https://doi.org/10.15407/scine21.03.086

KUPERSTEIN, L. M. (https://orcid.org/0000-0001-6737-7134),
LUKICHOV, V. V. (https://orcid.org/0000-0002-3423-5436),
RADETSKA, A. O. (https://orcid.org/0009-0009-5687-5651),
and DUDATYEV, A. V. (https://orcid.org/0000-0002-7944-2404)

Vinnytsia National Technical University,
95, Khmelnytske shose, Vinnytsia, 21021, Ukraine,
+380 432 56 0848, vntu@vntu.edu.ua

SYSTEM FOR ORGANIZING CYBER OPERATIONS IN THE CONTEXT OF MILITARY AGGRESSION

Introduction. *In the modern world, the importance of information and communication technologies, as well as the threats associated with cyberattacks during military aggression, has significantly increased. The widespread adoption of these technologies is accompanied by a high level of risk from cyber threats targeting various objects and management systems.*

Problem Statement. *Cyber operations have become a substantial technique for conducting warfare in the context of military conflict. Access to sensitive military, economic, or strategic data can support their execution and implementation. The leakage of this information can cause significant damage to the enemy, both militarily and politically, undermining their authority and potentially disrupting or even destroying specific military and political plans. Attacks on communication and management systems, or their complete disabling, can lead to collapse and devastation in the enemy's ranks, ultimately resulting in their defeat. Therefore, it is crucial to conduct research and improve methods for cyber operations, as well as to ensure effective defense against such threats.*

Purpose. *The primary aim of this research is to enhance the organization of cyber operations in military contexts by utilizing essential principles of management and offering recommendations for their optimization.*

Materials and Methods. *This research is based on an analysis of theoretical sources on cyber operations, as well as practical examples of previous cyber incidents in military settings.*

Results. *A framework for cyber operations has been developed. The main stages of cyber operations within the management domain have been explored. A typical management system structure has been proposed. Key recommendations for improving the management and functionality of cyber operation systems have been provided.*

Conclusions. *This study highlights the significance of developing and implementing effective management strategies. The improvement of these processes is vital to ensuring reliable security and a robust response to cyber threats during military conflict.*

Keywords: cyber operation, cyber weapons, cyber attack, cyber war, military aggression, management functions.

Citation: Kuperstein, L. M., Lukichov, V. V., Radetska, A. O., and Dudatyev, A. V. (2025). System for Organizing Cyber Operations in the Context of Military Aggression. *Sci. innov.*, 21(3), 86—98. https://doi.org/10.15407/scine21.03.086

In the modern world, there is a constant tendency to increase and spread the use of information and communication technologies and systems in all aspects of the life of a modern person, society, and the state. Along with the spread of information technologies, the risks also increase and the amount of cyberattacks on various objects and management systems is growing significantly. That is why the modern information network mentions that security violations of networks and systems are getting more frequent [1]. Even at the national level, there are messages from officials and employees of many countries regarding cyberattacks and cyberweapons being used to achieve political and strategic goals [2].

The issue of using cyberattacks as a type of warfare against the opponent during militaristic or political conflicts is particularly acute. After all, in times of military aggression, cyberattacks and cyberweapons are effective methods of warfare against the enemy's control and communication systems or resources.

By implementing cyber-attacks on enemy resources, it is possible to gain access to secret military, economic, or strategic data, the leak of which may cause significant damage to the adversary both in the military and in the political arena and undermine its authority or destroy certain military or political plans. Impact on the communication and control systems of critical infrastructure objects and/or disabling them can cause collapse and destruction in the ranks of the enemy and lead to his defeat. At the same time, damage to the information and communication systems of the enemy with the help of cyberspace can cause even more damage than classical weapons systems. Therefore, at present, work on research and development of a system for organizing and conducting cyberattacks that take place in the conditions of military aggression is extremely relevant.

Following the current state of technological development, new means of warfare appear, among which those used in cyberspace can be singled out. Having analyzed the known cases of cyberattacks during the entire period of the Russian Federation's military invasion of Ukraine, it was found that the denial-of-service attacks (DDoS-attacks) was the lion's share of the total number of attacks. In 2022, CERT-UA processed more than 2194 powerful cyberattacks, and in the first quarter of 2023 — 700. Moreover, 88.8% of all incidents are DDoS attacks [3]. Attacks are aimed both at important objects of state and social infrastructure and at private or commercial services, the failure of which can deliver a heavy blow to the enemy side.

During the Russian-Ukrainian war, many groups that carried out cyberattacks on enemy resources and facilities appeared. It has become one of the strongest cyber volunteer movements to counter the aggressor since official cyber troops are currently not formed within the Armed Forces, but only separate units within various power structures [4—6]. At the same time, the organization, structure, and management system of cyber volunteers have many shortcomings that significantly reduce the effectiveness of cyber-attacks. Among the problems are varying levels of IT knowledge and skills, as well as an absence of centralized management and control. Usually, the number of participants in these groups decreases over time as well as their motivation to carry out attacks. It happens due to the poorly developed communication between participants and organizers and improperly formed processes of conducting cyber operations. Such groups usually don't have well-defined goals and guidelines, and the tools used are too complex for the average user without proper skills. Such users make up a large part of the participants in attacks. That is why it is expedient to develop a system of organizing cyberattacks in case of military aggression to increase the efficiency of their functioning and development.

