Кибербезопасность в российском банковском секторе: угрозы и перспективы

Крайнова Евгения Михайловна, студентка 4-ого курса финансового факультета РЭУ им. Г.В. Плеханова, г. Москва, Российская Федерация

E-mail: evgmihailovna98@gmail.com

Ростовцева Анастасия Романовна, студентка 4-ого курса финансового факультета РЭУ им. Г.В. Плеханова, г. Москва, Российская Федерация

E-mail: rostovtseva1998anastasia@gmail.com

Аннотация

В работе представлено явление кибер-безопасности в банковском секторе. Представлены текущие угрозы и тенденции развития деятельности. Рассмотрены методы снижения рисков атак на клиентов и банковских организаций на примере компаний и государственных учреждений. На примере практики США изучены дополнительные перспективы развития кибер-безопасности. Данное сравнение могут быть использованы для разработки практических рекомендаций по дальнейшему применению в Российской Федерации.

Ключевые слова: кибер-безопасность, кибер-преступность, финансовые организации, центральный банк, утечка информации.

Cyber-safety in banking sector: Russia and USA

Krainova Evgenia Mihailovna, student, Plekhanov Russian University of Economics, Moscow, Russian Federation

E-mail: evgmihailovna98@gmail.com

Rostovtseva Anastasia Romanovna, student, Plekhanov Russian University of Economics, Moscow, Russian Federation

E-mail: rostovtseva1998anastasia@gmail.com

Abstract

The paper presents the phenomenon of cyber security in the banking sector. Current threats and trends of activity development are presented. The methods of reducing the risks of attacks on customers and banking organizations on the example of companies and government agencies are considered. Additional prospects for the development of cyber security are studied on the example

of the us practice. This comparison can be used to develop practical recommendations for further application in the Russian Federation.

Keywords: cyber security, cybercrime, financial institutions, Central Bank, information leakage.

At the present day, banking sector's involvement in virtual sphere becomes more and more common: mobile and contactless payments, P2P (Person to Person) services, prospective of blockchain technology implementation, etc. The main target of performance improvement and strong competition in the activity is their client orientation. Thus, collecting all customer's data, banks should provide confidentiality in virtual space.

However, there is a common issue in an implementation of security. According to experts of Positive technology about 61% of online banks have a low level of security and it was discovered that both productive and testing operating systems have at least one critical vulnerability [6]. This fact demonstrates that the structure of cyber-security is having difficulties in obtaining complete isolation from possible hacker attacks. Moreover, another issue is added to the phenomenon. Recently, Sberbank reported of a leak of two hundred clients' data, which was performed by the bank's employee possibly through physical extraction of data [5]. In other words, the personal information was not protected from the inside forces. Taking that into consideration, we can say that there are various weaknesses in the safety of banking virtual space.

Thus, the objective of the work is to study possible risks of cyber-safety of banking sector and their elimination using the practices of Russian and foreign organizations.

The essence of the phenomenon is realized by the governmental bodies of Russia. Central Bank of the Russian Federation, is focused on providing of cyber security measures under the tendencies of distant remote access to financial services, use new technologies and using of the Internet as a market (see table 1) [1]. Thus, it is aimed at reducing loss of clients' finance, financial institutions' reputation and operation difficulties and increasing the implementation of innovation activities.

Table 1. Threats and objectives of Central bank of Russia in information security

Type of threat	Direction of activity
Financial losses of clients	Monitoring of indicators of the level of financial losses
Financial losses of individual financial institutions	Providing stable operation of institutions in case of computer attacks
Disruption of operational reliability and	Monitoring the level of banking and financial

continuity of financial services	transactions made without the consent of customers
Systemic crisis development in the event of information security incidents	Promotion of innovative financial technologies to ensure the necessary level of information security

Let us study the Russian banking practical implementation of methods. In order to fight against financial loss, center for monitoring and response to computer attacks in the credit and financial sphere of the information security Department of the Bank of Russia FinCERT is working on the reducing of malicious software, use of deceiving Internet sites and spam attacks. It operates within the agreement with Coordination center of the national domain of the Internet, the Internet Development Fund, MSK-IX (Moscow Internet Exchange), the Fund for the promotion of Internet technologies and infrastructure. They cooperate in order to remove the domain from the search engines and block the interaction with the website [7].

