European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.03.69

FETDE 2020
International Conference on Finance, Entrepreneurship and Technologies in Digital Economy

ARTIFICIAL INTELLIGENCE TECHNOLOGY AND INVESTMENTS GUARANTEES IN BANKING: THE CYBERSECURITY ASPECT

Ella Gorian (a)*
*Corresponding author

(a) Vladivostok State University of Economics and Service, Vladivostok, Russia, ella.gorian@gmail.com

Abstract

Investment banking is a new prospective service in banking. Sensitive information circulating within is a main target of cyber-attacks. Many developers offer new security solutions based on Artificial Intelligence technologies. Artificial intelligence technologies are gaining popularity in the banking and financial sectors, which can significantly save industry costs. Still the existing artificial intelligence software solutions are relatively primitive and costly. Additional factors that complicate the performance of security functions are malicious data manipulation by attackers, as well as the interconnectedness of systems connected to AI within the banking system. As a result, artificial intelligence technologies cannot work autonomously, and human supervision is needed. In addition, many investment market industry participants underestimate cyber security issues as influential factor and investors are deprived of essential guarantees. Those market players who include and implement cybersecurity issues in their management strategies gain the sustainable position and market share. Such cybersecurity management strategy should include such outputs as personal data, M&A data, outsourcing of processes and services, risk assessment, etc.

Keywords: Artificial intelligence, cybersecurity, CII, investment banking, rights of investors

https://doi.org/10.15405/epsbs.2021.03.69
Corresponding Author: Ella Gorian
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Artificial intelligence (AI) technologies are becoming increasingly popular in the banking and financial sectors. According to Business Insider Intelligence analysts, about 80% of banking institutions with assets of more than $100 billion and slightly less than half of banks with assets of less than $100 billion are currently implementing AI projects. The results predicted are to be impressive: over the next three years, the industry will significantly save $447 billion, while only in the front office (working with clients) and the middle office (combating payment fraud) is expected to save $416 billion (Digalaki, 2019). In Russia, the leadership in the use of AI technologies maintains Sberbank of Russia: on the basis of decisions made by AI, 100% of credit cards, more than 90% of consumer loans and over 50% of mortgage loans are issued, and by 2020 AI technologies will be responsible for making about 100% of credit decisions. Since July 18, 2019 Sberbank of Russia uses AI technologies in its mobile application. The core issues of AI application in banking and financial sectors are: launching and promoting new financial services; remote customer verification and fraud protection technologies; agent-client interaction at the stock exchange; digitalization of financial services; sceptical attitude of bank shareholders towards FinTech technologies, despite the fact that more than 50% of Russian banks are actively investing in FinTech start-ups, lack of solutions in the B2B segment; cybersecurity and new regulatory opportunities; the use of artificial intelligence in FinTech companies. The use of AI technologies in the field of retail banking services is becoming a standard technological process; the next level is investment banking.

Guarantees of investor rights are the essential clauses of all international treaties in the field, and they also form the central part of the state mechanism for investment protection. So far as the legal mechanism of investment protection has been widely discussed both by academics and practitioners (Alekseenko, 2019), informational and organizational aspects is a relatively new subject of research. Increased vulnerability risks of sensitive information are inherent for investment banking that becomes more popular among “classical” banking and financial institutions (Sharma, 2020). Being a part of banking and financial sectors, investment banking comprises a critical information infrastructure (CII) that estimates it in a scope of CII mechanism protection.

2. Hypothesis

AI technologies are used for CII protection but at the same time they can be used as cyber-attack tools (for example, malware). Therefore the use of AI technology by FinTech companies should be a part of their management strategy which includes such outputs as personal data, M&A data, outsourcing of processes and services, risk assessment, etc.

3. Methodology

In this study the general (system-structural, formal-logical and hermeneutic methods) and special legal methods of scientific knowledge (comparative legal and formal-legal methods) have been applied.

4. Literature review

The researched topic is poorly represented in the Russian scientific literature. A number of scientific studies by scientists from Singapore and China consider the organizational, legal and technical features of ensuring the information security of financial and banking systems in the aspect of a decentralized approach (each subject is separate from the whole system) (Baluta et al., 2017; Ter, 2018), however, in a case of outsourcing of processes, as it actually takes place, the vulnerability of the banking system becomes a decisive factor determining the need for centralized development of outsourcing standards, including in the case of using the so-called cloud technologies. Some Singapore researchers pay attention to this, but from the technical side of the problem (Challa, 2018; Li et al., 2019), leaving out of sight its organizational and legal aspects. An important point in ensuring cybersecurity is a risk management system that allows you to allocate all available resources depending on a particular scenario of negative impact on the operating systems of financial and banking institutions (Jin et al., 2020; Zhang et al., 2018).

