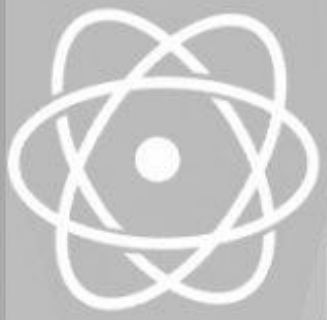


SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

Vol6 No3
September 2022

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 1-12 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

METHODS OF PREPARING AND CONDUCTING MODERN HYBRID WARS.

Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv, Ukraine
Volodymyr Artemov, National Aviation University, Doctor of pedagogical sciences, Professor, Kiev, Ukraine
Mykola Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor, Kyiv, Ukraine
Yulia Khokhlachova, National Aviation University of Kiev, PhD in Technical Sciences, Associate Professor Kiev, Ukraine
Tyna Pirtskhalava, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ABSTRACT: The analysis of the conduct of wars and armed conflicts shows that confrontation in the military sphere is increasingly moving into the verbal, i.e. informational space. Information warfare implements asymmetric solutions and involves special measures. Destructive influence on the object is also achieved by carrying out informational and psychological operations directed against a person, a group, society and the state and affect their moral and emotional stability, as well as decision-making motives. Such influence is achieved through modern electronic means of communication and mass information. Based on the example of Ukrainian-Russian relations, the article examines the goals of information and psychological warfare, as well as the methods and models of influence used today.

KEYWORDS: *information warfare, information confrontation, disinformation, psychological impact, information attack*

Introduction

The modern world is characterized by systemic instability, imbalance and chaos. Qualitatively new dangers and threats of a global scale were added to the challenges and threats of the "Cold War" era. Almost all military conflicts of the late 20th and early 21st centuries did not develop and proceed according to the classical schemes of military art. Military actions in the East of Ukraine and the analysis of the situation preceding these events allowed us to conclude that Ukraine was faced with a sophisticated form of war, in which informational aggression via informational influence takes place before the capture of territories.

The analysis of the conduct of local wars and armed conflicts shows that confrontation in the military sphere is increasingly moving into the verbal, i.e. informational space [1-4]. Information warfare implements asymmetric solutions and involves special measures. Destructive impact on the object is also achieved by conducting informational and psychological operations (IPO), which are directed against a person, group, society and the state and affect their moral stability, emotions and decision-making motives.

Modern war (hybrid war) is increasingly becoming a war to defeat and destroy the enemy's consciousness and consolidate the consciousness of the population of one's own state. Ukraine, unfortunately, became an example of such a situation. It is the object of a well-organized and planned information war on the part of the Russian Federation. Therefore, the issue of identifying and counteracting the informational-psychological impact (IPI) on the object (person, group, society and state) is relevant right now.

It should be taken into account that even before the full-scale invasion of Ukraine, Russia tried to occupy the Ukrainian information space and did everything to distort information about the European Union, about the European integration and NATO, in order to bombard Ukrainians with false historical facts about Ukraine and Russia. In fact, it uses the Ukrainian space to divide society and

implement the Kremlin's plans for Ukraine, namely political and cultural expansion. At the same time, the Kremlin used such methods as follows [5,6]:

- imposition of opinions about the inability of the current military-political leadership of Ukraine to manage the country and make rational decisions, which leads to unjustified casualties among the forces of the operation of the joint forces;
- creation of the idea that business interests are more important for the Ukrainian elite than the interests of the state and events in the East;
- dissemination of the views that the Ukrainian armed forces in the East of Ukraine are demoralized and unable to conduct combat operations, and their personnel do not trust the military leadership;
- imposition of the idea that that Ukraine cannot survive without Russia, its economic and industrial potential;
- support for the topic of Malaysian Boeing with the accusation of Ukraine in concealing the facts, shelling by the forces of the combined forces operation of the area of the airplane accident.

The target audience of the Kremlin's IPI was the internal population of Russia and Russian-speaking diasporas abroad, the population of Ukraine (including the audience of the occupied regions of Donbas and Crimea), the audience of Western countries, and the audience of states close to Russia in terms of political views.

Therefore, it is very important to take into account Russia's intentions and its information potential, which consists of very powerful mass media.

In addition, the authors remind the readers that the history of relations between Ukraine and Russia is a history of a constant struggle, which has been going on for many centuries. For Ukraine it is a matter of protecting its independence, whereas for Russia it is a matter of making slaves of Ukrainians

Main part

In the era of globalization processes, the mass media confidently occupied a prominent place among the means of communication. Globalization itself is a phenomenon, which would not be possible without the activity of modern electronic means of communication and mass media that cover the entire planet.

Mass media play almost the most important role in the modern political life of most states. They act as the main subject of forming public opinion in society about events and phenomena occurring in the world and in every country. At the same time, a reverse pattern can be observed: the more developed the information network of the state is, the fewer opportunities remain for using information for the benefit of any one entity, and vice versa - with a less developed network, there are more opportunities for its monopolization and the provision of information in a distorted or incomplete form.

Now everyone understands that we live in the information sphere and we will never escape from it.

It is safe to say that in such a short period of time, the process of reprogramming society took place very quickly.

Before, certain difficulties could have been experienced, inasmuch as it was necessary to somehow convey information to a person, as people did not always understand it. Today, by connecting to the Internet, you can get any information. The web helps translate any text you have into any language.

It should be noted that information and psychological warfare is not an action of today. Many methods of information warfare arose thousands of years ago with the emergence of information systems - the history of human learning, this is a kind of constant information warfare.

It should be noted that the main goals of informational and psychological warfare (IPsW), which includes IPO and IPI, are:

- ensuring decision-making and prompting the authorities of the victim (object) country to take actions that would satisfy the needs of the aggressor country;
- undermining the legitimacy of the political power and international authority of the victim country;
- destabilization of the situation in the victim country, provoking political protests, social conflicts, undermining the moral and psychological state of the population of the victim country;
- undermining the defense capability of the victim country and the combat capability of its armed forces;
- supporting the actions of internal forces aimed at destroying or harming their state, including by corrupting the authorities and political elite;
- replacement of the socio-cultural identity of the entire population or part of it in the victim country, altering the national values and foundations of state formation.

At the same time, active participants in these actions are the military and political leadership of the Russian Federation, its armed forces and special services, as well as pro-Russian forces of Ukrainian society and pro-Russian political figures of some countries of the world.

A full range of communication channels are used to achieve important goals: mass media (electronic and printed), television, the Internet, and social networks. At the same time, all methods and means of IPI and IPO are used.

IPI has two methods of influence [7,8]: law and speech. The influence of the word is not in the victorious use of weapons and in terrorist acts. The word itself shows that this type of influence is a painful phenomenon, exciting, thrilling, and affecting the nerves of the people. Nevertheless, IPI should be considered one of the main means of hybrid warfare: offensive propaganda helps to weaken the enemy, defensive propaganda strengthens the morale of the country that has become the object of the attack.

It should also be taken into account that the sources of information danger can be natural (objective) and intentional.

When considering the theory of IPI in the political sphere, it should be taken into account that the danger occurs at the strategic, operational and tactical levels.

Basically, the political elite should act at the strategic level, and the information units of the political clan - at the operational and tactical levels.

According to experts, IPsW consists of actions taken with the aim of achieving information advantage in providing national, military, strategic and political ways of influencing the information and information systems of the enemy while simultaneously strengthening and protecting one's own information and information systems and infrastructure.

Further development of hybrid warfare with the advent of cyberspace was developed in the form of cyber warfare and IPsW.

Conceptual questions and foundations of the theory of the network -centric system of management and organization of combat operations and cyber operations and the actual consideration of military operations and their organization from the standpoint of military cybernetics were formulated for the first time by N.V. Ocharkov (1977-1984 chief of the General Staff of the USSR Armed Forces) in the late 1970s and early 1980s of the 20th century.

Consecutive, typical component stages of a hybrid war were defined in this concept as follows:

– innovative aggression (cyber war, economic pressure, information and psychological attacks, etc.);

– the use of irregular armed formations or private armies (separatist movement, Cossacks, self-defense);

– official military action or show of force (identified uniforms, weapons, official identification of participation in the conflict).

The IPO of the Russian Federation in Crimea was planned according to Ocharkov 's concept and the system model of the enemy based on Warden 's theory. The basis of this theory is the concept of "centers of gravity". An object with a critical cybernetic infrastructure ("center of gravity" according to Warden) is the point where the object or subject of influence is most vulnerable. According to this theory, if we consider the object or a subject of influence as a system with a critical cybernetic infrastructure, it can be presented as a system consisting of five rings (Fig. 1) [7, 10].

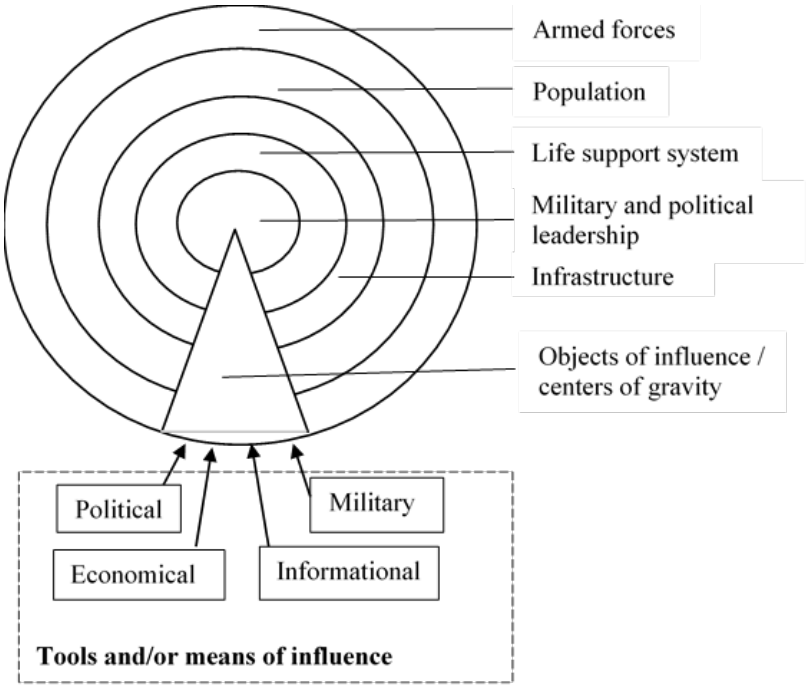


Fig. 1. The influence model is built according to Warden 's theory.

At the heart of Warden 's model is the military-political leadership and national leaders, who form a critical component in the architecture of the national security system and the system and are protected by the other four rings. Thus, the second ring is the life support system, production, electric and nuclear plants, enterprises of various purposes, oil supply plants, banks, which during the war are vital for ensuring the functioning of the military-industrial complex.

State infrastructure - highways, railways, power lines - create the third ring.

The fourth ring is the population (society), and the fifth outer ring stands for the armed forces.

This model implements the "war from the inside - outside" scheme. It should be taken into account that Warden's model works well in conflict zones, when the armed forces are considered by the local population as an external aggressor.

In contrast to this model, Russia for a long time had the support of the local population and significant military formations of the Black Sea Fleet on the territory of the Autonomous Republic of Crimea, which were not perceived by it as an aggressor or enemy (Fig. 2) [7]

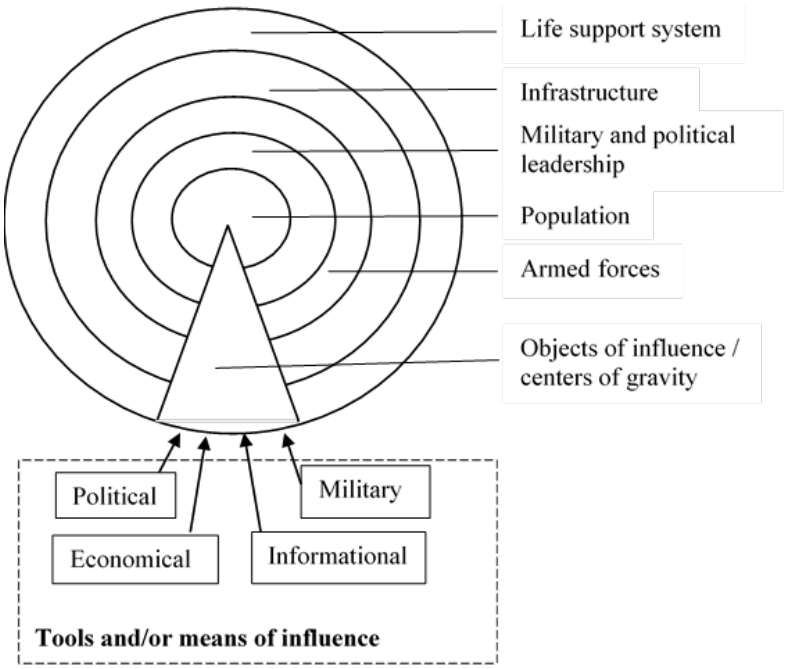


Fig. 2. The influence model used by Russia in Crimea

Russia exerted a long-term, planned and intended influence on the population of the Republic of Crimea with the aim of perceiving the servicemen of the Russian Federation as defenders of the population and correcting the "historical mistake" regarding the accession of Crimea to Ukraine in 1954. With the beginning of the Revolution of Dignity, a powerful influence on the leadership of Crimea and the city of Sevastopol began, and along with this, a massive influence on the personnel of the Armed Forces of Ukraine. It should be taken into account that the IPI of the Armed Forces of Ukraine was carried out constantly, for example, the housing issue of Russian servicemen was resolved, and the material support of Russians was an order of magnitude higher than that of Ukrainian servicemen. In addition, every second resident of Sevastopol was connected with the Russian Black Sea Fleet. 24,000 military personnel permanently lived in the city. The military and the Black Sea fleet for Sevastopol are enterprises, work, wages, social infrastructure. The fleet seemed to grow into the city. Therefore, the introduction of the Russian armed forces into Crimea and Sevastopol went without opposition and had the signs of a prepared and planned IPO, aimed primarily at Russians and, on the other hand, at Ukrainian and Western communities. At the same time, the main objects of the transport infrastructure, life support systems and military objects of the Armed Forces of Ukraine were first taken under control.

The annexation of Crimea showed that it was a well-planned and organized operation. It should be noted that pro-Russian organizations in the Republic of Crimea have been used as the 5th column of

the Kremlin in Crimea for years. They were financed by the Russian government, and their leaders were agents of influence of the Russian special services and actively conducted anti-Ukrainian activities.

All this created comfortable conditions for Russian information and propaganda activities. On the territory of Crimea, television channels and radio broadcasts of Russian channels were rebroadcast by Crimean television and radio channels, and Ukrainian versions of Russian newspapers were distributed among the residents of Crimea.

Through the mass media of the Russian Black Sea Fleet, the Russian side continued to actively influence the information space of the Republic of Crimea. Under the guise of defending the interests of the Russian-speaking population of the region, the naval mass media organized an information company aimed at shaping the image of Russia as the only reliable guarantor of stability in the region. The capabilities of the fleet's information support bodies were widely used for the distribution of relevant materials. With the active support of the Russian Black Sea Fleet, Moscow administration created the most powerful urban cable network in Sevastopol.

Numerous Russian figures actively spoke in the pro-Russian mass media: political scholars, philosophers, religious preachers, who conveyed relevant ideological references.

The Russian Orthodox Church and its controlled Ukrainian Orthodox Church of the Moscow Patriarchate, as well as various brotherhoods of the Ukrainian Orthodox Church of the Moscow Patriarchate, were actively involved in inciting the ideas of autonomism, separatism and Russian chauvinism.

For many years, Russia conducted subversive activities in Crimea and carried out anti-Ukrainian propaganda. Moreover, almost all pro-Russian organizations in Crimea cooperated with various special services of Russia. The Main Intelligence Department of the General Staff of the Ministry of Defense and the intelligence units of the Black Sea Fleet, the Foreign Intelligence Service of Russia, and the Federal Security Service of Russia had the greatest influence on the socio-political situation in Crimea.

The tactics of the hybrid war used by Russia in Crimea were also used in the East of Ukraine with some changes (Fig. 3) [5]. Thus, the main influence was concentrated on the population of Donbas. The next objects of IPI were state infrastructure and the life support system. The fourth and fifth rings of influence became the Armed Forces and the military and political leadership of Ukraine.

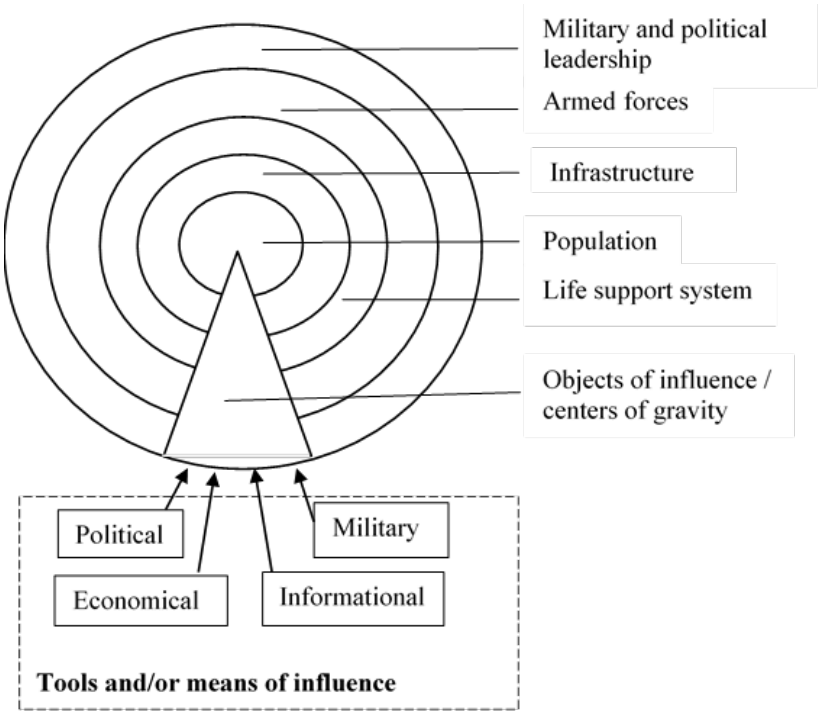


Fig. 3. The influence model used by Russia in Donbas

A feature of Russia's IPO in Donbass and Ukraine was and is the constant search and use of relevant information sources capable of forming the necessary public opinion. At the same time, the main influence was exerted on the spheres of revision of the history of Ukraine and Russia and inter-confessional relations.

To solve these problems, Russia used the methods as follow: [11,12]:

1) groups of special journalists (3-4 people), who have clear instructions on how to cover events in the East of Ukraine and work directly for Russian information channels;
2) operative groups of psychological operations, which numbered 2-4 people and performed the following tasks on the territory of the occupied Donbass:

– oral propaganda, including work with the local population;

– dissemination of propaganda literature and other information;

– creation of local propaganda groups in annexed settlements, organization and coordination of their actions;

– favoring the work of the Russian mass media, gathering information and identifying the most pressing problems of the population in order to use this as an informational opportunity;

– monitoring the current moral and psychological state of the local population.

3) psychological operations unit, located near Rostov-on-Don together with the command post of the intelligence center of the Main Intelligence Directorate of the General Directorate of the Armed Forces of Russia.
Its tasks are as follows [3]:

● collection, processing and analysis of information regarding the current moral and psychological state of the population of Ukraine and units of terrorist and military formations;

● management of units of psychological operations performing special tasks with IPI;

- development and implementation of IPO on the territory of Ukraine;
- the use of agents of subversive psychological work in unoccupied regions of Ukraine, who will perform the following assignments:
  - to create sabotage and propaganda groups in unoccupied regions of Ukraine:
  - train local groups to conduct subversive propaganda campaigns;
  - to provide groups with the necessary material and technical property;
  - direct holding of rallies, protest actions and distribution of propaganda materials.

The information situation in Ukraine worsened after the tragedy with the Malaysian Boeing. It was during this period that the Ukrainian media space was able to create a rather powerful information barrier to Russian propaganda. The Kremlin tried to create an informational noise with a huge number of versions around the liner disaster in order to distract the attention of the audience from the real causes of the tragedy and to find the most plausible option for Russia. However, Ukraine has won in this information struggle.

The hybrid war has reached a new level. Information influences are applied more powerfully and purposefully. Thus, Belarus under the leadership of Russia conducted an information operation in the countries of the Middle East (Syria, Iraq, Afghanistan) to attract residents of these countries (mainly Kurds) to "employment" in Germany. The migration crisis on the border of Belarus with the EU countries actually began in 2021, after Lukashenko promised to loosen controls abroad for migrants due to EU sanctions against his regime.

Thus, Poland, Lithuania and Latvia faced a large increase in the number of migrants from Belarus. Belarusian travel agencies issued illegal migrants from the countries of the Middle East with visas for entering Belarus, travel permits, and provided them with plane tickets for a flight to Minsk. Migrants were transported to the borders with the European Union in an organized manner by Belarusian security forces. Thus, with the hands of Lukashenka, Moscow tried to destabilize the situation in the EU and provoke a new migration crisis. At the same time, the mass media of Belarus and Russia carried out directed propaganda about the inhumane treatment of Polish border guards towards migrants.

In November 2021, the situation worsened, when migrants without permission to enter Europe tried several times to break through to Poland from the territory of Belarus.

Numerous investigations confirm that migrants were purposefully invited to Belarus with the support of the Minsk authorities, although Minsk denies this. According to the estimates of the special services of Germany, 800-1000 migrants arrived in Minsk every day. At the same time, Lukashenko said that he will not protect Europe from the molasses of illegal migrants. In turn, the Belarusian Ministry of Defense threatened to involve Russian troops in "ensuring the country's security".

At the same time, it should be noted that Putin is ready for the escalation of the so-called hybrid conflict - a combination of military and other means for the purpose of destabilization, in particular, in the use of humanitarian crises, similar to the situation on the Polish-Belarusian border.

