УДК 004

# INFORMATION ENCRYPTING AND THE ROLE OF CYBERSECURITY IN THE MODERN WORLD

Н. А. КАЗЫМОВ
Научный руководитель А. А. РАЗМАХНИНА
Белорусско-Российский университет

Since ancient times people have wanted their information to be protected. Humanity has created many ways of encrypting information: from Cesar's more primitive cipher to the famous German encrypting machine Enigma.

Nowadays there are two basic systems of encrypting information – symmetric and asymmetric.

However, cryptographers in the past faced an important drawback of symmetric encryption systems. All the involved parties had to have a key to transmit and to decrypt a message. If there were many channels of communication using the same description key, some of which were not sufficiently protected, intruders could intercept the secret key.

But the problem of key distribution was resolved in 1976. American cryptographers M. Hellman and W. Diffie developed an idea of obtaining private keys by transmitting them through an open channel.

Since this event, the development of asymmetric encryption systems has begun. So, what is the essence of an asymmetric cryptosystem?

Each part must have a pair of keys – private and public. The receiving part generates their own pair of keys before receiving the message. The sender receives the public key and encrypts the message. It can only be decoded using the recipient's private key.

Therefore, the encryption key, also known as public key, is accessible to everyone, but only the private key owner can decrypt and read the contests.

Today the internet provides unlimited possibilities to humanity: from socializing with people from all corners of the globe and online-shopping to transmitting huge amounts of data and international cooperation. However, if there is a criminal at the other end of connection, these possibilities become the Achilles's heel of the whole system. For example, criminals use the Internet for stealing confidential information, large scale fraud and theft.

Spies and terrorists can attack important objects of infrastructure being on the other side of the planet. They can easily brake the work of networks that connect financial establishments, deny people accesses to their personal data and can make power go down. The danger becomes even bigger if we talk about military departments.

The cybersecurity problem is one of the highest priorities in the modern world. Nowadays the main spy weapon is not a knife, but a USB. As our dependence on the global network continues to grow, the number and sophistication of cyber threats is increasing. Also the number of companies that develop new products and methods of protection of information is growing.

According to statistics, in 2019, the number of cyber threats has increased in comparison to the previous year. Targeted attacks have become a bigger priority than mass attacks. The main targets of criminals are scientific and educational sphere, the financial sector and government departments.

The majority of cybercrimes belong to one of the two categories. The first category includes crimes, which main target is devices themselves. The other group comprises crimes where hacked computers are used to commit other crimes. In many cases, hackers use such types of cyber threats as hacking, spam and fishing using malware and web vulnerabilities, data selection, social engineering, DDoS, etc.

Talking about hacking, the criminals use software vulnerability. When too many people know about vulnerabilities, firstly hackers attack users that have outdated versions of software. Therefore, you need to update the software in a timely manner.

The sheer number of ads messages coming to e-mail may annoy many of us. It is spam. Spam is annoying, however, it can also be really dangerous. Especially, if spam is used as a part of fishing. Spammers and cybercriminals send spam by mail in huge quantities. Spam aims at extorting money from users who respond to messages, distributing malware, receiving personal data – passwords, credit card number – etc.

There are different types of malware cyber threats: from worms and trojans to spyware. In fact, no user or company is fully protected from this type of attack. For example, hacker group TA505 uses bank trojan Dridex, encryption program Cryptomix, trojans ServHelper and FlawedAmmyy that allow hackers to remotely control the victim’s computer. They also use plugin Upxxec, which can detect and disable a large number of anti-virus protection tools.

In the process of selecting data, hackers use previously stolen or acquired on the Darknet databases of logins and passwords. The target of such kind of attacks is to gain access to the system and confidential information of different companies and users.

As previously noted, sometimes cybercriminals hunt not only for victim’s personal data, but also for their PC’s. They use computing abilities of your device for cryptocurrency mining. Such kind of activity is called cyberjacking. The mechanism of cyberjacking is forced mining while visiting web-sites, where corresponding software is installed. Hackers crack web-resources and mask lines of code. Moreover, mining scripts were even found on the Internet giant – YouTube.

Social engineering methods are very popular among criminals: forging or using compromised corporate e-mail addresses and sending fishing e-mails. Malicious links may be blocked by e-mail protection. However, hackers use links to compromised resources such as SharePoint. Hackers place there links to fake pages, where the victim enters their personal data. If fishing link is attached to the message the means of protection would block it. However, links placed on the SharePoint are not on the “blacklist” and blocked.

Distributed network attacks are called DDoS (Distributed Denial of Service). Criminals use web resources restrictions on a number of requests that can be processed at the same time. Frequently, a cybercriminal uses a network of infected computers – a “zombie-network” – to send a very large number of requests to the victim’s resource. Because the criminal coordinates all the actions of the “zombie-network”, the attack may be too powerful for the victim’s web-resource. Moreover, the criminal may demand money to stop the attacks.

So, how can we protect our computers from cyber attacks? If you want to fully protect your device, you must use an antivirus or a comprehensive solution for Internet security, such as Kaspersky Total Security, Avast, ESET NOD32, Dr. Web, etc. Antivirus software allows you successfully scan, detect and remove malware before it damages the system.

One of the most important points is to update software on time to reduce the chance of hacking. In addition, the latest security patches will be used to protect your computer.

A common reason why hackers get access to private information is elementary human negligence. You should use strong password that will be hard to pick up. While creating the password try to avoid using obvious words and phrases, such as *password*, *mypass228, qwerty,* etc. Also you should not use personal data – the name of a child or pet, your pseudonym, important dates – this information can be known to other people, and also easily found.

Never give your private information before you make sure that transmission channel is reliable. Also, you should make sure that you talk to the right person. By the way, if the speaker introduces themselves as an employee of a company and asks you for data you should call back the official number of the company. It’s advisable to use another device, because criminals can stay on the line or listen to your phone.

And finally, don’t follow the links in the spam e-mails or on unfamiliar sites, if you don’t want to become a victim of scammers. Pay attention to the URL addresses of sites. If it looks like spam or does not look legitimate, it is better not to take risks.

But if you have become a victim of a cybercriminal try to understand how it happened.

Carefully review the history of the latest banking transactions. If you find any operation suspicious, immediately ask the bank to provide full information about it. So, the bank can check, if it is fraudulent.

In conclusion, sound balance between freedom of actions in the Internet and providing cybersecurity and protection of personal data is needed in the modern world.