According to the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine," the term "cyberattack" can be considered targeted (intentional) actions in cyberspace, which are carried out with the help of electronic communications (including information and communication technologies, software, software and hardware, other technical and technological means and

equipment) and aimed at achieving one or a combination of the following goals: violation of confidentiality, integrity, availability of electronic information resources processed (transmitted, stored) in communication and/or technological systems, obtaining unauthorized access to such resources; violation of security, stable, reliable and regular mode of operation of communication and/or technological systems; the use of the communication system, its resources, and means of electronic communications to carry out cyberattacks on other objects of cyber protection [7].

The concept of a kill chain (Kill Chain) can determine the stages of attacks on a cybersecurity object. The term "Cyber Kill-Chain" was originally introduced by Lockheed Martin Corporation as part of their Intelligence Driven Defense [8] model to identify and prevent cyber intrusion processes. A cyberattack kill chain is a series of steps that trace the stages of a cyberattack from the early stages of recon to data extraction [9]. It consists of 7 stages: reconnaissance, arming, delivery, implementation, establishment, management and control, and execution of actions. This list of stages of cyberattacks is general. The sequence of stages of cyberattack implementation and their number may vary depending on the type and kind of attack that is planned to be carried out.

The concepts of "cyber weapon" and "cyberattack" are interrelated. After all, cyberweapons are an important tool and means of conducting cyber operations for one of the parties of the conflict. It is thanks to the use of cyber weapons that their implementation becomes possible. At the same time, cyber weapons should be considered not only as a tool of attack but also of defense.

Heimdal Security, a company that ensures and provides cyber defense services, gives the following definition: the term "cyber weapon" means an advanced and complex piece of code that can be used for military or intelligence purposes. The company claims that the term recently emerged from the military industry to refer to malware that can be used to gain access to an adversary's computer networks [10].

P. Paganini defines cyberweapons as some software code intended to be used to implement a certain threat or cause physical, functional, or mental damage to structures, systems, or living beings [11].

S. Mele gives the following definition of a cyberweapon: a device or any set of computer instructions aimed at illegally damaging a system that functions as a critical infrastructure, its information, data, or programs contained in it, or corresponding to them, or even intended to facilitate the interruption (full or partial) or change in the operation of such a system [12].

Therefore, after analyzing the above definitions, it can be concluded that the term "cyberweapons" can be considered certain software and/or hardware, created and/or used to cause certain damage to the adversary and/or obtain a certain military advantage, for example, such as establishing control over information resources (television, radio, Internet, etc.), unmanned aerial vehicles, disabling enemy equipment, destroying or replacing important information, identifying enemy targets, organizing traps, spreading disinformation, etc. [13, 14].

In the modern history of the development of information and communication systems, many attempts to use cyber weapons have been recorded [15]. After research and analysis of known cases and precedents of the use of cyber weapons during military operations, the main directions and types of cyberattacks using cyber weapons were determined. The consequences of using cyber weapons can be very diverse and lead to severe destructive results.

Vandalism — vandalizing Internet pages, replacing their content with offensive or propaganda images. The result is a blow to the authority of the state both in the world and among the population. A vivid example can be considered the attack on several state websites of Ukraine in January 2022, when an attempt to open them did not display the content of the website, but a picture with a warning in Ukrainian, Russian, and Polish about the punishment of Ukrainians for the actions of the OUN of the UPA [16].

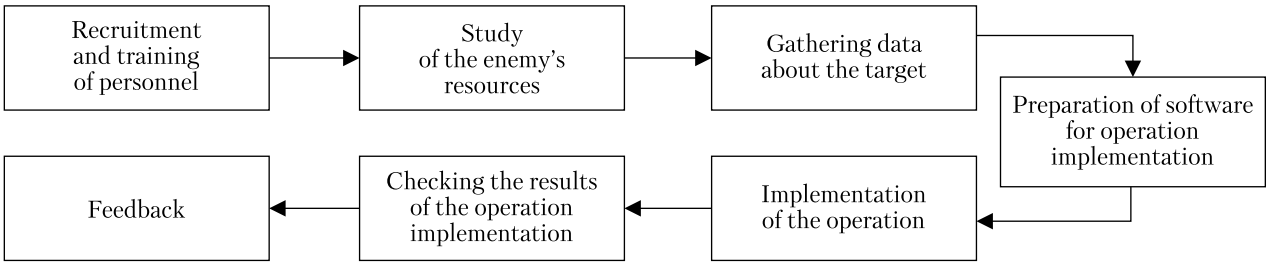

Fig. 1. The structure of cyber operations organization technology

Propaganda — sending propaganda messages or inserting propaganda into the content of other pages, spreading fake news. The consequence is the promotion of a favorable point of view on certain events on the part of the enemy, as well as the disorientation of the population. An example is the creation of clones of Ukrainian news sites to promote fake news in June-September 2023 [17].