This migration crisis, along with hacker attacks and Russia's ultimatum regarding their security, has greatly strained relations between the West and Russia.

The activity of Russian special services and propagandists in social networks, at least in Ukraine, has long been known. The "trolls" hired by them began their active work during Euromaidan in 2014. After the seizure of Crimea and the outbreak of the war in Donbas, which has been going on for eight years, they waged an active and powerful information war against Ukraine, and since 2020, the IPI and IPO have increased.

Russia 's cyber war became the escalation of the situation around Ukraine with the accumulation of troops near the Ukrainian borders and the threat of further escalation of aggression. The accumulation of Russian troops near the Ukrainian borders has become an element of blackmailing the world community and putting pressure on it in order to fulfill all the Kremlin's demands. At the same time, the Russian Federation and its mass media declared on all state channels that it was in danger and that all states and NATO personally wanted to attack it. Therefore, it is unclear what kind of danger Russia can be in when the federation itself is the aggressor and attacker.

And on February 24, 2022, Putin launched a special operation against Ukraine, that is, a large-scale aggression against a sovereign state. It should be pointed out that the information war reached a new level. The mass media, as the mouthpiece of the aggressor, focused on the following topics: the defense of the LNR and the DPR from the attack of Ukraine, the de-Nazification and demilitarization of Ukrainian society, namely the protection of the Russian-speaking population.

On the night of February 23 to 24, Russian hacker groups (ART 28, ART 29, Vermin, Sandworm and others) carried out a number of powerful cyber attacks on the websites of state institutions and mass media of Ukraine. These actions echo the actions of Russia, the aggressor in the war with Georgia in 2008, [3] when they carried out cyber attacks on Georgian state websites. But Ukraine's cyber defense worked powerfully, which made it possible to protect most websites and, first of all, mass media.

According to the Russian plans announced by their mass media, they were supposed to capture Kyiv in twelve hours, and completely occupy Ukraine in ninety-six hours. But these plans failed.

Therefore, the Russian mass media began to manipulate the population of Ukraine and the world community that their plans are the liberation of Luhansk and Donetsk regions in full and the creation of the Kherson People's Republic. At the same time, Russian "mouthpieces" falsely cover the situation at the front. They are engaged in praising the Russian military, which inflicts only pinpoint strikes on military targets. And not a word about the bombing of civilian objects and shootings of the civilian population (elderly people, women and children).

They are silent about the fact that the army has a direct instruction regarding the genocide of Ukrainian citizens (Bucha, Irpin, Makariv and other cities). In addition, they abuse and torture the population of the eastern regions, which have been captured and where hostilities are taking place, and are mostly Russian-speaking. Therefore, the thesis about the protection of the Russian-speaking population from the so-called nationalists remains unclear.

Moreover, Russian mass media compromise and discredit themselves. For example, they showed on television how they prepared a mannequin for filming and declared that it was preparation for the falsification of the events in Bucha. However, the film worker, who participated in shooting the film, claimed that it was preparation for the filming of a Russian TV series, where this mannequin was supposed to be thrown from a high-rise building. And this is a repeated situation.

And what can be said about the statement of the Russian media regarding the creation of American biological laboratories in Ukraine, which develop various viruses, and also developed Covid -19 and where the pandemic spread from?

In addition, the Russian mass media put a lot of fakes on the Internet, which the Russians themselves refute. And what are the statements of their television "mouthpieces" about nationalists, humiliating the Russian-speaking population and other lies, that the Russian army does not have a direct order to shoot Ukrainian civilians and that only Ukrainian nationalists do it. At the same time, the " telekillers " of federal Russian TV channels are brainwashing the population of Russia and zombifying their citizens about the tasks of the war in Ukraine. Kremlin propagandists accuse Ukraine of all mortal sins and more acutely present the image of Ukraine as an aggressor and a Banderiv - fascist entity. In our opinion, this is an IPO and IPO against the citizens of Russia and the world society.

Taking into account the methods and means that should be carried out primarily by the anti-IPI units of Ukraine during the period of hostilities on the territory of the state, it should be noted:

– generating content and counter -information operations that will work for the unification of Ukrainians,

– carrying out a quality check of this information and combating fakes,

– campaigning and propaganda that would highlight the real intentions of the aggressor,

– clarification of the goals of foreign policy and actions to establish peace in Ukraine,

– informing the world community, influential foreign, political, governmental, business and cultural circles, as well as foreign media about actions to establish peace and end the war in Ukraine,

– discrediting the military and political leadership of Russia.

In today's environment, it is very important to study and take into account the mental state, political attitudes of society. Research of public opinion makes it possible to take into account not only the moods that lie on the surface, but also the hidden psychological tendencies of political processes, and accordingly choose such measures that would be adequate to the situation that has arisen. Knowing the state and dynamics of public opinion means fulfilling the basic requirement that is necessary for making the right political decision. [thirteen]

Public relations play an important role in society. Initially, mass media were created to inform the public about key events in the life of the country and power structures, and they gradually began to perform another equally important function - influencing the consciousness of their audience in order to form a certain attitude to the facts, phenomena and reality that are reported. This influence is carried out with the help of methods of propaganda and propaganda agitation developed over more than one thousand years. [14]

To achieve the influence of mass media on modern opinion, people actively use them to satisfy their needs. Therefore, mass media is very versatile and is expressed in [14]:

– informativeness of the public;

– instructions to society, determination of society's behavior;

The results of media influence can be:

– changes in society's behavior;

– changes in society (because behavior and instructions cannot be equated);

– changes in society's knowledge as a consequence of its simple informativeness.

It should be noted that mass media have a great influence on society as a whole and on an individual person.

The influence of mass media can be short-term and long-term. The reaction to a specific message, news, event is fleeting. The complex and constant influence of various channels of information affects the deep layers of public and human consciousness.

Global mass media form a universal, global system of values. For a developing society, building, maintaining and protecting a symbolic system is one of the main tasks. If the symbolic system is destroyed, then the society drastically changes the traditional patterns of behavior, which can have unpredictable consequences. Symbols that form a society into a nation and a people may be under threat.

Destructive influence on the existing system of values in society is carried out primarily thanks to information and mass media as universal channels of its transmission, it can be stated that mass media are not just subjects of influence on mass consciousness, but also a tool through which it is directly

formed. Mass media create their own reality by forming new myths and stereotypes, often detached from life. At the same time, since such a reality is perceived by millions and even billions of consumers at the same time, it becomes the one that deserves trust [14,15]

So, we can distinguish three main channels of mass communication: television and the Internet, radio and the press. Each of the mentioned types of mass media has its own characteristics that determine the success of its influence on the audience.

First of all, mass media cannot be considered as equally effective tools of information dissemination. Radio, television (Internet) and the press answer three fundamentally different questions and, accordingly, each of them covers its own aspect of a certain event. The radio answers the questions: "What?", "What happened?". Television and the Internet provide an answer to the questions "How?", "How did the thing that the radio already reported happen?" The press explains: "Why?", "Why did exactly what the radio talked about and how it was shown on television and the Internet happen?" Such is the objective "division of labor" between the main communication channels. And only a systematic approach, based on three complementary answers, can give a comprehensive picture of what really has happened.

Conclusions

Currently the information war between Ukraine and Russia has reached its peak, while it should be taken into account that a full-scale war is going on. Everything that appears in the mass media, in social networks, in Russian information resources, must be carefully studied, analyzed and filtered. In the age of the Internet, it is simply impossible to completely secret certain actions. The information policy of any state should be such that there is no underestimation of the possibilities of informational and psychological weapons, and measures to counter influences that would satisfy the aggressor.

REFERENCE

1. Manoilo A.V. Non-force resolution technologies contemporary conflicts /A.V . _ Manoilo - M : Hotline-Telecom, 2008-392p.

2. Panaryn N.N. Technology of information warfare/N.N. Panarin-M: Izd. Security world, 2003-320p.

3. Pirtschalava L.G., Information and analytical security assurance: monograph/ L.G. Pirtschalava, V.A. Khoroshko, Yu.E. Khokhlacheva , M.E. Shelest -K: FOP Yamchinsky A.V., 2021-470p.

4. Rastorguev S.P. Information war. Problems and models/S.P. Rastorguev-M: Radio and Communication, 1999-416p.

5. Zelinsky S.A. _ Informational and psychological impact on mass consciousness/S.A. Zelinsky - M: Izd "Algorithm", 2000-464p.

6. Leontieva A.S. Propaganda as an informational and psychological component of political processes / A.S. Leontiev - Lviv: LNU named after I. Franka, 2004-296p.

7. Pevtsov G.V. Information and psychological operations of the Russian Federation in Ukraine: models of influence and directions of countermeasures/G.V. Pevtsov, S.V. Zalkin S.O. Sidchenko , K.I. Khudarkovskii // Science and Defense, No. 2, 2015.-p.28-32

8. Bukharin S.N. Methods and technologies informational wars / S.N. Bukharin - M: Academic project, 2007-382p.

9. Balanyuk Yu.V. Informational and psychological influences in cyberspace/Y.V. Balanyuk, V.V. Kozlovskyi, V.O. Khoroshko, Yu.E. Khokhlacheva -K: CP " Comprint " 2020-109 p.

10. Hryschuk R.V. Fundamentals of cyber security/R.V. Hryshchuk, Yu.G. Danyk - Zhytomyr: ZhNAEU, 2016-636p.

11. Buriachok V.L. Information and cyberspace: security problems, methods and means of combating/V.L. Buryachok, H.M. Gulak, V.B. Tolubko -K: LLC "SIK GROUP UKRAINE", 2015-449p.

12. Artemov V. Lytvynenko O., Khoroshko V. , Brailovskyi M. Information War in Modern Conditions. Part 2. // SPCSJ v 5, #3, 2021. - p 11-24

13. Chaldin R. Psychology of influence/R. Chaldin St. Petersburg: Peter, 2016-336p.

14. M. I. Prokofiev. Information war as a form of information warfare, part 1. / M. I. Prokofiev, L. M. Skachek , V.O. Khoroshko // Legal normative and metrological support of the information protection system in Ukraine, Issue 1 (37), 2019.-p.7-24.

15. Artemov V, Brailovskyi N., Opirskyi I., Ivanchenko I., Khoroshko V. _ Information War in Ukraine // SPCSI , v.4 , No. 4, 2020- p.28-34 .

Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 13-24 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

PERFORMANCE INDICATORS OF FUNCTIONING OF THE INFORMATION PROTECTION AND CYBER SECURITY SYSTEM OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Черноног Александр Александрович, Директорат политики цифровой трансформации и информационной безопасности в сфере обороны, Министерство обороны Украины, Киев, Украина
Oleksandr Chernonoh, Directorate of digital transformation and information security policy in the field of Defense, Ministry of defense of Ukraine, Kiev, Ukraine
к.т.н., Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Candidate of Engineering Sciences, Lesya Kozbtsova, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
д.п.н., профессор Козубцов Игорь Николаевич, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Doctor of Pedagogical Sciences, Professor, Igor Kozubtsov, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., доцент Здолбицкая Нина Васильевна, Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Engineering Sciences, associate professor Nyna Zdolbytskaia, Lutsk National Technical University, Lutsk, Ukraine
к.т.н., Кошелюк Виктор Андреевич, Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Engineering Sciences, Vyktor Kosheliuk, Lutsk National Technical University, Lutsk, Ukraine
к.т.н., Штаненко Сергей Станиславович, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Candidate of Engineering Sciences, associate professor Sergei Sctanenko, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine

АННОТАЦИЯ. В научной статье решена частная научно-техническая проблема по необходимости выбора возможных показателей эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры. Научная новизна полученного результата заключается в том, что впервые предложены непротиворечивые показатели и критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры. Практическое значение работы заключается в том, что на основе полученных показателей и критериев в дальнейшей работе на их основании разработать частную методику оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

КЛЮЧЕВЫЕ СЛОВА: *показатели, критерии, оценки, эффективность, функционирование, система защиты информации и кибербезопасности, объекты критической информационной инфраструктуры*.

ABSTRACT. The scientific article solves a private scientific and technical problem of the need to select possible indicators of the effectiveness of the information security system and cybersecurity of critical information infrastructure facilities. The scientific novelty of the obtained result lies in the fact that for the first time consistent indicators and criteria for evaluating the effectiveness of the information security system and cybersecurity of critical information infrastructure objects are proposed. The practical significance of the work lies in the fact that, based on the obtained indicators and criteria, in further work on their basis, to develop a private methodology for evaluating the

effectiveness of the information security system and cybersecurity of critical information infrastructure facilities.

KEYWORDS: *indicators, criteria, assessments, efficiency, functioning, information security and cybersecurity system, critical information infrastructure facilities*.

ВВЕДЕНИЕ

Постановка задачи и связь ее с важными научными задачами. Система защиты информации и кибербезопасности объектов критической информационной инфраструктуры (СЗИКБ ОКИИ) – это сложный комплекс программных, криптографических, организационных и других средств, методов и мероприятий, предназначенных для защиты информации и кибербезопасности [1]. От уровня обеспечения зависит значение эффективности функционирования СЗИКБ ОКИИ. Без преувеличения зависит безопасность любого государства. В связи с этим возникает научная задача каким образом и по каким показателям оценить эффективно ли функционирует построенная и настроенная СЗИКБ ОКИИ.

Отсутствие единой методологии оценивания эффективности функционирования СЗИКБ ОКИИ приводит к нерациональным шагам по модернизации и усовершенствованию, чрезмерной необоснованной закупки «новых» программных, программно-аппаратных комплексов, криптографических, организационных и других средств, методов и мероприятий, предназначенных для защиты информации и кибербезопасности. Эта научно-техническая проблема возникла вследствии противоречия:

в необходимости иметь СЗИКБ ОКИИ, относительно новой системы, которой ранее не существовало прототипа;

в отсутствии единого подхода и методологии оценивания эффективности функционирования СЗИКБ ОКИИ.

Для решения противоречивых составляющих общей проблемы, сформулируем научную задачу исследования: определить и обосновать вероятностно возможные показатели, по которым возможно объективно определять некую эффективность функционирования СЗИКБ ОКИИ.

АНАЛИЗ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ

В работе [2] для оценки эффективности системы защиты информационной системы, автор применял показатель *E* степень достижения цели этой системой.

В работе [3] автором для оценки эффективности подразделений защиты информации применялись показатели экономической эффективности.

В условиях неопределенности [4] авторы придерживаются единого мнения и используют математическую модель оценки эффективности функционирования системы по критерию предотвращения потерь. По сути, ЗВ является разницей потерь до и после реализации мероприятий, направленных на повышение уровня информационной или кибербезопасности, и в целом отражает ту часть прибыли, которая могла быть потеряна.

Применение данного подхода затруднено вследствие отсутствия подходов к расчету В1 и В2. В связи с этим актуализируется сформулированная новая научная задача.

Предложенная в работе [5] методика обеспечивает вычисление и оценки эффективности выполнения мероприятий обеспечения кибербезопасности объектов критической информационной инфраструктуры организаций.

В авторской работе [6] эффективность функционирования системы защиты информации и кибербезопасности, определялась по показателям: киберзащищенности; коэффициентом укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты; коэффициентом технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты; коэффициентом укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты; коэффициентом укомплектованности штатных должностей системными администраторами; коэффициентом укомплектованности штатных должностей обслуживающим персоналом; киберзахищенностью по результатам penetration testing.

Таким образом с анализа последних исследований и публикаций по данному направлению исследований можно сделать выводи:

1) решаемая проблема не является новой, а вот результат исследования может отображать новое решение;

2) решение научной задачи является приоритетным направлением исследований [1] не только для Украины, но для многих развивающихся стан.

ЦЕЛЬ СТАТЬИ

Охарактеризовать математические показатели и критерии такого оценивания эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Под «эффективностью СЗИКБ ОКИИ» ($E_{СЗИКБ}$) в данном исследовании будем понимать степень соответствия достигнутых результатов поставленным целям по защите информации.

Оценка эффективности может осуществляться в процессе создания, приемки и эксплуатации СЗИКБ. Ключевым понятием является критерий оценки – признак, основание принятия решения по оценке эффективности на соответствие выдвинутым требованиям. Для осуществления такой оценки нужны объективные показатели эффективности.

Показатель эффективности – это некоторая величина, характеризующая степень достижения системой любой из поставленных перед ней задач.

К показателям эффективности выдвигаются следующие требования:

иметь определенный физический смысл;

быть пригодным для количественного анализа;

иметь простую и удобную форму;

отражать одну из значимых сторон функционирования системы;

обеспечивать необходимую чувствительность.

Единичные (частные) показатели эффективности, отражают какую-то из значимых сторон функционирования системы (вероятность обнаружения нарушителя или вероятность его нейтрализации силами охраны и т.п.).

Согласно принятого нами определения эффективности ($E_{П(СЗИКБ)}$) в подготовке решения задачи было изучено дополнительно мировой опыт и рекомендации руководящих документов [7-17]. Результатом синтетической переработки нами предлагаются множество показателей эффективности. Их числовые значения величин, примем для характеристики (описания) степени достижения исследуемой системой защиты информации и кибербезопасности, поставленных перед ней задач.

Система связи показателей $E_{(СЗИКБ)}$ эффективности СЗИКБ ОКИИ составлен для наглядности в табличной форме (табл. 1).

Таблица 1. Система связи показателей $E_{(СЗИКБ)}$ эффективности СЗИКБ ОКИИ

Показатели $E_{П(СЗИКБ)}$	Частичные показатели $E_{ЧП(СЗИКБ)}$	Индикаторы частичных показателей ($И_{Ч(СЗИКБ)}$)
ID. Идентификация рисков кибербезопасности	ID. AM. Управление активами	ID. AM-1. Физическое оборудование и системы на ОКИ идентифицированы и задокументированы. ID. AM-2. Программное обеспечение, используемые ОКИ для предоставления жизненно важных услуг и функций, идентифицированы и задокументированы. ID. AM-3. Телекоммуникации и потоки данных ОКИ идентифицированы и задокументированы. ID. AM-4. Внешние информационные и информационно-телекоммуникационные системы, промышленные системы, которые взаимодействуют с информационно-телекоммуникационными и другими системами ОКИ учтено. ID. AM-5. Критичность активов (оборудования, данных, программного обеспечения) ОКИ определен согласно оценке их влияния, на предоставление жизненно важных услуг и функций ОКИ.

		ID. AM-6. Обязанности штатного персонала ОКИ и партнеров организации (например, поставщиков, клиентов, и т.п.) обеспечения кибербезопасности и в определенно и закреплено в соответствующих документах.
	ID. BE. Среда предоставления жизненно важных услуг и функций	ID. BE-1. Роль ОКИ в цепи поставки товаров и услуг определено и сообщено всем поставщикам организации. ID. BE-2. Место и роль ОКИ в системе оказания жизненно важных услуг и функций сектору (подсектору) критической инфраструктуры определено и сообщено всем поставщикам организации. ID. BE-3. Приоритетность целей, задач и мероприятий по обеспечению кибербезопасности предоставления жизненно важных услуг и функций установлено и сообщено. ID. BE-4. Зависимости и важнейшие процессы для обеспечения предоставления жизненно важных услуг и функций установлено. ID. BE-5. Требования к устойчивости ОКИ по обеспечению предоставления жизненно важных услуг и функций установлено.
	ID. GV. Управление безопасностью	ID. GV-1. Правила (политики) кибербезопасности ОКИ установлены и задокументированы. ID. GV-2. Обязанности по обеспечению кибербезопасности ОКИ скоординировано и согласовано с обязанностями персонала ОКИ и с внешними партнерами. ID. GV-3. Правовые и нормативные требования по обеспечению кибербезопасности ОКИ, в том числе обязательства по защите неприкосновенности частной жизни (приватности), осознано и управление ими осуществляется. ID. GV-4. Процессы управления безопасностью и управление рисками направлено на решение вопроса обработки рисков кибербезопасности.
	ID. RA. Оценка рисков	ID. RA-1. Уязвимости активов ОКИ проанализированы, было выявлено и задокументировано. ID. RA-2. Информация об угрозах безопасности и уязвимости получена с форумов обмена информацией и официальных источников. ID. RA-3. Угрозы кибербезопасности (модель угроз) как внутренние, так и внешние определены и задокументированы. ID. RA-4. Потенциальные последствия (уровень ущерба), которые могут нанести угрозы в следствие их реализации на непрерывное предоставление жизненно важных услуг и функций, и вероятности их реализации определен. ID. RA-5. Для определения риска применяются данные относительно угроз, уязвимостей, их вероятностей и уровня ущерба использовано для

		определения риска кибербезопасности. ID. RA-6. Меры реагирования на риск кибербезопасности определены и их приоритетность установлено.
	ID. RM. Стратегия управления рисками организации	ID. RM-1. Процессы управления рисками определены, согласованы с партнерами организации и управляются. ID. RM-2. Допустимый уровень риска кибербезопасности определено и четко выражено. ID. RM-3. Определение допустимого уровня риска основывается на роли ОКИ как составной части сектора критической инфраструктуры и анализе рисков, присущих соответствующему сектору критической инфраструктуры.
	ID. SC. Управления рисками системы снабжения	ID. SC-1. Процессы управления рисками кибербезопасности системы снабжения определено, согласовано с партнерами организации и управляются. ID. SC-2. Поставщики (распорядители) информационных систем, товаров и услуг для ОКИ идентифицировано, уровень их критичности оценены в соответствии с политикой управления рисками кибербезопасности с учетом рисков, присущих системе снабжения. ID. SC-3. Поставщики товаров и услуг, партнеры, в соответствии с договором, могут внедрять мероприятия, направленные на достижение цели политики информационной безопасности/кибербезопасности ОКИ и плана управления рисками поставки. ID. SC-4. С поставщиками осуществляется планирование и тестирование реагирования по соответствующим политикам реагирования на киберинциденты и восстановление состояния кибербезопасности.
PR. Киберзащита	PR. AC. Управление идентификацией, аутентификацией и контроль доступа	PR. AC-1. Идентификаторы и данные для проверки подлинности авторизованных пользователей, администраторов и процессов назначаются, верифицируются, администрируются, отзываются (отменяются) и проверяются. PR. AC-2. Физический доступ к ОКII защищен и управляется. PR. AC-3. Осуществляется контроль и управление удаленного доступа. PR. AC-4. Права доступа установлены с применением принципов минимальных привилегий и распределения обязанностей. PR.AC-5. Целостность телекоммуникационной сети защищено (например, сегментация сети). PR.AC-6. Аутентификация пользователей, администраторов, устройств и других активов осуществляется (например методами однофакторной, многофакторной проверки подлинности) в соответствии с установленным

