UDK 004.9

Vitalii Savchenko *(Doctor of Science, the Chief of IT Educational Department)*[1]
Serhii Kononenko *(the Chief of Simulation Center)*[1]
Victor Bobylov *(PhD, the Leading Scientific Fellow)*[1]
Liudmyla Drok *(the Instructor of Department)*[1]

[1]*National Defense University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

COORDINATION MODEL FOR THE NATIONAL CYBER SECURITY SYSTEM OF UKRAINE

The purpose of this paper is to discuss current challenges in cyberspace of Ukraine by analyzing recent cyber threats and cyber attacks to governmental agencies and Ukrainian power networks. Russian aggression against Ukraine and the threats in cyberspace prompted Ukrainian leadership to review its cyber security legislation and organizational structures. The new Cyber Security Strategy of Ukraine, signed in March 2016, set the key players, measures and priorities of Ukrainian National Cyber Security System but doesn't give any mechanisms for its implementation while the main problem is in lack of coordination between the elements. Executive bodies as well as scenarios of their application are suggested.

Key Words: *Cyber Security Strategy; cyber threats; cyberspace.*

Introduction

The need for provisions of legislation and organization on cyber security has grown in Ukraine for a long time. The cyberspace becomes a separate area of security and warfare, along with the traditional "Earth", "Air", "Sea" and "Space". In the military sphere, there is a rapid transformation from the "Concept of Battlefield" to the "Concept of Battlespace", where appropriate armed forces of world-leading countries have become more active [1]. Considering the widespread using of modern information technologies in the field of defense and security, as well as the development of the Ukrainian Armed Forces Command – and – Control (C2) system based on Net-Centric strategy, cyber protection of Ukraine is becoming increasingly vulnerable to cyber threats.

Problem Statement. The problems which make difficult the fight against cyber threats linked primarily with the lack of clear legal regulation of the national state policy on cyber security. There is no state coordination structure for prevention and counteractions of cyber threats in Ukraine. The growth of threats to critical infrastructure, the growth of cyber crime, computer piracy and violations of copyright are results of legislative and organizational lacks.

The new Cyber Security Strategy of Ukraine [1], signed in March 2016, was the first document that set out key subjects and roles of the National Cyber Security system. But it didn't show the ways of coordination between the players in emergency cases of cyber threats realization.

So, the **aim of this paper** is to explore current challenges in cyberspace, the structure of the National Cyber Security system and to suggest appropriate algorithm of coordination for the cases of cyber attack on information infrastructure objects.

1. Challenges and Recent Cyber Attacks

Last two years were not easy for the Armed Forces of Ukraine (AFU). It is due to the challenges faced not only the AFU but the Ukraine as a whole country. The military was drawn into combat against illegal armed groups in the Eastern part of Ukraine. Concurrently with the warfare, the AFU is building up its defensive capabilities and carried out the necessary reforms. Now we can state with confidence that the AFU have significantly increased the level of combat readiness over the last two years. [2]

However, Ukraine and its Armed Forces now face a variety of external cyber threats. This is evidenced by a series of cyber attacks that have been committed against Ukraine in recent time. Ukraine has started to suffer from cyber threats straight after the Revolution of Dignity, but the conflict in the East of Ukraine led to an increased number of preplanned high-level cyber attacks. Russia has applied cyber warfare tactics against Ukrainian websites as a part of its military operations [3]. Some of these perfidious attacks were physically hosted in Ukraine, while others are not. Russia has conducted a cyber operation to support its occupation of Crimea Peninsula. Russia designed the cyber espionage operation called Armageddon to provide military superiority for its leadership by hitting Ukrainian governmental and law enforcement's agencies. This cyber operation included DDoS attacks against Ukrainian media and targeted attacks against Ukrainian Central Election Commission (CEC) websites in 2014. [3]

On the day of the presidential elections, a powerful cyber-attack on the resources of the CEC was conducted. The cyber-attack was aimed at garbling the results. Following the elections, the next morning, the whole country was to find out that not Petro Poroshenko but the leader of the far-right party had won. The Russian Federation's propagandistic arguments were to confirm this. The Security Service of Ukraine (SSU) and the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) discovered the attack in time and

managed to prevent it.

