DOI: https://doi.org/10.15407/kvt211.01.005

**ODARCHENKO R.S.**[1], DSc (Engineering), professor,
Head of the Telecommunication and Radio Electronic Systems Department
https://orcid.org/0000-0002-7130-1375, e-mail: odarchenko.rs@ukr.net
**BONDAR S.O.**[2],
Acting Head of Intelligent Control Department
https://orcid.org/0000-0003-4140-7985, e-mail: seriybrm@gmail.com
**SIMAKHIN V.M.**[2], PhD student,
Researcher of Intelligent Control Department
https://orcid.org/0000-0003-4497-0925, e-mail: thevladsima@gmail.com
**SIERIEBRIAKOV A.K.**[2], PhD student,
Researcher of Intelligent Control Department
https://orcid.org/0000-0003-3189-7968, e-mail: sier.artem1002@outlook.com
**PINCHUK A.D.**[1], student
https://orcid.org/0000-0003-3567-0445, e-mail: pinchuk.ad87@gmail.com
**SAMOILENKO V.V.**[1], student
e - mail : vladss1954@gmail.com
**STANKO P.O.**[3], PhD (Engineering),
associate professor of the Information Technologies Department
https://orcid.org/0000-0001-5794-3593 e-mail: p_stanko@ukr.net

[1] National Aviation University,
1, Lubomyra Huzara ave., 03058, Kyiv, Ukraine
[2] International Research and Training Center for Information
Technologies and Systems of the National Academy of Sciences of Ukraine
and the Ministry of Education and Science of Ukraine,
40, Acad. Glushkova av., Kyiv, 03187, Ukraine
[3] University of New Technologies,
5A, Metrobudivska str., 03065, Kyiv, Ukraine

# RESEARCH OF THE MAIN MEANS AND INTERMEDIATE RESULTS OF THE RUSSIAN-UKRAINIAN CYBERWAR: CYBERVOLUNTEER INITIATIVES

***Introduction.*** *This research paper examines the current state of cyberwarfare in the world. The issues regarding definition of the very term "cyberwar" are discussed. The historical beginning of the Russian-Ukrainian cyberwar, its course and current state are considered, as well as the main means of its conduct are examined. It has been determined that this cyberwar was the world's first full-scale global cyberwar. The main attention is paid to the* *cybervolunteer IT army of Ukraine, which appeared in the course of this cyberwar and is successfully combating with the russian federation on the cyberfront.*

***The purpose of the paper** is to show the process of waging a real cyberwar today, the application of the means for its carrying out, and conduct a study of its intermediate results; using Ukraine as the example to show the efficiency and effectiveness of the work of cybervolunteer initiatives.*

***The results.** An analysis of the main existing approaches to conducting cyberwarfare was carried out, and the types of cyberattacks that are most often used were determined. It has been determined which directions and means of conducting cyberspace the russian federation focuses on. The IT activities of the Ukrainian army were studied, the key areas of work were determined and their detailed classification was given. In the course of the study, the main indicators of the effectiveness of the cyberarmy of Ukraine were determined and statistical data on the work of key areas were collected, on the basis of which the efficiency, effectiveness and problems that arise during the fight on the cyberfront were analyzed.*

***Conclusions.** For the first time, the process of waging the Russian-Ukrainian cyberwar was examined in detail, with an emphasis on the activities of cybervolunteer initiatives of Ukraine. Determining the key areas of their activity made it possible to investigate the effectiveness and determine the intermediate results of this cyberwar. After analyzing all the data, recommendations were made to improve efficiency and effectiveness in the fight on the cyberfront.*

***Keywords:** cyberfront, cyberwar, approaches to waging cyberwars, cyberweapons, Russian-Ukrainian cyberwar, cybervolunteer initiatives, IT Army of Ukraine.*

## INTRODUCTION

With the beginning of the active development of the information space in the world, which was first of all aimed at facilitating all communication, speeding up various production processes, the so-called cyberspace emerged, which is a new space for conducting warfare. The rapid informatization of the world has led to the growing interdependence of the state on cyberspace. The Internet has become crucial for the society, economy, army of a modern country etc. This has become a new challenge for national security, and the term "cyberwar" is being used more and more often. The main targets of cyberwars are critical infrastructure, which are the financial system, hospitals, energy companies, government agencies, information infrastructure, and the adversary's psyche. This phenomenon is not clearly documented, NATO in 2016 only recognized cyberspace as an arena of military operations alongside the traditional spheres — land, sea and air [1]. Despite all this, massive cyberattacks on countries have occurred in the past.

The world's first cyberattack took place in November, 1982. Then the American special services deliberately introduced a bug into the Canadian software for managing the Trans-Siberian gas pipeline, causing a strong explosion in a deserted area [2].

The next challenge for society was the "Morris Worm" — this was the first case of an Internet worm. In 1988, it temporarily disabled about 10% of computers worldwide that were then connected to the Internet [3].

After that, a number of cyberattacks were carried out, in particular on the computers of the Rome Aviation Development Center, the "Code Red" and "Stuxnet" worms, the appearance and activities of the hacker group "Anonymous" and others [2, 4].

These cyberattacks became the root of the global problem of world society — cyberwars. To this date, four cases of cyberwars are known: cyberattacks against

Estonia (2007), cyberattacks against Georgia (2008), Russian-Ukrainian cyberwar (from 2014 to the present day) and cyberwar against IS militants (2016) [5–8].

The event in Estonia in 2007 is considered the world's first case of cyberwar — massive cyberattacks aimed at the country's national security. Then the government of Estonia decided to dismantle the monument to the Bronze Soldier of Tallinn, which honored the Soviet soldiers who liberated the country. For russia, such actions turned out to be unacceptable, relations between the two countries became tense. This provoked a riot called "Bronze Night". russian intelligence agencies launched massive DoS cyberattacks that escalated into larger and more distributed Denial of Service (DDoS) attacks. They included botnets of computers from many countries launched against government, banking, media and political party websites in Estonia [5].

A large number of various cyberattacks in the world are still happening today. According to Security Magazine, there are more than 2,200 cyberattacks every day — 1 attack every 39 seconds [9]. However, the most significant event is considered to be the Russian-Ukrainian cyberwar, which has been going on for the eighth year.

## RUSSIAN-UKRAINIAN CYBERWAR

The catalyst for the Russian-Ukrainian cyberwar, which eventually became the world's first full-scale cyberwar, was the political situation of Ukraine in November 2013. At that time president V. Yanukovych refused to sign the political association agreement with the European Union (EU), which provoked mass protests by citizens and the "Revolution of Dignity" as the result.

Cyberattacks by russia began even before this event. The first massive cyberattack for Ukraine was the closure of the ex.ua service, which was subjected to numerous DDoS attacks. The next wave of denial-of-service attacks began on December 2, 2013. Opposition websites were the targets of DDoS attacks, most of which came from commercial botnets. Activists have also conducted cyberattacks against the Ukrainian government, using tools such as the Low Orbit Ion Cannon (LOIC) to launch the same attacks on the president's website.

The annexation of the Crimean peninsula in 2014 marked the beginning of the "Hybrid War". In this conflict phase, russia carried out five cyber operations against Ukraine. These included election interference, sabotage of critical infrastructure, and economic warfare. The most famous of them are the damage to the information systems of Ukrainian government institutions by a virus known as Snake/Uroborus/Turla, a series of attacks on energy companies of Ukraine (2015–2016) using the BlackEnergy Trojan program, and a massive hacking attack in 2017 using a family computer worm Petya – NotPetya. In response to this, the Ukrainian hackers of the cyber alliance also conducted their own cyber operations.

On the part of Ukraine, a number of reforms in the cybersecurity sector were carried out: the official status of the cyberthreat response team in Ukraine CERT-UA was established, the decision of the National Security Council of Ukraine "On the Cyber Security Strategy of Ukraine" was put into effect, and a national cybersecurity coordination center was created [10–12].

Cyber attacks from russia did not stop. Ukraine received a powerful cyberattack in January 2022, which is described in [13]. During the month of February, other cyberattacks were also performed: a DDoS attack on a number of banks and state portals of Ukraine, which included attempts to hack and deface web resources [14–15].

However, this cyberwar has become a truly full-scale global cyberwar, starting at the end of February of this year, when russia launched a full-scale armed invasion on the territory of Ukraine. This was accompanied by massive cyberattacks on government resources of the state. As a result, on February 26, the Minister of Digital Transformation of Ukraine M. Fedorov announced the creation of the IT Army of Ukraine to fight on the cyberfront [16]. It was assumed that IT specialists would participate in this cybervolunteer army, but now anyone can contribute to the victory in this war. The IT Army of Ukraine includes both Ukrainian and foreign volunteers [17]. The key task of the military is to launch DDoS attacks on russian web resources. The well-known hacker group Anonymous, described in [18], also took the side of Ukraine. russian cyberattacks continue. This is how attempts were made to attack DDoS attacks on the UkSATSE resources and a recorded brute force attack on the company's postal services [13], the Ukrtelecom telecommunications company, state bodies, etc. [19–20].

Subsequently, russia began to attack not only Ukrainian resources, but also foreign resources, which once again confirms the fact of a global cyberwar. The russian hacker group "Killnet" has declared a "cyberwar" against the governments of countries that they say support "Nazis and Russophobia". These countries are the USA, Great Britain, Germany, Italy, Latvia, Romania, Lithuania, Estonia and Poland [21].