		риском нарушения безопасности.
	PR. AT. Осведомленность и обучение	PR. AT-1. Все сотрудники ОКИ знакомы и прошли подготовку по вопросам кибербезопасности. PR. AT-2. Пользователи (администраторы) с преимуществами доступа понимают свои обязанности по вопросам кибербезопасности. PR. AT-3. Партнеры организации понимают свои обязанности по вопросам кибербезопасности. PR. AT-4. Руководство ОКИ понимает свои обязанности по вопросам кибербезопасности. PR. AT-5. Персонал по обеспечению физической и информационной безопасности понимает свои обязанности.
	PR. DS. Безопасность данных	PR. DS-1. Данные, которые хранятся, защищены. PR. DS-2. Данные, передаваемые защищены. PR. DS-3. Управление активами осуществляется соблюдением правил удаления, передачи и размещения. PR. DS-4. Необходимые способности для обеспечения доступности активов созданы и поддерживаются. PR. DS-5. Защита от утечки данных внедрено. PR. DS-6. Механизмы проверки целостности используются для верификации программного обеспечения, программно-аппаратных средств и целостности информации. PR. DS-7. Среды разработки тестирование отделены от производственной среды.
	PR. IP. Процессы и процедуры киберзащиты	PR. IP-1. Базовая конфигурация информационно-телекоммуникационных систем/систем управления производственными процессами создана и поддерживается. PR. IP-2. Жизненный цикл разработки, эксплуатации и управления системами (SDLC) внедрена. PR. IP-3. Процессы (мероприятия) управление изменениями конфигурации внедрено. PR. IP-4. Резервное копирование информации производится, поддерживается и периодически тестируется. PR. IP-5. Правила (политика) и нормы физической безопасности операционной среды и оборудования организации (ОКИ) выполняются. PR. IP-6. Данные уничтожаются согласно политике безопасности. PR. IP-7. Процессы киберзащиты постоянно совершенствуются. PR. IP-8. Планы реагирования (реагирования на киберинциденты и обеспечения непрерывности бизнеса и планы восстановления (восстановление после киберинцидента и восстановления после аварии) имеющиеся и управляются. PR.IP-9. Планы реагирования и восстановления тестируются. PR.IP-10. План управления уязвимостями

		разработано и внедрено.
	PR. MA. Техническое обслуживание	PR. MA-1. Техническое обслуживание и ремонт активов ОКИ выполняются своевременно документируются с использованием определенных и контролируемых средств. PR. MA-2. Дистанционное обслуживание активов ОКИ одобрено, задокументировано и выполняется способом, что делает невозможным несанкционированный доступ.
	PR. PT. Технологии киберзащиты	PR. PT-1. Записи аудита (журналов событий) определены, задокументированы, внедрены и проверены в соответствии с политиками, правилами, процедурами по безопасности. PR. PT-2. Сменные носители защищены, а их использование ограничено в соответствии с правилами, процедур по безопасности. PR. PT-3. Контроль доступа к системам и активам осуществляется с применением принципа минимальных привилегий. PR. PT-4. Телекоммуникационные сети и сети управления защищены. PR. PT-5. Внедрение механизмов на ОКИ для достижения требований к устойчивости в случае чрезвычайных ситуаций и инцидентов в киберпространстве.
DE. Выявления киберинцидентов	DE. AE. Аномалии и киберинциденты	DE. AE-1. Эталоны сетевых операций и ожидаемых потоков данных для пользователей и систем установлены и управляются. DE. AE-2. Существует практика анализа выявленных событий. DE. AE-3. Данные о киберинциденты агрегируются и коррелируются с нескольких источников и датчиков. DE. AE-4. Существует процесс определения возможных воздействий киберинцидентов. DE. AE-5. Пороги оповещения о киберинцидентах встановлено.
	DE. CM. Непрерывный мониторинг кибербезопасности	DE. CM-1. Телекоммуникационная сеть (ОКИИ) отслеживается для выявления потенциальных киберинцидентов. DE. CM-2. Физическая среда отслеживается для выявления потенциальных киберинцидентов. DE. CM-3. Активность персонала отслеживается для выявления потенциальных киберинцидентов. DE. CM-4. Вредоносный код обнаруживается. DE. CM-5. Несанкционированный программный продукт обнаружено. DE. CM-6. Активность внешнего поставщика товаров и услуг отслеживается с целью выявления потенциальных киберинцидентов. DE.CM-7. Мониторинг неавторизованного персонала, соединений, устройств и программного обеспечения осуществляется на постоянной основе. DE.CM-8. Сканирование уязвимостей выполняется

	DE. DP. Процессы обнаружения киберинцидентов	DE. DP-1. Обязанности по выявлению киберинцидентов четко определено для обеспечения отчетности. DE. DP-2. Меры выявления киберинцидентов соответствуют всем применимым требованиям. DE. DP-3. Процессы выявления киберинцидентов протестированы. DE. DP-4. Информация о выявленных киберинцидентах сообщена партнерам организации. DE. DP-5. Процессы выявления киберинцидентов постоянно совершенствуются.
RS. Реагирование на киберинциденты	RS. RP. Планирование реагирования	RS. RP-1. План реагирования выполняется во время или после события.
	RS. CO. Коммуникации	RS. CO-1. Персонал знает свои обязанности и порядок действий в ситуациях, когда необходимо реагирование на киберинциденты. RS. CO-2. Факты о киберинцидентах задокументированы и сообщаются в соответствии с установленными критериями. RS. CO-3. Осуществляется обмен информацией о киберинцидентах в соответствии с планами реагирования. RS. CO-4. Координация с партнерами организации проводится в соответствии с планами реагирования. RS. CO-5. С целью достижения более широкой ситуативной осведомленности относительно состояния кибербезопасности осуществляется обмен информацией с основными субъектами национальной системы кибербезопасности и внешними партнерами организации.
	RS. AN. Анализ	RS. AN-1. Сообщение от систем обнаружения киберинцидентов исследуются. RS. AN-2. Влияние киберинцидентов осознано. RS. AN-3. Киберинциденты классифицированы в соответствии с планами реагирования. Электронные доказательства собираются и фиксируются должным образом. RS. AN-4. Создано процессы для получения анализа и реагирования на факторы уязвимости, обнаруженные организацией из внутренних и внешних источников.
	RS. MI. Минимизация последствий.	RS. MI-1. Киберинциденты устранены. RS. MI-2. Последствия киберинцидентов минимизировано. RS. MI-3. Впервые обнаруженные уязвимости устранены или задокументировано как принятые риски.
	RS. IM. Усовершенствования	RS.IM-1. В планах реагирования учтен полученный опыт. RS.IM-2. Планы реагирования обновлен.
RC. Восстановление состояния кибербезопасности	RC. RP. Планирование восстановления	RC. RP-1. План восстановления выполняется во время или после киберинцидентов.
	RC. IM. Усовершенствования	RC. IM-2. План восстановления обновлен. RC. IM-1. Планы восстановления учитывают

		полученный опыт.
	RC. CO. Коммуникации	RC. CO-1. Процесс связей с общественностью организован и является управляемым. RC. CO-2. Репутация после киберинцидентов восстанавливается. RC. CO-3. Меры по восстановлению сообщены внутренним и внешним партнерам организации, а также руководству.

Критерии оценки эффективности функционирования СЗИКБ ОКИИ.

Для оценки индикаторов частичных показателей $И_{ЧП(СЗИКБ)}$ рекомендуем применять следующие критерии табл. 2.

Таблица 2. Критерии оценивания индикаторов частных показателей $И_{ЧП(СЗИКБ)}$

Критерий $И_{ЧП(СЗИКБ)}$	Уровень
$И_{ЧП(СЗИКБ)}= 0$	не реализовано функцию
$И_{ЧП(СЗИКБ)} = 1$	реализована функция

Для оценки частичных показателей $Е_{ЧП(СЗИКБ)}$ рекомендуем применять следующие критерии табл. 3.

Таблица 3. Критерии оценивания частных показателей $Е_{ЧП(СЗИКБ)}$

Критерий $Е_{ЧП(СЗИКБ)}$	Уровень
$0 \le Е_{ЧП(СЗИКБ)} \le 0,25$	неудовлетворительное (НЗ)
$0,25< Е_{ЧП(СЗИКБ)} \le 0,5$	низкий (Н)
$0,5< Е_{ЧП(СЗИКБ)} \le 0,75$	средний (С)
$0,75< Е_{ЧП(СЗИКБ)} \le 0,9$	высокий (В)
$0,9< Е_{ЧП(СЗИКБ)} \le 1$	высокий (НВ)

Для оценки показателей $Е_{П(СЗИКБ)}$ рекомендуем применять следующие критерии табл. 4.

Таблица 4. Критерии оценивания показателей $Е_{П(СЗИКБ)}$

Критерий $Е_{П(СЗИКБ)}$	Уровень
$0 \le Е_{П(СЗИКБ)} \le 0,25$	неудовлетворительное (НЗ)
$0,25< Е_{П(СЗИКБ)} \le 0,5$	низкий (Н)
$0,5< Е_{П(СЗИКБ)} \le 0,75$	средний (С)
$0,75< Е_{П(СЗИКБ)} \le 0,9$	высокий (В)
$0,9< Е_{П(СЗИКБ)} \le 1$	высокий (НВ)

Критерии оценки эффективности функционирования СЗИКБ ОКИИ по обобщенному показателю представлены в табл. 5.

Таблица 5. Критерии оценки эффективности функционирования СЗИКБ ОКИИ по обобщенным показателем

Критерий $Е_{П(СЗИКБ)}$	Уровень
$0 \le Е_{СЗИКБ} \le 0,25$	Частичный
$0,25< Е_{СЗИКБ} \le 0,5$	Риск ориентирований
$0,5< Е_{СЗИКБ} \le 0,75$	Повторяющийся
$0,75< Е_{СЗИКБ} \le 1$	Адаптивный

Лингвистическое описание частичного уровня. **Практика киберзащиты.** Практическая деятельность по реализации мер киберзащиты и управлению рисками кибербезопасности не является формализованной. Деятельность по внедрению мер киберзащиты и управлению рисками носит произвольный и ситуативный характер. Приоритетность выполнения мероприятий киберзащиты непосредственно не учитывает цели

ОКИИ по управлению рисками, характеристики угроз, задачи по предоставлению жизненно важных услуг и функций.

Политика управления рисками. Ограниченное понимание риска кибербезопасности на организационном уровне. Информированность руководства и персонала организации о рисках кибербезопасности является недостаточной. Общий подход к управлению рисками кибербезопасности в масштабе всего ОКИИ не установлен. Меры киберзащиты внедряются нерегулярно, ситуативно, используя разнообразный практический опыт или информацию, полученную из внешних источников. Процессов, обеспечивающих внутренний обмен информацией о состоянии кибербезопасности, не зафиксировано.

Взаимодействие с другими ОКИ. Организация не понимает свою роль в экосистеме в отношении своих собственных зависимостей или зависимых от нее других субъектов. Организация не обрабатывает или получает информацию (исследования угроз, лучшие практики, технологии) от других организаций (потребители, поставщики, зависимые от нее или организаций, от которых она зависит, организаций анализа и распространения информации, исследователи, государственные органы) и не распространяет такую информацию. Организация вообще не осознает рисков кибербезопасности, связанных с услугами, которые она предоставляет и которыми пользуется.

Лингвистическое описание рискориентированного уровня. **Практика киберзащиты.** Практика реализации мер киберзащиты и управления рисками утверждается руководством организации, но может не устанавливаться как общая политика для организации. Приоритетность деятельности по кибербезопасности и потребности защиты напрямую зависят от целей организационного риска, среды угроз или требований по предоставлению жизненно важных услуг и функций.

Политика управления рисками. Существует осознание риска кибербезопасности на организационном уровне, но общий подход организации к управлению риском кибербезопасности не установлено. Информация о кибербезопасности распространяется в рамках организации на неофициальной основе. Рассмотрение кибербезопасности в целях и программах организации может происходить на некоторых, но не на всех уровнях организации. Оценка рисков кибербезопасности для организационных и внешних активов происходит, но обычно не повторяется или одинаково не проводится.

Взаимодействие с другими ОКИ. В целом организация понимает свою роль в экосистеме в отношении своих собственных зависимостей или зависимых от нее других субъектов, но не обоих. Организация обрабатывает и получает некоторую информацию от других организаций, создает на основании нее собственную информацию, но может не распространять такую информацию между другими организациями. Кроме того, организация осознает риски кибербезопасности, связанные с услугами, которые она предоставляет и которыми пользуется, но не действует последовательно или по утвержденным правилам.

Лингвистическое описание повторяющегося уровня. **Практика киберзащиты.** Практика реализации мер киберзащиты и управления рисками в организации является официально утвержденной и определена как политика. Результаты киберзащиты регулярно отслеживаются и меры киберзащиты регулярно обновляются на основе применения процессов управления рисками к изменениям в требованиях по предоставлению жизненно важной функции, меняющихся угроз и технологического ландшафта.

Политика управления рисками. В организации существует общий подход к управлению рисками кибербезопасности. Политики информирования о рисках, процессах и процедурах определены, реализуются по назначению и пересматриваются. Существуют последовательные методы эффективного реагирования на изменения риска. Персонал обладает знаниями и умениями выполнять назначенные им обязанности. Организация последовательно и точно контролирует риск кибербезопасности для активов организации. Связанные и не связанные с кибербезопасностью главные исполнители регулярно общаются о риске кибербезопасности.

Взаимодействие с другими ОКИ. Организация понимает свою роль в экосистеме в

отношении своих собственных зависимостей или зависимых от нее других субъектов и может способствовать более широкому пониманию сообществом рисков. Организация регулярно обрабатывает и получает информацию от других организаций, что дополняет собственную созданную информацию и распространяет ее между другими организациями. Организация осознает риски кибербезопасности, связанные с услугами, которые она предоставляет и которыми пользуется.

Лингвистическое описание адаптивного уровня. **Практика киберзащиты.** Организация адаптирует свою практику в области кибербезопасности на основе предыдущих и текущих мероприятий по кибербезопасности, включая полученные результаты и прогнозные показатели. Благодаря процессу непрерывного совершенствования, что предполагает передовые технологии и практики кибербезопасности, организация активно адаптируется в меняющихся киберугроз и своевременно и эффективно реагировать на киберугрозы, которые развиваются и усложняются.

Политика управления рисками. В организации существует общий подход к управлению риском кибербезопасности, который использует политику, процессы и процедуры с учетом рисков для решения потенциальных киберинцидентов. Взаимосвязь между риском кибербезопасности и целями организации четко осознается и учитывается при принятии решений. Главные исполнители контролируют риск кибербезопасности в том же контексте, что и финансовый риск, и другие риски для организации. Управление рисками кибербезопасности является частью организационной культуры и развивающийся на основе осознания предыдущей деятельности и постоянного осознания деятельности в своих системах и телекоммуникационных сетях. Организация может быстро и эффективно учитывать изменения в том, как подходить к обработке и сообщать о риске.

Взаимодействие с другими ОКИ. Организация понимает свою роль в экосистеме в отношении своих собственных зависимостей или зависимых от нее других субъектов, способствует более широкому пониманию сообществом рисков. Организация получает, создает и пересматривает приоритетную информацию для продолжения анализа этих рисков по мере развития ландшафта угроз и технологий. Организация распространяет эту информацию как внутри организации, так и снаружи для дальнейшей проработки. Организация использует информацию в режиме реального времени или почти в режиме реального времени и последовательно реагирует на риски кибербезопасности, связанные с услугами, которые она предоставляет и которыми пользуется.

ВЫВОДЫ

Таким образом, на современном этапе развития науки решена научно-техническая проблема с неопределенностью по каким показателям проводить процедуру оценивания выбора эффективность функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры. На данный момент усматривается при оценке эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры два ключевых показателя по функциональной способности и технической надежности.

В работе рассмотрено показатели оценивания по показателю функциональной способности.

НАУЧНАЯ НОВИЗНА

Впервые предложены показатели и критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

ПРАКТИЧЕСКОЕ ЗНАЧЕНИЕ РАБОТЫ

На основании полученных показателей и критериев в дальнейших работах возникает возможность разработать методику оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Представленное исследование не исчерпывает всех аспектов указанной проблемы. Теоретические результаты, полученные в процессе научного поиска, составляют основу для

дальнейшего обоснования методики оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Закон України “Про основні засади забезпечення кібербезпеки України”. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

2. Маслова Н.А. Методы оценки эффективности систем защиты информационны систем. Искусственный интеллект. 2008. № 4.С. 253–264.

3. Андреев К. Метод оценки экономической эффективности подразделения по защите информации. Информационная безопасность. 2010. №5. URL: http://www.itsec.ru/articles2/ Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii.

4. Ефимов Е.Н., Лапицкая Г.М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности. Бизнес-информатика. 2015. №1(31). С. 51–57.

5. Козубцова Л.М., Хлапонин Ю.І., Козубцов І.М. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури організацій. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. №2(41). С. 17–22.

6. Козубцова Л.М., Рудоміно-Дусятська І.А., Сновида В.Є. Обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк, 2021. Випуск №45. С. 19–25. URL: http://cit-journal.com.ua/index.php/cit/article/view/315/405.

7. International Energy Agency (2021) Enhancing Cyber Resilience in Electricity Systems. URL: https://webstore.iea.org/download/direct/4359.

8. International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO, Geneva, Switzerland). URL: https://www.iso.org/standard/54534.html.

9. National Institute of Standards and Technology and North American Electric Reliability Corporation (2020) Mapping of NIST Cybersecurity Framework v1.1 to NERC CIP Reliability Standards. URL: https://doi.org/10.18434/mds2-2348.

10. North American Electric Reliability Corporation (2021) NERC CIP Enforceable Standards. URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

11. National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). URL: https://doi.org/10.6028/NIST.CSWP.04162018.

12. National Institute of Standards and Technology (2021) National Online Informative References Program. URL: https://csrc.nist.gov/projects/olir.

13. Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. URL: https://doi.org/10.6028/NIST.SP.800-53r4.

14. International Society of Automation (2013) ISA 62443-3-3:2013 – Security for industrial automation and control systems Part 3-3: System security requirements and security levels (ISA, North Carolina, USA). URL: https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu.

15. Department of Energy (2021) Cybersecurity Capability Maturity Model. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

16. Center for Internet Security (2021) CIS Controls V8. URL: https://www.cisecurity.org/controls/.

17. Information Systems Audit and Control Association (ISACA) (2021) Control Objectives for Information and Related Technologies. URL: https://www.isaca.org/resources/cobit.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 25-34 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ინფორმაციული უსაფრთხოების რისკების მართვა: სტანდარტები და გამოწვევები

INFORMATION SECURITY RISK MANAGEMENT: STANDARDS AND CHALLENGES

აკაკი შეყელაძე, საქართველოს ტექნიკური უნივერსიტეტი
Akaki Shekeladze, Georgian Technical University

ანოტაცია: კიბერსივრციდან მომდინარე საფრთხეებისა და მსოფლიოს სხვადასხვა წერტილში განუწყვეტლივ მიმდინარე კიბერშეტევების პარალელურად, უფრო და უფრო დიდი მნიშვნელობა ენიჭება ინფორმაციის დაცვას. ინფორმაციისთვის შექმნილისაფრთხეებისა და რისკების მართვა შეუძლებელია შესაბამისი მიდგომისა და მეთოდოლოგიის გამოყენების გარეშე. მოცემულ სტატიაში მიმოვიხილავთ ინფორმაციული უსაფრთხოების რისკების მართვის არსს, მის საჭიროებას და პროცესის ადმინისტრირების შესაძებლობებს ისეთი საერთაშორისო სტანდარტების გამოყენებით, როგორიცაა ISO, NIST, COBIT და სხვა. ასევე, შევეხებით შესაბამის გამოწვევებს და მათთან გამკლავების შესაძლო საშუალებებს.
საკვანძო სიტყვები: *ინფორმაციული უსაფრთხოება, ინფორმაციული უსაფრთხოების რისკი, ინფორმაციული აქტივი, კიბერსაფრთხეები, ISO27005, NIST RMF*

ABSTRACT: ALONG WITH CYBER THREATS AND CYBER ATTACKS CONTINUOUSLY OCCURRING IN ANY PART OF THE WORLD, INFORMATION SECURITY GAINS MORE AND MORE IMPORTANCE. THREATS AND RISKS REGARDING INFORMATION CANNOT BE ADDRESSED WITHOUT ADEQUATE APPROACH AND STRUCTURED METHODOLOGIES. THIS PAPER WILL COVER INFORMATION SECURITY MANAGEMENT CONCEPT, ITS NECESSITY AND MANAGEMENT OF THE PROCESS VIA USING INTERNATIONAL STANDARDS, INCLUDING ISO, NIST, COBIT, ETC. WE WILL ALSO COVER CHALLENGES IN THIS REGARD AND WAYS TO TACKLE WITH THEM.

