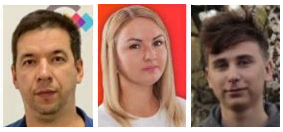
State Information Policy. Cyber Security As A Component Of Ukraine's National Security

Roman Efimenko, Vladyslav Khotunov, Kateryna Kholupnyak *

ISMA University of Applied Science, Latvia

Cherkasy state business college, Ukraine

**Corresponding author's e-mail: vkhotunov@gmail.com, Katyakholupnyak@gmail.com, romanefimen322@gmail.com*



Abstract

The formation of the information society not only allows us to expect greater efficiency and a successful society, but also gives new impetus to traditional threats without the security of the state and creates new challenges for the national security system. In such conditions, the search for new opportunities to secure the security of the state becomes especially important, given the formation of a new field of confrontation - cyberspace. Given the level of penetration of ICT in all critical areas of life of people and nations, so it is possible to provide confrontation in cyberspace and cyberwarfare.

Keywords: security system, cybercrime, cyber security

1 Introduction

Ukraine needs to create an adequate security system in a transforming world, where the challenges of national security are increasingly becoming different from the traditions of threats. [1].

In Ukraine, the system of protection of cybersecurity of the state involved low military and law enforcement agencies. Among them are the Ministry of Defense of Ukraine (and its special units - in particular the Main Intelligence Directorate), the Security Service of Ukraine. At the same time, the activities of these agencies are not always adequately secured..

Overview

In terms of efficiency and consequences of the use of air weapons, which is the term that is often used, it can be equated to a weapon of mass cinema. Therefore, cyber is one of the main security concerns.

Russia launched a hybrid war against Ukraine four years ago. This type of war that the aggressor country may remain publicly uninvolved in such a conflict and covert military operations. A number of leading Western experts rightly call it the "war of the new generation" or the "war of the new generation." [6]

Thus, the functioning and protection of the homeland as information, cyberspace is a military task of the state in the context of actions with Russia in the course of our country [4].

It is known that in recent years various sectors of the Ukrainian economy and the social life of ordinary citizens have become very vulnerable in cyberspace. Public and private companies are constantly suffering from periodic cyberattacks, for which, as it turned out, they were not ready at all. It is a pity, but we must also state the fact that Ukraine does not have even today any effective tools to prevent attacks and their effective counteraction, and all existing cybersecurity measures are mostly unsystematic and, as a result, unsuccessful. [3]

The threat to state cybersecurity in the form of cyber intervention can be both external and internal.

In addition, every society needs rules, standards, norms, regulations, instructions and other documents to feel protected in cyberspace, at least in legal terms. Sectoral regulations on cyber risks are now emerging, and there is growing interest in this area from the legislature. Ukraine is developing safety standards for critical infrastructure.

Decision

Anyone who has access to the Internet can become a victim of cybercrime. Today, there are many schemes and tools used by cybercriminals, the most common of which are:

- Carding - fraud with payment card data and systems.
- Phishing is the substitution of a website or web page.
- Vishing - taking the confidential data of the cardholder, using phone calls under the guise of a bank employee.
- Online fraud - the creation of fictitious online stores, imitation sales of goods or services.
- Piracy is the illegal use or distribution of intellectual property.
- Card-sharing - hacking access to watch satellite and cable TV.
- Social engineering is a tool for manipulating and managing people.
- Malware - the creation and distribution of malware.
- Dissemination of illegal content - information that promotes extremism, terrorism, drug addiction and

violence.

By following the personal rules of protection, you will be able to turn the weakness of the human factor into an advantage that will serve as a reliable protection. Here are some tips to help you protect yourself from cybercrime:

- Installing and updating antivirus software on your computer.
- Create passwords with different numbers, characters and special characters, as well as change them periodically.
- Do not use the same password on all sites, devices.
- Store data backups on devices that do not have network access.
- Prevention of theft of personal information.

These rules and guidelines will help reduce the risk of personal data leakage and should be followed by every Internet user.

Conclusion

The main goal of the "Cyber Security Strategy of Ukraine" (one of the fundamental legislative documents) is to create conditions for the safe functioning of cyberspace of the state, its use in the interests of society and the individual. The document also provides a set of measures aimed at combating cyber threats, deepening international cooperation in this area, ensuring the protection of state electronic information resources and information infrastructure. To implement this strategy, the National Security and Defense Council established the National Cyber Security Coordination Center as a working body of the Council. [5]

References

[1] In the world, two dozen countries are engaged in cyber weapons - McAfee // Cybersecurity.ua.

[2] MilitaryandSecurityDeploymentsInvolvingthePeople'sRepublicofChina.

[3] Buryachok VL Cyber security - the main factor of sustainable development of modern information society / A.L. Beetroot // Modern special equipment: coll. Science. work. - 2011

[4] Lukyanchuk RV State policy in the field of cyber security in the conditions of anti-terrorist operation / R.V. Lukyanchuk // Bulletin of the NAPA: Coll. Science. work. - 2015. - Issue. 3. - P. 110-116.

[5] On the decision of the National Security and Defense Council of Ukraine of April 28, 2014 "On measures to improve the formation and implementation of state policy in the field of information security of Ukraine" / Decree of the President of Ukraine of 1 May. 2014, № 449/2014. [Electronic resource]. - Available from http://www.prezident.gov.ua

[6] Wojciechowski, AV Cybersecurity as an important component of the system of protection of national security of European countries [Electronic resource] / AV Wojciechowski // Journal of Eastern European Law. - 2018. - № 53. - P. 26-37.