One of the types of attacks in cyberwar (or a type of cyberweapon) is the spread of propaganda and disinformation [22–23] in order to exert psychological influence on the population and destabilize the situation in the country as much as possible, which russia is currently using. Since the beginning of the full-scale armed invasion on the territory of Ukraine, russia has begun to massively spread its own propaganda and disinformation in all possible social networks. In order to effectively combat this, the Cyber Police Department of Ukraine created another unit of the cybervolunteer movement [24]. The main tasks of which are to send mass complaints to posts/pages/channels in social networks in order to block these resources. There is also the Internet Army of Ukraine [25], whose work is aimed at drawing the attention of the world community to what is happening in our country, spreading true information and calling on various companies to stop their activities in russia.

Currently, Ukraine has a significant advantage on the cyberfront and reacts in a coordinated manner to all cyberattacks from russia [26].

## ANALYSIS OF RESEARCH AND PUBLICATIONS

The topic of cyberwarfare is very common nowadays, especially against the background of current events taking place in the world. In general, a large number of scientific works are devoted to the analysis of the very concept of "cyberwar". However, as a result of research, there are many different and contradictory definitions, starting from the non-existence of cyberwar and ending as a direct threat for the present and future. Despite all this, there is still no clear definition of this concept. In their study, Hughes and Kolarik found that out of

159 articles on cyberwarfare, 103 (65%) failed to offer a clear definition of cyberwarfare [27].

Thus, in his book [28], the former White House adviser on combating terrorism argued that cyberwarfare is "the actions of a nation state aimed at penetrating the computers or networks of another country in order to cause damage or disruption." This definition has become perhaps the most influential in research on this issue and is the most cited (in Google Scholar) work on cyberwarfare.

The well-known Ukrainian scientist O. Merezhko offered his own definition of the discussed concept: "Cyber war is the use of the Internet and other related information and technological means by the state with the aim of harming the military, economic, political and information security of another country, as well as its sovereignty." [29]

According to J. Carr, cyberwar is the art and science of fighting without fighting or winning opponents without shedding their blood [30]. By this definition, the author means that actions taken during cyberwar should not result in victims in the real world.

S. Hildreth says that the term "cyberwar" can be used to describe various aspects of protection and attack on information and computer networks in virtual space, as well as depriving the adversary of the ability to perform similar actions [31].

IEEE (Institute of Electrical and Electronics Engineers) in its works [32–33] defines the concept of cyberwar as "A subgroup of information war that includes actions in cyberspace. Cyberspace is any virtual reality containing a collection of computers and networks. There are many cyberspaces, but the most relevant for cyberwarfare is the Internet and related networks that share media with the Internet" and provides the principles of cyberwarfare and their description. In [33], they conducted a study of how principles of physical warfare can be adopted into cyberwarfare, looking at nine principles of warfare used by the US military and their ease/difficulty in integrating into cyberwarfare.

In [34], three topics are proposed as bases on the way to defining the term "cyberwar":

- alarmists – cyberwar is an immediate danger to the United States and its allies;
- skeptics – cyberwarfare is both a concept and a reality, controversial and ambiguous, and its existence depends on how we define cyberwarfare;
- realists – a certain form of conflict in cyberspace exists, and it can be understood through existing international legal structures and norms of state behavior.

In doing so, the key variables of each topic are actions, actors, consequences, geography and goals, which are also explained in the study.

[35] discusses the key factors determining the advantages of cyberwarfare. First of all, cyberwars/cyberattacks are now the most popular among state and non-state actors, due to their difficulty in identifying the source of the attack, as they have the ease of falsifying data in cyberspace. Second, there is a difficulty in attributing cyberattacks (these difficulties are listed and described in the source).

In [35–37], the stages of a cyberattack execution are given. Analyzing these sources signifies, that in [37] these stages are more widely studied. Thus, they are: intelligence, information about the use of cyberweapons against the company, "launching an attack", exploiting security vulnerabilities, establishing a backdoor, exercising command and control and achieving the goals of the hacker. The steps include a variety of activities, from machine attacks to the use of social engineering. The article [36] lists the best-known tools for conducting a cyberattack and their use.

This article [38] describes the main elements of cyberattacks, which include hacking, malware, and DDoS attacks. A technical description of how each element of a cyberattack works and what software tools are used to support it is provided.

Heuristic classification of cyberattacks is given in [39]. It has been determined that cyberattacks are carried out at several levels. The proposed classification is not meant to be hierarchical or all-encompassing. The following levels are highlighted:

- government against government (in the context of kinetic battle);
- asymmetric warfare: a non-state actor against its own agencies or contractors or another government;
- government against critical infrastructure of another government (non-kinetic battle);
- criminal hackers against individual users.

This article [40] concerns US efforts to develop strategic "cyber deterrence" as a means against hostile action in global cyberspace.

Despite the large number of publications and studies devoted to this topic, the very phenomenon of "cyberwar" remains poorly studied, which is proven by the lack of a clear definition, and very little attention has been paid to the process of conducting a real cyberwar with definite results.

## SETTING RESEARCH OBJECTIVES

Thus, it is necessary to determine the key areas of research that will contribute to the further effective conduct of cyberwarfare. To achieve the goal, the following scientific problems must be solved:

1. To analyze the main existing approaches to waging cyberwars.
2. To analyze and classify the key areas of activity of the cybervolunteer IT army of Ukraine.
3. To analyze the main intermediate results of IT activities of the army of Ukraine.
4. Develop recommendations for IT activities of the Army of Ukraine.

## ANALYSIS OF THE MAIN APPROACHES TO CARRYING OUT CYBERWARS

In this section, we will analyze in detail the following types of cyberattacks (Fig. 1): DDoS (Botnet, LOIC), SQL-injections, Zero-day attacks, Malware (Petya/NotPetya, BlackEnergy3). The principle of operation, effectiveness and prevalence of these methods in modern cyber conflicts will be given.

**1. Zero-day attacks.** In order to perform a zero-day attack, you must first find a zero-day vulnerability. These are software vulnerabilities that are not yet known to either the users or the developers of this software. In general, these vulnerabilities are known only after attacks that are carried out with their help. It is very difficult to release a product in which there are no errors and vulnerabilities in modern times. Programs become more and more complex and larger over time, and with this, the probability of vulnerabilities in the code also increases. It seems that as long as software has bugs and developing exploits for new vulnerabilities is a profitable activity, we will be exposed to zero-day attacks. Automated techniques for finding zero-day attacks in field data

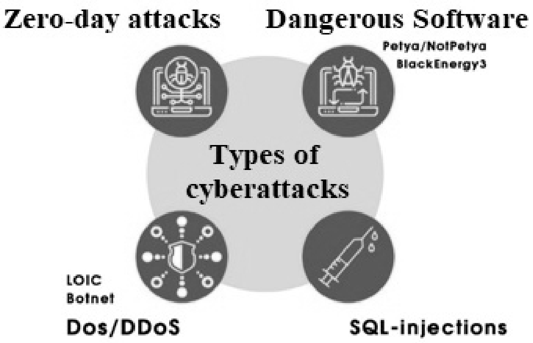


***Fig. 1.*** Types of cyberattacks

facilitate the systematic study of these threats. At the moment, attacks that use this vulnerability are the most dangerous.

**2. Malicious software.** A general term that includes many different viruses, worms, ransomware, Trojans, and loggers. In general, this term can be described as software that is used by attackers to achieve their goals. The following malware was actively used against Ukraine: Petya and BlackEnergy3. Petya is a family of viruses that target the Windows operating system. The main purpose of these viruses is to encrypt the victim's data and demand payment for their decryption.

BlackEnergy appeared in 2007 and represented a simple set of tools for creating Botnets and conducting DDoS attacks. In 2010, BlackEnergy2 with extended functionality was discovered. And in 2014, a third version was found, which was used in the world's first attack to disable the power system. Almost 30 substations were turned off and about 230,000 residents remained without power from one to six hours.

On December 24, 2015, in the Oblenergo attack, attackers demonstrated a variety of capabilities, including phishing emails, variants of the BlackEnergy3 malware, and manipulation of Microsoft Office documents that contained malware to gain a foothold in electricity companies' information technology (IT) networks.

Attackers have also shown the ability and willingness to target field devices at substations, write their own malicious firmware, and damage equipment beyond repair. In one case, the attackers also used phone systems to generate thousands of calls to the power company's call center to prevent customers from reporting power outages. However, the attackers' strongest capabilities were not in their choice of tools or experience, but in their ability to perform the long-term reconnaissance operations necessary to study the environment and execute a highly synchronized, multi-stage attack on multiple sites. As described above, this suggests that it was run by a government or military organization, such as the FSB or GRU, rather than an amateur group of hackers.

They had a large amount of information that was carefully analyzed. Before the attack, it was available from open sources; including a detailed list of infrastructure types [41]. Virtual private networks (VPNs) to the industrial control system (ICS) from the business network did not have two-factor authentication. Additionally, based on media reports, it appeared that employees did not have the ability to continuously monitor the ICS network and look for anomalies and threats with proactive protection measures. These vulnerabilities allowed the adversary to remain in the environment for six months or more to conduct reconnaissance of the environment and subsequently launch an attack.

**3. Botnet.** A common mechanism for launching a distributed denial of service (DDoS) attack against computer networks or applications. Such attacks overwhelm the victim's network bandwidth and resources, thus creating a denial of service for normal users. The attack is launched using a Botnet through a network of controlled computers. The software manages computers remotely and without human intervention. Bots are small scripts designed to perform certain automated functions. In large quantities, they provide the power of an entire computer. They are used for a wide range of tasks: sending e-mail (SPAM), installing spyware, spreading viruses and worms, and DDoS attacks.

