УДК 343.48

Y. V. Stoikivskyi
S. S. Nykyporets

CYBERCRIME IN UKRAINE: CHALLENGES AND OPPORTUNITIES TO COMBAT CYBERCRIME

Vinnytsia National Technical University

Анотація

В даній роботі розглянуто проблему кіберзлочинності в Україні, її виклики та можливості боротьби з цим явищем. Ростуть кількість та складність кібератак, загрожуючи національній безпеці та приватності громадян. Україна стикається з нестачею кібербезпекової свідомості, необхідними ресурсами та спеціалістами.

***Ключові слова*:** *кіберзлочинність, Україна, виклики, боротьба, кіберзагрози, кібербезпека, кібератаки, кібербезпекова свідоміcть, співпраця, захист даних, моніторинг, кваліфікація фахівців, громадська свідоміcть.*

Abstract

This paper discusses the problem of cybercrime in Ukraine, its challenges and opportunities to combat this phenomenon. The number and sophistication of cyberattacks are growing, threatening national security and the privacy of citizens. Ukraine is facing a lack of cybersecurity awareness, resources, and specialists.

***Keywords*:** *cybercrime, Ukraine, challenges, fight, cyber threats, cybersecurity, cyberattacks, cybersecurity awareness, cooperation, data protection, monitoring, qualification of specialists, public awareness.*

Introduction

Cybercrime is a serious threat that has become an integral part of the modern digital world. In Ukraine, this problematic phenomenon is of particular relevance, as our country is facing an increase in cyberattacks that threaten national security, the economy and personal privacy of citizens. Cyber threats are extremely diverse and complex, including fraud, identity theft, malware and other forms of criminal activity [1].

Basics

The regulatory framework in this area in Ukraine does not keep pace with the development of technology, which exacerbates the problem of cybercrime. At the level of individuals, cybercrime is associated with the use of pirated software: attackers can gain access to personal data. According to a 2011 study by the Software Industry Association (BSA), the piracy rate in Ukraine was 84%. According to the International Intellectual Property Alliance (IIPA), Ukraine is recognized as the world's "No.1 pirate".

Piracy creates favorable conditions for the development of cybercrime. According to Serhiy Demediuk, Head of the Cyber Police of Ukraine, losses from cybercrime in Ukraine in the first 8 months of 2016 amounted to about UAH 27 million. For example, in 2014, the consequences of cybercrime cost Ukrainians UAH 39 million.

In Ukraine, cybercrime includes infringement of copyright and related rights, fraud, illegal actions with transfer documents, payment cards and other means of access to bank accounts, equipment for their production; tax evasion, duties (mandatory payments), import, manufacture, sale and distribution of pornographic items, illegal collection for the purpose of use or use of information constituting a commercial or banking secret.

Any Internet user can become a target of cybercrime.

The most common types of such crimes are:

1) carding – the use of payment card details obtained from hacked servers of online stores, payment and settlement systems, as well as from personal computers (either directly or through remote access programs, "trojans", "bots");

2) phishing – is a type of fraud whereby customers of payment systems are sent e-mail messages allegedly from the administration or security service of the system, asking for their accounts and passwords;

3) fishing – is a type of cybercrime in which messages contain a request to call a certain landline number and ask for confidential cardholder data;

4) online fraud – fake online auctions, online stores, websites, and telecommunication services;

5) piracy – is the illegal distribution of intellectual property on the Internet;

6) card-sharing is the provision of illegal access to satellite and cable TV;

7) social engineering is a technology for managing people on the Internet;

8) malware is the creation and distribution of viruses and malicious software;

9) illegal content is content that promotes extremism, terrorism, drug addiction, pornography, and the cult of cruelty and violence;

10) refilling – illegal substitution of telephone traffic;