KEYWORDS*: Information Security, Information Security Risk, Information Asset, Cyber Threats, ISO27005, NIST RMF*

შესავალი

ხანძარი, წყალდიდობა, ძლიერი ყინვა, აფეთქება და ვულკანის ამოფრქვევა იმ მოვლენათა არასრული ჩამონათვალია, რაც საუკუნეების განმავლობაში კაცობრიობის მიერ ფიზიკური ინფრასტრუქტურის წინაშე მდგარ საფრთხეებად მიიჩნეოდა. თუმცა, 21-ე საუკუნეში, თითოეულ მათგანს უკვე ინფორმაციისა და ინფორმაციული სისტემების საფრთხედაც მიიჩნევენ და ისინი განგაშის საფუძველსაც ხშირად ქმნიან. ამას ემატება უშუალოდ კიბერსივრცეში არსებული საფრთხეები, როგორიცაა შპიონაჟი, ფინანსური თაღლითობები, საბოტაჟი, ინფორმაციის მოპარვა, დაკარგვა და სხვა.

მართლაც, ინფორმაციის მნიშვნელობამ დღეს უმაღლეს ნიშნულს მიაღწია, რითაც ის გახდა ყველაზე კრიტიკული აქტივი, რომელსაც ორგანიზაცია იღებს, ამუშავებს, ცვლის და ინახავს.

ორგანიზაციის ინფორმაციულ სისტემებში არსებული პერსონალური და კონფიდენციალური ინფორმაცია მოწყვლადია როგორც ზემოაღნიშნული ფიზიკური, ასევე კიბერსაფრთხეების წინაშე, რის გამოც ინფორმაციული უსაფრთხოების რისკების მართვას უფრო და უფრო დიდი მნიშვნელობა ენიჭება როგორც კერძო, ასევე საჯარო სექტორში.

ინფორმაციული უსაფრთხოების რისკების მართვა არის უსაფრთხოების წინაშე მდგარი საფრთხეების იდენტიფიცირების, შეფასებისა და მართვის უწყვეტი პროცესი. ის წარმოადგენს ორგანიზაციის მიერ რისკების მართვის განუყოფელ, მნიშვნელოვან ნაწილს, ვინაიდან მის საფუძველზე უნდა იყოს შეთავაზებული უსაფრთხოების ადეკვატური გადაწყვეტები ინფორმაციული სისტემებისა და მონაცემებისთვის.

სხვადასხვა საერთაშორისო სტანდარტები, როგორიცაა ISO, NIST წარმოგვიდგენენ ინფორმაციული უსაფრთხოების რისკის მართვის მეთოდოლოგიას, რომელთაც მსოფლიოში ფართოდ იყენებენ და მათგან მიღებულ სარგებელს დადებითად აფასებენ. თუმცა, ამ სტანდარტების დანერგვას სჭირდება გარკვეული რესურსი და ძალისხმევა, დაწყებული მმართველი რგოლის მხარდაჭერით და დასრულებული ფინანსური ინვესტიციით.

მოცემულ სტატიაში მიმოვიხილავთ ინფორმაციული უსაფრთხოების რისკების მართვის საჭიროების მიზეზებს, მის სარგებელს, რისკების მართვის პროცესს აღიარებული სტანდარტების მიხედვით და ამ პროცესში წარმოშობილ გამოწვევებს ქართული რეალობის კონტექსტში.

რა არის ინფორმაციული უსაფრთხოების რისკი?

ინფორმაციული უსაფრთხოების რისკი, საერთაშორისო სტანდარტების თანახმად, განიმარტება როგორც შესაძლებლობა იმისა, რომ კონკრეტული საფრთხე, ინფორმაციული აქტივ(ებ)ის სისუსტის გამოყენებით, ზიანს მიაყენებს აქტივს ან აქტივთა ჯგუფს და აღნიშნულით ზიანი მიადგება ორგანიზაციას.

ცხადია, იმ ეპოქაში, როდესაც კიბერთაღლითობას უამრავი მსხვერპლი ჰყავს, ერთ კიბერშეტევას კი შეუძლია ორგანიზაციას ასი ათასობით დოლარის ზარალი მოუტანოს, რეპუტაცია შეულახოს და, უფრო მეტიც, ინფრასტრუქტურა ფიზიკურად გაანადგუროს, საჯარო არეულობა გამოიწვიოს, ან ეროვნული უსაფრთხოების საკითხი კითხვის ნიშნის ქვეშ დააყენოს, საფრთხეების პრევენციის საჭიროებაზე ყურადღების გამახვილების საჭიროება აღარ დგას.

მართლაც, შეუძლებელია 21-ე საუკუნეში კერძო თუ საჯარო დაწესებულება ფუნქციონირებდეს შესაბამისი საფრთხეების იდენტიფიცირებისა და რისკების შეფასების გარეშე. ინფორმაციას და ინფორმაციულ სისტემებს შეიძლება საფრთხე შეუქმნას ფიზიკურმა ზიანმა (ხანძარი, ნგრევა, ყინვა), ბუნებრივმა პროცესებმა (წყალდიდობა, მიწისძვრა), ძირითადი სერვისების შეფერხებამ (კონდიცირების სისტემა დაზიანება, კვების შეწყვეტა), ინფორმაციის კომპრომეტირებამ (შპიონაჟი, დეზინფორმაცია, არასანქცირებული შეღწევა სისტემებში), ტექნიკურმა გაუმართაობებმა (მოწყობილობის გაუმართაობა, პროგრამის შეფერხებით მუშაობა), მესამე პირის არაავტორიზებულმა ქმედებებმა თუ სხვა.

ინფორმაციული უსაფრთხოების რისკების მართვა კი გულისხმობს როგორც ამ საფრთხეების, ასევე ამ საფრთხეების შესაბამისი მოწყვლადობის იდენტიფიცირებას. მაგალითისთვის, თუკი საფრთხედ მივიჩნევთ შპიონაჟს და ორგანიზაციას ქსელის დაუცველი არქიტექტურა აქვს, ამ შემთხვევაში, მან იცის, რომ ეს პრობლემა დაუყოვნებლივ გადასაჭრელია.

რაში გვჭირდება ინფორმაციული უსაფრთხოების რისკების მართვა?

ინფორმაციული უსაფრთხოების რისკების მართვას აქვს რიგი სარგებელი, კერძოდ [1]:

- ის ორგანიზაციას უჩენს კონკურენტულ უპირატესობას, ზრდის მის რეპუტაციას და მის მიმართ ნდობას, რაც საბოლოოდ ბიზნესის შედეგებზე აისახება;
- ის ამცირებს ინფორმაციული უსაფრთხოების ინციდენტის მოხდენის ალბათობას, ვინაიდან ორგანიზაციას აქვს ინფორმაცია შესაბამის საფრთხეზე და ამ საფრთხის თავიდან ასარიდებელ საშუალებებს იყენებს;
- ის საშუალებას აძლევს ორგანიზაციას მიიღოს სწორი გადაწყვეტილება, რომელიც ემყარება რეალურ რისკებს;
- ის ზოგავს ორგანიზაციის ხარჯებს ეფექტური და ეფექტიანი კონტროლის მექანიზმების დანერგვით;
- ის არის საქმიანობის უწყვეტობის წინაპირობა;
- ის ორგანიზაციას აძლევს სრულ ხედვას ინფორმაციული აქტივების წინაშე მდგარი გამოწვევების შესახებ.

უნდა აღინიშნოს ისიც, რომ მხოლოდ ამ პროცესის წარმატებით განხორციელების შემთხვევაში შეუძლია ორგანიზაციას იყოს სრულად თავსებადი ისეთ საერთაშორისო სტანდარტებთან, როგორიც არის ISO27001, NIST და სხვა. მეტიც, ინფორმაციული უსაფრთხოების რისკების მართვა ISO სტანდარტის ერთ-ერთი ძირითადი მოთხოვნაა და მის გარეშე ორგანიზაცია შესაბამის სერტიფიკატს ვერ მოიპოვებს.

რისკების მართვა სტანდარტების გამოყენებით

ინფორმაციული უსაფრთხოების რისკების მართვისთვის მნიშვნელოვანია განისაზღვროს მეთოდოლოგია. თითოეული ორგანიზაცია განსხვავდება თავისი შიდა და გარე გარემოს მიხედვით, სტრატეგიული მიზნებით, ამოცანებით, სტრუქტურით, ინფორმაციული სისტემებით, ქსელის არქიტექტურით. შესაბამისად, ზოგი საჭიროებს საბაზისო მიდგომას, ზოგი კი უფრო სიღრმისეული მეთდოლოგიის გამოყენებას. არსებობს ამ პროცესის მართვის რამდენიმე საერთაშორისოდ აღიარებული სტანდარტი, თუმცა რომელიმე მათგანის გამოყენება ვალდებულება ნამდვილად არ არის. ორგანიზაციას შეუძლია შექმნას საკუთარიც. მთავარი ისაა, რომ მეთოდოლოგია იყოს შესატყვისი ორგანიზაციასთან, მის მიზნებსა და სამუშაო პროცესებთან. წარმოგიდგენთ ყველაზე გავრცელებული მეთოდოლოგიებიდან რამდენიმეს [2]:

OCTAVE:
2001 წელს შექმნილი OCTAVE Allegro კონცენტირდება ინფორმაციულ აქტივებზე. ორგანიზაციის კრიტიკული აქტივები იდენტიფიცირდება და ფასდება მასთან დაკავშირებულ სხვა აქტივებთან მიმართებაში. ამ მეთდოლოგიის დადებით მხარედ მიიჩნევა მორგებისა და დოკუმენტირების შესაძლებლობა, ხოლო უარყოფით მხარედ მისი სირთულე.

FAIR:
FAIR არის რისკის ანალიზის რაოდენობრივი შეფასების მოდელი. ის სპეციალიზდება ფინანსურ შედეგებზე და არ მოიაზრებს ხარისხობრივ შეფასებას. მისი დადებითი მხარეა საფრთხეების, მოწყვლადობებისა და რისკების დონეების დაყოფა, ხოლო უარყოფითი მხარეა სირთულე.

COBIT:
„კონტროლის მექანიზმები ინფორმაციისა და ტექნოლოგიებისთვის“, რომელიც შეიქმნა ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ, ფოკუსირდება კონტროლის მექანიზმების იდენტიფიცირებაზე [3]. ის შედგება 37 პროცესისგან, რომლითაც იმართება და კონტროლდება ინფორმაცია და მასთან დაკავშირებული ტექნოლოგიები. COBIT არ გვთავაზობს რისკების შეფასების მეთდოლოგიას, მაგრამ ქმნის ინფორმაციული ტექნოლოგიების ორგანიზაციის საფუძველს. COBIT მოიცავს ინფორმაციული ტექნოლოგიების რისკების შემცირების კონტროლის მექანიზმებს.

ვინაიდან „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი ავალდებულებს კრიტიკული ინფორმაციული სისტემის სუბიექტებს, რომ მათი ინფორმაციული უსაფრთხოების პოლიტიკა იყოს თავსებადი სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO), აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (NIST) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ სტანდარტებსა და მოთხოვნებთან [4], ნაკლებად სავარაუდოა, რომ საქართველოს კრიტიკული ინფორმაციული სისტემის რომელიმე სუბიექტის ინფორმაციული უსაფრთხოების რისკების მართვის პროცესმა ამ სტანდარტებს გვერდი აუაროს.

NIST RMF:
NIST საერთაშორისო სტანდარტის რისკების მართვის ჩარჩო (RMF) არის სტრუქტირებული პროცესი, რომელიც მოიცავს ინფორმაციული უსაფრთხოებისა და რისკების მართვის პროცედურებს. კერძოდ, რისკების მართვა ხორციელდება შემდეგი ეტაპებით [5] (ნახ.1):

ნახაზი 1. *NIST სტანდარტის რისკების მართვის ჩარჩო*

- მომზადება - პირველ ეტაპზე ხდება იმგვარი პროცედურების განხორციელება ორგანიზაციაში, რითაც ის მოემზადება საკუთარი უსაფრთხოების რისკების მართვისთვის RMF ჩარჩოს გამოყენებით. ეს, მაგალითისთვის, მოიცავს როლებისა და პასუხისმგებლობების განსაზღვრას;
- კატეგორიზება - ხდება მოვლენების შეფასება ინფორმაციის ხელმისაწვდომობას, მთლიანობასა და კონფიდენციალურობასთან მიმართებაში, საფრთხეების კლასიფიცირება და შესაბამისი პირების ინფორმირება;
- შერჩევა/აღმოჩენა - ორგანიზაცია აღრიცხავს მოვლენებს, რომლებიც უქმნის საფრთხეს ინფორმაციის უსაფრთხოებას;
- დანერგვა - ამ ეტაპზე ინერგება კონტროლის მექანიზმები შესაბამისი რისკების საპასუხოდ;
- შეფასება - ამ დროს ფასდება დანერგილი კონტროლის მექანიზმების ეფექტურობა და სისწორე, რომ ის პასუხობს უსაფრთხოების პრობლემებს და შესაბამის მოთხოვნებს;
- ავტორიზება - მენეჯმენტის მხრიდან ხდება უსაფრთხოების რისკებისთვის დანერგილი კონტროლის მექანიზმების დამოწმება;
- მონიტორინგი - მოიცავს აღწერილი ეტაპების მონიტორინგის უწყვეტ პროცესს.

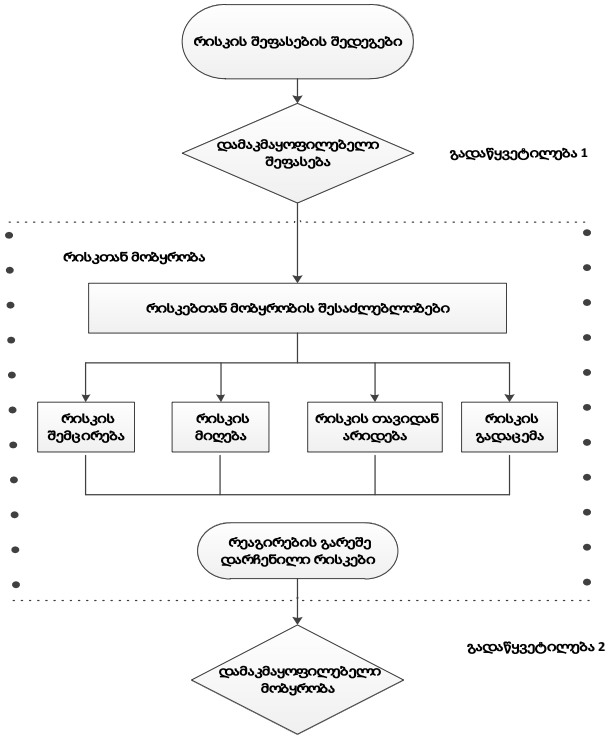
ISO 27001/27005:
ISO ინფორმაციული უსაფრთხოების სტანდარტის თანახმად, ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შედგება შემდეგი პროცესებისგან:

- ორგანიზაციული გარემოს განსაზღვრა - მოიცავს საჭირო კრიტერიუმების დადგენას ინფორმაციული უსაფრთხოების რისკების მართვის გამოყენების სფეროსა და ჩარჩოების განსაზღვრას, ასევე ორგანიზაციული სტრუქტურის შექმნას, რომელიც განახორციელებს ინფორმაციული უსაფრთხოების რისკების მართვას. ამ პროცესში ხდება შიდა და გარე პროცესების, შეზღუდვების, საჭიროებების, მიზნების გათვალისწინება;
- რისკების შეფასება - მოიცავს რისკის ანალიზს (შედგება რისკების იდენტიფიცირებისგან და რისკების მიახლოებითი შეფასებასისგან) და რისკის დონის დადგენას;
- რისკებთან მოპყრობა - მოიცავს არჩევენს რისკებთან მოპყრობის შესახებ (ნახ.2);
- რისკების შესახებ ინფორმირება;
- რისკების მონიტორინგი და განხილვა.

რისკების შეფასებისთვის პირველ ეტაპს წარმოადგენს რისკების იდენტიფიკაცია. ამ პროცესში შემავალ ინფორმაციას წარმოადგენს ორგანიზაციის ინფორმაციული აქტივები. თითოეული აქტივისთვის უნდა დადგინდეს შესაბამისი საფრთხე. საფრთხე, წარმოშობის წყაროს მიხედვით, შეიძლება იყოს შიდა, გარე და ბუნებრივი. აუცილებელია მოწყვლადობების იდენტიფიკაცია, რომელი სისუსტეებით სარგებლობაც წარმოადგენს საფრთხეს აქტივებისთვის ან ორგანიზაციისთვის.

შემდეგ ხდება რისკების მიახლოებითი შეფასება. ის შეიძლება ჩატარდეს დეტალურობის სხვადასხვა დონეზე და დამოკიდებულია აქტივის კრიტიკულობაზე, წინა გამოცდილებაზე (ინციდენტებზე), ცნობილ მოწყვლადობებზე. რისკების მიახლოებითი შეფასება შეიძლება იყოს როგორც ციფრული (რაოდენობრივი), ასევე თვისობრივი (ხარისხობრივი). მიახლოებით შეფასებული რისკი წარმოადგენს ინციდენტის სცენარის და მისი უარყოფითი შედეგების ალბათობის კომბინაციას.

შემდეგ ხდება გადაწყვეტილების მიღება რისკებთან მოპყრობასთან დაკავშირებით, სადაც წარმოდგენილია შემდეგი ვარიანტები:



ნახაზი 2. *რისკებთან მოპყრობის ქმედება*

1. რისკების შემცირებისთვის (შემსუბუქება) საჭიროა კონტროლის მექანიზმის სწორად შერჩევა. კონტროლის მექანიზმების შერჩევის და მათი დანერგვის დროს უნდა მოხდეს შეზღუდვების გათვალისწინება, როგორიცაა: ტექნიკური, სამართლებრივი, საკადრო, ფინანსური, დროითი და სხვა.
2. თუ რისკის დონე შეესაბამება რისკის მიღების კრიტერიუმებს, მაშინ არ არის აუცილებელი დამატებითი კონტროლის მექანიზმის დანერგვა და ხდება რისკის დაშვება.
3. რისკის თავიდან არიდება გამართლებულია, როდესაც რისკებთან მოპყრობის სხვა ვარიანტების განხორციელების დანახარჯები მეტია სარგებელზე და ასეთ დროს ხდება რისკის მთლიანად აღმოფხვრა.
4. რისკის გადაცემა გულისხმობს გადაწყვეტილებას გარკვეული რისკების მესამე მხარისთვის გაზიარების შესახებ. ეს შეიძლება იყოს ქვეკონტრაქტორი კომპანია ან დაზღვევა.

აღსანიშნავია, რომ ISO27001 სტანდარტით მოცემული ოთხი ვარიანტი არ არის ურთიერთგამომრიცხავი, ვინაიდან გარკვეულ შემთხვევებში გამართლებულია მათი კომბინაციაც.

როგორც ვნახეთ, სხვადასხვა სტანდარტების ანალიზის შედეგად დგინდება [6], რომ პირველი ეტაპი უნდა იყოს ინფორმაციული აქტივების იდენტიფიცრება. ეს აქტივები შეიძლება იყოს სერვერები, ქსელური მოწყობულობები, სისტემები, კომპიუტერული ტექნიკა და ნებისმიერი მოწყობილობა, რომელშიც ინახება, მუშავდება და გაიცვლება

ინფორმაცია. აქტივი შეიძლება იყოს დოკუმენტიც, ორგანიზაციაში დასაქმებული თანამშრომლებიც.

მეორე ეტაპი არის საფრთხეების იდენტიფიცირება აქტივებთან მიმართებაში. საფრთხე არის უცნობი ინციდენტის პოტენციური მიზეზი, რომელმაც შეუძლია ზიანი მოუტანოს ორგანიზაციას. ეს შეიძლება იყოს ქურდობა, მავნე პორგრამული უზრუნველყოფა, ბუნებრივი მოვლენები, ინფორმაციის გამჟღავნება და სხვა.

მესამე ეტაპი არის მოწყვლადობების იდენტიფიცირება. ეს შეიძლება იყოს სარეზერვო ასლების არარასებობა, დაშიფვრის არარსებობა, არასაიმედო პაროლები, დაბალი კიბერცნობიერება, ქსელური დაცვის ეკრანის შეუსაბამობა, ბიზნესის უწყვეტობის გეგმის არქონა და სხვა.

მეოთხე ეტაპი არის საფრთხის ალბათობის დადგენა. ალბათობის დადგენისთვის შესაძლებელია სტატისტიკის, ანგარიშების გამოყენება. ალბათობის დონეები შეიძლება იყოს როგორც რაოდენობრივი, ასევე თვისობრივი (მაგ.: დაბალი, საშუალო, მაღალი).

მეხუთე ეტაპზე ალბათობა უნდა დავუკავშიროთ გავლენას. შესაძლოა, ალბათობა იყოს დაბალი, ხოლო საფრთხის სიმძიმე ძალიან მაღალი, ან პირიქით და ეს შემთხვევები განსხვავებულ სურათს იძლევა. სწორედ ალბათობისა და გავლენის ურთიერთშეკავშირება გვაძლევს საშუალებას შევაფასოთ რისკი. რისკის შეფასებისთვის, ასევე შეგვიძლია გამოვიყენოთ შკალა, ან შევაფასოთ ის ხარისხობრივად.

წარმოგიდგენთ რისკების შეფასების მაგალითს (ცხრ.1), სადაც ვიყენებთ რაოდენობრივ მეთოდს და ალბათობასა და გავლენას ვაფასებთ 1-დან 5 ქულამდე. ბოლო სვეტში ვიღებთ რისკის შეფასების შედეგს.

