УДК 004.4

Антонюк Г. О.,
Столяренко О. В.

CYBERSECURITY IS A SPECIALTY OF THE FUTURE

Вінницький національний технічний університет

Анотація

У цій статті мова йде про формування теорії кібербезпеки та кіберзлочинства у сучасному світі. Хакерство – один із найбільших чинників зламів програмного забезпечення. Кожна сфера діяльності потребує захисту від несанкціонованого доступу та злочинства. Наголошується на необхідності користувачів бути обережними користувча із персональними даними . Фахівці з кібербезпеки є одними із найбільш затребуваних на ринку праці. Спеціальність 125 «Кібербезпека» в університетах України розвивається з кожним роком.

Ключові слова: кібербезпека, кіберзагрози, кіберзлочинці, захист, хакерство, несанкціонований доступ, фахівці, спеціальність, інформаційні технології, комп'ютерні системи і мережі, сучасні технології, програмне забезпечення конфіденційної інформації, атаки злочинців, користувач.

Abstract

The article deals with the formation of the theory of cybersecurity and cybercrime in the modern world. Hacking is one of the biggest factors of software cracking. Each sphere of activity requires protection from unauthorized access and crime. The user must be cautious with personal data. Cybersecurity experts are among the most needed in the labor market. Specialty 125 "Cyber Security" at Ukrainian universities is developing more and more every year.

Keywords: cyber security, cybercrime, protection, hacking, unauthorized access, specialists, specialty, information technology, computer systems and networks, modern technologies, software of confidential information, attacks by criminals, user.

Cyber security [1] is a set of measures to protect computer systems and networks and software from digital attacks. Such attacks are usually aimed at gaining access to confidential information, its changes and destruction, extortion by users of financial resources or violation of the normal operation of companies. The implementation of effective cybersecurity measures is now a rather challenging task, as the number of devices and applications that can be protected is rapidly increasing, and attackers are becoming more inventive.

Today the urgency of the problem of cybersecurity is beyond doubt. Every day, each of us faces the need to use information technology [2]. From social networks, placing information about their personal data on the Internet before using ATMs, bank accounts, etc. In this regard, the question arises whether this problem is regulated by domestic legislation and how to protect themselves from cybercriminals. Proper protection against cybercriminals is primarily a matter for the citizens themselves, who often reluctantly and carelessly relate to electronic payments and their personal data. The personal data you provide to the bank is the most sought after fraudsters, namely: surname and name, mobile phone number, email address. Usually such information is sold on the "black" market, and subsequently used for sending SMS, spam, telephone calls of advertising character. Very often these data are intercepted in public places with open Wi-Fi access when using email or social networks. In this case, experts advise you to use the information security tools offered by mail servers or social networks.

Hacking was born and developed for decades as a form of social protest and the departure of the real world into the world of cyberspace. However, in recent years there has been a tendency towards taking cyberterrorism [3].

Today, the phenomenon of hacking is primarily associated and flares ever stronger and stronger with cyberwar - a war in which there are no rules or laws, and goals justify any means and methods.

Hacking, as a phenomenon officially considered out of the law, but in fact it is one of the driving forces of our society on the path of scientific and technological progress.

Different kinds of hacker attacks occur constantly. Cyberattacks can cause unavoidable damage to the company. They can cause tangible damage, such as stopping services; they can ruin public confidence in the company; they can lead to the leak of important information that can affect corporate survival. Moreover, now such attacks are a certain market of services. Each of them should bring some benefits to the customer. For

example, there are hackers whose task is to detect the vulnerability of the system to eliminate them. At the same time, there are those who sell information about the weaknesses of a system in the "black" market, so that it could then be used for attacks.

Unfortunately, cybercrime is constantly improving and goes hand in hand with technologies, which, in turn, makes it difficult to detect and counteract these unlawful actions. It is worth remembering that in practice the lost funds are very difficult to compensate, because the guilty person in such a situation is not easy to find, the bank bears responsibility only if it is proved that the crime was committed by his fault.

Currently, banks are actively cooperating with law enforcement agencies to prevent crime related to interference with computer systems, but cybercrime laws and practices indicate significant gaps in this area.

The implementation of effective cybersecurity measures is now a rather challenging task, as the number of devices and applications that can be protected is rapidly increasing, and attackers are becoming more inventive.