Some researches study the specific functions of investment banking (Battista, 2015; Bradford, 2012) leaving behind the brackets such issues as ensuring investors' rights. The other authors analyse the protection of investors' rights without any connections to the cyber security aspects (Lu & Wu, 2019).

5. Results and discussions

The Russian banking sector is a leader in the implementation of innovative technologies in comparison with European countries. The explanation for this is an active and initiative role the monetary authority of the Russian Federation (Bank of Russia) plays while regulating the activities of infrastructure projects (digital identification, fast payment system) and cybersecurity issues. Many Russian banking institutions attract ready-made FinTech solutions (as the outsourcing of services) that contribute the investment activity.

The leadership in the implementation of AI technologies in the investment banking possess the United States and China. Nowadays AI is actively used to ensure cyber security of the following areas: the fight against money laundering and fraud; aggregation of security data; monitoring cyber threats and preventing cyber-attacks. It should be noted that all products, including AI technologies, were developed by private sector - numerous FinTech companies. As indicated earlier in our studies, ensuring cybersecurity is impossible without close cooperation between private and public sector entities (Gorian, 2018). AI technologies are used primarily to ensure the following issues: 1) money laundering and fraud; 2) security data aggregation; 3) cyber threats monitoring and cyber-attacks prevention.

Money laundering and fraud. Most significant AI technology in this field is OpenMLEngine offered by Feedzai. This program allows security professionals to create their own fraud detection models using patterns that already exist in the software. The Feedzai platform usually integrates into the systems of a bank or service provider and warns risk analysts only of cases of fraud that are really considered as high-risk (based on predefined factors), thereby speeding up fraud detection processes and reducing the number of false positives.

OpenMLEngine is integrated into the operational systems of the 10 largest US banks. This risk assessment system analyses new applications for account opening and approves only with the low risk fraud profile. The platform was deployed at the core of the bank's existing corporate systems using its own data centres. This allowed the program to become the central decision-making mechanism in the process of registering customers on the Internet and verifying identity, verifying compliance and assessing the risk of fraud in real time. In those cases when the software doesn't have enough data to make a decision when submitting an online application, it automatically generates additional customer-specific questions envisaged by the bank adaptation group. The system ensures that high-risk applications are sent to security experts for manual verification, and the risk factors are understandable to facilitate decision making in order to reduce the time spent by security experts in each case. As a result, the number of approved applications increased by 70%, and the time spent on manual verification decreased. Despite the increase in users of banking services, the number of fraudulent activities has decreased (Bharadwaj, 2019).

Security data aggregation. DefenseStorm creates software for automating cybersecurity processes using machine learning: PatternScout and ThreatMatch monitor internal systems in real time to search for abnormal processes. Software tools help the bank to detect and to identify cyber security threats in its network, which saves long-term security costs and avoids data leaks. Using machine-based pattern recognition based on saved network data, the platform can support company-wide security and operations. Such SaaS solutions can help banking information security personnel to access data related to security events through a single control panel. Employees can log in the control panel and quickly respond to security threats identified by the software. For example, in the case of LiveOak Bank, DefenseStorm helped to solve the problem of data centers combined and located in different states of the USA to support performing leasing and deposit operations for small and medium enterprises. As a result, the bank information security staff was able to use the SaaS analytical solution to update existing LiveOakBank data management and analytics systems. After integration, LiveOakBank was able to optimize the search for big data, as a result, the detection of cyber incidents improved by 50-60%: if earlier employees spent 15-60 minutes on the detection and definition of the process as cyber threats, then after integration of the platform this time was reduced to 1-5 minutes (Bharadwaj, 2019).

Cyber threats monitoring and cyber-attacks prevention. Darktrace has developed EnterpriseImmuneSystem software that uses machine learning to detect and respond to cyber threats in digital environments such as the cloud, virtual networks, IoT (Internet of things) and industrial control systems. The popular product of EnterpriseImmuneSystem software is DarktraceThreatVisualizer - a control panel is used by information security banking staff to monitor cyber threats in real time. To date, users of the software product are more than 40 companies (Bharadwaj, 2019).

PatternEx offers AI-based software that can detect the user's malicious intent and predict and prevent cyber-attacks. The VirtualAnalyst platform analyses data (for example, IP addresses, users or sessions) of millions of users and detects suspicious actions (transactions from IP addresses used to carry out fraudulent activities). The templates compiled by the platform are evaluated by information security analysts who confirm the actual and false attacks. These decisions are used as the templates for the next data collection.