The issue of cybercrime is extremely important at the state level. Critical infrastructure facilities, such as energy facilities, transportation, and the banking sector, are most often targeted by cyberattacks. The cost of defence is usually 10 times more expensive than the attack itself. Therefore, cybersecurity is a priority in the policies of many countries. To find out about the state of cybersecurity in Ukraine, GURT turned to Dmytro Dubov, Head of the Information Security Department at the National Institute for Strategic Studies: "Ukraine's idea of cybersecurity is still quite abstract, but active work is underway in this direction. Various agencies are now dealing with cybersecurity: The State Service for Special Communications and Information Protection, the Security Service of Ukraine, the Ministry of Internal Affairs, and the National Bank. Each agency takes security measures and keeps statistics on relevant indicators, but their activities cover only their own areas of responsibility. There is no holistic policy yet, nor are there any universal indicators of cybersecurity that could characterize its level," commented Dmytro Dubov [2].

Every year, cybercrime is becoming a growing threat to society, the economy, and the security of states. Ukraine is no exception, as the involvement of citizens in the digital environment is growing, and with it the risk of becoming a victim of a cyberattack. Cyber threats are becoming increasingly complex and sophisticated, causing serious damage to both individuals and organizations.

The purpose of this paper is to analyze the challenges associated with cybercrime in Ukraine, as well as to highlight opportunities and ways to combat this problem. The study is aimed at identifying the key causes and factors that contribute to the growth of cybercrime, as well as identifying potential strategies and solutions to effectively counter this threat.

Ukraine is facing an increase in the number and sophistication of cyberattacks, which has serious implications for national security, economic development, and personal privacy. Cyber threats are becoming increasingly intelligent and sophisticated, using new technologies and methods to achieve their goals.

The lack of adequate cybersecurity awareness among citizens, businesses and organizations is a serious challenge. Many people are not aware of the risks associated with the use of digital technologies and do not take appropriate measures to protect their personal data and confidential information.

Insufficient cooperation between different sectors, including government, law enforcement, business and academia, makes it difficult to fight cybercrime. Cyberattacks often cross borders and require joint efforts to effectively counter them [3].

Conclusion

Cybercrime in Ukraine is a serious threat that requires immediate attention and effective measures to combat. The increasing number and sophistication of cyberattacks, lack of cybersecurity awareness, and insufficient cooperation between different sectors complicate the situation.

However, government agencies, law enforcement, business and academia have the capabilities and resources to counter cyber threats. Raising cybersecurity awareness, strengthening cooperation and coordination, developing technical means and improving the skills of specialists are important ways to effectively combat cybercrime.

Targeted focus, rapid response and continuous improvement of security measures are necessary to ensure success in countering cyber threats. It is only through joint efforts and partnerships between different sectors that a stable and secure digital space for all Ukrainian citizens can be ensured.

A general awareness of cyber threats, improved technical means, and increased cooperation are the main components of a successful fight against cybercrime. Only by utilizing these opportunities and focusing on preventive activities will Ukraine be able to effectively counter this threat and ensure the safety of its citizens in the digital world.

REFERENCES

1. Cybercrime URL: http://safe-city.com.ua/kiberzlochynnist-i-litni-lyudy.
2. Cybercrime in all its manifestations: types, consequences and ways to combat it URL: https://gurt.org.ua/articles/34602.
3. Cybercrime in Ukraine URL: https://www.dsnews.ua/ukr/spec/v-gosudarstve-kak-v-biznese-kakie-podhody-iz-mira-predprinimateley-mogut-usilit-kiberbezopasnost-v-ukraine-01112021-441499.

Стойківський Юрій Володимирович – студент групи УБ-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: stojkivskijurij@gmail.com

Никипорець Світлана Степанівна – викладач англійської та німецької мов, кафедра іноземних мов, Вінницький національний технічний університет, e-mail: fotinia606@gmail.com

Stoykivkiy Yurii Volodymyrovych – student of group УБ-21б, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: stojkivskijurij@gmail.com

Nykyporets Svitlana Stepanivna – Teacher of English and German, Department of Foreign Languages, Vinnytsia National Technical University, e-mail: fotinia606@gmail.com