There are a large number of different tools that allow you to implement a distributed denial of service attack. In Ukraine, 2 Low-Orbit Ion Cannon (LOIC) tools were actively used by activists at the Revolution of Dignity and BlackEnergy (third iteration) by russian hackers against the Ukrainian government and critical infrastructure [42].

LOIC is a widely available open source program developed by Praetox Technologies that is used for network stress testing, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on Dignity Revolution. To activate LOIC, an attacker simply runs a program, enters a target URL or IP address, and then determines whether to launch a TCP, UDP, or HTTP flood. TCP and UDP modes send message strings and packets to selected ports on the target device, while HTTP flood mode sends an endless series of GET requests.

The widespread availability of LOIC means that attackers can easily recruit other users for a coordinated attack. In addition, its ease of use allows anyone, regardless of knowledge and experience, to perform potentially serious DDoS attacks. At the same time, users cannot route attack traffic through a proxy. As a result, their IP addresses are fully visible, making them easy to track.

Small-scale LOIC attacks can be detected and blocked with basic network traffic monitors and firewalls. However, such defenses can be overcome by a coordinated attack, and protection against them can only be implemented with special and individual security solutions.

**4. SQL injections.** When we enter our information (like login credentials etc.) into the input fields provided in a web form of a web application, it forms part of a SQL query written on the server to be executed against the database. For example, when we log into our mailbox, we specify a username and password. The username and password are part of the internal SQL query. An SQL query is then executed against the database to verify that the provided login credentials match the data present in the database tables. An attacker who does not know the login credentials but wants to gain access to the mailbox in a dishonest way provides SQL code instead of valid input in the test fields of the web form. This malicious code modifies the structure of the original SQL query and therefore allows an attacker to gain access to information to which he is not authorized.

Illegitimate SQL code from the web application interface is called SQL-injections. SQL-injections posed a serious threat to the security of web application data. These were the most popular and most damaging attacks used by hackers to attack databases. An attacker provides SQL code instead of entering legitimate information into the fields of a web form, and thus changes the SQL query to the database, obtaining the information he needs.

The rise of SQL-injection attacks is due to the fact that many web applications did not perform any validation of the data entered by the user. This increases the chances of an attacker gaining unauthorized access to the application's database. To prevent this, it is possible to implement a data check for malicious code [43]. SQL injections are not effective at this time. Almost all libraries are shielded and protected from malicious code execution.

## ANALYSIS AND CLASSIFICATION OF KEY AREAS OF ACTIVITY OF THE CYBERVOLUNTEER INFORMATION TECHNOLOGY ARMY OF UKRAINE

Starting from February 24, 2022, three key areas of activity of the cybervolunteer IT army of Ukraine were formed, each of which forms a separate community (Table 1).

It is worth noting that these communities are official, which were created by the state bodies of Ukraine, but proactive Ukrainians have created other "partisan" cyber communities that operate in the same directions.

So, in general, we have the following directions: cyberattacks (DDoS) on enemy sites and services (Fig. 2a), the fight against propaganda and disinformation (Fig. 2b), spreading of true information about events in Ukraine, appealing to world politicians and brands (Fig. 2c). Thus, the IT activities of the Ukrainian army cover the key areas of attack by russia and gain a significant advantage in cyberwarfare, which brings its positive results.

Cyberattacks on russian governmental cites and media recourses (DDoS)

Fight with propaganda and desinformation at social media platforms: Telegram, Instagram, Facebook, Twitter, TikTok, Youtube

True information about events in Ukraine distribution, appeals to world's polititians and brands

***Fig. 2.*** Classification of the key areas of activity of the Cyber Volunteer Army of Ukraine

***Table 1.*** Classification of cybervolunteer initiatives

| Initiative | Brief description | Main activity | Basic tools |
|---|---|---|---|
| IT army of Ukraine | A community of IT specialists and ordinary people, volunteers, from all over the world. Specialists of various levels have created and continue to create automated systems of attacks on russian information resources and services. | The goal is to ensure the maximum complication of the operation of russian state websites and services - DDoS attacks. | To carry out "manual" DDoS attacks, the following tools are used:<br>● MHDDoS/MHDDoS Proxy<br>● Db1000n<br>● Distress<br>● LOIC<br>Community volunteers created programs with automated attacks (targets are automatically downloaded from the community site, just run the program). The installer includes fully automated MHDDoS Proxy, Db1000n, Distress. In addition, an attack automation bot was created for greater efficiency.<br>A fully automated program UAShield and Dripper[44] is also often used. |
| "Dream" platform | Synergy of the Cyber Police Department and the volunteer movement. | This department is responsible for combating russian propaganda and disinformation in social networks: Telegram, Instagram, TikTok, Facebook, Twitter, YouTube. | The platform includes the following projects:<br>- Telegram channel "StopRussia \| Mriya" is a community of all concerned Ukrainians and not only, who blocks and opposes hostile aggression on the Internet.<br>- The "Mriya Automatic" service is an automated service for combating russian propaganda.<br>- Bot «russiaussia \| Mriya" — receives information about fake resources, which are checked by our moderators and sent to be blocked by interested citizens [24]. |
| Army of Ukraine Internet | Responsible for working with the global community. The main volunteers are Ukrainians, but an international legion Internet Troops of Ukraine was additionally formed [45]. | The key tasks are spreading the truth about everything that is happening in Ukraine during the war with russia. There are also various calls to world politicians to pay attention to the situation in Ukraine and not remain indifferent, to stop supporting the aggressor country, and calls to global brands to stop doing business in the russian market [25] . | Admins provide post topics, indicative texts, images and links to politicians/brands' social networks. The posts themselves are written in the following social networks: Twitter, Facebook, Instagram, LinkedIn. |

## ANALYSIS OF THE MAIN INTERMEDIATE RESULTS OF INFORMATION TECHNOLOGY ACTIVITIES OF THE UKRAINIAN ARMY

The activities of cybervolunteer initiatives began from the first days of the full-scale invasion of the aggressor country. After all, between the armed invasion, russia also launched a full-scale cyberwar against Ukraine.

To analyze the results, a statistical data collection was carried out on the performance of tasks in the time period 05.03–09.09.2022, which is presented in Fig. 3 (when analyzing the received data, we will not pay much attention to September, because the month is not full). Tasks came from the telegram channels IT army of Ukraine, StopRussia Channel | Mriya, Internet Army of Ukraine and a number of "partisan" channels. These tasks were collected in the telegram chat created by enterprising specialists and students of the IT field.

The histogram shows:

- fight against propaganda and disinformation — the number of complaints sent to pages/channels/individual posts in social networks;
- posts in social networks — the number of written posts;
- DDoS — the number of russian sites that were subjected to cyberattacks.

At the same time, it should be noted that for greater efficiency, complaints were sent repeatedly to some pages/channels/posts, and cyberattacks on certain russian sites are also repeated.

Let's consider in more detail the direction of combating disinformation and propaganda (Fig. 4).

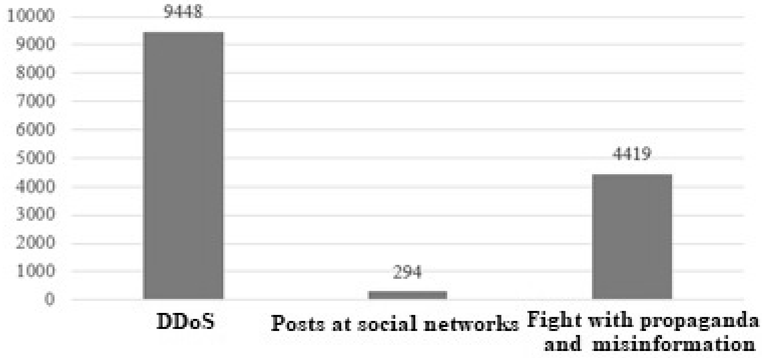


***Fig. 3.*** The number of completed tasks by direction

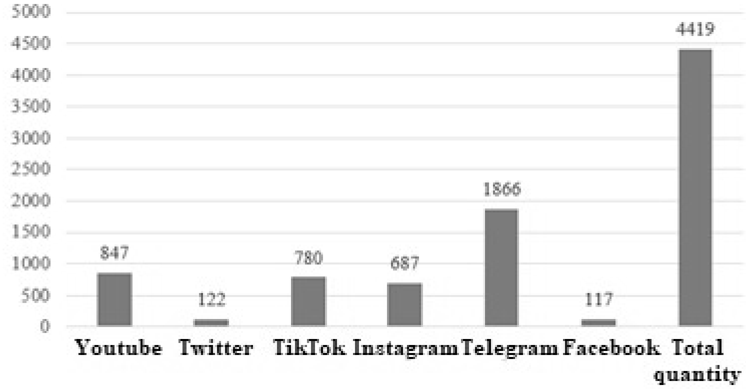
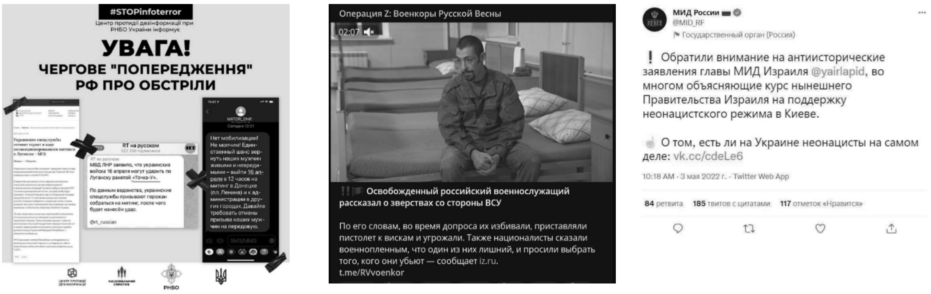


***Fig. 4.*** Fight against propaganda and disinformation



#STOPinfoterror

Центр протидії дезінформації при РНБО України інформує

УВАГА!