Collecting information — hacking private pages or servers to obtain information or replace it with a fake one. The consequence is gaining access to important information, the disclosure of which can cause significant damage to the enemy. An example is the hacking of the databases of the "Russia-Africa 2023" economic summit in June 2023 and the Roskomnadzor database in March 2022 [18, 19].

Denial of service — attacks on various sites, services, and systems, the main purpose of which is to disrupt or prevent their correct operation. A clear example is organized massive DDoS attacks on the enemy's state, media, and financial services [19].

Attacks on critical infrastructure facilities — attacks on systems that support the vital activity of cities, and their infrastructure, such as telephone and banking systems, water supply, electricity, fire protection, transport, etc. The consequences are disruption of the functioning of important systems, organizations, and structures, which can lead to collapse and mass panic among the population. An example is regular attacks on Ukrainian banking services, mobile operators, and providers by the enemy from the very beginning of full-scale military operations [19].

The purpose of this article is to improve the process of organizing cyberattacks in conditions of military aggression by mapping management functions to the stages of cyberattacks and developing general recommendations for their implementation.

The technology of organizing cyber operations can be presented in the form of several successive interrelated stages. The success of the stage depends to a greater extent on the quality of the organization and the performance of work in the previous one. At the same time, the success of all components is important because it directly affects the efficiency of the organization of the system as a whole.

The technology includes the following stages:

- recruitment and training of personnel;
- study of the enemy's resources;
- gathering data about the target;
- preparation of software for attack implementation;
- implementation of the attack;
- checking the results of the attack implementation;
- feedback.

The technology for organizing cyberattacks is shown in Fig. 1.

Management is an extremely important aspect in the system of organizing cyberattacks for a volunteer cyber army. This can be justified for several reasons:

- Coordination of actions and resources. Management allows determining what tasks and goals should be achieved within the framework of cyberattacks. It also helps allocate resources, including human capital, hardware, and software, to achieve these goals.

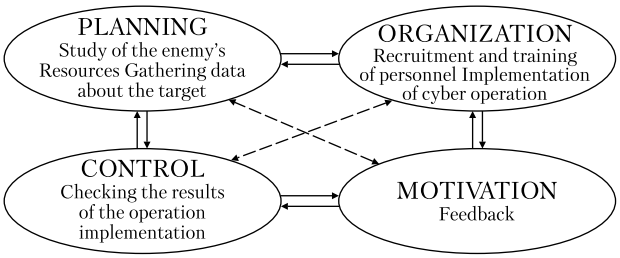

Fig. 2. Coordination of the main stages of cyber operations and management functions

- Planning and strategy. Effective management includes the development of strategies and plans to achieve the goal. In the context of cyberattacks, this means developing attack plans, selecting targets and methods of attack, and setting priorities and timelines for execution.
- Resources usage optimization. Volunteer cyber forces are often limited by financial resources. Management helps make efficient use of limited resources, ensuring maximum impact and results within constraints.
- Ensuring security and privacy. Management also plays a key role in ensuring the security and privacy of cyberattack operations. This includes protecting information and coordinating efforts to detect and deflect potential countermeasures from the targeted party.
- Monitoring and analysis of results. Management includes systems for monitoring and analyzing the results of a cyberattack. This allows evaluating the effectiveness of attacks and making timely adjustments to the strategy.
- Development and improvement of skills. Management helps the organization improve the qualifications and skills of its volunteers. This may include training, coaching, and curriculum development.
- Increasing influence. Effective management helps an organization achieve greater impact on goals and achieve its strategic goals.

So, in our opinion, management is a key element of organizing a cyberarmy, as it helps to achieve coordination and efficiency in conducting cyberattacks. Without appropriate management, it can be difficult to achieve the desired results and ensure the safety of operations.

At each of the stages (Fig. 2), several actions are performed that meet the requirements for the main functions of management [20]. The result of mapping management functions to the stages of organization and conduct of cyber operations is presented in Fig. 2.

Alignment of the main stages of cyber operations and management functions [21] will improve the understanding of processes and, as a result, increase their effectiveness.

Let's consider each of the stages in detail and describe the main processes.

Stage 1. Selection and training of personnel. At this stage, there is a search and formation of a team of people who will participate in the preparation and implementation of cyber operations. The necessary number of people is determined and the skills and abilities most developed in each of those involved in the work are determined. Based on the received data, people are divided into certain functional groups, and an idea is formed about whether it is necessary to carry out certain exercises and training to increase the level of knowledge of group members.

Stage 2. Study of the enemy's resources. During the investigation of the enemy's resources, the search and collection of information about potential objects and systems of the enemy, attacks on which cause him significant losses in economic, reputational, technical, or organizational aspects, takes place. Analysis and research of objects of military infrastructure, financial sphere, and state institutions are carried out. Based on the received information, a database of the enemy's critical resources is formed, in which all possible targets for attacks are collected.

Stage 3. Gathering data about the target. During target data collection, reconnaissance and data collection is performed on each attack target. At this stage, an in-depth search and collection of information from open sources about the structure and functioning of the object is performed. Its web resources and network infrastructure are scanned,

and IP addresses, domain names, and subdomains are determined. A check is made for the presence of open ports, running services, and scanning for vulnerabilities. Based on the received information, the attack vector is formed, and the collected information about the object is stored in the database.