Despite the rapid prevention of the cyber-attack by Ukrainian specialists, the next day Russian news presented the information showing "the Ukrainian CEC website" with garbled results of the cyber-attack. [4] In other words, the cyber-attack did not take place, but Russian news showed the results that had been planned. This is the case when cyber weapons are used in propaganda campaigns. Moreover, when cyber-attacks are used as propaganda, whole society suffers, because propaganda has mass effect.

Next cyber attack was conducted by Russian hackers and foreign hackers' groups which belonged to Russia. In December 2015 they attacked Ukrainian electric power infrastructure. Virtually, Russia tests on Ukraine new systems for knocking out the critical infrastructure via cyberspace.

Hackers used a Russian-based internet provider and made phone calls from inside of Russia as part of a coordinated cyber attack on Ukrainian power grid [5]. The incident was considered as the first known electricity outage caused by a pre-planned cyber attack and has raised fears not only in Ukraine but also abroad. This is evidenced by numerous independent investigations conducted by foreign experts [6]. This cyber incident has shown one more time how vulnerable could be objects of critical infrastructure.

The investigation shows that Russian government was not directly involved in the attack which knocked Ukrainian electricity supplies to thousands of customers in different parts of Ukraine. The outcomes of this cyber attack prompted Ukrainian leadership to review its legislation in cyber defense and relevant organizational structures.The attack on the systems took at least six months to prepare, the evidence has been found that hackers started collecting information no less than six months before the attack. The malicious software which was used to infect the power grid network was also been detected in the networks of Ukrainian Railway Company and large mining company [5].

Hackers attacked three power distribution companies and then flooded those companies call centers with fake emergency calls to avoid genuine customers reporting. According to a representative of one of the power companies, attackers established linkage to company's network from a sub-network which belonged to Russian internet service provider. One possible explanation is that it was an attempt to destabilize Ukraine as a whole country. Also possible, that it was a test probe to determine future exploited vulnerabilities.

The Russian secret services and international hacker groups connected to them are behind of cyber-attacks against Ukraine [4]. In all, hackers hit Ukrainian government, business, media, and commercial websites [3]. There are cyber attacks on the banking sector, to the public establishment and it can be considered as cybercrime and cyber espionage. State and private companies are unprepared to cyber attacks and suffer from them.

According to the statistical data, only 41.8% of the Ukrainian population is now online, in comparison with 84.2% in the United States and 61.4% in Russia [3]. In spite of this, a variety of sectors of the Ukrainian economy and life are vulnerable and unprotected in cyberspace [7].

As long as Ukrainian society will be entered the digital world, there will be more and more cyber threats accordingly. That is why Ukraine and other countries are faced with the task to adhere to all laws of cyber security to ensure measures to protect its citizens and infrastructure.

2. Legislative and Organizational Changes

Recently, the level of cyber protection in Ukraine was rather low. Evidence of this is not only cyber attacks mentioned above, but also numerous events of illegal collection, storage, use and distribution of personal data, illegal financial transactions, theft and online fraud. Unfortunately, Ukraine had no effective instruments for prevention of cyber attacks, all measures of cyber protection were unsystematic and ineffective. Also, there was a little cyber security legislation in Ukraine. However, recent challenges prompted Ukrainian leadership to review cyber defense and make serious changes in legislation and organization of cyber protect.

2.1. Legislative changes. The new Cyber Security Strategy of Ukraine was approved by the President of Ukraine on March 15, 2016 [8]. The purpose of the new Cyber Security Strategy of Ukraine (CSSU) is to create conditions for the safe cyberspace, using one for the benefit of individuals, society, and the state [1, 7, 8].

