Plakhin N. S., Koshar K. D.
gr. 17DKK-1
Belarus State Economic University
Scientific adviser – candidate of sociology, associate professor Naumov D. I.

ENSURING CYBER SECURITY IN THE BANKING SECTOR OF THE REPUBLIC OF BELARUS

Daily activity of banking systems is closely connected with the use of modern computer technologies and is fully dependent on reliable and uninterrupted operation of electronic computer systems. The world experience testifies to the unconditional vulnerability of any company due to the fact that cyber crimes have no national boundaries, therefore hackers have the opportunity to be equally threatening information systems anywhere in the world. The concepts of "cybercrime" are increasingly found on the tapes of the world's media and almost daily attract the attention of the public.

The security system as a whole is a continuous process of identification, analysis and control. There are a number of basic principles according to which information security of the Bank is ensured. Namely, access to the Bank's data is protected by an identification system, that is, passwords or electronic keys. One of the most common ways to steal banking information is to use backup, take out data on a medium or simulate hacking, but not for the purpose of theft of material resources, but to access information on the server. Daily backups performed by organizations reduce the risk of complete loss of important information. Strict accounting of channels and servers, as well as measures to ensure the technical protection of information and the security of the Bank, imply the protection of backups. Ensuring uninterrupted power supply of equipment containing valuable information, limited access to safes and protection against information leakage in an acoustic way. Modern methods made it possible to improve the system of cryptography, as well as to implement such measures as electronic digital signature (EDS). It serves as an analogue of the handwritten signature and has a direct link to the electronic key, which is stored at the owner of the signature. The key consists of two parts: open and closed, and is protected by a special code. It is also necessary to emphasize the importance of careful and regular work with the staff, as information security largely depends on the quality and accuracy of the requirements imposed by the security service. According to statistics, about 80% of offenses are committed by Bank employees, that is, those who directly had or has access to data [1].

In addition to the internal factor, there is also a technical threat to the information security of banks. These include break-ins of information systems, persons who do not have direct access to the system, criminal or competing organizations. Receive information in this case is made with the use of special audio or video equipment. One of the modern forms of hacking is the use of electric and electromagnetic radiation, providing attackers with the ability to obtain confidential information.

The danger and threat to the software can also be a variety of malicious media computer viruses, software bookmarks that can destroy the entered codes. The best known way to solve virus problems of the software are licensed antivirus programs that successfully cope with this problem. To protect Bank information from internal and external leaks will help a competent specialist in this field and software that allows you to monitor and block the transfer of information to removable media.

To analyze the effectiveness of the measures taken, it is necessary to keep a record, which will mark the efficiency and effectiveness of the applied means of information protection in the Bank.

The specifics and peculiarities of the security system, of course, are individual for each individual Bank. Consider the provision of information security on the example of the national Bank of the Republic of Belarus.

During 2018, it is planned to create the FinCERT Center. Within its framework, a system of monitoring and countering cyberattacks to the credit and financial sphere will work. The center will be responsible for interaction and exchange of information between banks, other credit and financial institutions, SOFTWARE developers, equipment suppliers, Telecom operators and law enforcement

agencies. Its task is to promptly notify the system participants about the detected threats to eliminate vulnerabilities and counter cyberattacks [2].

At the moment, the main measures of the NBB to ensure information security are technological measures aimed at improving the reliability of the procedure for the transfer of information of the payment system and the identification of the cardholder, security measures when conducting transactions with plastic cards directly in the units that produce, issue and service them. To ensure the safety during the maintenance of terminal equipment (ATMs, information kiosks, terminals), including measures for the prevention and/or detection of illegal actions with the terminal equipment by third parties during its operation, the organization of distribution and consolidation of staff credentials (keys, business cards operators and administrators, passwords, access rights). Security is also ensured when using the Internet network by the Bank's employees, when accessing the Bank's customer services via the Internet (Internet-banking), when using e-mail, both intra-corporate and via the Internet [3].

In conclusion, it can be noted that because of the economic importance of banking systems and ensure their information security is imperative. Since the information in the database of banks is a real material value and therefore the requirements for the storage and processing of this information will always be increased.

1. Information security of banks [Electronic resource] – Access mode: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/informatsionnaya-bezopasnost-bankov.html 2. National Bank: information security in the financial sector will be a priority for banks [Electronic resource] – Access mode: https://benefit.by/news/4223/nacbank_informacionnaya_bezopasnost_v_finansovoy.html 3. Development of information security policy of the Bank [Electronic resource] – Access mode: http://www.cbt.by/main.aspx?guid=1841