Stage 4. Software preparation. During the preparation of the software for the implementation of the attack, the tools that will be used to carry out the attack are selected or developed. Software tools are selected based on information obtained during data collection about the target. It is based on this information that certain requirements are put forward for the software and its configuration, and the necessary amount of resources for an effective attack is determined.

Stage 5. Implementation of the attack. At the stage of implementation of the attack, a cyberattack is carried out on a certain object or several objects that were selected as a target at the stage of researching the enemy's resources. The implementation of a cyberattack is carried out with the help of software tools that were selected at the previous stage.

Stage 6. Checking the results of the attack. Verification of the results of the attack can be carried out both after the attack is completed and, if possible, during its execution, which is more appropriate for timely response in case of insufficient impact on the object. If there is no positive result, it is necessary to change the attack tactics and repeat it. The final check, after the attack is completed, allows us to make sure that the required target and level of damage from the attack have been achieved.

Stage 7. Feedback. At the feedback stage, communication is established between the participants who carried out the attack and its organizers. It is important to convey information about the results of the cyber operation to all members of the group. The general release of information about the results of cyberattacks can significantly motivate everyone involved in its implementation and raise the level of their work. In addition, it is necessary to receive feedback from activists regarding the actions taken. It is also important to constantly maintain communication between all members of the groups, holding various meetings and questionnaires, in the context of expressing their opinions, ideas, and suggestions for improving processes and increasing the efficiency of activities as a whole.

THE MANAGEMENT STRUCTURE OF THE CYBER OPERATIONS ORGANIZATION SYSTEM

To ensure the proper functioning of the system, it is necessary to provide the availability of personnel who will perform the management and implementation of all stages of the proposed technology. The rational distribution of duties and roles is one of the main components of the successful outcome of a cyber operation.

After studying the classification and analysis of each of the possible types of management structures, it was decided that it would be appropriate to use a functional management structure to manage the system of organizing cyberattacks [21]. Its essence is that certain specific functions are performed by specialized management bodies and individual experts who have the necessary qualifications and knowledge. During the organization of this structure, specialists of the same profile are mostly united in structural subdivisions or departments, the main task of which is to perform only those functions in which all members are specialized.

The proposed structure of the personnel management system is shown in Fig. 3.

The cyber operations organizer is the main leader and moderator of work in the system. His duties include ensuring the operation of all system links and establishing connections between them. It is he who selects and appoints personnel to the role of group leaders at all stages of operation. The organizer of cyberattacks must be a person with deep knowledge in the cyber security field.

The group working with activists searches for, recruits, and organizes people who will carry out

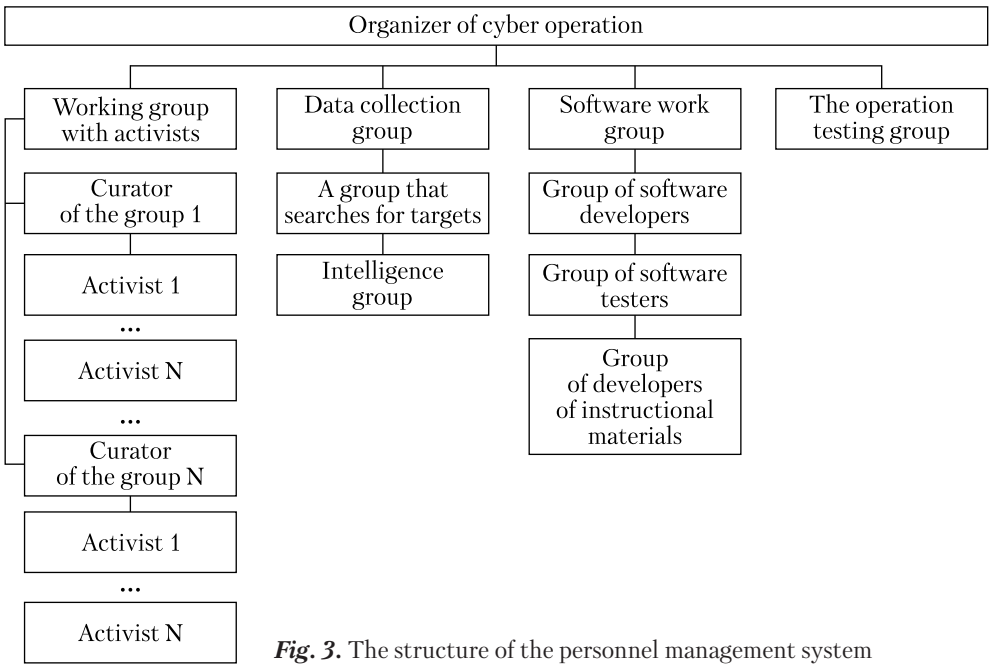

Fig. 3. The structure of the personnel management system

attacks and further divides them into groups. People involved in cyber operations can be individuals with specialized knowledge in the IT field, as well as ordinary activists — individuals without specialized knowledge and skills in the field of IT and cyber security. Each group is headed by a leader. His responsibilities include issuing tasks for conducting attacks, specifying targets, and coordinating the work of the attackers. The head of the group can be a person with or without existing knowledge in the IT field, preferably with leadership and management skills.

