SATBAYEV UNIVERSITY

Computing & Engineering

Volume 2 (2024), Issue 2, 21-28

https://doi.org/10.51301/ce.2024.i2.04

Analysis of vulnerabilities in the network of second-tier banks and development of a methodology for their identification and elimination

R. Kulanbayev*

Satbayev University, Almaty, Kazakhstan

**Corresponding author: kulanbaev.ramazan@gmail.com*

Abstract. This report analyzes the vulnerabilities of information systems of second-tier banks, with an emphasis on identifying and eliminating weaknesses in their protection. The main attention is paid to the audit of existing security systems and key threats affecting the work of banking institutions. The methodology for eliminating the identified vulnerabilities is presented, as well as recommendations for improving security procedures and organizational measures aimed at increasing the resilience of information systems to cyber-attacks.

Keywords: *information security, banking systems, auditing, vulnerabilities, cyber threats, protection methods, security systems, organizational measures.*

1. Introduction

In the modern world, the banking industry occupies a key place in ensuring financial stability and economic development. Second-tier banks, which are commercial institutions, play an important role in providing financial services such as loans, deposits and settlement transactions. However, their active use of digital technologies and network infrastructures makes them an attractive target for cybercriminals. Every year, the number and complexity of attacks on financial organizations are increasing, which requires an increasingly comprehensive approach to ensuring information security.

The relevance of the study is due to the need to protect second-tier banks from threats related to the exploitation of vulnerabilities in their networks. Identifying, analyzing and eliminating such vulnerabilities are key tasks that need to be addressed to prevent financial losses, leaks of confidential data and breaches of customer trust. In the context of the dynamic development of cyber threats, an important task is to develop a methodology that allows you to quickly identify existing vulnerabilities, eliminate them and prevent the emergence of new threats.

The purpose of this work is to analyze the vulnerabilities of second-tier banking networks and develop a methodology for their identification and elimination. To achieve it, it is necessary to study existing threats and vulnerabilities in the networks of financial organizations, explore approaches and tools for auditing bank security systems, propose a methodology for identifying and eliminating vulnerabilities, considering the characteristics of second-tier banks and test it in practice, evaluating its effectiveness and applicability.

The scientific novelty of the research lies in the creation of an integrated approach to the analysis and elimination of vulnerabilities, considering the unique characteristics of the network infrastructure of second-tier banks. The practical significance of the work is determined by its contribution to ensuring the information security of financial organizations, which strengthens their resistance to cyber-attacks and customer trust.

The research is aimed at solving one of the most important tasks of the current stage of development of the banking industry - ensuring the security of the network infrastructure of second-tier banks.

As shown in Figure 1, the assets of second-tier banks in Kazakhstan vary significantly, where the leading positions are held by Halyk Savings Bank of Kazakhstan and Kaspi Bank.

Data for January 1, 2024

No.	Bank's name	Controlling stakeholder	Bank assets as of January 1, 2024 (billion tenge)
1	Halyk Savings Bank of Kazakhstan	Holding Group ALMEX JSC	14943
2	Kaspi Bank	Kaspi Group JSC	6689
3	Bank CenterCredit	Bakhytbek Rymbekovich Baiseitov	5261
4	Otbasy bank	National Managing Holding «Baiterek» JSC	3996
5	ForteBank	Bulat Zhamitovich Utemuratov	3444
6	Jusan Bank	First Heartland Securities JSC	2869
7	Eurasian Bank	Eurasian Financial Company JSC	2759
8	Freedom Bank Kazakhstan	Freedom Finance JSC	2211
9	Bereke Bank	National Managing Holding «Baiterek» JSC	2076
10	Bank RBK	KCC Financ LLP	2044
11	Citibank Kazakhstan	Citibank, N.A.	1087
12	Altyn Bank	China CITIC Bank Corporation	889
13	Home Credit Bank Kazakhstan	Home Credit and Finance Bank LLC	803
14	Shinhan Bank Kazakhstan	Shinhan Bank	475
15	Nurbank	JP Finance Group LLP	466
16	Bank of China in Kazakhstan	Bank of China Limited	417
17	Industrial & Commercial Bank of China (Almaty)	Industrial and Commercial Bank of China	349
18	KZI Bank	T.C. Ziraat Bankası A.Ş.	233
19	VTB Bank Kazakhstan	PJSC VTB Bank	226
20	Al Hilal Islamic Bank	Al Hilal Bank PJSC	178
21	Zaman-Bank	Tasbulat Abguzhinov	25