The CSSU defines following main priorities for safe, stable and reliable cyberspace in Ukraine [1, 7]:

development and adaptation of state policy in the cyber security, achieving of its adequacy to standards of the European Union (EU) and NATO;

creating a national framework in this area, harmonization of regulations in the field of electronic communications, cyber protection, cyber security in accordance with standards of the EU and NATO;

development of cyber security technologies for mobile communication tools;

development of electronic infrastructure for communications;

development and improvement of state control system of information security and a system of information security audit;

development of international cooperation in the cyber security, support for international initiatives in the cyber security which meet the national interests of Ukraine, strengthening the cooperation between Ukraine and the EU and NATO in order to strengthen state cyber security capabilities. Regarding this, the CSSU defines that cyber defense of critical infrastructure should primarily includes following [1, 7]:

improving the legal framework of critical infrastructure;

development and maintenance of the State Register of critical infrastructure's objects;

development and implementation of a procedure

for information exchange between government agencies, private business, and citizens regarding threats to critical infrastructure's objects.

According to the CSSU, the development of cyber security potential of Ukraine has to include the implementation of the following main activities [1, 7]:

protection of technological processes of critical infrastructure's objects from unauthorized intrusion in their work;

development and implementation of joint actions protocols, including information exchange in real-time mode;

implementation of state strategic planning in the field of electronic communications, information technology, information security and cyber protect;

deployment a special unit of the AFU which will be responsible for cyber security and cyber protect on strategic, operational and tactical levels;

development of cyber security and cyber protect capabilities of existing units of the AFU, SSSCIPU, SSU, National Police of Ukraine (NPU), state intelligence agencies, achievement of interoperability with the relevant units of NATO-members;

restriction for any objects that are under control of an state-aggressor or countries, with special economic and other preventive sanctions which approved by the national or international level as a result of aggression against Ukraine, as well as the restriction of the use of products, technologies and services of these objects and countries, to ensure cyber protect of Ukrainian information resources, strengthening of state control in this sphere.

The CSSU foresees following measures against cybercrime in Ukraine [1, 7]:

establishment of an effective and convenient network of contact centers for reporting the events of cyber crime and deception, improving the efficiency of enforcement bodies to react to cybercrime;

improvement of procedures of collection of electronic evidence;

implementation of blocking of certain information resources by communication operators and service providers in accordance with the court decision;

determination of an order on fixing and saving of computer data, data about traffic by operators and providers;

training of judges, investigators and prosecutors for operation with evidence of a cyber crime;

implementation of a special procedure for an interception in the case of cyber crime investigation.

According to the measures listed above, one of the priority tasks for Ukraine will be to ensure the security and reliability of communications. This requires the use of the latest technologies. Given the current state of telecommunication systems and security tools, it will not be an easy task.

An important factor is that the CSSU clearly determines critical infrastructure such as energy, transport, oil and gas pipelines, sea and river ports etc.

In addition, the CSSU defines the concept of active cyber defense which implies the need for the military, political, technical and other measures, as well as the creation and development of necessary units/forces, assets and tools for an adequate response to aggression in cyberspace. This comprehensive protection can also be used as assets to prevent military conflicts and threats in cyberspace. In other words, Ukraine should create a mechanism for responding to cyber attacks.

2.2. Organizational changes. Next important factor, which is defined in the strategy, is the creation of special units of the Armed Forces of Ukraine, which have never existed before, and the development of such units in other government agencies. This measure requires the involvement of specialists for these units and requires additional funding. At the same time, it is important that such experts would have the necessary qualifications for cyber defense, which, in turn, requires the creation of training systems for such specialists.

In connection with the CSSU, the National Coordination Center for Cyber Security (NCCCS) is established by the Council of National Security and Defense as its working body [9].

The NCCCS will be responsible for coordination of activities of the agencies involved in the national security and defense in the framework of the CSSU. This will increase the effectiveness of public administration in the development and implementation of cyber security state policy.

The main tasks of the NCCCS are following: analysis of cyber security, control and analysis of the state of readiness of the subjects of cyber security to counter cyber-threats, control and analysis of the implementation of legislation, data collection and analysis on the state of critical infrastructure, etc.