The data collection group is engaged in the search and identification of targets for attacks and the collection of information about them. This personnel can be divided into two subgroups, one of which searches for targets, and the other conducts reconnaissance.

The target search group is responsible for forming a database of possible objects to which the attack vector will be directed. Her responsibilities include research and analysis of critical enemy control processes and systems. Based on the received data, a list of objects is formed, attacks on which may cause significant damage to the enemy.

The reconnaissance group is responsible for forming a database of properties and specifications of the objects that have been selected as targets. It is desirable that people who have well-developed knowledge and skills in working with computer networks, understand the basic principles and principles of their operation, and know how to collect and analyze information from open sources should be involved in this work.

The software responsible group deals with the selection of existing tools or the development of new ones that are necessary for conducting a cyber operation. This staff is divided into three groups: developers, testers, and developers of instructional materials.

The developer group searches for and selects means of attack or their development or modification of existing ones. These actions are performed based on the data received from the intelligence group.

The tester group checks the correctness of the software and, if possible, its effectiveness. Also, the responsibilities of the members of this group include setting up the software tools that will be used to carry out attacks.

The instruction organizer group writes and designs instructions that specify the principles of working with software tools that will be used during attacks, as well as describe the actions that activists shall perform during the implementation of attacks.

This category of personnel should include people with advanced knowledge and skills in the IT field.

The attack verification group is responsible for recording and analyzing the results of cyberattacks. Its duties include monitoring the condition and behavior of the target, as well as recording its response to the use of cyber weapons. This category of personnel can include people who are professionals in the field of information technologies, as well as ordinary users with general IT knowledge.

SYSTEM FUNCTIONING ALGORITHM

The developed system should ensure the successful conduct of a cyber operation on the object, as a result of which significant damage will be inflicted on the enemy and an advantage over him will be obtained, which can be used to achieve victory. That is why the development of the algorithm for the functioning of the cyber operation organization system was carried out.

Let's consider in more detail the procedure and stages of system functioning in the event of a cyber operation.

Step 1. Selecting the target. At this stage, the object or system of the enemy's infrastructure to be targeted by a cyber operation, is determined.

Step 2. Search for the object of the cyber operation. The formation of knowledge about its structure, methods, and ways of functioning is taking place. An assessment of the level of security and preparation of the facility for cyber operations on it is carried out.

Step 3. Choosing an attack method. During this stage, the method of attack on the object is selected, and the procedure for the attack is created and described. These procedures are performed based on the data obtained during the previous stage.

Step 4. Cyber operation. After choosing the attack method and its description, the process of conducting a cyber operation to the object is directly implemented.

Step 5. Checking the results of the cyber operation. After the cyber operation has been carried out, its results are checked. If the received data and the damage inflicted on the enemy satisfy the attacker, then the work of the system is considered completed. In the opposite case, the selection of the cyber operation method is reviewed, the necessary corrections are made and a new operation is carried out.

RECOMMENDATIONS FOR THE ORGANIZATION AND CONDUCT OF CYBER OPERATIONS

Potential types of attacks. The used DDoS attacks are one of the most effective methods of cyber warfare in war [22]. The implementation of this type of attack on bank servers will lead to problems with conducting financial transactions. During an attack on state services, it is possible to disrupt the functioning of state administration bodies. Conducting an attack on military critical infrastructure facilities can lead to disruptions in the operation of important systems. All these actions can cause panic among the ranks of the enemy and lead to collapse.

A deface attack is an attack on a site during which the appearance of a web page or its content is changed [23]. By using this attack, you can exert psychological influence on the enemy, spread disinformation, or undermine authority in the political arena.

XSS attacks are a type of attack in which malicious scripts are injected into websites [24]. Using the implementation of this type of attack, it is possible to steal confidential information or gain access to passwords and user logins. This provides an opportunity to gain access to the enemy's resources and steal or replace important data for him.

SQL injection is one of the common ways of hacking websites and programs, which work with

databases, based on introducing arbitrary SQL code into a query [25]. By implementing this type of attack, it is possible to gain access to the enemy's databases. Based on the received information, you can learn about the enemy's plans, and get information about his strategic resources and their locations.

By introducing Trojan programs, viruses, and worms into the information and communication systems of the enemy, it is possible to gain control over them or disable them.

Social engineering attacks are based on psychological manipulation [26]. By implementing this type of attack, it is possible to exert psychological influence on the enemy by disclosing confidential information or stealing digital assets and using them further for their purposes.

Communication and connection between participants. Telegram channels and chats, which were created during the beginning of Russia's military aggression in 2022, and aimed at organizing and conducting massive DDoS attacks, are a clear example of the organization of communication between participants in the system of organizing cyberattacks. With the help of these channels, you can disseminate information about the goals of attacks, convey to users instructions for conducting attacks, and receive feedback and suggestions from them regarding the organization of work and ways to improve it. Using this method of communication allows the attraction of a large number of people from completely different places to make attacks and personnel selection. However, it has several disadvantages, usually, these channels and groups are open and anyone can get there, especially enemy agents who can get access to information about the future targets of the attack and the methods and tools, which will be used during its implementation. Based on the received information, it will be much easier for the enemy to counter attacks. To solve this problem, it is possible to implement some measures aimed at checking the people who will be involved in the work.