აქტივი	საფრთხე	მოწყვლადობა	რისკის მფლობელი	გავლენა (1-5)	ალბათობა (1-5)	რისკი
სერვერი (ტექნიკური უზრუნველყოფა)	კვების წყვეტა	უწყვეტი კვების წყაროს (UPS) არარსებობა	ინფორმაციული უსაფრთხოების მენეჯერი	4	2	**6**
	ხანძარი	ცეცხლმაქრის არარსებობა		5	3	**8**
ხელშეკრულება (დოკუმენტი)	წვდომის მიღება არაავტორიზებული პირის მიერ	ხელშეკრულება დატოვებულია მაგიდაზე	აღმასრულებელი დირექტორი	4	4	**8**
	ხანძარი	ხანძრისგან დამცავი სისტემის არარსებობა		4	3	**7**

სისტემის ადმინისტრატორი (ადამიანი)	ავარია	სხვამ არავინ იცის პაროლი	დეპარტამენტის უფროსი	5	3	**8**

ცხრილი 1. *რისკების შეფასება*

ბოლო ეტაპზე ხდება გადაწყვეტილების მიღება რისკებთან მოპყრობასთან დაკავშირებით. სხვადასხვა სტანდარტების მიხედვით, ეს შეიძლება იყოს [7]: რისკის შემცირება (შემსუბუქება), რისკის თავიდან არიდება, რისკის გადაცემა, რისკის მიღება. წარმოგიდგენთ შესაბამის მაგალითს (ცხრ.2):

აქტივი	საფრთხე	მოწყვლადობა	რისკთან მოპყრობა	დანერგვის საშუალება
სერვერი	ხანძარი	ცეცხლმაქრის არარსებობა	რისკის გადაცემა	დაზღვევის პოლისის შესყიდვა
პორტატული კომპიუტერი	არაავტორიზებული პირის მიერ წვდომა	არასაიმედო პაროლი	რისკის შემცირება	პაროლების წესის შემუშავება
სისტემის ადმინინისტრატორი	სამსახურის დატოვება	შემცვლელი კადრის არარსებობა	რისკის შემცირება	სისტემის მეორე ადმინისტრატორის დასაქმება

ცხრილი 2. *რისკებთან მოპყრობა*

გამოწვევები

ინფორმაციული უსაფრთხოების რისკების მართვა, ცხადია, საკმაოდ კომპლექსური პროცესია, რომელიც მოითხოვს გარკვეულ ძალისხმევას ორგანიზაციის თითოეული რგოლისგან. რისკების მართვის პროცესის ჩავარდნის მიზეზები ხშირად ხდება [8]:

- მმართველი რგოლის მხარდაჭერის არარსებობა: ინფორმაციული უსაფრთხოება იმართება მენეჯმენტის გადაწყვეტილებების საფუძველზე. მმართველი რგოლის მხარდაჭერის არარსებობა იწვევს რესურსების ფლანგვას, არასწორ შეფასებებს, რაც საბოლოოდ რისკების შეფასების შედეგების უგულებელყოფამდე მიგვიყვანს;
- ინფორმაციული უსაფრთხოების პოლიტიკის/პროცედურების არარსებობა: შესაბამისი დოკუმენტების არარსებობა მიგვიყვანს რისკების შეფასების არასისტემურ მიდგომასთან;
- არასწორი მართვა: მიუხედავად რისკების მართვის მნიშვნელობისა, ზოგჯერ ის არ იმართება, როგორც პროექტი და არ განიხილება ოპერაციად. რისკების მართვის პროცესის გაუთვალისწინებლობა გადაწყვეტილების მიღების, დაგეგმვის და აღსრულების პროცესში იწვევს რესურსების არამიზნობრივ ხარჯვას;
- აქტივების მფლობელი დაუდგენელია: შეუძლებელია ინფორმაციული უსაფრთხოების რისკი შეფასდეს აქტივების მფლობელის ჩართულობის გარეშე. როდესაც აქტივებს არ გააჩნიათ მფლობელი, მის წინაშე მდგარი საფრთხეების და შესაბამისი მოწყვლადობების ჯეროვნად მოკვლევა და შემდეგ ინფორმაციული უსაფრთხოების რისკების მართვის პროცესში გამოყენება შეუძლებელია;

- რისკების მართვის მეთოდოლოგიის შერჩევა: ზოგიერთი ორგანიზაცია რისკების მართვისთვის იყენებს რამდენიმე მეთოდოლოგიას, რითაც მართვის პროცესი კიდევ უფრო ჩახლართული ხდება.

ასევე, მივიჩნევ, რომ ამ პროცესში გამოწვევას წარმოადგენს კადრების დეფიციტი და კვალიფიკაციის ნაკლებობა. ინფორმაციული უსაფრთხოების რისკების მართვა კომპლექსური პროცესია და მასზე პასუხისმგებელი პირი უნდა ფლობდეს შესაბამის ცოდნას. ამის მიუხედავად, საქართველოში ჯერ კიდევ მრავლად შევხვდებით კრიტიკული ინფორმაციული სისტემის სუბიექტებს, რომელთაც არ ჰყავთ ინფორმაციული უსაფრთხოების მენეჯერი ან ინფორმაციულ უსაფრთოებაზე პასუხისმგებელი პირი.

დასკვნა

ამრიგად, არის თუ არა ორგანიზაცია კრიტიკული ინფორმაციული სისტემის სუბიექტი, მისთვის ნათელი უნდა იყოს ის პრობლემები, რომლებიც აღმოცენდება ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის არარსებობის შემთხვევაში. თანამედროვე სამყაროში არ არსებობს ორგანიზაცია, რომელიც არ ფლობს პერსონალურ და კონფიდენციალურ ინფორმაციას, რის გამოც გარდაუვალი ხდება ინფორმაციულ ტექნოლოგიებთან დაკავშირებულ გამოწვევებზე რეაგირება.

ინფორმაციული უსაფრთხოების რისკების მართვა არ წარმოადგენს ინფორმაციული უსაფრთხოების მენეჯერის ერთპიროვნულ პასუხისმგებლობას. პირიქით, ეს არის მაღალი რგოლის მენეჯმენტის მიერ გასააზრებელი და მისაღები გადაწყვეტილება, რომელშიც ორგანიზაციას გარკვეული ინვესტიცია დაჭირდება. თუმცა, ჩადებული რესურსი შეუძლებელია ჩაითვალოს ფუჭად, ვინაიდან რისკების შემცირებით სუბიექტი მნიშვნელოვნად ამცირებს ინფორმაციული უსაფრთხოების ინციდენტების ალბათობას, თავიდან ირიდებს რეპუტაციულ და ფინანსურ ზიანს, რაც, საბოლოო ჯამში, ხაზს უსვამს გაღებული ძალისხმევის სისწორესა და ეფექტურობას.

იმისთვის, რომ რისკების მართვის პროცესთან დაკავშირებით სუბიექტი არ შეხვდეს ჩვენ მიერ განხილულ პრობლემებს, მან საწყის ეტაპზე შეიძლება გაითვალისწინოს ISO 27001 Academy-ს მიერ წარმოდგენილი რისკების მართვასთან დაკავშირებულ რჩევები [9]:

- სწორი მეთდოლოგიის არჩევა - საჭიროა სწორი მეთოლოგიის არჩევა და საჭიროებისამებრ მისი გამარტივება;
- სწორი საშუალების არჩევა - რისკების მართვის პროცესში რეკომენდებულია პროგრამული უზრუნველყოფის გამოყენება. ზოგიერთ შემთხვევაში, ჩახლართულ პროგრამას სჯობს Microsoft Office Excel-ის ფორმის გამოყენება;
- საჭირო პერსონალის ჩართვა - საჭიროა მმართველობითი რგოლის ჩართვა ამ პროცესებში, ვინაიდან სტრუქტურული დანაყოფების უფროსებმა იციან, რის უკან იმალება პრობლემები;
- მიზანი არ არის სრულყოფილება - რისკების მართვა უწყვეტი პროცესია. პირველ ეტაპზე, შეუძლებელია ყველა საფრთხის გამოვლენა და აღწერა.

რაც შეეხება კონკრეტულ სტანდარტებს, მხოლოდ ორგანიზაციაზეა დამოკიდებული ის, თუ რომელ მიდგომას აირჩევს ინფორმაციული უსაფრთხოების რისკების მართვისთვის და ის იცვლება საქმიანობის სფეროს, მასშტაბების, ამოცანების, საჭიროებებისა და

შესაძლებელობების მიხედვით. თუმცა, მნიშვნელოვანია სტატიაში განხილული მეთოდოლოგიების გათვალისწინებაც, ვინაიდან მოცემულმა სტანდარტებმა უკვე მრავალწლიანი აპრობაცია გაიარეს და მათი ეფექტურობის ხარისხი კითხვის ნიშნის ქვეშ კიბერუსაფრთხოების ექსპერტებს ნამდვილად არ დაუყენებიათ.

გამოყენებული ლიტერატურა

1. James, Dave. n.d. “Seven Solid Benefits of Information Risk Management.” Ascentor. Accessed July 17, 2022. https://insights.ascentor.co.uk/blog/2012/02/seven-solid-benefits-of-information-risk-management
2. Refile, Olivia. 2020. “Information Security Risk Management: A Comprehensive Guide.” Linford & Company LLP. Accessed July 17, 2022. https://linfordco.com/blog/information-security-risk-management
3. Simplelearn. 2022. “What is COBIT? Understanding the COBIT Framework.” Accessed July 17, 2022. https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article
4. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი
5. NIST. n.d. “Risk Management Framework for Information Systems and Organizations.” Accessed July 17, 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
6. PECB. n.d. “Information Security Risk Management.” Accessed July 17, 2022. https://pecb.com/pdf/articles/61-pecb-information-security-risk-management.pdf
7. Infosec. 2018. “Risk treatment options, planning and prevention.” Accessed July 17, 2022. https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/
8. Walid Al-Ahmad, Bassil Mohammad. 2013. “Addressing Information Security Risks by Adopting Standards.” INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE. Accessed July 17, 2022. https://www.ijiss.org/ijiss/index.php/ijiss/article/view/20
9. Kosutic, Dejan. n.d. “ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide.” Accessed July 17, 2022. https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/

Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 35-49 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

საარჩევნო პროცესების კიბერუსაფრთხოება - საუკეთესო პრაქტიკა
ELECTION CYBER SECURITY – BEST PRACTICES

ანდრო გოცირიძე, კიბერუსაფრთხოების კონსულტანტი. ბიზნესის და ტექნოლოგიების უნივერსიტეტი-ბტუ
Andro Gotsiridze – Cybersecurity Consultant, Business and Technology University - BTU

აბსტრაქტი: არჩევნები, როგორც დემოკრატიული წყობის ძირითადი ატრიბუტი რუსული ჰიბრიდული ომის ერთ ერთი მნიშვნელოვანი სამიზნეა. ევროპის სახელმწიფოთა თუ აშშ-ის საარჩევნო პროცესები, რეფერენდუმი ან მოსახლეობის ნების გამოხატვის სხვა პროცესი მრავალჯერ გახდა რუსული კიბეროპერაციების სამიზნე.

არჩევნების შედეგებით მანიპულირებას რუსეთი როგორც ტექნიკური, ისე ფსიქოლოგიური ეფექტის მქონე კიბეროპერაციებით ცდილობს. ტექნიკურ ეფექტს იძლევა სტანდარტული კიბერშეტევა, ხოლო ფსიქოლოგიურ ზემოქმედებას: ამომრჩევლის აღქმის შეცვლას, მანიპულაციას, პროცესისადმი ნდობის შერყევას კი კრემლის მიერ მხარდაჭერილი აქტორები საინფორმაციო ოპერაციების მეშვეობით ახორციელებენ.

კიბერშეტევა ხშირად საინფორმაციო ოპერაციის ჩასატარებელ სერიოზულ ინსტრუმენტს წარმოადგენს და ინფორმაციული უპირატესობის მოპოვებას ისხავს მიზნად. ზოგჯერ, კიბერშეტევა საინფორმაციო ოპერაციის პარალელურად ხორციელდება. მაგალითად, კიბერშეტევის შედეგად ხდება ელექტრონული ფოსტიდან ან სოციალური ქსელის ანგარიშიდან ინფორმაციის არასანქცირებული მოპოვება, ხოლო შემდგომ, მოპოვებული მაკომპრომეტირებელი მასალა ორიგინალის ან ფაბრიკაციის სახით ვრცელდება ინტერნეტში.

სტატიაში განხილულია საარჩევნო პროცესებში ხშირად გამოყენებული კიბერშეტევებისა და საინფორმაციო ოპერაციების ტექნიკები, საფრთხეები, საფრთხის აქტორები და რისკების მართვის საუკეთესო პრაქტიკა. დასასრულს, მოყვანილია რამდენიმე პრაქტიკული რჩევა საარჩევნო პროცესების ადმინისტრირებაში ჩართულ პირთა კიბერჰიგიენისთვის. ნაშრომი ძირითადად ორ მიზანს ემსახურება: არჩევნების კიბერუსაფრთხოების, კიბერშეტევებისა და საინფორმაციო ოპარაციების შესახებ ცნობიერების ამაღლებას საარჩევნო პროცესში ჩართული ნებისმიერი მხარისათვის და

საარჩევნო ადმინისტრაციის თანამშრომლებისათვის რისკების შემცირების სტრატეგიის შეთავაზებას.

საკვანძო სიტყვები:*კიბერ უსაფრთხოება, უსაფრთხოება, საუკეთესო პრაქტიკა, არჩევნები, ჰიბრიდი*

ABSTRACT: Elections as the core attribute of democracy is one of the main target of Russian hybrid warfare. Lately, elections, referendums, or other process expressing free will of a society appear as a target of Russian cyber operations.

Russia attempts to manipulate elections with cyber operations having technical and psychological effects. While standard cyber-attacks achieve technical effects, Kremlin backed actors using information operations achieve psychological effects, such as alter of perception, manipulation, and distrust.

Cyber-attack often serves as a serious tool for information warfare and is used to take advantage on adversaries. Sometimes, cyber-attack is implemented parallel to psychological operation. For example, the one can use cyber-attack for unauthorized gathering of information from target`s email or social media. Then, the attacker can use this information as an authentic or fabricated and disseminated to denigrate the target.

The article discusses cyber-attacks and information operations, threats, threat actors, techniques and risk mitigation best practices. At the end, it delivers practical cyber hygiene advises for election administration staff.

KEYWORDS: *Cyber security, security, best practices, elections, warfare, hybrid.*

არჩევნები, ხალხის მიერ საკუთარი ნების გამოხატვა, დემოკრატიის ფუძემდებლური პრინციპია. ხალხის ნდობას მხოლოდ არჩევნების გზით მოსახლეობის მიერ მხარდაჭერილი მთავრობა იმსახურებს, შესაბამისად, უმნიშვნელოვანესია არჩევნების პროცესისა და მისი შედეგების მიმართ ნდობის მაღალი ხარისხი. სწორედ ამიტომ, არჩევნები, როგორც დემოკრატიული წყობილების ძირითადი ატრიბუტი რუსული ჰიბრიდული ომის ერთ ერთი მნიშვნელოვან სამიზნეს წარმოადგენს. უკანასკნელ პერიოდში რუსული კიბეროპერაციების შედეგებს ტექნიკურ, კინეტიკურ ეფექტთან ერთად ფსიქოლოგიური ზემოქმედებაც დაემატა და სახელმწიფოთა საარჩევნო სისტემები, რეფერენდუმი ან მოსახლეობის ნების გამოხატვის სხვა პროცესი მრავალჯერ გახდა რუსული კიბეროპერაციების სამიზნე.

ხშირად, არჩევნების კიბერუსაფრთხოებაზე საუბარი ხმის მიცემის ელექტრონულ პროცედურების გამართულობაზე დაიყვანება, თუმცა ეს ასე არ არის. კიბერუსაფრთხოების პერსპექტივიდან, საარჩევნო პროცესის ნებისმიერი ეტაპი, რომელიც მოიცავს ელექტრონული მოწყობილობის ან სივრცის გამოყენებას, რისკის შემცველია. კომპიუტერული სისტემები და პროგრამული უზრუნველყოფა საარჩევნო პროცესის ყველა კომპონენტშია წარმოდგენილი, რაც ამ პროცესებში სისუსტეების არსებობასაც გულისხმობს. კიბერშეტევის პოტენციური ვექტორი შესაძლოა იყოს როგორც ტექნიკური, ასევე ადამიანური ფაქტორი და მოიცავდეს როგორც თავად საინფორმაციო სისტემას, ასევე მათ, ვინც ქმნის ან მართავს ამ მას. სახელმწიფო სექტორზე, ბიზნესსა თუ ინდუსტრიაზე განხორციელებულ თავდასხმებში, კიბერინციდენტების უმეტესობა ძირითადად, მავნე აქტორების მიერ ადამიანური ფაქტორის გამოყენებითაა განპირობებული. კომპიუტერული სისტემებისა და პროგრამული უზრუნველყოფის ვენდორები ასევე წარმოადგენენ მეტად მოწყვლად სამიზნეს. ამ მხრივ გამონაკლისს არც საარჩევნო სისტემების კიბერუსაფრთხოება წარმოადგენს.

არჩევნების კიბერუსაფრთხოების კონტექსტში, კიბერშეტევის[1] გავრცელებული სახეებია ფიშინგი, DDoS შეტევა, Defacement, MITM და სხვა. კიბერშეტევა ხშირად **საინფორმაციო ოპერაციის**[2] ჩასატარებელ მნიშვნელოვან ინსტრუმენტს წარმოადგენს და **ინფორმაციული უპირატესობის**[3] მოპოვებას ისახავს მიზნად [1-4]. საინფორმაციო ოპერაციების კიბერელემენტი მოიცავს დაინტერესების ობიექტების ქსელების კომპრომეტაციას ისეთი ინფორმაციის მოპოვების მიზნით, რომელიც შესაძლოა გამოყენებულ იქნას დაშინების, შანტაჟის, დისკრედიტაციის ან ფალსიფიკაციის მიზნით, ასევე მასმედიის საშუალებებში კონტროლირებადი გავრცელებისთვის.

---

[1] ქსელზე თავდასხმის ერთ ერთი ფორმა, რომლის მიზანს კომპიუტერის ან კომპიუტერული ქსელის მწყობრიდან გამოყვანა, შეფერხება, განადგურება, მასზე არასანქცირებული კონტროლის მოპოვება, მასში არსებული კონტროლირებადი ინფორმაციის მთლიანობის დარღვევა ან მისი არაავტორიზებული დაუფლება წარმოადგენს.

[2] არჩევნების კიბერუსაფრთხოების კონტექსტში საინფორმაციო ოპერაცია წარმოადგენს საინფორმაციო კონტენტის გავრცელებას საზოგადოებრივი აზრის მანიპულაციის ან საზოგადოების ქცევაზე გავლენის მოხდენის მიზნით. **კონტენტი** *ცრუ და ნამდვილი ინფორმაციის ნაზავია, რომელიც მიმართულია სამიზნე აუდიტორიის დაბნევის, დემორალიზაციისა და მასზე გავლენის მოპოვებისკენ.* ***სამიზნე აუდიტორია*** *ზოგჯერ საკუთარი მოსახლეობა და ქვეყნის შიდა პოლიტიკური ელიტაა, თუმცა, არცთუ იშვიათად, სამიზნეს სხვა ქვეყნების მოსახლეობის გარკვეული ჯგუფები, ეთნიკური, რელიგიური უმცირესობა და პოლიტიკური ელიტა წარმოადგენს.*

[3] რუსულ სამხედრო და პოლიტიკურ წრეებში დამკვიდრებული ტერმინია და გულისხმობს ინფორმაციის მიღების, დამუშავებისა და გავრცელების შესაძლებლობას, რომელიც ხელს უშლის მოწინააღმდეგეს იმავე ფუნქციის განხორციელებაში.

ციფრული ტექნოლოგიების ბუმმა, შემტევი კიბერშესაძლებლობების განვითარებამ სახელმწიფოებს უპრეცენდენტო მასშტაბის საინფორმაციო ოპერაციების განხორციელების საშუალება მისცა, რადგან ამგვარი ოპერაციებისათვის საჭირო კიბერინსტრუმენტები უკიდურესად იაფი და ხელმისაწვდომია. საინფორმაციო ოპერაციების ტაქტიკა გულისხმობს მცდარი ან შეცდომაში შემყვანი ინფორმაციის გავრცელებას, მოპარული ინფორმაციის კონტროლირებად გაჟონვას ინტერნეტში, სოციალური ქსელების გამოყენებას ანტაგონისტული განწყობების გასაღვივებლად, პოლარიზაციის გასაღრმავებლად და პოლიტიკური კონფლიქტის გასაჩაღებლად.

როგორც უკვე აღინიშნა, კიბერშეტევა, ხშირად, საინფორმაციო ოპერაციის უმნიშვნელოვანესი ინსტრუმენტია. მაგალითად, კიბერშეტევის შედეგად ხდება ელექტრონული ფოსტიდან ან სოციალური ქსელის ანგარიშიდან ინფორმაციის არასანქცირებული მოპოვება, ხოლო შემდგომ, მოპოვებული მაკომპრომეტირებელი მასალა ორიგინალის ან ფაბრიკაციის სახით ვრცელდება ინტერნეტში, სადაც, ისევ კიბერტექნოლოგიების - ტროლინგის ან ბოტების მეშვეობით ხდება სასურველი აზრის ფორმირება[5-8].