The NCCCS predicts and detects the potential and real cyber security threats and provides operational information and analytical support on cyber security issues. In addition, the NCCCS is involved to international and inter-agency cyber-exercises and training. The NCCCS has the right to request and receive necessary information for the resolution of questions relating to its competence and uses the information from databases of the governmental agencies, special systems and communication networks, and other technical equipment [9].

Figure 1 depicts governmental agencies which are responsible for national cyber security and defense according to last changes. The basis of the organization of national cyber security system are Security Service of Ukraine (SSU); State Service of Special Communication and Information Protection of Ukraine (SSSCIP); the Ministry of Internal Affairs (MIA) of Ukraine with its Department on Combating Cybercrimes; the Ministry of Defense of Ukraine (MOD); the General Staff with its Electronic Warfare Troops; the intelligence agencies (the Defense Intelligence Service and the Foreign Intelligence Service).

These agencies have different domains and priorities, and, unfortunately, they rarely collaborate on common problems [3].

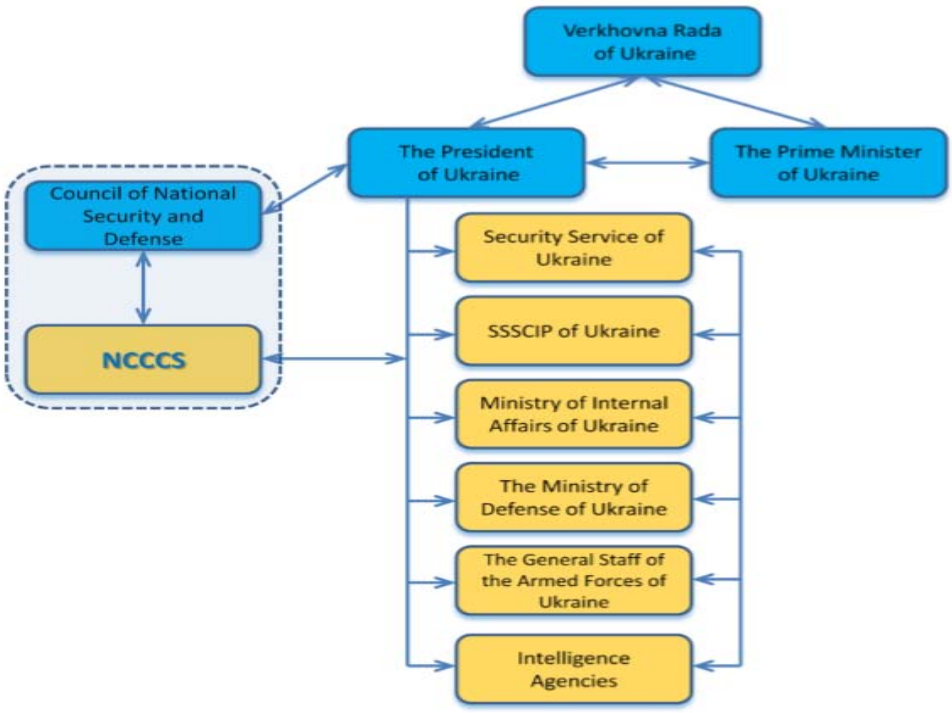

Figure 1. Organization of the cyber security system of Ukraine

The SSSCIP is the only organization that exclusively works on cyber security issues. Its main activities are following: interaction with the administration domain UA; protection of state information resources; interaction with state authorities; international cooperation in the protection of information resources; unified antivirus protection system; and determining the level of protection of information and telecommunication authorities' systems.

The SSSCIP could be the basement of the National Cyber Security system in the field of rapid reaction on cyber attacks and incidents. But, being as a one of the actors it doesn't have enough authority to manage other cyber security subjects. So, the system needs an outside manager, free from another internal charges.

From the other side the NCCCS has enough authority but also can't be such body as it was created more as long-term management brunch than rapid reaction team.