When recruiting members of groups to be involved in cyber operations, it is necessary to check them. This can be done by filling out a special questionnaire, in which all those who wish to join the group must provide data to confirm their identity. Another option for the selection of participants is their involvement only if there are familiar persons who already participate in the work of the system and who can vouch for them.

For communication between participants in the process of organizing and carrying out cyberattacks, you can also use special applications and messengers, which encrypt data and transmit it through secure channels. Another communication option is the use of a proprietary software tool.

To increase the interest of participants and increase the number of active users, it is necessary to provide certain actions, the implementation of which will increase their motivation. It is necessary to send a daily report on the results of successful attacks, which, for example, indicate how many targets have already been eliminated and the effectiveness of the attack as a whole. It is also possible to develop a system of rewards for active participation in the work or provide new ideas that can improve the conduct of attacks.

Reconnaissance and gathering data on the target. When collecting information about the target of a future attack, the first thing to do is to familiarize yourself with the structure and organization of the object's work. It is necessary to find out the type and purpose of the target's activity, with whom it cooperates and whose services it uses, from where it carries out its activity. It is also necessary to familiarize yourself with public notices, financial reports, and other documents related to the object of the attack. An important source of information is the research and analysis of data published on social networks (LinkedIn, Facebook, Instagram, Twitter) on the pages of persons related to the object of the attack. With their help, you can create an idea about the staff.

It is necessary to collect information related to the technical aspects of the organization of work, such as the definition of IP addresses and domain names, open ports and running services, as well as

network topology. Among the basic tools that can help and greatly facilitate the process of searching and gathering information, the following can be distinguished: command line utilities (ping, nslookup, traceroute), dnsmap, SubBrute, dnsrecon, recon-ng, nmap, whois, Maltego, Shodan.

You can also use the Google Hacking technique that is also known as Google Dorks [27], to collect information about the object of the attack. Google's hacking searches can be used to identify web vulnerabilities, gather information, identify error messages that reveal sensitive information, identify specific types of files that are directly relevant to the target, and files that contain credentials or other sensitive information.

To obtain more detailed information about search and information collection algorithms and an extended list of software tools that can be used in the data collection process, it is recommended to read the "Open Source Intelligence Tools And Resources Handbook" [28].

Work with software. The software tools that will be used to carry out the attack can be either ready-made developed applications or created by the participants themselves.

In the case when a decision was made to use ready-made software for an attack, its search and selection from all possible presented options is carried out based on the requirements for the availability of functionality and capabilities that would satisfy the attack. If the search for software tools does not yield satisfactory results or the found tools do not fully meet the requirements, it is necessary to carry out the process of developing your tools or modifying existing ones.

After choosing or developing your means of conducting an attack, it is necessary to carry out its testing. Based on the conducted inspections, its effectiveness and feasibility of use for conducting a cyber operation are determined.

For all members of groups carrying out attacks to be able to use the software tool, it is necessary to create instructional materials for its use. The developed instructions should be concise and clear. When writing them, it is necessary to take into account the fact that not all persons who will work with tools for conducting attacks have specific knowledge in the field of information technologies.

Checking the results of the attack. Checking during cyberattacks is necessary to record the object's reaction to the actions taken against it during the attack process. Fixing changes in the state of the target will help to better coordinate the process of the attack. After all, on the side under attack, situations may arise when actions aimed at its implementation are recorded. In response to such actions, those who control and protect the object of the attack can make certain changes in the mechanisms of the target's functioning, and thus establish certain protective procedures that will make the successful implementation of a cyberattack impossible. Therefore, by checking the results of the attack, it is possible to prevent an undesirable result or quickly change tactics.

Verification after the completion of the cyberattack process is necessary to finally make sure of the success of its implementation. This stage of verification includes control recording of the state of the object of the attack, after its completion, as well as the recording of data indicating the period during which the attacked party was able to detect the fact of a cyberattack against it and eliminate the consequences.

Data obtained as a result of inspections must be documented and systematized. Based on the collected information, it is necessary to make changes in the technique of conducting operations in the future. Also, after analyzing the results of the checks, it is necessary to modernize the collected information about the enemy's resources and capabilities. After analyzing reactions to attacks, it is possible to expand the idea of existing defense mechanisms and assess the competence of the enemy.

Not all of the recommendations and instructions listed above are mandatory. The given information is of a recommendation nature only and is not obliged to be implemented exactly. However, if these actions and procedures are observed and

implemented, it is possible to significantly improve the performance of the cyberattack system.

The development of a system for conducting cyber operations was carried out to improve the processes of organizing cyberattacks in conditions of military aggression due to the mapping of management functions to the stages of conducting cyber operations, which allows for improved understanding and transparency of managing such a complex system as a cyber army. This, in turn, will make it possible to significantly increase the productivity of the relevant structures, because, without competent system management, it is practically impossible to successfully achieve the set goals and stable development.