ЧЕРГОВЕ "ПОПЕРЕДЖЕННЯ" РФ ПРО ОБСТРІЛИ

Украинские спецслужбы готовят теракт в ходе несанкционированного митинга в Луганске – МГБ

RT на русском
522 256 підписників

RT на русском
МВД ЛНР заявило, что украинские войска 16 апреля могут ударить по Луганску ракетой «Точка-У».

По данным ведомства, украинские спецслужбы призывают горожан собраться на митинг, после чего будет нанесён удар.

@rt_russian

MATERI_DNR
Сегодня 12:31

Нет мобилизации! Не молчим! Единственный шанс вернуть наших мужчин живыми и невредимыми – выйти 16 апреля в 12 часов на митинг в Донецке (пл. Ленина) и к администрации в других городах. Давайте требовать отмены призыва наших мужчин на передовую.

a) spread of fakes about shelling

Операция Z: Военкоры Русской Весны

‼️ Освобожденный российский военнослужащий рассказал о зверствах со стороны ВСУ

По его словам, во время допроса их избивали, приставляли пистолет к вискам и угрожали. Также националисты сказали военнопленным, что один из них лишний, и просили выбрать того, кого они убьют — сообщает iz.ru.
t.me/RVvoenkor

b) example of Telegram posts

МИД России
@MID_RF
Государственный орган (Россия)

❗ Обратили внимание на антиисторические заявления главы МИД Израиля @yairlapid, во многом объясняющие курс нынешнего Правительства Израиля на поддержку неонацистского режима в Киеве.

☝ О том, есть ли на Украине неонацисты на самом деле: vk.cc/cdeLe6

10:18 AM · 3 мая 2022 г. · Twitter Web App

84 ретвита 185 твитов с цитатами 117 отметок «Нравится»

c) example of Twitter posts

***Fig. 5.*** Posts examples

It can be seen from this that russian propaganda and disinformation gained the greatest distribution in the Telegram social network. It should be understood that this direction has an impact on both sides of the conflict. For the population of Ukraine, it is a psychological influence with the aim of increasing panic at the prospect of an armed invasion, and for the population of russia, it is a psychological influence with the aim of exacerbating enmity between the two nations.

Initially, the posts were written about russia's active military actions, where and how the strikes were carried out, which cities/villages were captured, which played a significant role in the psychological impact on the population of Ukraine, in other words, all this caused a large-scale panic, which led to the destabilization of the entire situation in the country. Further, the topics of the posts were related to the spread of fake information about enemy "labels", weapons used against Ukraine. It is worth noting that pseudo-Ukrainian Telegram news channels were also created, where disinformation was also spread. The most vulnerable population groups are residents of the temporarily occupied territories of Ukraine. There, such channels spread quickly, and the posts were about condemning the actions of the Armed Forces. That is, people were instilled with the idea that their cities were being shelled by the Armed Forces, and the russian army was saving them. There was also a trend of accusing the Armed Forces of Ukraine of shelling peaceful cities of Ukraine, after which the russian military attacked the mentioned cities in posts (Fig. 5 a) [46]. In addition, a constant theme for the posts is that the people of Ukraine are neo-Nazis and Russophobes who need to be destroyed. Below are examples of posts (Fig. 5 b, c).

Let's take a closer look and analyze the number of tasks for each social network separately: YouTube (Fig. 6), Twitter (Fig. 7), TikTok (Fig. 8), Instagram (Fig. 9), Telegram (Fig. 10), Facebook (Fig. 11).

**YouTube.** Judging by these statistics, we can conclude that there were two waves of spreading russian propaganda and disinformation on the YouTube social network. Moreover, after each wave we can see a downward trend. Since complaints about most channels have been submitted repeatedly, the performance of these tasks is quite effective. There are also difficulties with the content blocking process: not everything is blocked, it is blocked only for Ukraine, or it is limited by the age policy.

The very content of russian propaganda and disinformation, in particular the analysis of situations taking place at the front, was aimed at both sides of the conflict. The target audience was people over the age of 40. At the same time, on the part of Ukraine, on the YouTube platform, truthful information about everything that was happening was spread. It is obvious that the authorities of the russian federation were not satisfied with this, so they decided to block the platform on the territory of their country in order to continue the influence of propaganda on the russian population. As a result, they switched to RuTube — their own video hosting platform. It is worth noting that the blocking of YouTube has not become a significant obstacle, because using a VPN, it is also possible to view and download videos on this platform. From the economic side, this affected russian bloggers to a greater extent, for whom channel monetization was suspended and advertising orders decreased.

**Twitter.** There was one wave of propaganda attacks on Twitter at the start of the full-scale russian invasion. Sending complaints to those pages and posts showed results and this content was significantly reduced, from the second half of May to the first half of September there was no task to work on this social network. However, russian activity has been observed recently, so the Cyber Police Department should focus its attention during monitoring on Twitter as well, which will be discussed in the recommendations. This social network is also blocked for russia, but no one forbids the use of VPN.

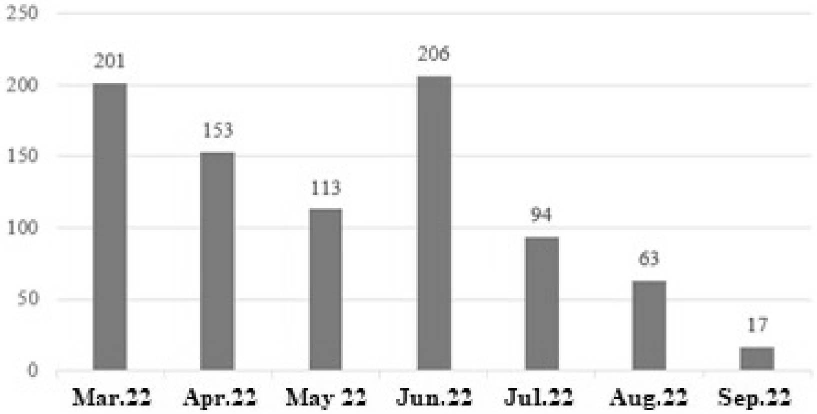


***Fig. 6.*** The number of submitted complaints (completed tasks) on YouTube channels

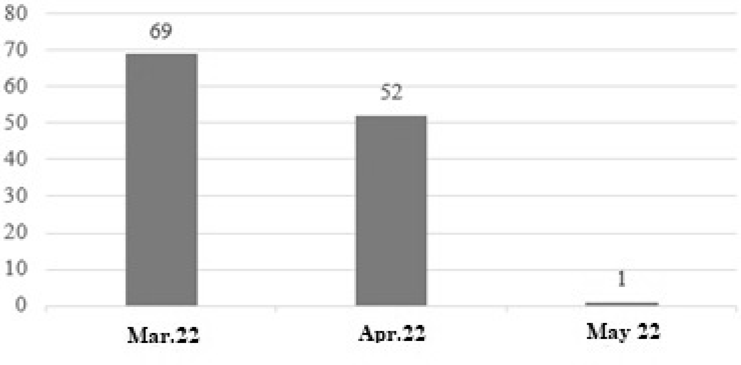


***Fig. 7.*** The number of submitted complaints (completed tasks) on Twitter pages

**TikTok.** Propaganda in TikTok began to massively appear after two months of war and is aimed mostly at young people. In general, there is a significant number of publications with aggressive enemy propaganda — false information about the invasion, the Armed Forces and Ukraine as a whole. Currently, TikTok is blocked for the russian federation, but VPN also solves this problem. As practice shows, blocking here is quite effective.

It is noted that TikTok will be "derusified". The Ministry of Digital Transformation announced that Ukraine will now be part of the European administrative region. Before that, what was happening in the Ukrainian TikTok space was monitored from the Moscow office [47].

**Instagram.** Hostile propaganda and disinformation on Instagram began to gain momentum gradually and reached its peak in June. Now this activity has declined, because all sent complaints make themselves known, so Instagram blocks such content. However, sometimes posts on such topics are not blocked globally, but only for residents of Ukraine. Instagram is also blocked for russia, but a VPN is actively used to bypass this blocking.

