UDK 004.056.5:336.71

CURRENT CYBER SECURITY TRENDS OF BANK ACCOUNTS AND BANK BUILDINGS

assistant Bulaga V.A., student Perederii I.A
Kharkiv National University of Radio Electronics,
Department of CHRIST,
e-mail: victoria.bulaga@nure.ua, illia.perederii@nure.ua

Abstract. This work is dedicated to the importance of financial security of the banking system of Ukraine and conducting a comprehensive assessment of the current situation. An analysis of the protection and insecurity of the current bank was carried out. The technical details of the bank's security system have been reviewed. Cybersecurity of banking and banking sectors is an important part of our economy. However, cyber-attacks are becoming increasingly sophisticated, and banks are at risk of losing their efforts to protect the data of their clients. By keeping up to date with the latest security technologies and best practices, banks can continue to provide their clients with safe and reliable banking services.

Introduction.

Today, everyone has their own bank account in a bank, their security is a very important economic aspect in the development of Ukraine and any continent in general. The security of the country consists of the security of its structures and, first of all, the security of its primary economic sector. This is evidenced by the reaction of the impact of market competition on the economy of the country as a whole and the economy of an individual enterprise or bank. For the country's socially oriented economy, competition is the engine of its development and improvement, and it is in the interests of the state to protect it by all possible means. Thus, banking security from one bank is an integral part of the national security system, along with its elements such as technical security, energy, military, environmental, information security and others. At the same time, it should be taken into account that one of the most dangerous threats to the economy of Ukraine is the violation of its financial and banking system. Today, the situation is such that thieves are trying more and more to hack our cards and take your money, so the purpose of this essay is to talk about how the banking system protects your savings, and what to do if you lose your card, and how not to lose all your money.

Main part.

Today, the banking system of Ukraine is experiencing difficult times, reacting like a litmus test to changes in both the economic and socio-political environment of the country. The socio-political crisis in Ukraine in 2013-2014 caused a deep economic crisis, which most affected the banking sector. Increased demands have always been placed on bank security systems, and it is impossible to imagine a bank without security and alarm systems, access control

systems and video surveillance. In order to get permission to open a bank office, additional office and branch, you need to pass the security system to a special commission. Security measures include organizational measures, information support, regulatory and methodological materials, work with personnel, physical protection, countermeasures, etc.

Bank access control system.

The main purpose of the SCD in the bank is to prevent unwanted persons from entering the premises protected by the bank. The network access control system to the bank must work under the control of the central server of the system within the branch. It is desirable that the SCD of all branches and additional offices of the bank work within the framework of a single system with administration and control from the central office.

Video control in the building and the adjacent territory of the bank.

Situational video surveillance for the bank is the main tool of operational control of the security service. When equipping a bank with video surveillance systems, the principle of total control of the entire territory is adhered to. The only exceptions are offices in the office part of the bank. Video cameras monitor: the operating room, the self-service area, ATMs and terminals, the cash desk and cash register cabins, the storeroom and cash flow paths, the collection area, the courtyard and the perimeter. Modern technologies allow obtaining high-quality images, which is very important for conducting investigations and transferring materials to law enforcement agencies. The resolution of IP cameras and HD-SDI reaches FullHD and more, and the speed is up to 60 fps. It is impossible to hide from such a camera. The skin detail of what happened will be captured in minute detail.

Video surveillance in the bank to monitor customer service and marketing tasks.

Today, video analysis systems offer a wide range of tools that help improve the efficiency and control of the banking branch:

1. Counting visitors.
2. Calculation of queue length.

Software and hardware means of information protection.

All SEP payment documents before being sent from the bank are processed by hardware and software means of information protection, which ensure compliance with the following requirements from the point of view of information security: the transmitted information must be closed, that is, the message can be read only by those to whom it is addressed; integrity – accidental or intentional damage to the message at the stage of its transmission will be detected during its reception; authenticity of the sender (when receiving a message, you can clearly determine who sent it).