At the same time, issues of control and regulation of the use of cyber weapons and their consequences during military operations at the international level remain relevant. Conducting cyber operations must have both a legal and an ethical basis, despite the popular saying "In war, any means is useful." This necessity arises from the importance of ensuring compliance with international standards and humanitarian principles, even in cyberspace, where the rules of military law still need to be developed and clarified. One of the key documentary bases for this is the document "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" [29]. This document is the result of the collective work of experts in international law and cyber security and provides recommendations and interpretations on how existing norms of international law can be applied to cyber operations. Its presence indicates the importance of considering cyberspace as a new and complex field for regulation. At the same time, it remains important to develop and observe the rules for conducting cyber operations in the context of ensuring the protection of the civilian population.

In addition to cyber operations, information and psychological operations can also be the effective tools in military confrontation, the results of which are presented by the authors in [30]. Tracking informational injections and disinformation of the adversary is equally important in cyber operations planning [31]. This will enhance the effectiveness of cyber operations by understanding the informational environment, comprehending the adversary's intentions, safeguarding own infrastructure. Such tools can become as additional effective means within the proposed system.

REFERENCES

1. Brooks, D. (2023). *The importance of modern-day data security platforms*. Security Intelligence. URL: https://security-intelligence.com/posts/importance-modern-day-data-security-platform (Last accessed: 10.05.2024).
2. Dr. Stevens, T., Dr. Burton, J. (2023). *NATO and strategic competition in cyberspace*. NATO REVIEW. URL: https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html (Last accessed: 10.05.2024).
3. Kurochko, N. (2023, September). *Powerful DDoS attacks and other cyber threats of the end of 2023: what businesses should prepare for and how to protect themselves from them*. Speka. URL: https://speka.media/ponad-2500-potuznix-ddos-atak-ta-novi-prognozikiberekspertiv-do-cogo-gotuvatisya-biznesu-pndqwv (Last accessed: 10.05.2024) [in Ukrainian].
4. *Situation Center for Cybersecurity*. Security Service of Ukraine. URL: https://ssu.gov.ua/ sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky (Last accessed: 10.05.2024) [in Ukrainian].
5. *Cyberpolice*. (n.d.). Cyberpolice. URL: https://cyberpolice.gov.ua (Last accessed: 10.05.2024) [in Ukrainian].
6. *Communications and Cyber Security Forces*. Ukrainian Military Pages. URL: https://www.ukrm ilitary.com/p/signal-troops.html (Last accessed: 10.05.2024) [in Ukrainian].
7. Ovsyanyk, Y. (2022, March 5). *Cyber Cossacks — fighters of the invisible front*. URL: https://zbruc.eu/node/110961 (Last accessed: 10.05.2024 [in Ukrainian].
8. On the Basic Principles of Ensuring Cybersecurity of Ukraine, Law of Ukraine No. 2163-VIII (2022) (Ukraine). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Last accessed: 10.05.2024) [in Ukrainian].
9. Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*.