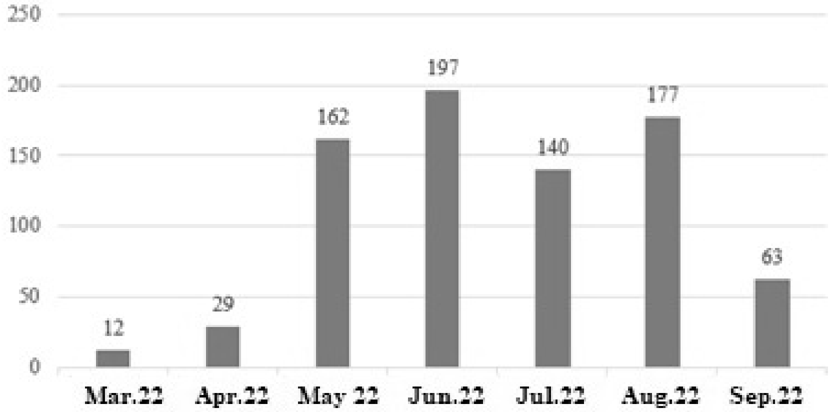


*Fig. 8.* The number of submitted complaints (completed tasks) on TikTok accounts

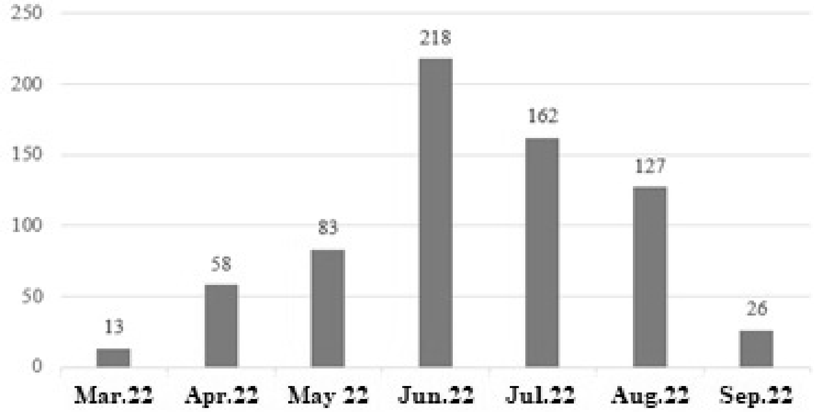


*Fig. 9.* The number of submitted complaints (completed tasks) on Instagram pages

**Telegram.** We can see that the most "active" month was March, then activity started to decline. This is related to "switching" to other social networks. There are also certain problems with blocking resources in the messenger, there is a strict policy, which results in more detailed verifications. In most cases, Telegram does not consider russian propaganda and disinformation to be dangerous for society, there are also cases of blocking them exclusively for the region of Ukraine.

**Facebook.** Again, we see that at the beginning of the war there was the greatest spread of enemy propaganda, then another wave, but much smaller in scope. In general, recently Facebook has become "cleaner" and is also blocked for the russian region, a VPN is used to bypass this blocking. However, it should be noted that there were more publications on this social network refuting hostile kremlin propaganda and disinformation.

The main indicator of the effectiveness of task performance is the number of blocked enemy information resources. With the help of the chatbot "russiaussia | Mriya" a total of 9206 resources are blocked (as of 09/19/2022). This number is growing every day, which shows the effectiveness of the entire cybervolunteer community. The number of blocked resources for each social network is shown separately in Fig. 12.

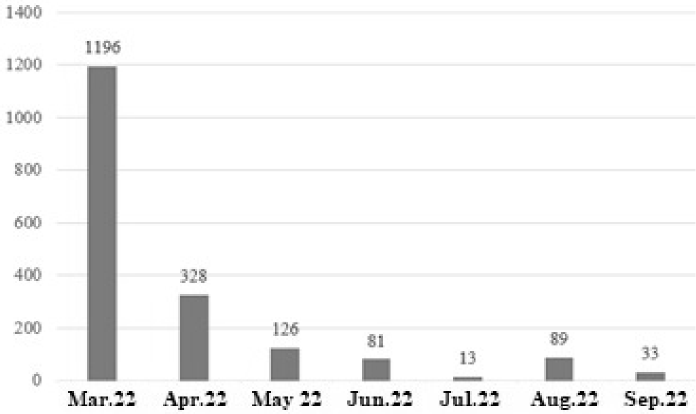


***Fig. 10.*** The number of submitted complaints (completed tasks) on channels, communities, bots in Telegram

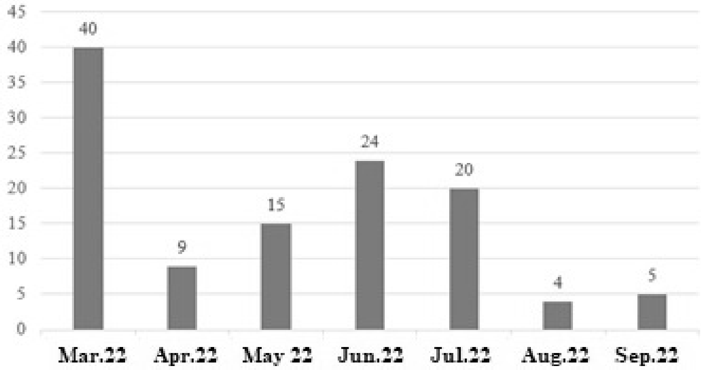


***Fig. 11.*** The number of submitted complaints (completed tasks) on Facebook pages and communities

**Writing posts in social networks.** This direction had the largest number of tasks for cybervolunteers in March, which is connected with the beginning of the war. The number of tasks gradually decreased, as evidenced by the downward trend of the histogram. The main indicator of effectiveness here is the positive reaction of the world community to posts written in social networks. In particular, there were posts on the topic of banning the issuance of visas to russians, addressed to the government officials of Latvia, the Czech Republic, Lithuania, Poland, Slovakia, Denmark, Belgium, the Netherlands, Estonia, and all of them stopped the issuance of visas [48]. There were also posts about helping Ukraine with weapons, after which the governments of some countries also provided weapons for our state. Calls by global brands to stop their business in the sian federation are also working. This is how Adidas, Apple, Dell, Cropp, Audi, IKEA and many others left the market of the aggressor countries. Wizz Air also responded to the criticism, so they are suspending the resumption of flights from Moscow to Abu Dhabi [49]. One of the recent results is that Norway suspended the simplified visa regime for russians [50]. Below are examples of written posts (Fig. 14).

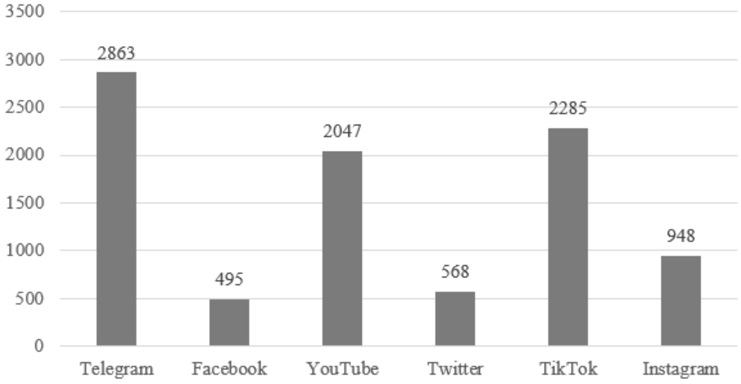


***Fig. 12.*** The number of blocked resources for each social network

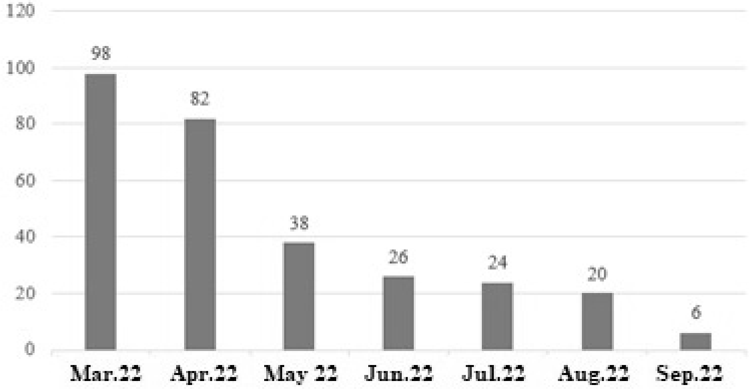
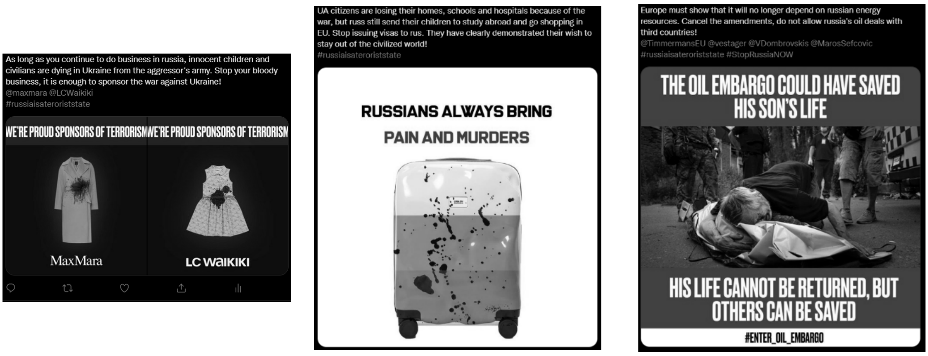


***Fig. 13.*** Number of written posts (completed tasks)



As long as you continue to do business in russia, innocent children and civilians are dying in Ukraine from the aggressor's army. Stop your bloody business, it is enough to sponsor the war against Ukraine!
@maxmara @LCWaikiki
#russiaisateroriststate

UA citizens are losing their homes, schools and hospitals because of the war, but russ still send their children to study abroad and go shopping in EU. Stop issuing visas to rus. They have clearly demonstrated their wish to stay out of the civilized world!
#russiaisateroriststate

Europe must show that it will no longer depend on russian energy resources. Cancel the amendments, do not allow russia's oil deals with third countries!
@TimmermansEU @vestager @VDombrovskis @MarosSefcovic
#russiaisateroriststate #StopRussiaNOW