In order to protect transactions of customers against such websites, financial institutions have developed applications with the mechanism of identification before use of funds. However, with the development of fraud, it is necessary to use programs that help with identifying the threat of attack. For an example, nowadays in Russia there is a development of adaptive security platforms, Wallarm as an example, that creates specialized rules for network resources and scans banks' resources for vulnerabilities. This helps to improve inside protection against cyber threats [3].

What is more, that it was recommended for banks to separate the employees that report insider information and ones who are responsible for transactions, in order to reduce human factor in financial and data loss [4]. We can see that both governmental and banking spheres of Russian federations are involved in risk-management against the threats.

Based on the Russian experience, it is easy to see that under the development of technologies cyber-attacks have become a significant threat to the security of banks and credit institutions, which cannot be ignored because it entails financial and reputational losses.

The problem which Sberbank recently has faced is certainly the first in the banking history of Russia, but other foreign banks suffered from the theft of personal data in such large volumes before. The most famous case happened in 2016 with the Central Bank of Bangladesh which lost about $81 million from its banking account as a result of using the cheap equipment and poor measures of cyber-safety. Scheduled system update was performed but the criminals were never found.

Another vivid example is the largest Bank of the USA - JP Morgan Chase. As a consequence of the largest cyber-raid in history, data of 76 million families and 7 million

companies were stolen. As a result, in 2016 the Bank increased annual expenses on cybersecurity to $ 500 million in order to improve testing and analytics systems.

Thus, in the last few years, an international trend has emerged: banks began to allocate more funds to prevent cyber-attacks and combat them. In the course of its research, Deloitte found that companies spend for cybersecurity on average 10% of the total budget allocated to IT-departments, as well as about 30% of the budget of the whole company [12]. However, money is often not the decisive factor determining the effectiveness of the measures taken. Let us consider some other factors and trends identified in the study of the company Deloitte that are also important in reducing the cyber-risks of a financial company [14]:

- Accountability from the top - the Board of Directors and top-management should be interested in the effectiveness of the measures taken for cyber-safety of a bank and monitor their proper implementation;
- General responsibilities. This factor is based on the previous one, assuming a centralized approach;
- Several methods of defense which should be independent from each other;
- Spread of cyber risk-purchase of insurance covering all possible risks of loss;
- External support.

Undoubtedly, by 2018 both large and small American financial institutions could develop their own systems to eliminate or minimize cyber-risks and the list of these factors can be continued by them. However, there are set of certain characteristics according to which the Bank is considered as mature by the National Institute of Standards and Technology (NIST) - involvement of senior management, introduction of cybersecurity in the overall business strategy of a bank and strengthening of the position of the relevant cyber-safety department in a financial institution.

At the same time, there are no reasons to think that top-managers are ignorant about cyber-threats for their own business. According to PwC's 19th Annual Global CEO Survey, 69% of CEOs from financial services companies are partially or extremely concerned about cyber-threats, compared to 61% of CEOs across all sectors [13].

Nowadays, cyber-risks are recognized not only by CEOs but also by the USA state, which is taking measures to maintain stability in the economy. Due to this, NATIONAL CYBER STRATEGY of the United States of America with new strategy of cyber-space development was presented to world community in September, 2018 by Donald Trump and the White House. American government promised to its citizens that a comprehensive understanding of risks at the national level by identifying national critical functions would be developed and also it will mature their cybersecurity offerings and engagements to better manage those national risks in 7 key areas,

among which, of course, the banking sector and finance [11]. This document is also interesting because the USA announced list of its "competitors" which includes Russia, China, Iran, and North Korea [10].