Researchers emphasize that at the moment the most widespread and successful in application are those AI-technology tools which are aimed at detecting fraud and combating money laundering, and in the next 3-5 years, software products will solve the problem real-time fraud threats detection (Bharadwaj, 2019).

Although the above-discussed fields of AI technologies applications deal with the technical side of investment banking there are some other aspects to be considered as the cyber security targets (Sharma, 2020): pending M&A transactions, top-level executives, mobile and tablets. The key solution is a proper cyber security management strategy to be maintained and launched within every FinTech company. It must comprise the appropriate technical solutions and procedures to minimize the risks in following fields: 1) autonomous devices; 2) IoT security; 3) data security; 4) digital platforms. Many investment market participants rely on outsourcing processes and services and national monetary authorities draft relevant regulations to ensure the flawless performance of financial sector. The same refers to risk management procedures to be carried by every bank or financial institution. As many investment banking participants are getting involved in a fierce competition nowadays the one and only who succeeds is that who implement the cyber security strategy to ensure the investors rights and to protect their interests.

6. Conclusions

Despite the existing software solutions with AI to ensure the cyber security of banks, they are considerably primitive and high-priced. Only large banks and financial institutions have sufficient budget and personnel to use AI technologies, and the quality of the tasks completed by the programs is still far from perfect. As it was mentioned above, ensuring of cybersecurity in the context of the implementation of AI depends on a number of conditions, both technical and organizational, and legal ones in nature. Along with the problems of protecting the rights and legitimate interests of investors, problems arise in determining the type and extent of liability in the case of outsourcing of certain processes and services, as well as issues of risk assessment and management.

Acknowledgements

The reported study was funded by RFBR, project number 20-011-00454 «Ensuring the rights of investors in the banking and financial sectors in the context of the digitalization of the economy in the Russian Federation and the leading financial centers of East Asia: a comparative legal aspect».

References

Alekseenko, A. P. (2019). New Russian Model BIT and the Practice of Investment Arbitration. *Manchester Journal of International Economic Law, 16*(1), 79-93.

Baluta, T., Ramapantulu, L., Teo, Y. M., & Chang, E. C. (2017, December). Modeling the Effects of Insider Threats on Cybersecurity of Complex Systems. *Proceedings of the Winter Simulation Conference (50th Anniversary)*, 4360-4371.

Battista, P. (2015). The Taxation of Crowdfunding: Income Tax Uncertainties and a Safe Harbor Test to Claim Gift Tax Exclusion. *Kansas Law Review, 64*, 143-186.

Bharadwaj, R. (2019, October). *AI for Cybersecurity in Finance – Current Applications.* https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications

Bradford, C. S. (2012). The New Federal Crowdfunding Exemption: Promise Unfulfilled. *Securities Regulation Law Journal, 40*(3), 1-58.

Challa, S. (2018). *Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems.* Future Generation Computer Systems.

Digalaki, E. (2019, June). *The $450B opportunity for the applications of artificial intelligence in the banking sector & examples of how banks are using AI.* https://www.businessinsider.com/the-ai-in-banking-report-2019-6

Gorian, E. (2018, October). Singapore’s Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection. In *The International Science and Technology Conference" FarEastCon"* (pp. 1-9). Springer, Cham.

Jin, Z., Liu, G., & Yang, H. (2020). Optimal consumption and investment strategies with liquidity risk and lifetime uncertainty for Markov regime-switching jump diffusion models. *European Journal of Operational Research, 280*(3), 1130.

Li, Z., Liu, X., Wang, W. M., Vatankhah Barenji, A., & Huang, G. Q. (2019). CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign. *Enterprise Information Systems, 13*(1), 1-33.

Lu, Z., & Wu, S. (2019), Analysis on the Protection of Investors’ Rights in Network Public Welfare Crowdfunding. *5*(1), *Dispute Resolution*, 9-13.

Sharma, J. (2020, January). *The Importance for Cyber Security in Investment Banking Industry.* https://hackernoon.com/the-need-for-cyber-security-in-investment-banking-industry-o0q2hnl

Ter, K. L. (2018). Singapore's cybersecurity strategy. *Computer Law and Security Review, 34*(4), 924-927.

Zhang, P., He, Y., & Chow, K.-P. (2018). Fraud track on secure electronic check system. *International Journal of Digital Crime and Forensics, 10*(2), 137-144.