კიბერშეტევების ან საინფორმაციო ოპერაციების საშუალებით არჩევნებზე ზეგავლენის მოხდენის, დემოკრატიული პროცესების დისკრედიტაციის მისწრაფება და შესაძლებლობა ბევრ აქტორს შეიძლება ჰქონდეს როგორც ქვეყნის შიგნით, ასევე მის ფარგლებს გარეთ. ესენია:

- სახელმწიფოები
- ორგანიზებული კიბერკრიმინალი ან ცალკეული ჰაკერები
- ტერორისტული ორგანიზაციები
- ინსაიდერები
- პოლიტიკურად მოტივირებული ჯგუფები
- ჰაქტივისტები

აქტორებისათვის მოტივაციას არჩევნებში ჩარევისათვის შესაძლოა წარმოადგენდეს:

- სახელმწიფოს ეროვნული ან გეოპოლიტიკური ინტერესები
- ფინანსური მოგება
- რეპუტაციის გამყარება
- ანარქიის და ქაოსის პროვოცირება
- შურისძიება
- პოლიტიკური ოპოზიციის სუბვერსია
- დემოკრატიული პროცესებისა და წყობისადმი ნდობის შესუსტება

ჰაკერები თუ ორგანიზებული კიბერკრიმინალური დაჯგუფებები სერიოზულ საფრთხეს წარმოადგენენ არჩევნებისთვის. კიბერდამნაშავეები წარმატებით ახორციელებენ საცალო ბიზნესისა და ფინანსური ინსტიტუტების ქსელებში შეღწევას, რათა მოიპოვონ ფინანსური ინფორმაცია, პერსონალური მონაცემები, საცხოვრებელი თუ ელექტრონული ფოსტის მისამართები და სამედიცინო ჩანაწერები, რაც წარმოადგენს საბაზისო ინფორმაციას კრიმინალური ოპერაციებისათვის. უკანასკნელ პერიოდში ჰაკერების კიბერშეტევათა ვექტორმა საარჩევნო სისტემებისკენაც გადაინაცვლა, სადაც დიდი რაოდენობით ძვირადღირებული ინფორმაციაა დეპონირებული. ამგვარი თავდასხმების მოტივაცია მრავალგვარია: ფინანსური სარგებელი, თავის გამოჩენის სურვილი თუ უბრალოდ საკუთარი შესაძლებლობების გამოცდა.

თუმცა, არჩევნებზე ზეგავლენის მოხდენის მსურველთა შორის ყველაზე დიდ საფრთხეს, როგორც კიბერშეტევის პოტენციალის, ასევე დაინტერესების მხრივ, მაინც სახელმწიფოები და მათთან აფილირებული კიბერაქტორები წარმოადგენენ. შემტევი კიბერპოტენციალის თვალსაზრისით, რუსეთი ერთ ერთ მოწინავე პოზიციას იკავებს მსოფლიოში და საქართველოსადმი მტრულად განწყობილ ერთადერთ ქვეყანას წარმოადგენს. კრემლი საქართველოს მისი გავლენის სფეროდ მოიაზრებს, რის გამოც ჩვენი ქვეყანა რუსეთის ჰიბრიდული ომის სამიზნეა, ამ ომის არეალი კი გარდა დიპლომატიური, ეკონომიკური, სამხედრო, პოლიტიკური, კულტურული, სოციალური, რელიგიურ თუ საინფორმაციო სფეროებისა, მოწინააღმდეგე ქვეყნების მთავრობების ან ინსტიტუტების დელეგიტიმიზაცია, დემოკრატიული პროცესების ძირგამომთხრელი საქმიანობაცაა.

არჩევნების შედეგებით მანიპულირებას რუსეთი როგორც ტექნიკური, ისე ფსიქოლოგიური ეფექტის მქონე კიბეროპერაციებით ცდილობს. ტექნიკურ ეფექტს იძლევა სტანდარტული კიბერშეტევა, ხოლო ფსიქოლოგიურ ზემოქმედებას: ამომრჩევლის აღქმის შეცვლას, მანიპულაციას, პროცესისადმი ნდობის შერყევას კი კრემლის მიერ მხარდაჭერილი აქტორები საინფორმაციო ოპერაციების მეშვეობით ახორციელებენ. უკანასკნელი ათწლეულის მანძილზე, ევროპისა თუ აშშ-ის საარჩევნო პროცესები მრავალჯერ გახდა ამგვარი ზემოქმედების სამიზნე.

რუსეთის კიბერაქტივობების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. გარდა მოწინააღმდეგის ქსელის მწყობრიდან გამოყვანის ან მისი ექსპლოატაციის მიზნით წარმოებული კიბერთავდასხმებისა, რუსეთი კიბერსივრცეს იყენებს ფსიქოლოგიური ეფექტის მისაღწევად, რაც კრემლის სასარგებლოდ ადმიანების ქცევის ან ცნობიერების შეცვლის მცდელობებს გულისხმობს.

ამრიგად, რუსული კიბეროპერაციების შედეგი, ერთის მხრივ, შეიძლება იყოს მნიშვნელოვანი ზარალი და მსხვერპლიც კი, მეორეს მხრივ კი, კრემლის

სასარგებლოდ ცნობიერების შეცვლა, პრორუსული ელიტის ფორმირება-გაძლიერება, რაც კონვენციური მოქმედებების წინაპირობა შეიძლება გახდეს.

რუსულ კიბეოპერაციებში, სხვა აქტორებთან ერთად, მნიშვნელოვან როლს თამაშობს საგარეო დაზვერვის სამსახურისა (Служба Внешней Разведки) და თავდაცვის სამინისტროს გენერალური შტაბის მთავარი სადაზვერვო სამმართველოს (Главное Разведывательное Управление) კიბერდანაყოფები. ეს უწყებები ხვა რეზონანსულ კიბერშეტევებთან ერთად, პასუხისმგებელნი არიან აშშ საპრეზიდენტო არჩევნების პროცესში დემოკრატიული პატრიის სერვერებიდან ინფორმაციის დაუფლებაზე.

სამხედრო დაზვერვის მთავარი სამმართველო, რომლის კიბერდანაყოფი ბოლო ატრიბუციამდე APT 28 -ის სახელით იყო ცნობილი, პასუხისმგებელია ასევე ევროპის ქვეყნების თავდაცვის სექტორის საინფორმაციო სისტემებიდან ინფორმაციის მოპარვასა და საქართველოს სახელმწიფო სტრუქტურების და ჟურნალისტური წრეების წინააღმდეგ 2008-14 წლებში განხორციელებულ კიბერჯაშუშობის კამპანიაზე. რაც შეეხება APT 29-ს, საგარეო დაზვერვის სამსახურის კიბერდანაყოფს, მისი სახელი უკავშირდება აშშ სახელმწიფო დეპარტამენტის, თეთრი სახლის, პენტაგონის და სხვა სახელმწიფო უწყებების სისტემებიდან არასაიდუმლო ინფორმაციის გაჟონვას. არჩევნებთან დაკავშირებულ პროცესებში ორივე დაჯგუფება ფიგურირებს: არსებული მონაცემებით საგარეო დაზვერვის სამსახურს თითქმის 1 წელი ჰქონდა წვდომა აშშ-ის დემოკრატიული პარტიის კომუნიკაციის საშუალებებზე, ელექტრონულ ფოსტასა და ჩატის კონტენტზე.

არასასურველ კანდიდატთა მაკომპრომეტირებელი ინფორმაციის ან მათ საზიანოდ დეზინფორმაციის გავრცელება დაზვერვის წყაროების ან კონტროლირებადი მედიის საშუალებით სათავეს ჯერ კიდევ ცივი ომის დროიდან იღებს. უკანასკნელი წლების მოვლენებმა კი ცხადყო, რომ კიბერსივრცე რუსეთის მიერ ხშირად არის გამოყენებული მოწინააღმდეგე ქვეყნების მთავრობების ან ინსტიტუტების დელეგიტიმიზაციის მიზნით და გადაიქცა ძირგამომთხრელი საქმიანობის ასპარეზად: არჩევნებში ჩარევის მიზნით კიბეროპერაციების გამოყენების პრეცედენტი რუსეთმა ჯერ კიდევ უკრაინის კონფლიქტისას შექმნა, როდესაც 2014 წელს უკრაინის საარჩევნო ინფრასტრუქტურაზე განახორციელა მასირებული შეტევა.

პრეზიდენტ იანუკოვიჩის გაქცევის შემდგომ უკრაინაში ჩატარდა საპრეზიდენტო არჩევნები. არჩევნებადე 4 დღით ადრე პრორუსულმა დაგჯუფებამ „კიბერბერკუტმა“ მოახერხა ცენტრალური საარჩევნო კომისიის პროგრამის სისტემური ფაილების წაშლა. კომისიამ შეძლო სარეზერვო ასლებიდან მასალების აღდგენა, თუმცა ინციდენტმა ოცსაათიანი შეფერხება გამოიწვია და დაგვიანდა არჩევნების შედეგების გამოცხადება.

ინფრასტრუქტურის ექსპლოატაციის[4] შედეგად კიბერბერკუტმა არჩევნებამდე ოთხი თვით ადრე მოიპოვა წვდომა საარჩევნო კომისიის ადმინისტრაციულ მონაცემებსა და შიდა ელექტრონულ ფოსტაზე. სარჩევნო კომისიის კომპრომეტირებული საიტი აჩვენებდა **ფაბრიკაციას**, თითქოსდა არჩევნებში გაიმარჯვა ულტრამემარჯვენე კანდიდატმა. მიუხედავად ოფიციალური უარყოფისა, რუსული მედია ავრცელებდა აღნიშნულ ინფორმაციას. უკრაინის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის მონაცემებით, ინციდენტის გამომწვევ მალვეარს[5] ადრე რუსული სამხედრო დაზვერვა იყენებდა.

2016 წელს, აშშ-ის საპრეზიდენტო საარჩევნო მარათონისას რუსული კიბერაქტორების მიერ განხორციელდა მრავალმხრივი კამპანია დემოკრატიული პროცესებისადმი ხალხის რწმენის შესარყევად, საპრეზიდენტო კანდიდატის საქმიანი რეპუტაციის შესალახად და საარჩევნო პოტენციალის შესამცირებლად. ამ კამპანიაში გამოყენებულ იქნა როგორც საინფორმაციო ოპერაციები (პოლიტიკური პროცესის დელეგიტიმიზაციის მიზნით სოციალური მედიის ყალბი ანგარიშების მეშვეობით პოლარიზაციის გაზრდის 2014 წლიდან დაწყებული კამპანია), ისე, კიბერთავდასხმები, რომელთა საშუალებითაც ორმა რუსულმა აქტორმა, სამხედრო დაზვერვის მთავარმა სამმართველომ და საგარეო დაზვერვის სამსახურმა არაავტორიზებული წვდომა მოპიოვა დემკრატიული პარტიის სერვერებსა და ელექტრონულ ფოსტაზე. მოპოვებული ინფორმაცია “Guccifer 2.0”-ის სახელით გამოქვეყნდა პლატფორმებზე DCLeaks.com და WikiLeaks, IRA-ს[6] მიერ მოხდა ამერიკის მოქალაქეების ათასობით ყალბი ანგარიშის შექმნა, რომელთა დისკუსიებმაც მოახდინეს გარემოს უკიდურესი პოლარიზაცია, ამავდროულად, ამავე ორგანზაციამ გაავრცელა ყალბი კონტენტი, რომელიც თითქოსდა მრჩეველი კანდიდატ კლინტონს ბენღაზის ინციდენტისას ამერიკელების მსხვერპლზე აკისრებდა პასუხისმგებლობას. ცხადია, არ არსებობს პირდაპირი მტკიცებულებები საარჩევნო ხმებით მანიპულირებისა ამჯამინდელი პრეზიდენტის სასარგებლოდ, თუმცა რუსულმა

[4] კიბერშეტევის ან კიბერშპიონაჟის შედეგად საინფორმაციო არხებიდან სადაზვერვო ინფორამციის მოხსნის და შეგროვების აქტი. განმარტებულია Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center. Cyber Threats to Elections – a Lexicon.

[5] **მავნე პროგრამული უზრუნველყოფა** - Malware, მალვეარი; კომპიუტერული პროგრამა, რომელიც გამოიყენება ინფორმაციულ სისტემებზე არასანქცირებული შეღწევის, სენსიტიური ინფორმაციის შეგროვების, მოპარვის, განადგურების, შეცვლის, კრიპტაციის ან კომპიუტერზე უკანონო წვდომის მოსაპოვებლად.

[6] **Internet Research Agency** იგივე **Trolls from Olgino**. სანკტ-პეტერბურგში ბაზირებული რუსული კომპანია, რომელიც ჩართულია გავლენის ოპერაციებში რუსული ბიზნესისა და პოლიტიკური ინტერესების სასარგებლოდ. მისი რამდენიმე წევრი ოფიციალურად მხილებულია აშშ-ის 2016 წლის საპრეზიდენტო არჩევნებში ცარევის მცდელობებში.

ჩარევამ გააღრმავა სოციალურ-პოლიტიკური უთანხმოება, მოახდინა საარჩევნო გარემოს პოლარიზაცია და განაპირობა მოსახლეობის რწმენის შერყევა არჩევნების შედეგებისადმი. DNC hack განიხილება, როგორც რუსეთის ხელისუფლების უმაღლეს დონეზე სანქცირებული ჩარევა აშშ-ის არჩევნებში, დემოკრატიულ პროცესების რწმენის შესუსტების და კონკრეტული კანდიდატის კომპრომეტაციის მიზნით.

2017 წლის 5 მაისს, საფრანგეთის პრეზიდენტის არჩევნებამდე ორი დღით ადრე მიზანმიმართული ფიშინგის გზით მოპოვებულ იქნა მაკრონის საარჩევნო გუნდის კუთვნილი რამდენიმე გიგაბაიტი ინფორმაცია, რომლის ავთენტურობა ან ცალსახა სიყალბე რთული დასადგენია. მასალა სპეციალურად შექმნილ პლატფორმაზე გამოქვეყნდა უშუალოდ არჩევნების წინ, რამაც გაართულა მაკრონის შტაბის მხრიდან რეაგირება. ამავდროულად, სოციალურ ქსელში გასავრცელებლად და ნეგატიური განწყობების გასამძაფრებლად ბოტების მიერ წარმოებულმა კამპანიამ დიდი როლია შეასრულა. ჩარევის მიზანი რუსეთისამდი პოზიტიურად განწყობილი კანდიდატის მხარდაჭერა იყო, რომელიც ამ შემთხვევაში უშედეგოდ დასრულდა.

გერმანიის ბუნდესტაგის არჩევნების წინ, 2015 წელს განხორციელდა ელექტრონული ფოსტის კონტენტის მოპარვა ბუნდესტაგის სერვერებიდან და კანცლერ მერკელის ქრისტიან-დემოკრატიული პარტიის საინფორმაციო სისტემებიდან, თუმცა ამ ინფორმაციის გამოქვეყნება არ მომხდარა. ამავდროულად, ნეგატიური განწყობების გაღვივების მიზნით, გერმანულენოვანმა რუსულმა გამოცემებმა სოციალურ ქსელში ბოტებისა და ტროლების ჩართულობით გააჩაღეს ანტისაიმიგრაციო აქცენტებზე დაფუძნებული კამპანია, რომელიც მიზნად ისახავდა პოლიტიკურ პოლარიზაციას, და საარჩევნო პროცესისადმი ნდობის შემცირებას და არჩევნების შედეგების დელეგიტიმიზაციას. პარალელურად, ხდებოდა ყალბი **კონტენტის** გავრცელება, რომელიც ემყარებოდა გერმანელი გოგონას არაბი მიგრანტის მიერ გაუპატიურების გამოგონილ ამბავს. გერმანული სპეცსამსახურების აზრით, რუსეთის მხრიდან არჩევნებში ჩარევა, შესაძლოა, არც იყო რომელიმე კანდიდატის ან პარტიის მხარდასაჭერად განხორციელებული, არამედ, რაც უფრო სარწმუნოა, მიზნად ისახავდა დემოკრატიული პროცესების და ზოგადად არჩევნების ინსტიტუტის დისკრედიტაციას. ამგვარი ჩარევის მთავარი მიზანი დემოკრატიული ინსტიტუტების გრძელვადიანი დისკრედიტაცია და ნებისმიერი მომავალი მმართველობისადმი მხარდაჭერის შესუსტებაა, რაც რუსული გეოპოლიტიკური ინტერესების რეალიზაციას უწყობს ხელს. აღნიშნულის დასტურად ის ფაქტიც გამოდგება, რომ თუმცა მერკელის პარტიამ არჩევნებში გაიმარჯვა, მაგრამ მან მიიღო საკუთარ ისტორიაში ყველაზე ნაკლები ხმა.

ამრიგად, ზემოაღნიშნული საარჩევნო ინციდენტების ანალიზი ცხადყოფს, რომ მოქმედებს სქემა, რომლის მიხედვითაც კიბერთავდასხმის შედეგად ხდება საინფორმაციო სისტემების პენეტრაცია, არსებული სენსიტიურ ინფორმაციაზე წვდომის მოპოვება და შემდგომ პოლიტიკური ფიგურების ან ინსტიტუტების დისკრედიტაციის

მიზნით მისი კონტროლირებადი გავრცელება. ნეგატიური განწყობების გაღრმავების მიზნით, ბოტებისა და ტროლების მიერ ყალბი პროფაილებისა ან ბლოგების გამოყენებით გავრცელებული ინფორმაციის კომენტირებით ხდება რუსული ნარატივის დამკვიდრება, ცრუ ინფორმაციის გავრცელება და სასურველი საზოგადოებრივი აზრის ჩამოყალიბება.

თუკი რუსეთის მხრიდან საქართველოს შიდაპოლიტიკური პროცესებით დაინტერესების ხარისხს, ქართული სახელმწიფო თუ კერძო სექტორის ქსელების მოწყვლადობას და რუსული დესტრუქციული კიბერაქტორების მიერ პენეტრაციის მასშტაბებს გავითვალისწინებთ, ცხადია, ქართულ საარჩევნო კამპანიაში რუსული ჩარევის ალბათობა ცალსახად ყურადსაღებია. ცნობილი ფაქტია, რომ კრემლთან დაკავშირებულ აქტორებს, ხანგრძლივი დროის განმავლობაში ჰქონდა არასანქცირებული წვდომა ქართულ სახელმწიფო, საკომუნიკაციო თუ ბიზნეს-ქსელებთან, რის შედეგადაც, სავარაუდოდ დიდი მოცულობა სენსიტიური ინფორმაციისა წლების მანძილზე ხვდებოდა რუსული სპეცსამსახურების ხელში[7]. ჩვენს არჩევნებში, გარდა არალეგალურად მოპოვებული მაკომპრომეტირებელი მასალებისა, გასავრცელებელი კონტენტის კიდევ ერთი წყაროდ იქცევა ხოლმე ღია რესურსებსა და სოციალურ ქსელებში არსებული ამა თუ იმ კანდიდატის ან მათი მხარდამჭერი პოლიტიკური ძალების მოსაზრებები თუ გამონათქვამები სენსიტიურ თემებსა და პროცესებზე.

შესაბამისად, უკიდურესად მნიშვნელოვანია მოხდეს არჩევნებში რუსული ჩარევის მაგალითების განხილვის შედეგად შეტევების ხშირად გამოყენებული ტექნიკების, კიბერსაფრთხეების, მეთოდიკების კლასიფიკაცია და რისკების მიტიგაციისათვის რეკომენდაციების შემუშავება.

დღემდე არსებული მონაცემებით, რუსეთი არჩევნებში ჩასარევად ყველაზე ხშირად კიბერთავდაცსხმებისა და სანფორმაციო ოპერაციების შემდეგ მეთოდებს იყენებს:

სოციალური ინჟინერია - ინტერნეტ-თაღლითობის ერთ-ერთი ტექნიკა, რომელიც იწვევს მანიპულირების გზით მომხმარებლის მიერ გაუცნობიერებლად კონფიდენციალური მონაცემების ჰაკერისთვის გამჟღავნებას, მის ინფიცირებულ ლინკზე გადასვლას ან/და კომპიუტერში მავნე პროგრამული უზრუნველყოფის ინსტალაციას. ეს

[7] Fire eye special report, 2014. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. ხელმისაწვდომია https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

მეთოდი წარმატებით გამოიყენება იმ მომხმარებლის მიმართ, ვინც ბოლომდე ვერ აცნობიერებს პერსონალური მონაცემების მნიშვნელობას ან მისი დაცვის ხერხებს.

ფიშინგი - კიბერკრიმინალის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლს მოტყუების გზით მოპაროს სენსიტიური ინფორმაცია ან/და მოახდინოს კომპიუტერის კომპრომეტაცია. გამოიყენება მეილი, რომელიც წარმოჩენილია როგორც სანდო წყაროსგან მიღებული შეტყობინება, როგორიცაა ბანკი ან ნებისმიერი სხვა ორგანიზაცია თუ პირი ვისთანაც მსხვერპლს შესაძლოა ქონდეს ურთიერთობა. მეილი შენიღბულია როგორც სასწრაფო შეტყობინება, რომელშიც დამატებითი ინფორმაციისთვის მოთავსებულია ვებ-ბმულები ან მიმაგრებული დოკუმენტები. ფიშინგ მეილში მოთავსებულ ბმულზე გადასვლის, ან ფაილის გახსნის შედეგად შესაძლებელია მოხდეს მსხვერპლის კომპიუტერში შეღწევა ან მისგან დამატებით სენსიტიური ინფორმაციის მოთხოვნა (პაროლი, მომხმარებლის სახელი, ბარათის ინფორმაცია და სხვა). ფიშინგ მეილები იგზავნება მასიურად, მაქსიმალურად მეტ ადრესატთან, რაც მათი წარმატების ალბათობას რეალურს ხდის.

ფიშინგის განსაკუთრებულ ფორმას წარმოადგენს ე.წ. **Spear-Phishing**, რომელიც განკუთვნილია მომხმარებლის ვიწრო და სპეციფიური წრისათვის (მმართველობა, გარკვეული ცოდნის, ინფორმაციის მატარებელი ჯგუფი). საჭიროებს კარგად მომზადებულ კონტექსტს ნდობის მოსაპოვებლად. გარდა ფინანსურად მოტივირებული კიბერკრიმინალისა, ფიშინგის სხვადასხვა ფორმა აქტიურად გამოიყენება სახელმწიფოთაშორის დესტრუქციულ კიბეროპერაციებში მოწინააღმდეგის ქსელის კომპრომეტაციისათვის.