3. Innovated Solutions for the National Cyber Security

To establish the really working mechanism of coordination between governmental and public bodies in the field of prevention and removal of unauthorized cyber actions the new National law has to be issued.

In particular, this new law has to cover:

1. Creation the Situation Center under the NCCCS, as main subdivision for operative security control of the critical infrastructure communication systems with tasks:

24/7 monitoring of attacks and incidents in the world information environment;

control the security of the state information resources and critical infrastructure communication systems;

monitoring of international criminal activity in a world cyberspace;

operative informing of state leaders about current threats in the field of cyber security;

development of suggestions in relation to the cyber security legislation improvement;

development of methodical materials for personnel education.

2. Creation the structures within mentioned bodies (see fig. 1) that will be responsible for the critical information infrastructure security Situation Centers and Computer Emergency Response Teams (CERTs) with tasks:

providing security for information resources and communication systems preventing violations of their confidentiality, integrity and availability;

warning and prevention of cyber threats realization;

cyber threats monitoring;

computer incidents analysis;

cyber threats investigation.

This approach is quite different from another one, issued earlier by the SSSCIP, where the SSSCIP declared themself as the main Ukrainian cyber security body, because as one of the National cyber security subjects it can't be higher than others.

3.1. Mechanism of Cyber Security Coordination. There are three basic principles that should be set into the basis of coordination mechanism for cyber security of the National critical information infrastructure:

1) constant control of world cyberspace;

2) centralized coordination for the cyber attacks/incidents respond;

3) spread realization of security measures for the objects of critical infrastructure.

The first principle can be realized by organization of 24/7 monitoring of the National critical infrastructure and the world cyberspace in Situation Centers. Such Situation Centers have to have a real time online network access and ability to collect and operate with all necessary information (operative, technical, statistical) for delivering urgent

solutions in the case of serious threats. In addition, the Situation Centers have to be able to exchange operative information with international partners as well as tracking the activity of international criminal (hacker) groups and individuals.

The second principle can be realized by organization of warning system between organizations and citizens in relation to the attempts of cyber attacks or incidents. Such system must include procedures and networks of information transfer from the critical infrastructure object owners up to the NCCCS Situation Center and in reverse order. In this case the NCCCS Situation Center will be responsible for the development of suggestions and measures (technical decisions) and delivering them to the performers. In some cases of dangerous threats the NCCCS Situation Center will inform all potential suffers. The plan of NCCCS Situation Center functioning in the cases of emergency situations is under the President of Ukraine signature so those decisions are obligatory for implementation by all subjects of the National cyber security system.

The third principle can be realized by the local Situation Centers or CERT that should be created under every subject of the National cyber security system. They react to the threats on the basis of the orders (recommendations) got from the NCCCS Situation Center. All executed measures should be reported to the NCCCS Situation Center.

3.2. Scenarios of Cyber Threat Neutralization. The general protocol of cyber security system functioning must envisage phases:

I. Monitoring Phase.

Permanent gathering and analysis by the NCCCS and other Situation Centers of intelligence information about threats in cyber space. Source of information: intelligent agencies, foreign CERTs, critical information infrastructure owners.

II. Reacting Phase.

This phase should be considered for the different categories of participants according to certain scenarios:

Scenario 1. Cyber attack/incident against citizens (private structures):

1) citizen (private structure) calls to authorities (Ministry of internal affairs, National police);

2) authorities (Situation Center, CERT) analyze the information, make a decision about fact of cyber attack/incident and generate solution to the citizen (private structure);

3) in the case of cyber attack/incident confirmation and presence of criminal evidences realization of inquisitional actions, searching and detention of the suspected persons, informing to the NCCCS Situation Center;

4) in case of massive similar cyber attacks immediate informing to the NCCCS Situation Center;

5) NCCCS Situation Center analyses the information and makes decision about other subjects warning and particular specific measures implementing (blocking of information resources, extracting the content etc.).

