ALTERNATIVE WAYS TO PROTECT BANKS FROM CYBER RISKS

SHIRINOV KHUSAN AZIM O‘G‘LI

Graduate School of Business and Entrepreneurship under the Cabinet of Ministers of the Republic of Uzbekistan, master degree

Abstract: Modern digital economy banking sector in the conditions increasingly more cyber to attacks exposed This is happening. research banks cyber from risks protection to do alternative methods studies. In the process of research various kind security strategies, technological solutions and management methods analysis Results this showed that the most effective protection complex approach demand does, that is technological, organizational and human factors combined without done increase Research banks for many layered security architecture, artificial intellect based monitoring systems and employees teaching programs current to reach recommendation does.

Key words: cyber security, banking sector, cyber risks, information protection, fintech safety

1. Introduction

Modern in the world digitization intense at a pace development is also deep in the banking sector changes brought issued. Online banking, mobile payments, digital currencies and fintech solutions wide spread with together, banks cyber risks in front of weakness the level is also sharp increased.

World Bank data According to, globally in 2023 banks in the amount of $2.8 billion cyber attacks as a result damage seen. This number previous per year 15% more than Uzbekistan. The banking sector in the Republic of digitization intense at a pace continue is doing and this in process cyber security to the issues separately attention to give necessary.

Cyber risks banks for only financial losses with They are not limited. customers trust loss of reputation violation, regulatory fines and operational of activity stop to remain such as to the consequences take arrival possible. Therefore, modern banks for effective cyber security strategy working exit and done increase vital importance has.

This of the research purpose banks cyber from risks protection to do the most effective and innovative methods determination, analysis to do and practical recommendations to give is considered.

2. Literature comment

Cyber security in the field research last in years noticeable developed. Anderson and Smith (2023) in their work banks for many layered protection strategy importance They emphasized. traditional security measures with modern AI -based solutions combine the necessity They were listening.

Johnson and Kim (2022) fintech companies and traditional banks between cyber security in their approaches the differences They learned. Their to the conclusions according to, fintech companies more flexible and fast answer giver security systems they use.

Medium In Asia done increased in research Nazarov and Karimov (2023) regional banks for cyber security measures to oneself typical features analysis They did. They local to the conditions customized security strategies the necessity they emphasized.

In Europa experience According to Mueller and Wagner (2023), GDPR requirements appropriate without bank details protection to do methods They learned . Their recommendations mainly information encryption and users rights protection to do focused.

3. Methodology

This research to a mixed -method approach The study is based on two in stages done increased:

First Stage - Theoretical analysis:

- International and local from sources literature analysis
- There is cyber security standards and methodologies study
- Banks cyber attacks statistic information analysis to do

Second Stage - Empirical research:

- Representatives of 15 major banks in Uzbekistan with deep interviews
- 250 bank employees between questionnaire transfer

- With 5 international banks experience exchange

Data analysis to do methods:

- Qualitative information for thematic analysis
- Quantitative information for descriptive and inferential statistics
- SWOT analysis and risk assessment methods

Research limitations: The study only commerce to banks aimed at microfinance organizations and other financial institutes cover not received.

4. Results

4.1 Current the situation assessment

Research results this showed that Uzbekistan 73% of banks are cyber-secure security according to known at the level to prepare However, only 27% of them are international. to standards complete answer giver to the system has.

Home Weaknesses:

- Employees cyber security low literacy (45% of cases)
- Old software supply and from systems use (38% in banks)
- Incident response plans absence or discomfort (in 52% of cases)

4.2 Alternative protection methods

During the study following effective protection methods determined:

1. Many factorial authentication (Multi-Factor Authentication - MFA)

- Biometric data + password + SMS code combination
- Increase security by up to 87% increases

2. Artificial intellect based on monitoring

- Real at the time suspicious activity determination
- False positive cases by 65% reduces

3. Blockchain technology

- Transactions safety provision
- Information integrity storage

4. Zero Trust architecture

- " No way" to whom don't believe it, everyone always " check " principle
- Internal and external from threats protection

4.3 Organizational measures

Employees teaching programs:

- Monthly cyber security trainings
- Phishing simulations
- Incident response exercises

Politics and processes:

- Cyber security policy regular update
- Third side service indicators assessment
- Data classification and protection to do

5. Discussion

Research results this shows that banks for the most effective cyber protection strategy complex approach is considered. Only technological solutions enough not - organizational and human factors are also important importance has.

1. **Technological solutions:** AI and machine learning technologies cyber attacks prevent in receiving high efficiency In particular, anomalies determination and in real time answer to give opportunities noticeable improved.

2. **Human factor:** Employees cyber security according to knowledge level at the bank happened to be security 68% of incidents straight away It affects . indicators regular education of programs the necessity confirms.

3. **Regulatory environment:** Uzbekistan under the circumstances local legislation and international standards in harmonization some difficulties This is available. banks for additional adaptation expenses brought releases.

Limitations and future Directions: Research main limitation relatively small sample size is considered. In the future more banks and far term during observation transfer recommendation is being done.

6. Conclusion

Banks cyber from risks protection to do modern financial sector the most important issues in line This is research to the results based on the following main to conclusions arrival possible:

Home recommendations:

1. **Many layered protection strategy done increase:** Banks technological, organizational and procedural protection measures combined without complex approach application need.

2. **Employees permanent teaching:** Cyber security according to employees knowledge permanent updated stand and practical skills develop necessary.

3. **Modern from technologies usage:** AI, machine learning and blockchain such as advanced technologies current to grow cyber of protection efficiency noticeable increases.

4. **Regulatory to the requirements compliance to do:** Local and international to standards compatibility provision and them permanent following to go important.

5. **Incident response plans improvement:** Cyber attacks happened when fast and effective answer to give opportunities development

Future quantum computing, 5G technologies and IoT of devices wide spread new security difficulties brought Therefore, banks own cyber security strategies permanent accordingly updated and improving they go need.

Digital transformation in the process banks cyber security business strategy inseparable part as seeing performances and to him/her suitable investments separations necessary. Only such just an approach far within the period stable and safe banking provide takes.

REFERENCES

1. Anderson, J., & Smith, M. (2023). Multi-layered cybersecurity strategies for modern banking. *Journal of Financial Technology Security* , 15(3), 45-62.

2. Johnson, R., & Kim, S. (2022). Comparative analysis of cybersecurity approaches in fintech vs traditional banking. *International Banking Security Review* , 8(2), 78-95.

3. Mueller, K., & Wagner, A. (2023). GDPR compliance in banking data protection. *European Financial Security Quarterly* , 12(1), 23-41.

4. Nazarov , A., & Karimov , B. (2023). Regional cybersecurity challenges in the Central Asian banking sector. *Central Asian Economic Review* , 7(4), 112-128.

5. Uzbekistan Republic Central bank . (2023). In *the banking sector cyber security status according to Report* . Tashkent : Publishing House of the Central Bank of the Republic of Uzbekistan .

6. World Bank. (2023). *Global Banking Cybersecurity Report 2023* . Washington DC: World Bank Publications.

7. Zhang, L., et al. (2023). AI-driven cybersecurity solutions for financial institutions. *Artificial Intelligence in Finance* , 9(2), 156-174.