10. Buckbee, M. *What is The Cyber Kill Chain and How to Use It Effectively*. Varonis. URL: https://www.varonis.com/blog/cyber-kill-chain (Last accessed: 10.05.2024).
11. *Cyber Security Glossary*. Heimdal security. URL: https://heimdalsecurity.com/glossary#C (Last accessed: 10.05.2024).
12. Paganini, P. (2012). *Cyber Weapons*. The Hacker New Magazine.
13. Kuperstein, L. M., Radetska, A. O. (2022). *Cyberweapons as an effective integral tool of military conflict: electronic scientific publications*. LI Scientific and Technical Conference of the Faculty of Information Technology and Computer Engineering. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15803/13286 (Last accessed: 10.05.2024) [in Ukrainian].
14. Knapczyk, P. (2023, 18 August). *Overview of the Cyber Weapons Used in the Ukraine — Russia War*. Trustwave. URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war (Last accessed: 10.05.2024).
15. Passeri, P. *What is a cyber weapon?* Hackmageddon. URL: https://www.hackmageddon.com/2012/04/22/what-is-a-cyber-weapon (Last accessed: 10.05.2024).
16. Stark, S. (2022, January 14). *Websites of Diia, MFA, SES, MoD hacked by hackers*. Ilounge journal. URL: https://ilounge.ua/ua/blog/sajty-diya-vzlomali-hakery (Last accessed: 10.05.2024) [in Ukrainian].
17. *Russians have created new clones of Ukrainian media*. (2023, September). Spravdi. URL: https://spravdi.gov.ua/ukrayina-prodaye-ditej-na-nelegalnyh-rynkah-i-uhylyanty-hovayutsya-u-vyshah-rosiyany-stvoryuyut-klony-ukrayinskyh-novynnyh-media (Last accessed: 10.05.2024) [in Ukrainian].
18. *Ukrainian hackers gained access to the databases of the Russia-Africa 2023 economic summit*. (2023, July 15). Inform Napalm. URL: https://informnapalm.org/ua/rosia-afryka-2023 (Last accessed: 10.05.2024) [in Ukrainian].
19. Boyko, I. (2022, March 10). *Anonymous hacked Roskomnadzor and leaked data to the network*. Unian. URL: https://www.unian.ua/world/anonymous-zlamali-roskomnaglyad-i-zlili-dani-v-merezhu-novini-svitu-11738668.html (Last accessed: 10.05.2024) [in Ukrainian].
20. Morgulets, O. B. (2012). *Management in the service sector*. Kyiv [in Ukrainian].
21. Nebava, M. I., Ratushniak, O. G. (2012). *Management of organizations and administration* [in Ukrainian].
22. Kupershtein, L., Voitovych, O., Baryshev, Y., Kolibabchuk, E. (2016). Investigation of simple Denial-of-Service attacks. *Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*. https://doi.org/10.1109/INFOCOMMST.2016.7905362
23. Romagna, M., van den Hout, N. J. (2017). Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats. *27th Virus Bulletin International (October, 2017, Madrid, Spain)*. URL: https://www.researchgate.net/publication/320330579_Hacktivism_and_Website_Defacement_Motivations_Capabilities_and_Potential_Threats (Last accessed: 10.05.2024).
24. Kirsten, S. *Cross site scripting (xss)*. Owasp. URL: https://owasp.org/www-community/attacks/xss (Last accessed: 10.05.2024).
25. Voitovych, O. P., Yuvkovetskyi, O. S., Kupershtein, L. M. (2016). SQL injection prevention system. *2016 International Conference "Radio Electronics & Info Communications" (UkrMiCo)*. IEEE. https://doi.org/10.1109/ukrmico.2016.7739642
26. *Social Engineering: Definition & 6 Attack Types*. URL: https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for (Last accessed: 10.05.2024).
27. *Google Hacking Database*. Exploit Database. URL: https://www.exploit-db.com/google-hacking-database (Last accessed: 10.05.2024).
28. Bielska, A., Kurz, N. R., Baumgartner, Y., Benetis, V. (2020). *Open source intelligence tools and resources handbook*. I-intelligence. URL: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf (Last accessed: 10.05.2024).
29. Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. I-Ii). Cambridge. URL: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf (Last accessed: 10.05.2024).
30. Dudatyev, A., Kupershtein, L., Voitovych, O. (2023). Information counterfeature: models of implementation and evaluation of information operations. *Electronic Professional Scientific Edition* "*Cybersecurity: Education, Science, Technique*", 4(20), 72—80. https://doi.org/10.28925/2663-4023.2023.20.7280 [in Ukrainian].
31. Baryshev, Y., Kupershtein, L., Maidanovych, V., Voitovych, O., Prokopenko, S. (2023). Information System for the Fact-checker Support. *CEUR Workshop Proceedings*, 3646, 127—138. URL: https://ceur-ws.org/Vol-3646/Paper_13.pdf (Last accessed: 10.05.2024).

Received 05.04.2024
Revised 19.09.2024
Accepted 19.09.2024

Л.М. Куперштейн (https://orcid.org/0000-0001-6737-7134),
В.В. Лукічов (https://orcid.org/0000-0002-3423-5436),
А.О. Радецька (https://orcid.org/0009-0009-5687-5651),
А.В. Дудатьєв (https://orcid.org/0000-0002-7944-2404)

Вінницький національний технічний університет,
Хмельницьке шосе, 95, Вінниця, 21021, Україна,
+380 432 56 0848, vntu@vntu.edu.ua

СИСТЕМА ОРГАНІЗАЦІЇ КІБЕРОПЕРАЦІЙ В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ

Вступ. У сучасному світі зростає важливість інформаційно-комунікаційних технологій та загроз, пов'язаних із кібератаками в умовах військової агресії. Поширення цих технологій супроводжується збільшенням ризиків кіберзагроз на різноманітні об'єкти та системи управління.

Проблематика. У контексті військових конфліктів кібероперації стають суттєвим методом ведення боротьби. За допомогою них можна отримати доступ до секретних військових, економічних чи стратегічних даних, витік яких може завдати значної шкоди супротивнику як на військовій, так і на політичній арені, підірвати його авторитет або знищити певні військово-політичні плани. Вплив на системи комунікації та управління або виведення їх з ладу здатні спричинити колапс та розруху у лавах противника і призвести до його програшу. Тому актуальним є дослідження і вдосконалення методів проведення кібератак для забезпечення ефективної оборони та захисту від цих загроз.

Мета. Вдосконалення етапів процесу організації кібероперацій у військовому середовищі шляхом застосування принципів менеджменту та розробка рекомендацій для його оптимізації.

Матеріали й методи. Дослідження базується на аналізі теоретичних джерел щодо кібероперацій, а також на використанні практичних прикладів з аналізу попередніх інцидентів кібератак у військовому контексті.

Результати. Проведено розробку технології роботи системи організації кібероперацій. Створено структури управління цією системою та розроблено алгоритм її роботи. Наведено рекомендації щодо управління та організації роботи на етапах функціонування системи.

Висновки. Розробка та впровадження стратегій менеджменту для оптимізації проведення кібероперацій у військовому контексті є вкрай важливими у сучасних реаліях. Вдосконалення цих процесів є ключовим для забезпечення ефективної захищеності та відповіді на кіберзагрози під час військових конфліктів.

Ключові слова: кібероперація, кіберзброя, кібератака, кібервійна, військова агресія, функції менеджменту.