WE'RE PROUD SPONSORS OF TERRORISM
WE'RE PROUD SPONSORS OF TERRORISM
MaxMara
LC WAIKIKI
RUSSIANS ALWAYS BRING
PAIN AND MURDERS
THE OIL EMBARGO COULD HAVE SAVED HIS SON'S LIFE
HIS LIFE CANNOT BE RETURNED, BUT OTHERS CAN BE SAVED
#ENTER_OIL_EMBARGO

a) appeal to MaxMara and LC Waikiki

b) regarding the suspension of visas  issuance to russians

c) #enter_oil_embargo

*Fig. 14.* Examples of posts

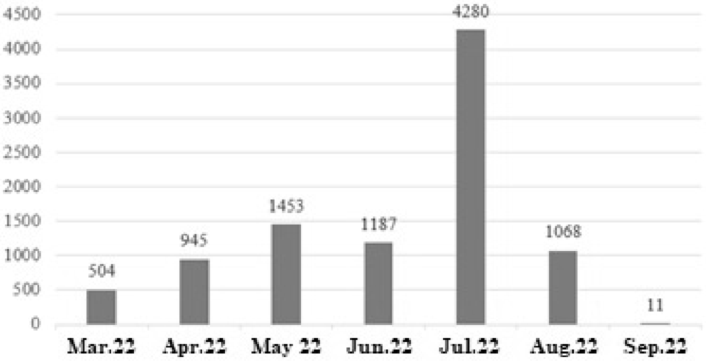
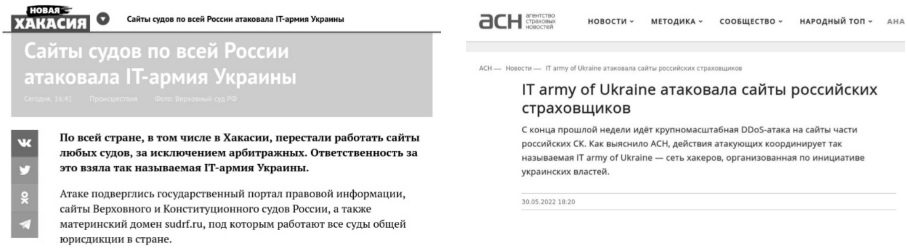


*Fig. 15.* Number of DDoS attacks on sites (completed tasks)



Сайты судов по всей России атаковала IT-армия Украины

Сайты судов по всей России атаковала IT-армия Украины

Сегодня, 16:41 Происшествия Фото: Верховный суд РФ

**По всей стране, в том числе в Хакасии, перестали работать сайты любых судов, за исключением арбитражных. Ответственность за это взяла так называемая IT-армия Украины.**

Атаке подверглись государственный портал правовой информации, сайты Верховного и Конституционного судов России, а также материнский домен sudrf.ru, под которым работают все суды общей юрисдикции в стране.

АСН — Новости — IT army of Ukraine атаковала сайты российских страховщиков

IT army of Ukraine атаковала сайты российских страховщиков

С конца прошлой недели идёт крупномасштабная DDoS-атака на сайты части российских СК. Как выяснило АСН, действия атакующих координирует так называемая IT army of Ukraine — сеть хакеров, организованная по инициативе украинских властей.

30.05.2022 18:20

*Fig. 16.* Report on the activities of the IT army of Ukraine

**DDoS attacks.** The number of DDoS attacks was the highest in July. But we note that in the spring there was a greater variety of information resources of the enemy, that is, they attacked a greater number of different sites. Over time, they began to work on individual resources and their subdomains. The work of the IT army of Ukraine initiative is quite effective, because the whole community works harmoniously. Note that even beginners can complete the tasks thanks to the provided detailed instructions. Report of this activity is given below (Fig. 16).

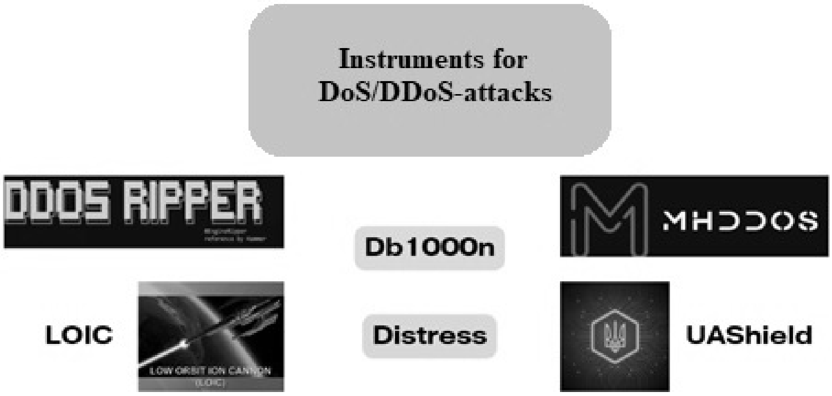


*Fig. 17.* The most used tools for DoS/DDoS attacks

The most used tools for conducting such attacks are: LOIC, MHDDoS/MHDDoS proxy, Db1000n, Distress, UAShield (Fig. 17). In general, there are a large number of different tools, the attack can be carried out with the usual "ping" command, most importantly is to carry them out synchronously.

## RECOMMENDATIONS REGARDING INFORMATION TECHNOLOGY ACTIVITIES OF THE ARMY OF UKRAINE

During the existence of the cybervolunteer army of Ukraine, its work has become quite coordinated and structured, due to which a significant advantage in cyberwarfare is achieved. However, it is possible to provide recommendations for the activities of each direction.

1. IT army of Ukraine: since this community includes not only professional cybersecurity specialists, but also volunteers, we recommend that they take already existing training courses in this direction, or create one specifically for them. This will significantly improve the performance of the entire community.
2. The "Mriya" platform: russian propaganda and disinformation activity on the social network Twitter fell between May and August 2022, but recently it has been increasing again. Therefore, we recommend that you start monitoring this social network again and publish practice tasks. It would also be worthwhile to publish more Telegram practice tasks.
3. More volunteers should be recruited in each direction. It is best to focus on young people, in particular older schoolchildren and students. We recommend holding online meetings regarding this activity in educational institutions. It is also possible to launch advertising in social networks. It is best to do this on Instagram and TikTok, because in these social networks the largest part of the entire audience is young people. In order to motivate young people to complete these tasks, from time to time raffles for thematic gifts can be carried out.
4. It is worth reviewing the number of tasks during the day and their publication. According to a poll on the Telegram channel StopRussiaChannel | MRIYA volunteers are ready for 9–10 tasks a day. However, from our own

experience, we note that the optimal number is 5–6 tasks. Taking into account that tasks are not published on Sunday, we recommend publishing 5-6 tasks on different social networks from Monday to Saturday, and 3 tasks on Sunday. Thus, the struggle on the information front will become more effective.

## CONCLUSIONS

Cyberwar has become a new challenge for all mankind. Technologies are constantly evolving and, accordingly, cyberattacks are becoming more serious and more destructive. Today we are observing a situation where entire cyber armies of volunteers are being created. The main problem is insufficient study of this issue by society.

This article examines the current situation with cyberwars in the world. As a result, the main approaches to conducting cyberwars were determined — the most frequent types of cyberattacks, their use and consequences were highlighted. Special attention is paid to the issue of the Russian-Ukrainian cyberwar and the cybervolunteer initiatives of the IT Army of Ukraine. The key areas of activity were determined and the main intermediate results were analyzed with the help of the collected statistical data. According to which, recommendations were given for greater efficiency of the entire IT of the Ukrainian army.

## REFERENCES

1. Cyber defence. NATO. URL: https://www.nato.int/cps/en/natohq/topics_78170.html
2. Cyberwar timeline. *InfoPlease*. URL: https://www.infoplease.com/world/cyberwartimeline#1980
3. 30 years ago, the world's first cyberattack set the stage for modern cybersecurity challenges. *The Conversation*. URL: https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449
4. The Age of Cyberwarfare. *Columbia Magazine*. URL: https://magazine.columbia.edu/rticle/age-cyberwarfare
5. Kaiser R. The birth of cyberwar. *Political Geography*. 2015, Vol. 46, pp. 11–20. URL: https://doi.org/10.1016/j.polgeo.2014.10.001
6. luciana aparecida santos Santos. The Georgia's Cyberwar. Academia.edu — Share research. URL: https://www.academia.edu/70338358/The_Georgia_s_Cyberwar
7. Cyber War and Ukraine. Center for Strategic and International Studies. URL: https://www.csis.org/analysis/cyber-war-and-ukraine
8. Howell K. U.S. begins cyberwar against ISIS. *The Washington Times*. URL: https://www.washingtontimes.com/news/2016/apr/6/us-begins-cyber-war-against-islamic-state/
9. Security Magazine. Security Magazine. The business magazine for security executives. URL: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
10. Wikimedia projects participants. Russian-Ukrainian cyberwarfare URL: https://en.wikipedia.org/wiki/Russian%E2%80%93Ukrainian_cyberwarfare.
11. Pakharenko G. Cyber Operations at Maidan: A First-Hand Account. Tallinn : NATO CCD COE Publications, 2015, 10p. URL: https://ccdcoe.org/uploads/2018/10/h07_CyberWarinPerspective_Pakharenko.pdf .
12. Maschmeyer L., Dunn Cavelty M. Goodbye Cyberwar: Ukraine as Reality Check. *Research Collection*. URL: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/49252/P10-3_2022-EN.pdf?sequence=2&amp;isAllowed=y
13. Pinchiuk A., Odarchenko R. Modern methods of the cyberwarfare conducting. XL Scientific and technical conference of young scientists and speciallists of G.E. Pukhov Institute of Modelling problems in energetics of the NAS of Ukraine. Proceedings of the scientific and technical confer

ence (Kyiv, 11 of May 2022 p.). G.E. Pukhov Institute of Modelling problems in energetics of the NAS of Ukraine, Kyiv, 2022, pp. 31–32

