The main cybersecurity risks in the banking sector and methods for managing them.

Isroilov Javokhirbek Abdugaffor ugli, 3rd year student of the Faculty of Cyber Security, Information Security direction of the Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi.
Teshaboyev Ikhtiyor Komil ugli, 3rd year student of the Faculty of Cyber Security, Information Security direction of the Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi.

Annotation. This article presents the main cybersecurity risks in the banking sector and methods for managing them

Keywords: Cybersecurity risks, banking, banking risks, data leakage, unauthorized access to cryptocurrency, customer protection, financial losses, cybercriminals.

Currently, the most serious security problems in the banking sector are online threats. Banks and other financial institutions process millions of transactions daily, with the majority of transactions going through digital payment platforms. It is for this reason that banks have become tempting targets for cybercriminals around the world.

As the financial world rapidly moves online, it is becoming increasingly vulnerable to cybercriminals. Comprehensive and robust security measures are required to protect virtual data and assets.

Cyberattacks are usually aimed at gaining access to confidential data, modifying or destroying it, extorting money from users, or disrupting business processes. The implementation of effective measures to protect operating systems, programs and networks from cyber attacks is a prerequisite for the successful operation of a financial business.

Experts identify three main cyber risks in the banking sector. These risks are always present in the activities of banks, and understanding them and knowing how to implement them can help implement more effective protection measures.

1. Illegal access to information or data leakage.

Cybercriminals are constantly looking for new ways to hack data. New banking services and online systems that allow you to quickly complete transactions and maintain user accounts anywhere in the world open a new door for cybercriminals. As transactions between banks and consumers become more digitized, hackers are

increasingly using banking systems and open networks for destructive activities. If banking systems are not sufficiently protected in terms of cyber security, they become vulnerable to criminals.

2. Penetration through mobile applications.

As more people access their bank accounts through mobile phone apps, cybersecurity risks in this area are on the rise. Most users do not protect their personal devices with additional software, which leaves them vulnerable to attacks. Using secure banking software is the key to preventing malicious activity through mobile apps and devices.

3. Unauthorized access to cryptocurrency.

The harsh reality is that, apart from cryptocurrency wallets and blockchain technology, there are not many ways to ensure cybersecurity in this area. Without the introduction of additional security measures, it is easier for attackers to steal cryptocurrency and the income of cybercriminals in this segment is growing. Building systems for managing the described cyber risks is important for all banking enterprises. Of course, customer funds must be physically protected, but now it is much more important that the money is digitally protected.

Here are a few reasons why cybersecurity is vital for any bank.

1. Prevent financial losses. Imagine that you go online to transfer funds from your account, for example, to pay rent for an apartment, and discover a series of large fraudulent payments in your journal. Usually, when this happens, the funds can still be returned if the client promptly contacts the bank to resolve this problem. When a similar situation occurs in a bank, it can take some time to analyze the causes and reverse malicious transactions. This not only affects the reputation of the bank, but also causes significant stress for the client. To prevent hacks, banks need to implement a cyber risk management plan that protects the banking network from all hacking attempts and ensures the financial security of bank customers.

2. Protect customer data. The moment a bank customer's personal information is stolen or hacked, the sheer scale of its distribution can make it difficult to restore the status quo. Cybercriminals sell personal information of bank customers on the black market for further unauthorized debiting of funds from accounts. As banks expand their clientele, they need to ensure that proper cybersecurity systems are in place to protect their network and, most importantly, their customers' personal information.

3. Maintain the reputation of the bank. According to a study by Security Magazine, 80% of customers are willing to give up continuing their business if their reputation is compromised, and 85% of these people will tell others about their negative

experience. Reputation is the basis of any modern business, especially when it comes to a bank. The use of effective cyber security practices and continuous monitoring of security have a positive impact on the reputation of the bank and contribute to building trust. This is extremely important in an industry that is responsible for the financial well-being and personal data of each of its customers.

4. Avoid penalties and claims from the regulator. If a bank becomes a victim of cyber threats and violations of customer data protection requirements become known, the regulator may intervene and impose sanctions on the bank.

Now that we understand the main risks in cybersecurity, as well as the reasons why cybersecurity is important in the banking sector, we can consider the mechanisms for protecting a financial institution from cybercrime. Here are some useful tools for such protection.

- ✔ Employee training.
- ✔ Constant monitoring of all information systems and regular audit.
- ✔ Selection of optimal automated solutions in the field of cybersecurity.
- ✔ Cyber risk insurance.

List of used literature

1. Kalaichidi, T.Yu. Banking risks in lending: credit risk / T.Yu. Kalaichidi // Colloquium-journal. - 2019. - No. 8-7 (32).

2. Mugu, S.Kh. Credit risk management in commercial banks /S.Kh. Mugu // Eurasian Scientific Association. - 2019. - No. 4-4 (50).

3. Moroz, N.V. Essence, causes and classification of bank credit risk / N.V. Frost // Business inform. - 2019. - No. 7 (498).

4. Yudina, A.A. Credit risk management in a commercial bank / A.A. Yudina // Economics and management of innovative technologies. - 2020. No. 1 (100).