Figure 1. Second-tier banks of the Republic of Kazakhstan as of January 1, 2024

1.1. Second-tier banks in Kazakhstan

All banks in Kazakhstan, except the National Bank, belong to the second level of the banking system, which is why

they are called «second-tier banks». Their activities are regulated by the Law «On Banks and Banking Activities» dated August 31, 1995 No. 2443. In accordance with this law, a second—tier bank in Kazakhstan is a legal entity engaged in commercial activities, the main purpose of which is to make a profit, regardless of the form of ownership. Such banks have the right to open subsidiary banks, branches and representative offices both in Kazakhstan and abroad. The activities of second-tier banks are regulated by the Constitution, laws of the Republic of Kazakhstan and regulations of the National Bank of the Republic of Kazakhstan.

The development of the banking sector has led to a significant increase in the volume of customer data, which has brought to the fore issues of reliable protection of information and users. There are often situations when both internal and external systems are subjected to unauthorized access attempts to obtain confidential customer data or disrupt the work of the organization.

As shown in Table 1, data protection in banks and other organizations plays a key role not only in ensuring information security, but also in maintaining financial stability, reputation and customer trust.

Table 1. The importance of data protection in banks and organizations: key aspects and characteristics

Reason	**Characteristic**	**Consequences in the absence of protection**	**Examples**
Confidentiality	Protection of personal data of clients	Data leakage, penalties for non-compliance with the law	Leakage of the bank's customer database
Financial stability	Protection against theft and unauthorized transactions	Financial losses, reputational risks	Fraudulent transfers
Reputation and customer trust	Customers' confidence in the safety of their information	Loss of customer trust, customer churn	Cyber-attack on the bank, leading to the refusal of customers from services
Compliance with legislation	Compliance with the requirements of standards and regulations	Fines, court proceedings	Non-compliance with GDPR or PCI DSS
Business continuity	Ensuring data availability and integrity	Disruptions in operation, disruption of business processes	A ransomware type attack blocking bank operations
Intellectual property protection	Preventing internal data leaks	Competitors get access to important information	Theft of commercial secret documents
Risk management	Minimizing the likelihood and consequences of cyber attacks	Increasing business risks	Insufficient network segmentation that simplifies attacks
Social responsibility	Customer and employee safety	Large-scale data leaks can affect thousands of users	Leaked credit card numbers and passport data

Modern banking is associated with the active use of online banking, mobile applications and cloud technologies. These tools provide customers with convenient access to financial services, simplify account management and reduce transaction time. However, their use also creates new challenges in the field of information security.

Key threats include:

– Phishing aimed at obtaining customer credentials.

– DDoS attacks that can disrupt the availability of services.

– Attacks on APIs that can be used to steal data or spoof operations.

To minimize these risks, banks should implement advanced security measures such as multi-factor authentication systems, modern antivirus solutions and tools for analyzing anomalies in traffic.

1.2 Information security audit: key aspects and stages

An information security audit is an independent assessment of the security of the information system of a bank or other company using modern technologies. It is conducted according to established criteria that allow you to quickly identify weaknesses in the system and comprehensively assess its effectiveness. It is important to note that the audit is carried out not only in case of incidents such as a data leak or a system malfunction. As shown in Figure 2, the official regulatory document on the information security requirements of banks in Kazakhstan:

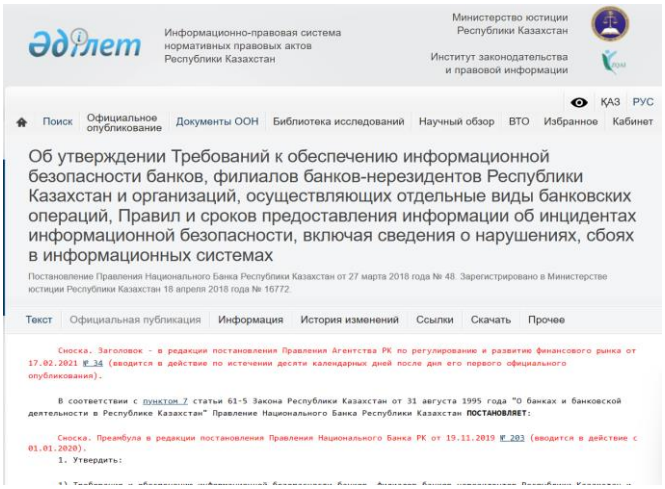

Figure 2. Requirements for ensuring information security of banks, branches of non-resident banks of the Republic of Kazakhstan

An audit is often ordered in the following situations:

– Carrying out reorganization in a credit and financial organization.

– Merging of various branches.

– Replacement of the management staff.

– Changes in legislation and other reasons.

The main objectives of the audit are:

– Analysis of external and internal threats to the information system (IS).

– Assessment of the level of IP security at the time of the audit.

– Search for vulnerabilities and problem areas.

– Formulation of recommendations for improving security measures.

– Information security audit includes comprehensive verification:

– The degree of protection of customer data.

– Compliance with bank secrecy.

– Reliability of financial transactions, especially in conditions of possible interference.

Types of audit:

– External audit — conducted by independent experts on the initiative of the bank's management or law enforcement agencies.

– Internal audit is a regular monitoring of information systems, which is carried out by the bank's employees according to established schedules and rules.

Stages of the audit:

– Defining the responsibilities of the auditors and coordinating the plan with the customer.

– Data collection, including information about the company's structure, security measures and the functioning of the system.

– Comprehensive or partial analysis.

– Assessment of the collected information and identification of problem areas.

– Development of recommendations and writing of the final report.

2. Materials and methods

2.1. Information security standards and requirements in the banking industry

An audit may also include checking the physical and electronic infrastructure, assessing the security of data with limited access, and identifying possible information leakage channels.

2.1.1. Risk management

Information security in the banking industry is strictly regulated by both international and national standards, regulations and laws that establish minimum requirements and basic principles for the protection of data, systems and transactions. Meeting these requirements not only helps to protect information and reduce risks, but also ensures compliance with legal obligations, which is especially important for financial institutions such as second-tier banks.

As shown in Figure 3, in the folder I have collected all the information security policies of banks and their certificates of compliance with information security standards:

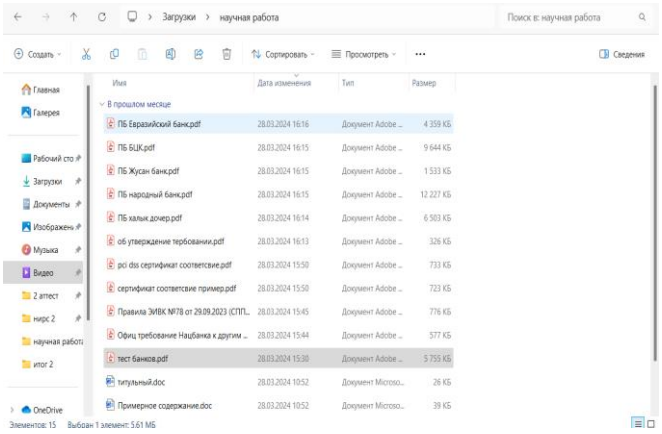

Figure 3. Documents of information security and certification banks

International standards in the field of information security are designed to establish uniform rules for data protection management for organizations in various industries, including banks. The main international standards include:

ISO/IEC 27001: one of the most common standards for information security management. It sets requirements for the creation, implementation, maintenance and improvement of information security management systems (ISMS) in organizations. Compliance with this standard helps to ensure a comprehensive approach to data protection, including risk management, monitoring and auditing.