SQL-injection - შეტევის ტექნიკა, რომელიც პროგრამულ უზრუნველყოფაში არსებული სისუსტეების გამოყენებით გზით უზრუნველყოფს კოდის „ინექციას“ და მონაცემთა ბაზაზე არასანქცირებულ წვდომას ან მანიპულირებას (მავნე კოდის დაგზავნა, მონაცემთა წაშლა, საწყისი გვერდის შეცვლა).

პორტების სკანირება - თავდამსხმელების მიერ ხშირად გამოყენებული ტექნიკა სამიზნე სისტემების სისუსტეების გამოსავლენად, ძირითადად გამოიყენება არასათანადოდ დაცულ სერვერებსა და ქსელებზე არაავტორიზებული წვდომის მოსაპოვებლად.

MITM (Man in the Middle)- შეტევის სახე, როდესაც თავდამსხმელი არაავტორიზებულად ერთვება ორი ან რამდენიმე მხარის კომუნიკაციაში და მოიპოვებს წვდომას მათ შორის მიმოცვლილ ინფორმაციაზე.

DDoS (A distributed-denial-of-service) - კომპრომეტირებული კომპიუტერების მეშვეობით გენერირებული დიდი რაოდენობით მონაცემთა მოთხოვნის ნაკადის

მიმართვა სერვერისკენ, რომელიც მიმართულია ქსელის გამტარობის და ოპერატიული მეხსიერების გადასავსებად, რასაც შესაძლოა შედეგად მოჰყვეს სამიზნე სისტემის მწყობრიდან გამოყვანა და ბიზნეს-პროცესის მოშლა.

ინსაიდერული შეტევა - შეტევა, რომლის დროსაც ყოფილი ან მოქმედი თანამშრომელი, ვენდორი, კონტრაქტორი ან სხვა ავტორიზებული პირი უფლებამოსილებას იყენებს მავნე ზემოქმედებისათვის.

საინფორმაციო ოპერაციები - პროპაგანდა, დეზინფორმაცია და სხვა საშუალებები, რომელთა გამოყენებაც ხდება ამომრჩევლის აზრის მანიპულირებისათვის, კიბერსივრცის ამ მიზნით გამოყენებამ წარმოუდგენლად გააფართოვა ამგვარი ოპერაციების შესაძლებლობები როგორც მასშტაბის, ასევე ეფექტის თვალსაზრისითაც. არჩევნების კონტექსტში ამგვარი ოპერაციები გამოიყენება არჩევნების შედეგებისადმი უნდობლობის დასათესად, ამა თუ იმ პოლიტიკური ძალის დისკრედიტაციისათვის, ასევე დემოკრატიული წყობის და მთავრობების დელეგიტიმიზაციისათვის.

ინფორმაციის კონტროლირებადი გაჟონვა - თავამსხმელები, ახდენენ რა სამიზნე ქსელის პენეტრაციას, განათავსებენ მოპარულ სენსიტიურ ინფორმაციას სოციალურ ქსელში ან სპეციალურ პლატფორმაზე. საარჩევნო სუბიექტების ბიუჯეტის, სპონსორების, საარჩევნო სისტემის სისუსტეებისა და სენსიტიური პროცესების შესახებ ინფორმაციის ან ფაბრიკაციის გაჟონვა არჩევნების შედეგებისადმი უნდობლობას იწვევს.

ცრუ ან შეცდომაში შემყვანი ინფორმაციის გავრცელება - სოციალური ქსელის თავდამსხმელის მიერ მიტაცებული ოფიციალური ანგარიშიდან ან სოციალური მედიისა და დაფინანსებული რეკლამის მეშვეობით მცდარი ან შეცდომაში შემყვანი ინფრმაციის გავრცელება არჩევნების დროის, ადგილის, შედეგების შესახებ, კანდიდატის, პოლიტიკური ჯგუფის დისკრედიტაცია ან არჩევნების შედეგებით მანიპულირება,

ანტაგონისტური განწყობების გაღვივება - ხშირად პოლარიზაციის გასამძაფრებლად გამოიყენება არსებული უთანხმოებები, სამეზობლო დავები, ეთნიკური, რელიგიური ან სხვა სახის უმცირესობების პრობლემატიკა. ადგილი აქვს ტრადიციული, ხშირად ყოფითი სამეზობლო დავის სახელმწიფოთაშორისი ურთიერთობების კონტექსტში გადატანას, ან ერთაშორისი ურთიერთობის უკიდურესად ნეგატიურ ჭრილში წარმოჩენას, ტრადიციულად სენსიტიურ საკითხებზე აქცენტირებას, ნეგატიურ პრიზმაში ნაჩვენები პრობლემატიკის ტირაჟირებას სოციალური ქსელებით და შემდგომ ამაზე დისკუსიის გამართვას ტროლების, „სასარგებლო იდიოტების“, თუ სხვა საშუალებების ჩართულობით, რაც, საბოლოო ჯამში ერთაშორისი ან სახელმწიფოთაშორისი ურთიერთობების რანგში აიყვანება.

მიუხედავად არჩევნების ტიპისა, კანონმდებლობისა თუ სისტემების მრავალფეროვნებისა, არსებობს საუკეთესო პრაქტიკა, რომელიც უზრუნველყოფს პროცესის კიბერუსაფრთხოებას, არჩევნების შედეგების მთლიანობის და სანდოობის დაცულობას, როგორც ტექნიკური ასევე შინაარსობრივი თვალსაზრისით. განვიხილოთ ზოგიერთი მათგანი და მათ დასამკვიდრებლად განსახორციელებელი ღონისძიებები:

1. **კიბერუსაფრთხოების პროაქტიული კულტურის დანერგვა.** წარმატებული კიბერშეტევების დიდი უმრავლესობა ადამიანურ ფაქტორთან - მომხმარებლის შეცდომასთან არის დაკავშირებული, ამიტომ კიბერუსაფრთხოების კულტურის დანერგვა, „ზემოდან-ქვემოთ“ პოლიტიკა რისკების შემცირების უმნიშვნელოვანესი ინსტრუმენტია. კიბერუსაფრთხოების ფესვგადგმული კულტურა, მომხმარებლის კიბერჰიგიენის გაცნობიერებული ჩვევები ასევე დიდწილად განაპირობებს თავდამსხმელის მხრიდან სისტემის სამიზნედ შერჩევის ალბათობის ხარისხს, განხორციელებული თავდასხმის წარმატებულობის მინიმიზაციას ან ფსიქოლოგიური ზემოქმედების მიზნით წარმატების აღქმის შექმნის შესაძლებლობას.
    - ტოპ-მენეჯმენტის ჩართულობა კიბერუსაფრთხოების საკითხებში;
    - ინციდენტების მართვის დეტალური გეგმის შემუშავება/იმპლემენტაცია
    - არჩევნების ადმინისტრირებაში მონაწილე პირთა სანდოობის შემოწმება
    - გარე რესურსების გამოყენება უწყებათაშორისი და საჯარო-კერძო თანამშრომლობის ფარგლებში
2. **სისტემის კიბერუსაფრთხოებისადმი კომპლექსური მიდგომა.** საარჩევნო სისტემის ნებისმიერი სეგმენტის კომპრომეტაციამ შესაძლოა გამოიწვიოს მთლიანად სისტემის პენეტრაცია. თავდამსხმელები ეძებენ სუსტ წერტილებს, რომელთა მეშვეობითაც ხდება სისტემაში შეღწევა. ინტერნეტთან კავშირის არმქონე სისტემის კომპრომეტაციაც კი შესაძლებელია გარე მეხსიერების და სხვა მობილური მოწყობილობების საშუალებით.
    - პროცესთან შემხებლობაში მქონე ყველა კომპიუტერის და მოწყობილობის დაცვა, მიუხედავად მათი კუთვნილებისა
    - კიბერუსაფრთხოების მენეჯმენტის ოპტიმიზაცია და ცენტრალიზება
3. **ძლიერი პასვორდისა და ორმაგი ავთენთიფიკაციის პოლიტიკის დანერგვა.** თავდამსხმელები სისტემის კომპრომეტირებისათვის ხშირად იყენებენ მომხმარებლის საავტორიზაციო მონაცემებს. რადგან პასვორდის გატეხვის ძირითადი მეთოდი ამ პასვორდის კომპონენტთა კომბინაციათა შესაძლო რიცხვზეა დამოკიდებული, მიზანშეწონილია 8 ან მეტსიმბოლოიანი, სათანადო წესით შედგენილი პასვორდის სავალდებულო გამოყენება. ასევე, აუცილებელია ორფაქტორიანი ავტორიზაციის პოლიტიკის დანერგვა.
4. **წვდომის კონტროლი და მენეჯმენტი.** ნებისმიერი ავტორიზებული მომხმარებელი წარმოადგენს თავდამსხმელთა სამიზნეს და ხშირად, ერთი მომხმარებლის კომპრომეტაცია საკმარისია ქსელზე სრული წვდომის

მოსაპოვებლად. შესაბამისად, რაც უფრო მეტ ადამიანს აქვს წვდომა სისტემასთან და რაც უფრო ფართოა მათი წვდომის არეალი, მით მეტია სისტემის კომპრომეტაციის საფრთხე.

- სისტემაზე ავტორიზებული წვდომის მქონე პირთა რაოდენობის შეზღუდვა
- ავტორიზებულ პირთათვის წვდომის მინიჭება მხოლოდ აუცილებელ მონაცემებზე, „მინიმალური უფლებების“ პრინციპით.
- მომხმარებლის წვდომის ავტომატური გაუქმება პოზიციის, კომპეტენციის სფეროს შეცვლისას ან სამსახურიდან დათხოვნისას

5. **მგრძნობიარე მონაცემების და სისტემების გამიჯვნა.** სისტემის ნებისმიერი სეგმენტი მნიშვნელოვანია, თუმცა აუცილებელია პრიორიტეტების განსაზღვრა მონაცემთა სენსიტიურობის თვალსაზრისით, რადგან დაცვის დამატებითი ღონისძიებები მოითხოვს დანახარჯებს და საოპერაციო პროცედურებს.
   - სენსიტიური მონაცემების შემცველი მოწყობილობების კონფიგურირება მხოლოდ კონკრეტული ქმედების განხორციელების შესაძლებლობით
   - მობილური მოწყობილობების გამოყენების სისტემური აკრძალვა
6. **მონიტორინგის, ლოგირების და სარეზერვო ასლების სისტემის შექმნა.** მონიტორინგი, ლოგების ჟურნალი და სარეზერვო ასლების სისტემა შესაძლებლობას გვაძლევს მოვახდინოთ შეტევის დეტექცია და ინციდენტის შემდგომ სისტემის აღდგენა.
   - მონაცემთა ბაზების ნებისმიერი ცვლილების ლოგირება და მონიტორინგი ადამიანური რესურსით თუ ანომალიის აღმომჩენი პროგრამული უზრუნველყოფით
   - სარეზერვო ასლების რეგულარული შექმნის ავტომატური პროცესის იმპლემენტაცია. ასლი შექმნის მომენტიდან უნდა იყოს Read only და მისგან მონაცემთა სრული აღდგენის შესაძლებლობის ტესტირება უნდა ხდებოდეს რეგულარულად.
7. **ვენდორის/კონტრაქტორის კიბერუსაფრთხოების ხარისხის გათვალისწინება.** საარჩევნო პროცესის პროგრამული უზრუნველყოფის, საოპერაციო სისტემის, სხვადასხვა სერვისის მომწოდებლის ან ავტორიზებული წვდომის მქონე კონტრაქტორის არასათანადო დაცულობა რეალური ინსაიდერული საფრთხეა სისტემისათვის, რადგან წარმოადგენს მონაცემთა განადგურების, შეცვლის ან გაჟონვის ერთ ერთ ყურადსაღებ მიმართულებას.

დასასრულს, რამდენიმე პრაქტიკული რჩევა იმასთან დაკავშირებით, თუ რა უნდა იცოდეს ნებისმიერმა საარჩევნო პროცესის ადმინისტრირებასთან შემხებლობაში მყოფმა პირმა. **კიბეროპერაციების დიდი უმრავლესობა**, მიუხედავად იმისა, რომ ისინი მტრული სახელმწიფოს სტრატეგიული ამოცანის - არჩევნებზე ზეგავლენის მოხდენის განხორციელებას ემსახურებიან **ადამიანური ფაქტორით, მომხმარებლის შეცდომითაა განპირობებული.** ფიშინგის, სოციალური ინჟინერიის სხვა შეტევების გამანადგურებელი შედეგების თავიდან აცილება მომხმარებლის კიბერჰიგიენის წესების

დაცვითაა შესაძლებელი. **კიბერჰიგიენა** არის საუკეთესო პრაქტიკა და აქტივობები კიბერუსაფრთხოების ასამაღლებლად, რომელიც **ემყარება მომხმარებლის გაცნობიერებულ ჩვევებს**:

- **კიბერუსაფრთხოების პრობლემატიკის სერიოზული აღქმა საარჩევნო ადმინისტრაციის მხრიდან.** აუცილებელია, ადმინისტრაციის ყველა დონე იზიარებდეს პასუხისმგებლობას რისკების შემცირებაზე, ხოლო მენეჯმენტი რეგულარულად ახდენდეს თანამშრომლების ცნობიერების ამაღლებას, როგორც კიბერუსაფრთხოების სტრატეგიულ თემატიკაზე, ასევე კიბერჰიგიენის თვალსაზრისითაც.
- **მნიშვნელოვანია რთული პასვორდის პოლიტიკა.** პასვორდი უნდა შეიცავდეს მინიმუმ 8 სიმბოლოს, მაღალი და დაბალი რეგისტრის ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს. კიდევ უფრო უსაფრთხოა პასფრაზის გამოყენება. (მაგალითად: **Don’twoRybeHeppy1, We@rethechamp1ons!, Ca1lmeIshm@el). პაროლის შესაქმნელად პიროვნებასთან დაკავშირებული სიტყვების გამოყენება,** როგორიცაა, მაგალითად: სახელები, დაბადების დღეების თარიღები და სხვა. არ არის მიზანშეწონილი.
- **დაუშვებელია კომპიუტერის უპასვორდოდ დატოვება ან პაროლის, სხვა საავტორიზაციო მონაცემების სხვისთვის განდობა, მიუხედავად მასთან ურთიერთობის ხარისხისა.**

- **ორმაგი ავტენტიფიკაციის (2FA) გამოყენება მიზანშეწონილია ყველგან:** სამსახურებრივ ანგარიშებზე, პირად ელექტრონულ ფოსტაზე, სოციალური მედიის გვერდებსა თუ მონაცემთა შენახვის სერვისებზე. ორმაგი ავტენტიფიკაციის მექანიზმი ანგარიშზე შესასვლელად, ავტორიზაციის გასავლელად მოითხოვს ორ ან რამდენიმე, სხვადასხვა სივრცეში არსებულ კომპონენტს: რაც ვიცით (მაგ. პასვორდი, კოდი), რაც გვაქვს (მაგ. ტოკენი, დიჯიპასი) რაც ახდენს ჩვენს იდენტიფიცირებას (მაგ. ბიომეტრია) და ა. შ. ავტორიზაციის მეორე დონისათვის მიზანშეწონილია SMS შეტყობინების ნაცვლად მობილური აპლიკაციის (მაგ.Google Authenticator, Duo, Authy) ან ფიზიკური მოწყობილობის გამოყენება.

- აუცილებელია **ლიცენზირებული და რეგულარულად განახლებული ოპერაციული სისტემის, პროგრამების, აპლიკაციების, ანტივირუსული უზრუნველყოფის გამოყენება**.

- რისკის შემცველია **მტრული სახელმწიფოს წარმოებული პროგრამებისა და აპლიკაციების გამოყენება**. აპლიკაციის ჩამოტვირთვისას, ყოველთვის მნიშვნელოვანია, რა ინფორმაციასა და რესურსზე (კამერა, მიკრიფონი,

მეხსიერება) ითხოვს იგი წვდომას და რამდენად საჭიროა ეს წვდომა მისი უშუალო ფუნქციის განსახორციელებლად

REFERENCE

1. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019
2. Sergiy Gnatyuk , Maksim Iavich , Giorgi Iashvili , Andriy Fesenko ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY, Scientific and practical cyber security journal, 2019
3. B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 380-388, doi: 10.1109/iThings/CPSCom.2011.34.
4. R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu and P. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," in IEEE Technology and Society Magazine, vol. 30, no. 1, pp. 28-38, Spring 2011, doi: 10.1109/MTS.2011.940293.
5. Zhiqiang Gao and N. Ansari, "Tracing cyber attacks from the practical perspective," in *IEEE Communications Magazine*, vol. 43, no. 5, pp. 123-131, May 2005, doi: 10.1109/MCOM.2005.1453433.
6. S. Musman, M. Tanner, A. Temin, E. Elsaesser and L. Loren, "Computing the impact of cyber attacks on complex missions," 2011 IEEE International Systems Conference, 2011, pp. 46-51, doi: 10.1109/SYSCON.2011.5929055.
7. M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions," in IEEE Access, vol. 9, pp. 7152-7169, 2021, doi: 10.1109/ACCESS.2020.3048839.
8. M. Elsisi, M. -Q. Tran, K. Mahmoud, D. -E. A. Mansour, M. Lehtonen and M. M. F. Darwish, "Towards Secured Online Monitoring for Digitalized GIS Against Cyber-Attacks Based on IoT and Machine Learning," in *IEEE Access*, vol. 9, pp. 78415-78427, 2021, doi: 10.1109/ACCESS.2021.3083499.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 50-56 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

პოსტ-კვანტური ხელმოწერის დიზაინის საწყისი კონცეფციები Verkle-ის ხის გამოყენებით

THE INITIAL CONCEPTS OF POST-QUANTUM SIGNATURE DESIGN USING VERKLE TREE

მაქსიმ იავიჩი, სამეცნიერო კიბერუსაფრთხოების ასოციაცია, კავკასიის უნივერსიტეტი
Maksim Iavich, Scientific cyber security association, Caucasus University
ავთანდილ გაგნიძე, სამეცნიერო კიბერუსაფრთხოების ასოციაცია, აღმოსავლეთ ევროპის უნივერსიტეტი
Avtandil Gagnidze, Scientific cyber security association, East European University
გიორგი იაშვილი, სამეცნიერო კიბერუსაფრთხოების ასოციაცია, კავკასიის უნივერსიტეტი
Giorgi Iashvili, Scientific cyber security association, Caucasus University

რეზიუმე: ნაშრომში აღწერილია ჰეშზე დაფუძნებული პოსტკვანტური ციფრული სქემები. გაანალიზებულია ციფრული ხელმოწერები Merkle-ს ხეზე დაყრდნობით. ნაშრომის ავტორები გვთავაზობენ ციფრული ხელმოწერის დიზაინის მეთოდოლოგიას ახალი ტექნოლოგიის, Verkle-ს ხის გამოყენებით. ისინი ასევე გვთავაზობენ პოსტ-კვანტური ხელმოწერის დიზაინის კონცეფციებს Verkle-ის ხის გამოყენებით.

საკვანძო სიტყვები: პოსტ-კვანტური, Verkle-ს ხე, Merkle-ს ხე, ციფრული ხელმოწერა, პოსტკვანტური ხელმოწერის დიზაინი, გასაღების გენერაცია, ხელმოწერის გენერაცია, ხელმოწერის ვერიფიკაცია

ABSTRACT: *The paper describes post-quantum hash-based digital schemes. It analyzes digital signatures based on Merkle tree. The authors of the papers offer the methodology of designing the digital signature using the novel technology, Verkle tree. They also offer the concepts of post-quantum signature design using Verkle Tree.*

KEYWORDS: *post-quantum, Verkle Tree, Merkle Tree, igital signature, post-quantum signature design, Key generation, Signature generation, Signature verification*

შესავალი

ბოლო დროს მსოფლიოს წამყვანი მეცნიერები და ინჟინრები დაუღალავად მუშაობენ კვანტური კომპიუტერების შექმნაზე. აღიარებული ლიდერები კვანტური კომპიუტერების განვითარებაში Google Corporation, Universities Space Research Association, federal agency NASA და D-WAVE, უკვე მზად არიან გარღვევის მოსახდენად კვანტური ტექნოლოგიის სფეროში. 2019 წლის ოქტომბერში Google-მა განაცხადა, რომ მიაღწია კვანტურ უზენაესობას, რამაც სერიოზული კამათი გამოიწვია, მაგრამ თუ გავითვალისწინებთ იმ ფაქტს, რომ ტექნიკური გიგანტები იბრძვიან პირველი კვანტური კომპიუტერების შესაქმნელად და მათ მნიშვნელოვან წარმატებებსაც მიაღწიეს ამ მიმართულებით, მსოფლიო შეიძლება დადგეს ახალი ეპოქის

ზღვარზე. Google თვლის, რომ მისი ამჟამინდელი ჩიპის დიზაინს შეუძლია გაზარდოს მეხსიერების მოცულობა 100-დან 1000 კუბიტამდე. IBM მას ფეხდაფეხ მოსდევს, რადგან ამტკიცებს, რომ 2023 წლის ბოლოსთვის შექმნის 1000 კუბიტზე მეტი სიმძლავრის და დაახლოებით 10-დან 50 ლოგიკურ კუბიტამდე სიმძლავრის კვანტურ პროცესორს. მან 2021 წელს უკვე წარმოადგინა 127 კუბიტიანი, ხოლო 2022 წელს 433 კუბიტანი პროცესორი. ჩინელი მეცნიერები ამტკიცებენ, რომ "Zuchongzhi 2" - 66 კუბიტიანმა კვანტურმა პროცესორმა, დავალება Google-ის პროცესორთან შედარებით 1 მილიონჯერ უფრო სწრაფად შეასრულა. ეს პროცესორი შეიქმნა ჩინეთის მეცნიერებათა აკადემიის კვანტური ინფორმაციისა და კვანტური ფიზიკის მოწინავე გამოცდილების ცენტრის მკვლევართა გუნდის მიერ შანხაის ტექნიკური ფიზიკის ინსტიტუტთან და შანხაის მიკროსისტემისა და საინფორმაციო ტექნოლოგიების ინსტიტუტთან ერთად [1-5].