14. DDOS attacks on several Ukrainian banks and state websites on February, 15. Systems for business. URL: https://sys2biz.com.ua/news/ddos-ataka-ryadu-bankiv-ta-derzhavnyh-portaliv-ukrayiny-15-lyutogo/
15. Molodan V. "Beware and wait for worth": hackers attacked websites of Ukrainian Ministries, «Diia»-website is disconnected - Delo.ua. Ukrainian and worldwide news online – Delo.ua main business portal. URL: https://delo.ua/society/xakery-atakovali-saity-ministerstv-ukrainy-i-ostavili-poslanie-391320/
16. FEDOROV. Telegram. URL: https://t.me/zedigital/1114
17. Ukrinform. Powerful 300-thousand IT-army have been established in Ukraine – Fedorov. Ukrinform — Ukrainian and world's relevant news. URL: https://www.ukrinform.ua/rubric-technology/3490947-v-ukraini-stvorili-potuznu-300tisacnu-itarmiu-fedorov.html
18. UYkiL. Who are Anonymous and why they are helping Ukraine to defeat russia. dev.ua. URL: https://dev.ua/news/anonimus-1648044015
19. Ukrinform. Details of the Ukrtelecom cyberattack have been revealed by State Service of Special Communications and Information Protection of Ukraine. Ukrinform – recent news of world and Ukraine. URL: https://www.ukrinform.ua/rubric-technology/3450201-u-derzspeczvazku-rozpovili-podrobici-kiberataka-na-ukrtelekom.html
20. The Economical Truth. Government reports about the new cyberattack on the governmental services. The Economical Truth. URL: https://www.epravda.com.ua/news/2022/04/8/685424/
21. Pavliuk O. Russian hackers claimed the "cyberwar" to states that are support "Nazis and russophobia". URL: https://suspilne.media/239999-rosijski-hakeri-ogolosili-kibervijnu-derzavam-aki-pidtrimuut-nacistiv-i-rusofobiu/
22. Cyber Warfare. URL: https://www.imperva.com/learn/application-security/cyber-warfare/
23. Hanna K. T., Ferguson K., Rosencrance L. What is cyberwarfare?. SearchSecurity. URL: https://www.techtarget.com/searchsecurity/definition/cyberwarfare
24. StopRussia | MRIYA. StopRussia | MRIYA. URL: https://mriya.social/
25. Ukrainian Internet Army. Telegram. URL: https://t.me/ivukr/8
26. Ukrinform. Ukraine organizedly reacts on russian cyberattacks — National Security and Defense Council of Ukraine. Ukrinform – recent news of world and Ukraine. URL: https://www.ukrinform.ua/rubric-technology/3563515-ukraina-zlagodzeno-reague-na-rosijski-kiberataki-rnbo.html
27. Daniel Hughes and Andrew Colarik. The Hierarchy of Cyber War Definitions. *Pacific-Asia Workshop on Intelligence and Security Informatics*.Springer, 2017, pp.15–33.
28. Richard A. Clarke, Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. Reprint edition. New York: Ecco, 2012, p.6.
29. Merezhko O. Cyberwar and cybersecurity problems at the international policy. Juridical Journal. 2009, 6, p. 94.
30. Carr J. Inside Cyber Warfare. USA, O'Reilly, 2010.
31. Hildreth S.A. Cyberwarfare. *Congressional Research Service Report for Congress*. No. RL30735, 19 June 2001.
32. Parks R.C., Duggan D.P. Principles of Cyberwarfare. *IEEE Security & Privacy Magazine*. 2011, Vol. 9, no. 5, pp. 30–35. URL: https://doi.org/10.1109/msp.2011.138
33. Samuel Liles .Applying Traditional Military Principles to Cyber Warfare. *4th International Conference on Cyber Conflict*. NATO CCD COE Publications, Tallinn. 2012, pp. 169–178.
34. Ashraf C. Defining cyberwar: towards a definitional framework. *Defense & Security Analysis*. 2021, pp. 1–21. URL: https://doi.org/10.1080/14751798.2021.1959141 (date of access: 02.10.2022).
35. Manoj Kumar. Cyber Warfare: New Dimension in Security and Strategy. Search eLibrary: SSRN. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2915653

36. Andress J., Winterfeld S. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier Science & Technology Books, 2013, 324 p.
37. Recognizing the seven stages of a cyber-attack — DNV. DNV. URL: https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack.html
38. J. H. Choi. On cyberattack mechanisms. *International Journal of Web and Grid Services*. 2013, Vol. 9, no. 4, pp. 351. URL: https://doi.org/10.1504/ijwgs.2013.057468
39. Zeadally S., Flowers A. Cyberwar: The What, When, Why, and How [Commentary]. *IEEE Technology and Society Magazine*. 2014, Vol. 33, no. 3, pp. 14–21. URL: https://doi.org/ 10.1109/mts.2014.2345196
40. Stevens T. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*. 2012, Vol. 33, no. 1, pp. 148–170. URL: https://doi.org/10.1080/13523260.2012.659597
41. Zetter Kim.(2016). Insidethe Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired. URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
42. Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *International Journal of Computer Applications*. 2012, Volume 49– No.7, (0975–8887)
43. Neha Singh, Ravindra Kumar Purwar. SQL INJECTIONS — A HAZARD TO WEB APPLICATIONS. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2012, No. 2, pp. 42–46.
44. Fight against the enemy on the IT-front official website — IT ARMY of Ukraine. Fight against the enemy on the IT-front official website — IT ARMY of Ukraine. URL: https://itarmy.com.ua/
45. Ukraine calls for entering International Legion of Internet Army Techukraine. Techukraine. URL: https://techukraine.org/2022/03/28/ukraine-calls-for-entering-international-legion-of-internet-army/
46. Routine portion of anti-Semitism from Russia. At Viber this time. Texty.org.ua — articles and data journalism for the people. URL: https://texty.org.ua/fragments/106581/ cherhova-portsija-antysemityzmu-vid-rosiyi-tsoho-razu-u-vajberi/
47. TSN-editorship. TikTok would be derussificated, but danger remains: how russian federation spreads propaganda inside the popular network. TSN.ua. URL: https://tsn.ua/ru/exclusive/tiktok-derusificiruyut-no-opasnost-ostaetsya-kak-rf-rasprostranyaet-propagandu-v-populyarnoy-socseti-2122417.html
48. Ukrainian Internet Forces. Telegram. URL: https://t.me/ivukr/1315
49. Ukrainian Internet Forces. Telegram. URL: https://t.me/ivukr/1242
50. Ukrainian Internet Forces. Telegram. URL: https://t.me/ivukr/1351

Received 20.11.2022

ЛІТЕРАТУРА

1. Кібербезпека. НАТО. URL: https://www.nato.int/cps/en/natohq/topics_78170.html
2. Cyberwar timeline. InfoPlease. URL: https://www.infoplease.com/world/cyberwartimeline#1980
3. 30 years ago, the world's first cyberattack set the stage for modern cybersecurity challenges. The Conversation. URL: https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449
4. The Age of Cyberwarfare. Columbia Magazine. URL: https://magazine.columbia.edu/article/age-cyberwarfare
5. Кайзер Р. The birth of cyberwar. Political Geography. 2015. Vol. 46. P. 11–20. URL: https://doi.org/10.1016/j.polgeo.2014.10.001
6. luciana aparecida santos Santos. The Georgia’s Cyberwar. Academia.edu — Share research. URL: https://www.academia.edu/70338358/The_Georgia_s_Cyberwar
7. Cyber War and Ukraine. Center for Strategic and International Studies. URL: https://www.csis.org/analysis/cyber-war-and-ukraine
8. Хауелл К. U.S. begins cyberwar against ISIS. The Washington Times. URL: https://www.washingtontimes.com/news/2016/apr/6/us-begins-cyber-war-against-islamic-state/

9. Security Magazine. Security Magazine | The business magazine for security executives. URL: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
10. Учасники проектів Вікімедіа. Російсько-українська кібервійна — Вікіпедія. Вікіпедія. Режим доступу: https://uk.wikipedia.org/wiki/Російсько-українська_кібервійна #Початок_конфлікту
11. Пахаренко Г. Cyber Operations at Maidan: A First-Hand Account : Книга. Tallinn : NATO CCD COE Publications, 2015. 10 с. URL: https://ccdcoe.org/uploads/2018/10/ Ch07_CyberWarinPerspective_Pakharenko.pdf .
12. Maschmeyer L., Dunn Cavelty M. Goodbye Cyberwar: Ukraine as Reality Check. Research Collection. URL: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/ 549252/PP10-3_2022-EN.pdf?sequence=2&amp;isAllowed=y
13. Пінчук А.Д., Одарченко Р.С. Сучасні підходи до проведення кібервійн. XL Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. *Матеріали наук.-техн. конф.* (Київ, 11 травня 2022 р.). Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Київ, 2022. С. 31–32
14. DDOS атака ряду банків та державних порталів України 15 лютого. Системи для бізнесу. URL: https://sys2biz.com.ua/news/ddos-ataka-ryadu-bankiv-ta-derzhavnyh-portaliv-ukrayiny-15-lyutogo/
15. Молодан В. "Бойтесь и ждите худшего": хакеры атаковали сайты министерств Украины, портал "Дія" отключен — Delo.ua. Останні новини України та світу онлайн — Головний діловий портал Delo.ua. URL: https://delo.ua/society/xakery-atakovali-saity-ministerstv-ukrainy-i-ostavili-poslanie-391320/
16. FEDOROV. Telegram. URL: https://t.me/zedigital/1114
17. Укрінформ. В Україні створили потужну 300-тисячну IT-армію — Федоров. Укрінформ — актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-technology/3490947-v-ukraini-stvorili-potuznu-300tisacnu-itarmiu-fedorov.html