Scenario 2. Cyber attack/incident against private (commercial) banks, subdivisions of the National Bank of Ukraine:

1) bank calls to the National Bank Situation Center (National Bank CERT);

2) National Bank Situation Center (National Bank CERT) is trying to block, remove or localize negative consequences by its own efforts (by efforts of the CERT);

3) immediate informing the NCCCS Situation Center. It analyses the information and makes decision about other subjects warning and particular specific measures implementing (blocking of information resources, extracting the content etc.);

4) informing the Security Service of Ukraine. In the case of cyber attack/incident confirmation and presence of criminal realization of prosecution actions, search and detention of the suspected persons.

Scenario 3. Cyber attack/incident against the objects of critical information infrastructure:

1) critical information infrastructure owner calls to the local Situation Center (local CERT);

2) local Situation Center (local CERT) tries to block, remove or localize the negative consequences by its own efforts;

3) immediate informing the NCCCS Situation Center. It analyses the information and makes decision about other subjects warning and some specific measures implementing (blocking of information resources, extracting the content etc.);

4) informing the Security Service of Ukraine. in the case of cyber attack/incident confirmation and criminal presence realization of prosecution actions, search and detention of the suspected persons.

III. Phase of generalization and cyber security system improvement.

On the basis of the recommendations, got from the NCCCS Situation Center the owner of critical information infrastructure carries out measures for improvement of the cyber security system, protocols of cooperation, reorganization of structures etc. The subjects of the National cyber security system conduct the analysis of existent legislation and, if necessary, make suggestions for changing of legislation in relation to the order of functioning and protocols of cooperation.

Conclusion

Despite the current challenges and the existing economic and financial difficulties, Ukraine has made some progress in the creation of a national cyber security legislation and organizational infrastructure. In addition to the new cyber-security strategy, Ukraine creates special units within the governmental agencies and the National Coordination Center for Cyber Security to coordinate and deal with cyber threats. These initiatives cannot be implemented fast enough and take time and require technical, financial and human resources. In the nearest future, the Ukrainian government will still rely on the protection system that will create by private businesses to protect their companies and business interests.

Today cannot be considered that the new Cyber Security Strategy of Ukraine will be a sufficient tool to protect Ukraine from cyber threats. The new strategy declares the plan for the necessary actions and requires changes in other laws and regulations of Ukraine. The strategy also envisages the creation of new units (such as

Situation Centers) within existing government agencies. Also, implementation of the CSSU requires not only a serious funding and investments as well as the tightening of responsibility for crimes committed in cyberspace.

Despite this, the Cyber Security Strategy of Ukraine and the National Coordination Center for Cyber Security are a good foundation for the changes in the area of cyber defense, but Ukraine still has to make significant efforts in protecting its cyber space.

Future researches have to be pointed to creation a really working protocols of cooperation between all National Cyber Security bodies.

References

1. Official website of the President of Ukraine, "Стратегія кібербезпеки України," О, 27 January 2016. [Online]. Available: http://www.president.gov.ua. [Accessed 7 October 2016]. **2. Ministry of Defense** of Ukraine, "White Book 2015 The Armed Forces of Ukraine," 2016. [Online]. Available: http://www.mil.gov.ua. [Accessed 15 September 2016]. **3. Kostyuk N.** "Ukraine:A Cyber Safe Haven?," in Cyber War in Perspective: Russian Aggression against Ukraine, Tallinn, NATO CCD COE Publications, 2015, pp. 113-122. **4. segodnya.ua**, "Кибератаки на Украину," 27 July 2016. [Online]. Available: http://www.segodnya.ua/ukraine/kiberataki-na-ukrainu-sovershila-rf-ispytyvaya-novoeoruzhie-snbo-737519.html. [Accessed 06 October 2016]. **5. Polityuk P.** "Ukraine sees Russian hand in cyber attacks on power grid," REUTERS, 12 February 2016. [Online]. Available: http://www.reuters.com/article/us-ukraine-cybersecurityid USKCN0VL18E. [Accessed 2 October 2016]. **6. ICS**, E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 18 March 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC _5.pdf. [Accessed 6 October 2016]. **7. Koval M.S.** "Ukraine's New Cyber Security Strategy, the Measures and Priorities Set Out in the Strategy, the Current State of Cyber Security Law in the Ukraine and Whether the New Cyber Security Strategy Is Enough to Adequately Protect the Ukraine Against Cyber Crime," 12 May 2016. [Online]. Available: http://www.lexology.com/library/detail.aspx?g =b73173dd-9b3e-4bc4-98ef-e588110bec4a. [Accessed 4 October 2016]. **8. Machuskyy V.** "New Cyber Security Strategy of Ukraine," 16 March 2016. [Online]. Available: http://ukrainianlaw.blogspot.com/2016/03/new-cyber-security-strategy-ofukraine.html. **9. UNIAN**, "Ukraine creates National Center for Cyber Security," 8 June 2016. [Online]. Available: http://www.unian.info/society/ 1369157-ukraine-creates-national-center-for-cybersecurity. html. [Accessed 4 October 2016].