The problem of protection from hacker attacks, Internet threats and hacker protection is becoming a reality every day. However, most users are not fully aware of the consequences of such attacks on computer networks and personal computers, which often do not adhere to the basic rules of safe conduct on the Internet. As a result, hackers easily turn the simplicity of the security tier, gaining new opportunities for committing various crimes.

Therefore, it is extremely important to systematically instruct users about the necessary cyber security measures, while not only working equipment, but also personal.

The task of every citizen for his own security - be vigilant and treat your personal data and payment cards with special care and attention.

Every year, due to the lack of cyber security specialists, requests for computer security services only increase. And with the development of IT-technologies, cybercriminals become almost limitless and this must necessarily be something to react.

Cybersecurity experts are among the most sought after in the labor market [4]. Now, no reputable company can do without the protection of its data. Accordingly, the demand for cyber security specialists is high. Their payment in Ukraine is $ 10,000. And the salary of small professionals starts at $ 300-400.

Why are their services so highly valued? Cyber threats have already moved to second place in the ranking of the most dangerous business risks. By 2020, the global damage from cybercrime could reach $ 2 trillion, and the company's cost to protect against hackers - $100 billion. According to the minimal estimates, only the Petya virus lost domestic economy 466 million, or 0.5% of GDP.

Today more than 50 Ukrainian universities teach specialty 125 cybersecurity. In the opinion of the exepts, many capable students are issued - Kyiv Polytechnic Institute, Kharkiv National University of Radio Electronics, as well as Vinnytsia National Technical University and Khmelnytsky National University [5].

Cybersecurity 125 is a field of training in Vinnitsa National Technical University, where the development and administration of software and hardware for information protection is studied in depth, as well as a specialty focused on the protection of computers, networks, programs and data from unintentional access, modification or destruction. Training of specialists at the educational and qualification levels of the bachelor's and master's degrees is provided for both full-time and part-time forms of training as well as the training of highly skilled personnel: graduate students and postgraduate students.

Technologies can combine humanity, they help us to clear borders between people, to develop business, to establish connections. But these same technologies make us vulnerable. It is important to combine the efforts of cybersecurity professionals to protect products, businesses and government systems.

Our goal is to make life better, to create the necessary conditions for us to grow and develop. We must understand the importance of cybersecurity, this is one of the key elements of our day.

We must strive to make Ukraine the center of cyber security in Eastern Europe in order to increase, and even introduce the full safety of everyone.

In cybersecurity, the essence of the future protection and safety of every inhabitant of the planet.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Захист програмного забезпечення [Електронний ресурс] - Режим доступу до ресурсу: http://kaplun.vk.vntu.edu.ua/file/773c4883cdd5fd27fab425e9304b3c01.pdf

2. Інформаційні технології та кібербезпека [Електронний ресурс] - Режим доступу до ресурсу: http://elit.sumdu.edu.ua/uk/abiturientam/spetsialnosti-fakultetu/192-kiberbezpeka.html

3. Хакерські атаки в світі: як і навіщо кібервоїни втручаються в політичні процеси [Електронний ресурс] – Режим доступу до ресурсу: https://ukr.segodnya.ua/world/hakerskie-ataki-v-mire-kak-i-zachem-kibervoiny-vmeshivayutsya-v-politicheskie-processy-1030346.html.

4. Майбутнє кібербезпеки: про що говорили на HackIT 4.0 [Електронний ресурс] - Режим доступу до ресурсу: www.epravda.com.ua/news/2018/10/19/641753/
5. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання [Електронний ресурс] - Режим доступу до ресурсу: file:///C:/Users/Admin/Downloads/kiberinterventsiya-ta-kiberbezpeka-ukrayini-problemi-ta-perspektivi-yih-podolannya%20(1).pdf

Антонюк Ганна Олександрівна
студентка 1 курсу групи КІТС-18б
Факультет менеджменту та інформаційної безпеки
Вінницького національного технічного університету
м. Вінниця
antonuchka.07.08@gmail.com

Столяренко Оксана Василівна
к. пед. н., доцент кафедри іноземних мов,
ВНТУ

Antonyuk Anna Alexandrivna
student of the group KITS-18b
Faculty of Management and Information Security
Vinnitsa National Technical University
Vinnytsya
antonuchka.07.08@gmail.com

Stoliarenko Oksana
Candidate of Pedagogy
Assistant Professor at the Department of Foreign Language,
VNTU