18 wUYkiL. Хто такі Anonymous і чому вони допомагають Україні перемогти росію. dev.ua. URL: https://dev.ua/news/anonimus-1648044015

19. Укрінформ. У Держспецзв'язку розповіли подробиці кібератаки на Укртелеком. Укрінформ — актуальні новини України та світу. URL: https://www.ukrinform.ua/ rubric-technology/3450201-u-derzspeczvazku-rozpovili-podrobici-kiberataka-na-ukrtelekom.html
20. Економічна правда. В уряді повідомляють про нову кібератаку на держоргани. *Економічна правда*. URL: https://www.epravda.com.ua/news/2022/04/8/685424/
21. Павлюк О. Російські хакери оголосили "кібервійну" державам, які підтримують "нацистів і русофобію". URL: https://suspilne.media/239999-rosijski-hakeri-ogolosili-kibervijnu-derzavam-aki-pidtrimuut-nacistiv-i-rusofobiu/
22. Cyber Warfare. URL: https://www.imperva.com/learn/application-security/cyber-warfare/
23. Hanna K. T., Ferguson K., Rosencrance L. What is cyberwarfare?. SearchSecurity. URL: https://www.techtarget.com/searchsecurity/definition/cyberwarfare
24. StopRussia | MRIYA. StopRussia | MRIYA. URL: https://mriya.social/
25. Інтернет Війська України. Telegram. URL: https://t.me/ivukr/8
26. Ukrinform. Україна злагоджено реагує на російські кібератаки — РНБО. Укрінформ — актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-technology/3563515-ukraina-zlagodzeno-reague-na-rosijski-kiberataki-rnbo.html
27. Daniel Hughes and Andrew Colarik. The Hierarchy of Cyber War Definitions. *Pacific-Asia Workshop on Intelligence and Security Informatics.* Springer, 2017. С. 15–33.
28. Richard A. Clarke, Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. Reprint edition. New York: Ecco, 2012. 6 с.
29. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві. Юридичний журнал. 2009. (6). 94 с.
30. Carr J. Inside Cyber Warfare. США, O'Reilly, 2010 рік.
31. Hildreth S.A. Cyberwarfare. *Congressional Research Service Report for Congress*. 2001. No. RL30735.

32. Parks R. C., Duggan D. P. Principles of Cyberwarfare. *IEEE Security & Privacy Magazine*. 2011. Vol. 9, no. 5. P. 30–35. URL: https://doi.org/10.1109/msp.2011.138
33. Samuel Liles. Applying Traditional Military Principles to Cyber Warfare. *4th International Conference on Cyber Conflict*. NATO CCD COE Publications, Tallinn. 2012. P. 169–178.
34. Ashraf C. Defining cyberwar: towards a definitional framework. Defense & Security Analysis. 2021. P. 1–21. URL: https://doi.org/10.1080/14751798.2021.1959141 (Дата звернення: 02.10.2022).
35. Manoj Kumar. Cyber Warfare: New Dimension in Security and Strategy. Search eLibrary: SSRN. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2915653
36. Andress J., Winterfeld S. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier Science & Technology Books, 2013. 324 p.
37. Recognizing the seven stages of a cyber-attack — DNV. DNV. URL: https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack.html
38. J. H. Choi. On cyberattack mechanisms. *International Journal of Web and Grid Services*. 2013. Vol. 9, №. 4. P. 351. URL: https://doi.org/10.1504/ijwgs.2013.057468
39. Zeadally S., Flowers A. Cyberwar: The What, When, Why, and How [Commentary]. *IEEE Technology and Society Magazine*. 2014. Vol. 33, №. 3. P. 14–21. URL: https://doi.org/10.1109/mts.2014.2345196
40. Stevens T. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*. 2012. Vol. 33, no. 1. P. 148–170. URL: https://doi.org/10.1080/13523260.2012.659597
41. Zetter Kim.(2016). Insidethe Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired. URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
42. Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *International Journal of Computer Applications.* 2012. Volume 49– No.7. (0975–8887)
43. Neha Singh, Ravindra Kumar Purwar. SQL INJECTIONS — A HAZARD TO WEB APPLICATIONS. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2012. No. 2. P. 42–46.
44. Офіційний сайт боротьби проти ворога на IT-фронті — IT ARMY of Ukraine. Офіційний сайт боротьби проти ворога на IT-фронті — IT ARMY of Ukraine. URL: https://itarmy.com.ua/
45. Ukraine calls for entering International Legion of Internet Army · Techukraine. Techukraine. URL: https://techukraine.org/2022/03/28/ukraine-calls-for-entering-international-legion-of-internet-army/
46. Чергова порція антисемітизму від Росії. Цього разу — у вайбері. Texty.org.ua — статті та журналістика даних для людей — Тексти.org.ua. URL: https://texty.org.ua/fragments/106581/cherhova-portsija-antysemityzmu-vid-rosiyi-tsoho-razu-u-vajberi/
47. Редакция ТСН. TikTok дерусифицируют, но опасность остается: как РФ распространяет пропаганду в популярной соцсети. ТСН.ua. URL: https://tsn.ua/ru/exclusive/tiktok-derusificiruyut-no-opasnost-ostaetsya-kak-rf-rasprostranyaet-propagandu-v-populyarnoy-socseti-2122417.html
48. Інтернет Війська України. Telegram. URL: https://t.me/ivukr/1315
49. Інтернет Війська України. Telegram. URL: https://t.me/ivukr/1242
50. Інтернет Війська України. Telegram. URL: https://t.me/ivukr/1351

Отримано 20.11.2022

*Одарченко Р.С.*[1], д-р. техн. наук, професор,
зав. каф. телекомунікаційних та радіоелектронних систем
https://orcid.org/0000-0002-7130-1375, e-mail: odarchenko.r.s@ukr.net
*Бондар С.О.*[2],
в.о. зав. відділу інтелектуального керування
https://orcid.org/0000-0003-4140-7985, e-mail: seriybrm@gmail.com
*Сімахін В.М.*[2], аспірант,
науковий співробітник відділу інтелектуального керування
https://orcid.org/0000-0003-4497-0925, e-mail: thevladsima@gmail.com
*Пінчук А.Д.*[1], студентка
https://orcid.org/0000-0003-3567-0445, e-mail: pinchuk.ad87@gmail.com
*Самойленко В.В.*[1], студент
e-mail: vladss1954@gmail.com
*Станко П.О.*[3], к-т. техн. наук,
доцент кафедри інформаційних технологій
https://orcid.org/0000-0001-5794-3593 e-mail: p_stanko@ukr.net

[1] Національний авіаційний університет,
1, просп. Любомира Гузара, 03058, Київ, Україна
[2] Міжнародний науково-навчальний центр інформаційних технологій
та систем НАН України та МОН України,
40, просп. Академіка Глушкова, 03187, Київ, Україна
[3] Університет новітніх технологій,
5А, вул. Метробудівська, 03065, Київ, Україна

# ДОСЛІДЖЕННЯ ОСНОВНИХ ЗАСОБІВ ТА ПРОМІЖНИХ РЕЗУЛЬТАТІВ РОСІЙСЬКО-УКРАЇНСЬКОЇ КІБЕРВІЙНИ: КІБЕРВОЛОНТЕРСЬКІ ІНІЦІАТИВИ

***Вступ.*** *У цій дослідницькій статті розглядається поточний стан кібервійн у світі. Обговорено проблематику з визначенням терміну «кібервійна». Розглянуто історичний початок російсько-української кібервійни, її перебіг та поточний стан, а також досліджено основні засоби її ведення. Визначено, що ця кібервійна стала першим у світі випадком повномасштабної світової кібервійни. Основну увагу приділено кіберволонтерській армії інформаційних технологій України, яка з'явилася в ході цієї кібервійни та веде успішну боротьбу з російською федерацією (рф) на кіберфронті.*

***Мета статті.*** *Показати процес ведення реальної кібервійни сьогодення, використання засобів її ведення та провести дослідження її проміжних результатів; на прикладі України показати ефективність та результативність роботи кіберволонтерських ініціатив.*

***Результати.*** *Проведено аналіз основних наявних підходів до ведення кібервійни та визначено типи кібератак, які найчастіше мають своє застосування. Визначено, на яких напрямах та засобах ведення кіберійни акцентує увагу рф. Досліджено діяльність IT війська України, визначено ключові напрями роботи та наведено їх детальну класифікацію. В ході дослідження було визначено основні показники ефективності діяльності кібервійська України та зібрано статистичні дані про роботу за ключовими напрямами, на основі яких було проаналізовано ефективність, результативність та проблеми, які виникають під час боротьби на кіберфронті.*

***Висновки.*** *Вперше детально розглянуто процес ведення російсько-української кібервійни, з акцентом на діяльність кіберволонтерських ініціатив України. Визначення ключових напрямів їх діяльності дало змогу дослідити ефективність та визначити проміжні результати цієї кібервійни. Проаналізувавши всі дані, було надано рекомендації для покращення ефективності та результативності в боротьбі на кіберфронті.*

***Ключові слова:*** *кіберфронт, кібервійна, підходи до проведення кібервійн, кіберзброя, російсько-українська кібервійна, кіберволонтерські ініціативи, IT армія України.*