In continuation of discussion of political issues and their effect on the level of cyber-safety in financial sector of a country it should be noticed that among the side effects of sanctions of the USA against Iran in 2018 could be cyber money laundering, so many banks could be at risk. Shortly before, Iranian hackers had stolen at least 31 terabytes of documents and data from US academic institutions, businesses and government agencies. The damage from the theft was estimated at $3.4 billion. According to experts, Iran had a huge need for hard currency and there was a possibility that it could seek help from other countries or criminal groups to conduct new cyber-attacks and evade sanctions [2].

To help financial institutions in identification of security gaps one more document was developed by Financial Services Sector Coordinating Council (FSSCC) which is the Financial Services Sector Cybersecurity Profile (Profile), v1.0. For this purpose, Cybersecurity Self-Assessment in 4 Easy and Repeatable Steps were defined:

- Determination the Institution's Impact Tier by completing the Impact Tiering Questionnaire;
- Institution's assessment with the corresponding Diagnostic Statement questions;
- Identification by the Institution of shortcomings and gaps in its cybersecurity risk management governance, processes, capabilities, and regulatory compliance posture;
- Development and implementation of a plan to close gaps and address shortcomings to satisfy the cybersecurity expectations of its Impact Tier [8].

The U.S. Bank, which has developed its own set of measures to reduce the risk of cyber-threats to its customers does not remain aloof. These measures are performed daily by the Bank's Cyber Defense Center, who sees its purpose in prediction of emerging threats to protect our employees and our customers [9]. In general, the policy of the U.S. Bank is based on usage of the newest technologies and methods of authentications, experience exchange with other financial institutions and investments in cyber-safety students. Thus, in the process of cooperation with other financial institutions, the Financial Services Information Sharing and Analysis Center (FS-ISAC) was established, where you can find about 7,000 institutions from over the world. The main purpose of this institution is to stop the cyber-attack and prevent it from spreading further.

Overall, comparing the experience of US and Russian Federation we can summarize the required activity for reducing the vulnerability of banking system against cyber-attacks:

- Full involvement of banking organizations into the cyber security;

- Constant monitoring of operations, customers and employees;
- Evaluation of existing ang possible threats for financial system;
- Implementing new instruments against external data theft
- Increasing investments for innovations in security;

It is challenging to think overhead of all possible risks concerning cyber-security. However, we believe that if both governmental and banking bodies take development as a permanent basis, it is possible to decrease the scale of the damage and be able to efficiently counter it.

Список использованных источников

1. FSSCC. The Financial Services Sector Cybersecurity Profile (Profile), v1.0, p.7 // Информационный портал BPI.com [электронный ресурс] – Режим доступа. – URL: https://bpi.com/wp-content/uploads/2018/10/Financial-Services-Sector-Cybersecurity-Profile-Overview-and-User-Guide-2018-10-25.pdf (дата обращения 06.10.2019).
2. How U.S. Bank protects customers from cyber threats // Информационный портал USbank.com [электронный ресурс] – Режим доступа. – URL: https://www.usbank.com/newsroom/stories/how-us-bank-protects-customers-from-cyber-threats.html (дата обращения 09.10.2019).
3. NATIONAL CYBER STRATEGY of the United States of America, 2018 // Официальный сайт Whitewhouse.com [электронный ресурс] – Режим доступа. – URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения 09.10.2019).
4. Pursuing cybersecurity maturity at financial // Информационный портал BPI.com [электронный ресурс] – Режим доступа. – URL: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (дата обращения 09.10.2019).
5. PwC. 19th Annual Global CEO Survey “Redefining business success in a changing world”, 2019, pp. 6 // Информационный портал BPI.com [электронный ресурс] – Режим доступа. – URL: https://www.pwc.com/gx/en/ceo-survey/2016/landing-page/pwc-19th-annual-global-ceo-survey.pdf (дата обращения 09.10.2019).
6. The state of cybersecurity at financial institutions Информационный портал BPI.com [электронный ресурс] – Режим доступа. – URL: https://www2.deloitte.com/us/en/insights/industry/financial-services/state-of-cybersecurity-at-financial-institutions.html (дата обращения 09.10.2019).

7. Банк России. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. – 2019. – С. 3 [электронный ресурс] – Режим доступа. – URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения 05.10.2019).

