit, web, crypto, stegano, forensic
PICO CTF	Jeopardy	Up to 8 participants	Exploit, web, crypto, stegano, forensic
FBCTF	Mixed	Unlimited	Reverse, exploit, web, crypto, stegano, forensic, PPC, misc

Table 6
Online cyber learning platforms

Name	Country	Price	Type of task
Mutillidae	USA	Free	Web
Test lab v.7	Russia	Free	Exploit
Hack This Site	USA	Partly free	Web
Hack Me	USA	Free	Web
Hacking Lab	Sweden	Partly free	Revers, Forensic, Crypto
Enigma Group	USA	Partly free	Web
Damn Vulnerable Web Application	USA	Free	Web

Enigma Group. The service is designed for those who want to understand how secure code is arranged and how hackers can attack systems. Contains vulnerabilities of web applications of different levels, cryptographic, logical tasks [25], etc. Damn Vulnerable Web Application. A vulnerable web application that can help cybersecurity professionals test their skills in a legal environment and web developers can better understand the processes of protecting their applications, which are written in PHP using MySQL [26]. Also of some interest is the approach to the gamification of cyber-training, where gamification is usually understood as the use of game techniques in non-gaming situations, including cyber defense. In general, the gamification of cyber-training can be divided into board games and computer games. The approach to conducting gamified desktop cyber exercises is to obtain certain situational tasks that are described in the cards or on the playing field. Thus, the Finnish company NIXU has released two sets of useful gaming cards – Nixu CyberBogies [27] and Nixu hACME social engineering playing cards [28]. The first set is used for group training to identify and analyze potential sources of information and cybersecurity threats. The second set is designed to demonstrate the capabilities of cyber attacks using social engineering. The rules are described in the instructions for the game, and the tasks themselves – on the cards that are distributed to participants.

Michelin's CERT has developed its own version of the card game (in English and French), the rules of which can be found in [29]. Forty-two cards are divided into 2 categories – defenders (green) and attackers (red). In each of the categories, there are actors, i.e. human characters (government hackers, analysts, and architects of information security, project managers, cybercriminals, etc.), and tools (attack detection systems, Wi-Fi protection systems, zero-day vulnerabilities, failure attacks, flash drive in the parking lot, etc.). Each character has three characteristics – the level of knowledge, the level of efficiency, and the level of detection. Tools can modify the characteristics of the characters in the direction of their strengthening or weakening.

The Japanese Network Security Association has introduced the SECWEREWOLF card game [30], which introduces participants to the role and activities of the incident response team. The game divides players into two teams, defenders and offenders, depending on which cards they received at the beginning of the game. During the game, defenders try to count cybersecurity offenders who commit cybercrimes and attempts to shift the blame for attack on someone else.

The presented board games are intended to acquaint participants with the field of cybersecurity and the actions of violators and security teams in general. The game d0x3d is closer to real tactics, techniques and procedures of both defense and attack! [31]. The game offers cards that describe the type of intruder and attacks, various objects to attack (switches, firewalls, databases, servers, etc.) and various attacks (financial information, intellectual property, etc.). There is also a list of actions that are possible to repel the attack.

The game Backdoors & Breaches is designed to conduct staff cyber exercises, the theme of which is to respond to incidents and study the tactics, techniques and procedures of attackers [32].

There are six different types of cards in this game. The first set of cards is called INITIAL COMPROMISE. These cards are red and show how an attacker will first gain access to your network. The second set of cards is called C2 and EXFIL. These cards are brown and show how an attacker would maintain access to a system that he has compromised. The third set of cards is called PERSISTENCE. These cards are purple and show how an attacker would maintain access to a compromised system. The fourth set of cards is called PIVOT and ESCALATE. These cards are yellow and show how an attacker will navigate the network and expand their privileges. The fifth set of cards is called PROCEDURES. These cards are blue and represent various procedures for responding to cases that the organization can use to detect and neutralize the attack. The sixth set of cards is called INJECTS. These cards are white and are drawn at different times of the game to add a random effect to the game. Recently, computer games have been introduced to improve cybersecurity knowledge and skills. Thus, Circadence's Project Ares game [33] allows teams from businesses, institutions and universities to improve cybersecurity skills by modeling the company's network and the cyber incidents that occur in it. The game provides a variety of scenarios and tasks for different numbers of participants, has its own system of rating and scoring, which allows competitions between participants. The Steam gaming platform offers ThreatGEN: Red vs Blue, [34] which is a turn-based strategy game designed to teach real-world cybersecurity concepts, as well as methods, strategies, and skills for both attack and computer security.