დაბოლოს, კვანტური კომპიუტერები შეძლებენ დღეისათვის არსებული კრიპტოგრაფიული კოდების გატეხვას, რომლებიც გამოიყენება კომუნიკაციებისა და ფინანსური ტრანზაქციებისთვის, ასე რომ, ამჟამად გამოყენებული ციფრული ხელმოწერის სისტემები უძლურია კვანტური კომპიუტერებით განხორციელებული თავდასხმების მიმართ, ამიტომ მსოფლიომ უნდა მიიღოს კვანტურ-რეზისტენტული კრიპტოგრაფია. ამჟამად გამოყენებული ციფრული ხელმოწერის სისტემების უსაფრთხოება ემყარება დისკრეტული ლოგარითმების გაანგარიშების პრობლემას და დიდი რიცხვების ფაქტორიზაციას. ზოგიერთი კრიპტოსისტემა, მაგალითად RSA - ოთხი ათასი ბიტიანი გასაღებით, გამოსადეგია კლასიკური კომპიუტერით განხორციელებული შეტევების წინააღმდეგ, მაგრამ აბსოლუტურად უსარგებლოა კვანტური კომპიუტერების მიერ განხორციელებული შეტევების წინააღმდეგ.

დღისათის RSA კრიპტოსისტემა თითქმის ყოველ ნაბიჯზე გამოიყენება, რადგან მას იყენებს მრავალი მსხვილი ორგანიზაცია, მაგალითად, სამთავრობო დაწესებულებები, ბანკები, კორპორაციების უმეტესობა, სამთავრობო ლაბორატორიები და უნივერსიტეტები. გარდა ამისა, ეს კრიპტოსისტემა გამოიყენება კომერციულ პროდუქტებში, ოპერაციულ სისტემებში, Ethernet-ში, ქსელურ ბარათებში, სმარტ ბარათებში და ასევე გამოიყენება კრიპტოგრაფიულ აპარატურაში. RSA BSAFE დაშიფვრის ტექნოლოგიას დაახლოებით 500 მილიონი მომხმარებელი ჰყავს, რომელთა რიცხვი სწრაფად იზრდება. RSA ალგორითმი არის ერთ-ერთი ყველაზე გავრცელებული საჯარო გასაღების კრიპტოსისტემა. ამიტომ RSA-ს გატეხვამ შეიძლება სრული ქაოსი გამოიწვიოს. მეცნიერები თვდაუზოგავად მუშაობენ RSA-ს ალტერნატივების შესაქმნელად, რომელიც კვანტური კომპიუტერების თავდასხმებს გაუძლებს. RSA-ს ალტერნატივად ჩვენ შეგვიძლია განვიხილოთ კრიპტოგრაფიულ ჰეშ ფუნქციაზე დაფუძნებული ციფრული ხელმოწერის ჰეშ სქემები. ჰეშ ფუნქციის კოლიზიისადმი მედეგობა არის ამ ხელმოწერის უსაფრთხოების გარანტი.

1. ჰეშზე დაფუძნებული ციფრული ხელმოწერის სქემა:

Lamport–Diffie-ის მიერ შემოთავაზებული ჰეშზე დაფუძნებული ერთჯერადი ხელმოწერის სქემა, განიხილება, როგორც ციფრული ხელმოწერის ალტერნატიული სქემა პოსტკვანტური ეპოქისთვის. ჩვენ ვხედავთ, რომ გასაღები და ხელმოწერის გენერირება ეფექტურია Lamport–Diffie-ის ერთჯერადი ხელმოწერის სქემაში, მაგრამ ხელმოწერის ზომა უდრის n2-ს, სადაც ჰეშირებული ბადის ზომა არის n, რაც საკმაოდ დიდია. Winternitz-ის მიერ შემოთავაზებული ერთჯერადი ხელმოწერის სქემა მნიშვნელოვნად ამცირებს ხელმოწერის ზომას, რადგან ამ სქემაში შეგვიძლია ერთი სტრიქონიანი გასაღების გამოყენება ჰეშირებული შეტყობინების რამდენიმე ბიტის ხელმოსაწერად [5], მაგრამ, ამ შემთხვევაში პრობლემის წინაშე ვდგებით, როდესაც ვიყენებთ ერთჯერადი ხელმოწერის სქემას გასაღებების დიდი რაოდენობის გასაცვლელად, რადგან ის იყენებს სხვადასხვა გასაღების წყვილს ყოველი შეტყობინებისთვის. ამ პრობლემის გადასაჭრელად Merkle-ის ციფრული ხელმოწერის სქემა იყენებს ოროობით ხეს, რათა თავიდან აიცილოს ვერიფიკაციის გასაღებების დიდი რაოდენობის გამოყენება ერთ საჯარო გასაღებთან. საჯარო გასაღები აქ არის ამ ხის ფესვი [6-12].

გასაღების გენერაცია: ხის სიგრძე არჩეულია როგორც H>=2. აქ ერთ საჯარო გასაღებს შეუძლია ხელი მოაწეროს 2H რაოდენობის დოკუმენტს. იქმნება 2H გასაღების წყვილი Xi და Yi, სადაც Xi არის ხელმოწერის გასაღები და Yi ვერიფიკაციის გასაღები, h (Yi) გამოითვლება და გამოიყენება ხის ფოთლებად. ხის თითოეული განშტოება არის მისი შვილების კონკატენაციის ჰეშ მნიშვნელობა.

a[1,0]=h(a[0,0] || a[0,1])

Merkle-ის კრიპტო სქემის საჯარო გასაღები არის ოროობითი ხის ფესვი, მის შესაქმნელად საჭიროა 2H წყვილი ერთჯერადი გასაღების გამოთვლა.

ხელმოწერის გენერირება: რენდომული ზომის შეტყობინება m, გარდაიქმნება n ზომის შეტყობინებად ჰეშის ფუნქციის საშუალებით. h (m) = ჰეში, და იქმნება ერთჯერადი ხელმოწერა რენდომული ერთჯერადი გასაღების Xarb-ის გამოყენებით, დოკუმენტის ხელმოწერა იქნება: ერთჯერადი ხელმოწერის, ერთჯერადი ვერიფიკაციის გასაღები Yarb, ინდექსის arb და ყველა "authi" მონათესავე ტოტის შეერთება Yarb- თან მიმართებაში.

Signature= (sig||arb|| Y_{arb}||$auth_0$,…,$auth_{H-1}$)

ხელმოწერის დადასტურება: Merkle-ის კრიპტო-სისტემის ხელმოწერის დამადასტურებელ ხელმოწერაში, sig-ის ერთჯერადი ხელმოწერა უნდა გადამოწმდეს Yarb-ის გამოყენებით, იმ შემთხვევაში თუ ეს სწორი იქნება, ყველა კვანძი a [i, j] გამოითვლება "authi", ინდექსის arb და Yarb გამოყენებით. თუ ხის ფესვი უდრის საჯარო გასაღებს, მაშინ ხელმოწერა სწორია.

2. Verkle vs Merkle

Verkle-ს ხეები არის Merkle-ს ხეების ძლიერი განახლება, რაც იძლევა ბევრად უფრო მცირე ზომის ვერიფიკაციის გამოყენების საშუალებას და უფრო ეფექტურია. Verkle-ს ხის სტრუქტურა ძალიან ჰგავს Merkle Patricia ხეს [13, 14].

სურათზე 1, აგებულია Verkle-ს ხე 9 ფაილისგან, სადაც განშტოების კოეფიციენტი არის 3. ფაილების k = 3 ზომის ქვეჯგუფებად დაყოფის შემდეგ, თითოეულ ქვეჯგუფზე გამოითვლება ვექტორის ვალდებულება შესაბამისი წევრობის მტკიცებულებებთან ერთად. ეს გვაძლევს ვალდებულებებს VC1, VC 2 და VC3. ვექტორული ვალდებულება VC4 გამოითვლება ამ სამ ვალდებულებასთან ერთად წევრობის მტკიცებულებებთან ერთად p9, p10 და p11 ვალდებულებებისთვის VC1, VC2 და VC3 შესაბამისად VC4 ვალდებულების მიმართ. Verkle-ს ხის საბოლოო გადაწყვეტა არის ძირეული ვალდებულება, რომელიც ამ შემთხვევაში არის VC4.

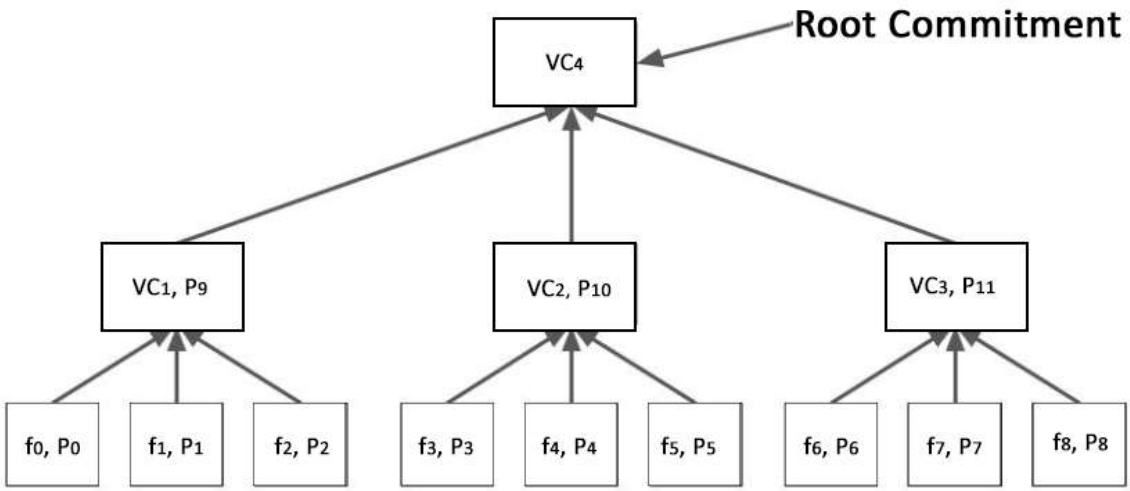


Fig1. Verkle Tree

Merkle-ს ხეში, მნიშვნელობის მტკიცებულება შედგება frlattern კვანძების მთელი ნაკრებისგან: მტკიცებულება უნდა შეიცავდეს ხეში არსებულ ყველა კვანძს, რომელსაც ყავს საერთო მშობელი ნებისმიერ კვანძთან იმ გზაზე, რომელიც მიდის დასადასტურებელ კვანძამდე.

ამ მიზეზით ხელმოწერა ძალიან გრძელი გამოდის. ჩვენ უნდა მივაწოდოთ frlattern კვანძები თითოეულ დონეზე, რადგან ჩვენ გვჭირდება შვილობილი კვანძის მთელი ნაკრები ამ კვანძის მნიშვნელობის გამოსათვლელად და ჩვენ უნდა გავაგრძელოთ ეს მანამ, სანამ არ მივაღწევთ ხის ფესვამდე.

მეორეს მხრივ, Verkle-ს ხეში ჩვენ არ გვჭირდება flattern კვანძების მიწოდება; ვინაიდან აქ, ჩვენ მხოლოდ ბილიკს ვუთითებთ. ამიტომაა, რომ Verkle-ს ხეები არის განიერი, ხოლო Merkle Patricia ხეები არა: უფრო დიდი სიგანის ხე ორივე შემთხვევაში უფრო მოკლე ბილიკამდე მიდის, მაგრამ Merkle Patricia ხეში ეს ეფექტი გადალახულია მთელი სიგანის მიწოდების საჭიროების მაღალი ღირებულებით. - 1 flattern კვანძი თითო მტკიცებულების განშტოებაზე.

Verkle-ს ხეში არ გვაქვს მსგავსი ეფექტურობის პრობლემა, რაც მას ბევრად უფრო ეფექტურს ხდის.

3. ახალი სქემა

Verkle-ს ძირეული ვალდებულება არის საჯარო გასაღები. იხილეთ ნახ. 2

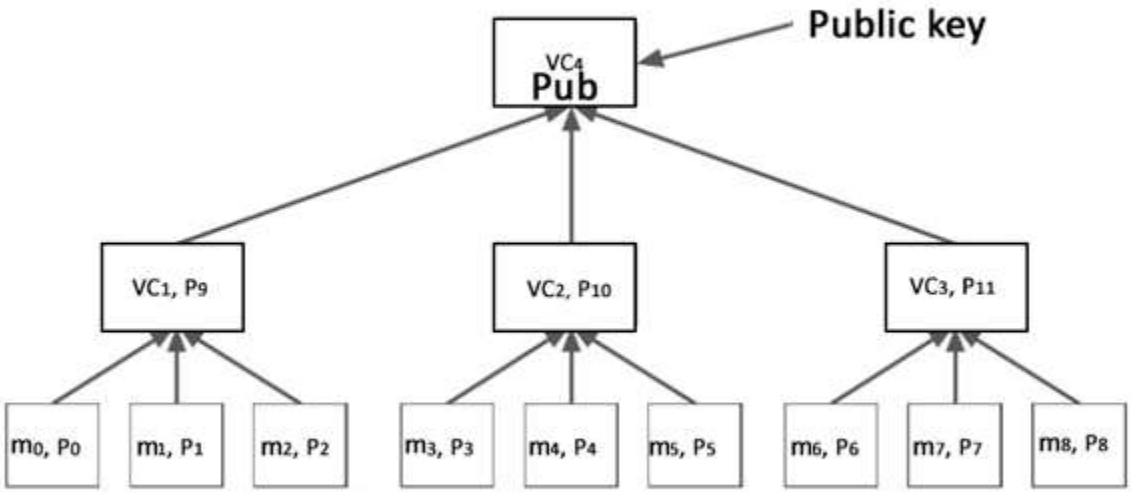


Fig 2. Verkle Signature Scheme

გასაღების გენერაცია: ხის სიგრძე არჩეულია როგორც H>=2. აქ ერთ საჯარო გასაღებს შეუძლია ხელი მოაწეროს 2H რაოდენობის დოკუმენტს. იქმნება 2H გასაღების წყვილი Xi და Yi, სადაც Xi არის ხელმოწერის გასაღები და Yi ვერიფიკაციის გასაღები, h (Yi) გამოითვლება და გამოიყენება ხის ფოთლებად. ხის თითოეული კვანძი არის მისი განშტოებების შეერთების ჰეშ მნიშვნელობა.

a[1,0]=h(a[0,0] || a[0,1])

Verkle-ს კრიპტო სქემის საჯარო გასაღები არის ძირეული ვალდებულება, მის დაგენერირებისთვის უნდა გამოითვალოს 2H რაოდენობის წყვილი ერთჯერადი გასაღები.

ხელმოწერის გენერირება: რენდომული ზომის შეტყობინება m, გარდაიქმნება ზომად n ჰეშის ფუნქციის საშუალებით. h (m) = ჰეში, და იქმნება ერთჯერადი ხელმოწერა რენდომული ერთჯერადი გასაღების Xarb-ის გამოყენებით, დოკუმენტის ხელმოწერა იქნება: ერთჯერადი ხელმოწერა, ერთჯერადი გადამოწმების გასაღები Yarb, ინდექსის arb მტკიცებულება და

ძირეული ვალდებულება. ხელმოწერა= (sig||arb|| Yarb||მტკიცებულება, ძირეული ვალდებულება)
ხელმოწერის გადამოწმება: Verkle-ში ციფრული ხელმოწერის გადამოწმებაკეთდება შემდეგნაირად, sig-ის ერთჯერადი ხელმოწერა უნდა გადამოწმდეს Yarb-ის გამოყენებით, თუ ეს სწორი აღმოჩნდება, ყველა დადასტურება VC [i] გამოითვლება "authi", ინდექსის arb და Yarb გამოყენებით. თუ ხის ფესვი უდრის ფესვის ვალდებულებას, ხდება ხელმოწერის ვერიფიკაცია.

4. დასკვნები

Verkle სქემა არის Merkle-ის სქემის ძლიერი განახლება, რომელიც იძლევა ბევრად უფრო მცირე ზომის ვერიფიკაციის საშუალებას. ნაცვლად ყველა "auth კვანძის" უზრუნველყოფისა თითოეულ დონეზე, ვერიფიკაციას სჭირდება მხოლოდ ერთი მტკიცებულება, რომელიც დაადასტურებს ყველა მშობელი-მემკვიდრე ურთიერთობას - ყველა ვალდებულებას თითოეული ფოთლის კვანძიდან ფესვამდე. ეს საშუალებას იძლევა ვერიფიკაციის ზომები შემცირდეს დაახლოებით 6-8-ჯერ, კლასიკურ Merkle-ს სქემასთან შედარებით.

ეს მოითხოვს უფრო რთულ კრიპტოგრაფიას, მაგრამ ამავდროულად ეს გვაძლევს მასშტაბირების გაზრდის შესაძლებლობას. საშუალოვადიან პერსპექტივაში, SNARK-ებს შეუძლიათ კიდევ უფრო გააუმჯობესონ მდგომარეობა: ჩვენ შეგვიძლია გამოვიყენოთ SNARK უკვე ეფექტური Verkle proof Verifier-ი, რათა ვერიფიკაციის ზომა შევამციროთ თითქმის ნულამდე, ან დავუბრუნდეთ SNARKed Merkle-ის მტკიცებულებებს, თუ/როცა SNARK-ები ბევრად უკეთესი გახდება.

შემდგომში, კვანტური გამოთვლების ზრდა გვაიძულებს გადავიდეთ STARKed მტკიცებულებებზე ჰეშებით, რადგან ეს უკანასკნელი ხაზოვან ჰომორფიზმებს, რომლებზეც Verkle-ს ხეები არიან დამოკიდებულნი დაუცველს ხდის. მაგრამ ჯერჯერობით, ეს იგივე მოგებას გვაძლევს მასშტაბირების მხრივ, რასაც მივიღებდით უფრო მოწინავე ტექნოლოგიებით. ჩვენ უკვე გაგვაჩნია ყველა ინსტრუმენტი, რომელიც გვჭირდება ამ ყველაფრის ეფექტური განხორციელებისთვის.

პოლინომიური ვალდებულებების კვანტური უზრუნველყოფის სქემა უნდა შეიცვალოს პოსტკვანტურ დაშვებებზე დაფუძნებული სქემებით.

ბიბლიოგრაფია:

1. Ladd, T., Jelezko, F., Laflamme, R. et al. Quantum computers. Nature 464, 45–53 (2010). https://doi.org/10.1038/nature08812

2. Divincenzo, D.P. (1997). Topics in Quantum Computers. In: Sohn, L.L., Kouwenhoven, L.P., Schön, G. (eds) Mesoscopic Electron Transport. NATO ASI Series, vol 345. Springer, Dordrecht. https://doi.org/10.1007/978-94-015-8839-3_18

3. Gardas, B., Dziarmaga, J., Zurek, W.H. et al. Defects in Quantum Computers. Sci Rep 8, 4539 (2018). https://doi.org/10.1038/s41598-018-22763-2

4. Lele, A. (2021). Quantum Computers. In: Quantum Technologies and Military Strategy. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-72721-5_3

5. J. Bardin, "Beyond-Classical Computing Using Superconducting Quantum Processors," 2022 IEEE International Solid- State Circuits Conference (ISSCC), 2022, pp. 422-424, doi: 10.1109/ISSCC42614.2022.9731635.

6. Dods, C., Smart, N.P., Stam, M. (2005). Hash Based Digital Signature Schemes. In: Smart, N.P. (eds) Cryptography and Coding. Cryptography and Coding 2005. Lecture Notes in Computer Science, vol 3796. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11586821_8

7. Buchmann, J., Dahmen, E., Szydlo, M. (2009). Hash-based Digital Signature Schemes. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_3

8. Rohde, S., Eisenbarth, T., Dahmen, E., Buchmann, J., Paar, C. (2008). Fast Hash-Based Signatures on Constrained Devices. In: Grimaud, G., Standaert, FX. (eds) Smart Card Research and Advanced Applications. CARDIS 2008. Lecture Notes in Computer Science, vol 5189. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-85893-5_8

9. M. Schneider and Shih-Fu Chang, "A robust content based digital signature for image authentication," Proceedings of 3rd IEEE International Conference on Image Processing, 1996, pp. 227-230 vol.3, doi: 10.1109/ICIP.1996.560425.

10. M. Iavich, G. Iashvili, R. Bocu and S. Gnatyuk, "Post-quantum digital signature scheme for personal data security in communication network systems", International Conference of Artificial Intelligence Medical Engineering Education, pp. 303-314, 2020.

11. Iavich, M., Gagnidze, A., Iashvili, G., Hash based digital signature scheme with integrated TRNG, CEUR Workshop Proceedings, 2018

12. Avtandil Gagnidze & Maksim Iavich & Giorgi Iashvili, 2017. "Some Aspects Of Post-Quantum Cryptosystems," Eurasian Journal of Business and Management, Eurasian Publications, vol. 5(1), pages 16-20.

13. Chen, H.; Liang, D. Adaptive Spatio-Temporal Query Strategies in Blockchain. ISPRS Int. J. Geo-Inf. 2022, 11, 409. https://doi.org/10.3390/ijgi11070409

14. Weijie Wang, Yale University Annie Ulichney, Yale University Charalampos Papamanthou, Yale University, BalanceProofs: Maintainable Vector Commitments with Fast Aggregation, Cryptology ePrint Archive, 2022