A number of auxiliary requirements, which allows for a more detailed analysis of possible non-standard situations:

1. An encrypted arbitration log is kept by means of information

protection, which stores the information processing protocol, as well as the contents of the processed files;

2. The date and time fields of processing are included in the encrypted message.

The main means of information protection in SEP are hardware. The secrecy of their keys is ensured technologically:

1. The keys are stored in a special electronic card, they can be read only with the help of a special block that performs the information encryption process. It is impossible to read the keys by other means;

2. An electronic card is issued to a bank with prior binding to a specific encryption unit of the same bank; a lost or stolen card will not work in another cipher block (for example, in the equipment of another bank);

3. In the case of theft of the block and the card at the same time from a specific bank, a mode of exclusion of this equipment from the list of SEP users is provided; the bank can continue working in the SEP after resolving legal and financial issues related to the loss of equipment and obtaining a new complex. The weakest point from the point of view of security is the area of payment preparation by the staff of the SEP participating bank. All registered more or less successful VAT attempts were by representatives of banks, which led to the theft of funds from their own bank, not from the state or from other banks. In all these cases, the individuals who attempted VAT had legal access to the system for preparing and protecting payment information, and their authority was exceeded (access to many or even all banking resources of the system).

In order to guarantee the security of information in this area, SEP participants are required to fulfill a number of organizational requirements:

1. Admission of only authorized persons to key operations of preparation of payment documents;

2. Performance by the responsible persons of the bank of constant, real and sufficient control over the state of the balance sheet and correspondent account of the bank. It is impractical to concentrate all powers regarding access to the bank's software and hardware in the person of one bank employee: a separate authorized person should be responsible for each area of payment processing (local network administrator, e-mail administrator, responsible for the work of ATM-3 SEP, etc.). In order to guarantee the security of information at the level of SEP participating banks, it is proposed to implement cross-overlapping of electronic signatures on payment documents. Banks are offered the use of software that implements a digital signature implemented on the basis of the RSA algorithm. Each participant in the exchange of electronic documents has two keys: 1. Secret, which must be carefully protected from outsiders and known only to its owner; 2. Open, which is distributed in the system and can be known to every member of the system.

The essence of the RSA algorithm

1. An electronic digital signature is based on a message processed with a

special secret key of the sender and the public key of the recipient.

2. During the verification of the electronic digital signature, the receiver's software complex forms a prototype of the electronic signature of the received message.

3. The received digital signature is decrypted with the public key of the sender and the secret key of the recipient of the message and the prototype of the electronic digital signature is calculated.

4. The received prototype is compared with the calculated prototype of the electronic digital signature. A match between these two signature prototypes (received and computed) shows that the message was signed by the specified sender of the information and received in the same form in which it was signed.

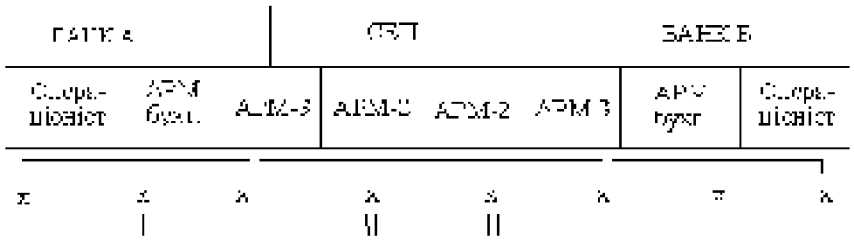

Fig. 1. The scheme of imposing an electronic digital signature in the SEP.

Conclusions.

Cybersecurity of bank accounts and bank buildings is a very important part of our economy. It is a top priority for banks as they handle sensitive financial information and transactions. By staying abreast of the latest security technologies and best practices, banks can continue to provide their customers with safe and secure banking services.

References:

1. Кібербезпека платежів. URL (https://rating.zone/chem-obernetsia-dlia-ukrayny-rekordnyj-rost-tsen-na-syrevye-tovary/)

(дата звернення: 27.02.2024)

2. Захист банківської інформації в СЕП: основні задачі та вимоги. URL:(https://osvita.ua/vnz/reports/bank/20375/)

(дата звернення: 28.02.2024)