3. Conclusions and prospects for further research

The results of the study allowed us to summarize the various approaches to the organization and conduct of cyber-training and to formulate criteria for their classification: levels of cyber-training, as well as the types and kinds that correspond to them. Due to the most practical orientation and conditions of cyber-training, special attention was paid to such types of exercises as Capture the Flag and Cyber Range (Red Team / Blue Team), and detailed explanations were given about their organization and scheme. In addition, attention is paid to existing platforms and online resources that allow you to organize independently these types of training, or use prepared online platforms. The gamification of cyber-training is singled out as a separate approach, where under gamification the application of game techniques in non-game situations, in particular in the field of cyber defense, is suggested. There are examples of both board and computer games that provide opportunities to improve cybersecurity skills. A further promising area of research, the authors consider the development of techniques, methods, and scenarios for cyber-training at all levels, as well as the

development of scientifically sound requirements for the selection and construction of a platform for cyber-training Capture the Flag and Cyber Range (Red Team / Blue Team).

4. References

[1] Cisco Annual Information Security Report 2018 URL: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf
[2] Kick J. Cyber Exercise Playbook / Jason Kick. – Wiesbaden, Germany, 2014.
[3] Ishaani Priyadarshini. Features and architecture of the modern cyber range: a qualitative analysis and survey. Spring 2018 URL: https://www.researchgate.net/publication/327835952_Features_and_Architecture_of_The_Modern_Cyber_Range_A_Qualitative_Analysis_and_Survey
[4] Bryan Scarbrough. Container-Based Networks: Lowering the TCO of the Modern Cyber Range . SANS Institute 2019 URL: https://www.sans.org/reading-room/whitepapers/testing/paper/39120
[5] Danik Yu.G. Fundamentals of cybersecurity and cyber defense: a textbook / Yu.G. Danik, P.P. Vorobienko, V.M. Chernega. – O.: O.S.Popov ONAT, 2018.
[6] Jason Kick. Cyber Exercise Playbook. The MITRE Corporation. 2014. URL: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf
[7] Department of Defense Cyber Table Top Guidebook. n 2 July 2018, CASE # 18-S-1835. URL: https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/The%20DoD%20Cyber%20Table%20Top%20Guidebook%20v1.pdf
[8] Petrenko CA, Petrenko AA Cyber teachings: methodical recommendations of ENISA. Questions of cybersecurity: scientific and practical journal – M.: №3 (11) – 2015
[9] On National and International Cyber Security Exercises – Heraklion, Greece: ENISA, 2012.
[10] Lukatsky A. Cyber teachings for company management URL: https://journal.ib-bank.ru/post/748.
[11] Locked Shields CCDCOE URL: https://ccdcoe.org/exercises/locked-shields/
[12] Cyber Range URL:https://www.ixiacom.com/solutions/cyber-range.
[13] CDeX URL: https://www.vectorsynergy.com/vector-synergy-cdex-cyber-defence-exercise-platform.
[14] Cisco Cyber Range URL: https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf.
[15] Cyberbit Range URL: https://ru.cyberbit.com/solutions/cyberbit-range/
[16] JYVSECTEC URL:https://jyvsectec.fi/cyber-range/
[17] Burnett R. National Cyber Range / Richard Burnett. – Orlando Sentinel, 2016
[18] OPEN CYBER CHALLENGE PLATFORM URL:https://opencyberchallenge.net/
[19] A. Litvinenko CTF: Capture The Flag. How hacking became a sport URL:https://xakep.ru/2016/06/14/ctf/
[20] Mutillidae URL: http://www.irongeek.com/i.php?page=mutillidae/mutillidae-deliberately-vulnerable-php-owasp-top-10
[21] Penetration test lab "TEST LAB" URL: https://lab.pentestit.ru/
[22] HackThisSite URL: https://www.hackthissite.org
[23] Hack.me URL: https://hack.me/
[24] Hacking-lab URL: https://www.hacking-lab.com/
[25] Enigma Group URL: http://www.enigmagroup.org/
[26] Damn Vulnerable Web Application (DVWA) URL: http://www.dvwa.co.uk
[27] Nixu CyberBogies URL: https://www.nixu.com/blog/gamify-your-threat-modeling-nixu-cyber-bogies
[28] Nixu hACME social engineering playing cards URL: https://www.nixu.com/blog/free-social-engineering-playing-cards
[29] Michelin CERT Github Resource URL: https://github.com/certmichelin/CERT-The-Card-Game
[30] Japan Network Security Association URL: https://www.jnsa.org/en/activities/game/index.html
[31] Game d0x3d! URL: https://github.com/TableTopSecurity/d0x3d-the-game
[32] Game Backdoors & Breaches URL: https://github.com/TableTopSecurity/d0x3d-the-game
[33] Game Project Ares компанії Circadence URL: https://www.circadence.com/products/project-ares
[34] Game ThreatGEN from Steam URL: https://store.steampowered.com/app/994670/ThreatGEN_Red_vs_Blue