8. Исаев М. Банки должны заранее подготовиться к возможным кибератакам Ирана // Информационный бизнес-портал Bloomberg (2019) [электронный ресурс] – Режим доступа. – URL: https://regnum.ru/news/polit/2508036.html (дата обращения 09.10.2019).

9. Как работает Валарм // Информационный сайт Валарм [электронный ресурс] – Режим доступа. – URL: https://docs.wallarm.com/ru/quickstart-ru/qs-intro-ru.html (дата обращения 09.10.2019).

10. Мошенник в банке: российские практики // Информационный бизнес-портал Bankir.ru [электронный ресурс] – Режим доступа. – URL: https://bankir.ru/publikacii/20161216/moshennik-v-banke-rossiiskie-praktiki-10008395/ (дата обращения 09.10.2019).

11. Сбербанк назвал версии утечки данных своих клиентов // Информационный бизнес-портал РБК [электронный ресурс] – Режим доступа. – URL: https://www.rbc.ru/finances/03/10/2019/5d960ab29a79471ea76e1769 (дата обращения 06.10.2019) .

12. Уязвимости онлайн-банков: подводим итоги анализа // Информационный бизнес-портал Positive Technologies [электронный ресурс] – Режим доступа. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-rbo-2019/ (дата обращения 06.10.2019).

13. ФинЦерт. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 1.09.2017-31.08.2018. – 2019. – 41 с.

References

1. FSSCC. The Financial Services Sector Cybersecurity Profile (Profile), v1.0, p.7 // Informatsionnyi portal BPI.com

https://bpi.com/wp-content/uploads/2018/10/Financial-Services-Sector-Cybersecurity-Profile-Overview-and-User-Guide-2018-10-25.pdf

2. How U.S. Bank protects customers from cyber threats // Informatsionnyi portal USbank.com

https://www.usbank.com/newsroom/stories/how-us-bank-protects-customers-from-cyber-threats.html

3. NATIONAL CYBER STRATEGY of the United States of America, 2018 // Ofitsial'nyi sait Whitewhouse.com

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

4. Pursuing cybersecurity maturity at financial // Informatsionnyi portal BPI.com

https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

5. PwC. 19th Annual Global CEO Survey “Redefining business success in a changing world”, 2019, pp. 6 // Informatsionnyi portal BPI.com

https://www.pwc.com/gx/en/ceo-survey/2016/landing-page/pwc-19th-annual-global-ceo-survey.pdf

6. The state of cybersecurity at financial institutions Informatsionnyi portal BPI.com

https://www2.deloitte.com/us/en/insights/industry/financial-services/state-of-cybersecurity-at-financial-institutions.html

7. Bank Rossii. Osnovnye napravleniya razvitiya informatsionnoi bezopasnosti kreditno-finansovoi sfery na period 2019–2021 godov, 2019, pp. 3

https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf

8. Isaev M. Banki dolzhny zaranee podgotovit'sya k vozmozhnym kiberatakam Irana // Informatsionnyi biznes-portal Bloomberg (2019)

https://regnum.ru/news/polit/2508036.html

9. Kak rabotaet Valarm // Informatsionnyi sait Valarm

https://docs.wallarm.com/ru/quickstart-ru/qs-intro-ru.html

10. Moshennik v banke: rossiiskie praktiki // Informatsionnyi biznes-portal Bankir.ru

https://bankir.ru/publikacii/20161216/moshennik-v-banke-rossiiskie-praktiki-10008395/

11. Sberbank nazval versii utechki dannykh svoikh klientov // Informatsionnyi biznes-portal RBK

https://www.rbc.ru/finances/03/10/2019/5d960ab29a79471ea76e1769

12. Uyazvimosti onlain-bankov: podvodim itogi analiza // Informatsionnyi biznes-portal Positive Technologies

https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-rbo-2019/

13. FinTsert. Otchet tsentra monitoringa i reagirovaniya na komp'yuternye ataki v kreditno-finansovoi sfere departamenta informatsionnoi bezopasnosti Banka Rossii 1.09.2017-31.08.2018, 2019, 41 p.