МОДЕЛЬ КООРДИНАЦИИ ДЛЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ

Виталий Анатольевич Савченко (начальник кафедры)[1]
Сергей Николаевич Кононенко (начальник центра имитационного моделирования)[1]
Виктор Евгеньевич Бобылёв (ведущий научный сотрудник центра)[1]
Людмила Владимировна Дрок (преподаватель кафедры) [1]

[1]Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье обсуждаются текущие угрозы национальной безопасности Украины в киберпространстве, анализируются недавние кибератаки на правительственные учреждения и сети электроснабжения страны. Конфликт на востоке Украины и не прекращающиеся попытки проникновения в информационные системы критической инфраструктуры государства подтолкнули руководство Украины к пересмотру как законодательства, так и организационных структур в области кибербезопасности. Подписанная в марте 2016 года Стратегия кибербезопасности Украины определяет ключевых субъектов обеспечения безопасности, устанавливает приоритеты и функции в области защиты киберпространства. Вместе с тем Стратегия не дает каких либо механизмов относительно ее реализации. В частности, основной проблемой является отсутствие координации предпринимаемых мер в случае осуществления кибератаки или инцидента. В статье предлагаются исполнительные механизмы координации а также рассматриваются различные сценарии взаимодействия субъектов в случае кибератаки.

Ключевые слова: *Стратегия кибербезопасности, киберугроза, киберпространство.*

МОДЕЛЬ КООРДИНАЦІЇ ДЛЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Віталій Анатолійович Савченко (д-р техн. наук, ст. наук. співробітник, начальник кафедри)[1]
Сергій Миколайович Кононенко (начальник центру імітаційного моделювання)[1]
Віктор Євгенович Бобильов (кан-т. воен. наук., ст. наук. співробітник, провідний науковий співробітник центру)[1]
Людмила Володимирівна Дрок (викладач кафедри) [1]

[1]Національний університет оборони України імені Івана Черняховского, Київ, Україна

У статті обговорюються поточні загрози національній безпеці України у кіберпросторі, аналізуються нещодавні кібератаки на урядові заклади та мережі електропостачання країни. Конфлікт на сході України та невпинні спроби проникнення в інформаційні системи критичної інфраструктури держави підштовхнули керівництво України до перегляду як законодавства, так і організаційних структур у сфері кібербезпеки. Підписана у березні 2016 року Стратегія кібербезпеки України визначає ключових суб'єктів забезпечення кібербезпеки, встановлює пріоритети та визначає функції в області захисту кіберпростору. Разом з тим Стратегія не дає реальних механізмів відносно її реалізації. Зокрема, основною проблемою є відсутність координації заходів, які вживаються у випадку кібератаки чи кіберінциденту. У статті пропонуються виконавчі механізми координації а також розглядаються різні сценарії взаємодії суб'єктів у випадку кібератаки.

Ключеві слова: *Стратегія кібербезпеки, кіберзагроза, кіберпростір.*