ISO/IEC 27002: This is a guide for the practical application of safety measures, complementing ISO/IEC 27001. It provides recommendations on aspects such as asset management, access control, cryptographic protection and physical security.

PCI DSS (Payment Card Industry Data Security Standard): a standard aimed at ensuring the security of payment card data. It is mandatory for organizations working with payment cards, including banks, and includes requirements for card data protection, transaction monitoring and auditing, and vulnerability management.

2.2. Banking security: standards and requirements

NIST Cybersecurity Framework: Developed by the US National Institute of Standards and Technology (NIST) and contains recommendations on cybersecurity management. Important elements include detection, protection, monitoring, incident response and recovery.

In addition to international standards, second-tier banks are also required to comply with national requirements, which vary from country to country. As a rule, they are set by central banks, financial regulators or government agencies and include:

– Data protection legislation: In many countries, there are laws that require the protection of personal data of customers. For example, the EU has a General Data Protection Regulation (GDPR), which sets strict requirements for the processing and storage of personal data. Other countries may have similar laws requiring banks to protect customer data and report security breaches.

– Requirements of central banks and regulators: Central banks often impose their own requirements on the information security of financial institutions, including mandatory audits, cyber incident reports, risk management and data protection.

– Cybersecurity legislation: In some countries, there are special laws governing cybersecurity in the financial sector. They may include the mandatory use of security technologies, regular penetration tests and rapid response to cyber threats.

– In addition to international and national standards, second-tier banks can follow industry recommendations that help implement best practices in the field of information security:

– Basel Standards on Risk Management: The Basel Committee on Banking Supervision develops recommendations on the management of operational and cyber risks for banks. These standards cover data protection, business continuity, and information risk management.

– COBIT: an IT management methodology that provides tools and standards for effective management and protection of information systems. COBIT helps organizations align IT processes with business goals and ensure a high level of security.

– CIS Controls: A set of 20 key actions that organizations must take to protect their systems. These measures include asset inventory, account management, and incident response.

In order to comply with regulatory requirements, it is necessary to constantly monitor and audit information security, including:

– Regular security audits: Independent audits help identify security gaps, assess vulnerabilities, and propose solutions to address them.

– Monitoring compliance with standards: monitoring the implementation of all mandatory procedures and requirements established by standards and regulations.

– Reporting and Incident response: It is important to respond to security incidents in a timely manner and provide reports to regulators on any serious cyber-attacks or violations.

In the Republic of Kazakhstan, information security issues in the financial sector are regulated by a number of legislative acts aimed at protecting data and banking systems:

– The Law of the Republic of Kazakhstan «On Communications»: regulates the protection of information transmitted over communication networks and obliges telecom operators to ensure its security.

– The Law of the Republic of Kazakhstan «On Informatization»: establishes rules for the protection of public and private information systems, including banking structures.

– The Law of the Republic of Kazakhstan «On Personal Data and their Protection»: regulates the collection, storage and protection of personal data, obliging banks to comply with the requirements for the protection of customer information.

The National Bank of the Republic of Kazakhstan puts forward its requirements for banks, including:

– Resolution on requirements for information systems of second-tier banks.

– Methodological recommendations on risk management and cybersecurity.

Kazakhstan also has an Integrated Information Security System (CSIS), which establishes the classification of information systems by security levels and requirements for cryptographic data protection. Banking systems often meet these requirements to provide a high level of protection.

Internal and external audits are key elements to ensure that the bank is in order and everything works as expected. But each of these types of audit has its own tasks and approaches.

2.3. Information security assessment and audit: standards and practices

Internal audit is like an internal audit. The bank's audit team analyzes documents, risk management processes and compliance with internal rules and legislation. In fact, they check how effectively the bank and its internal systems are functioning.

This audit is important in order to monitor the bank's operations, ensure compliance with internal standards and legislation, as well as for risk management. Internal auditors assess how well the bank is protected from possible threats and suggest ways to improve control mechanisms. This helps to prevent possible fraud and abuse.

This task is performed by the internal audit service. She is independent from the day-to-day operations of the bank, which allows her to objectively evaluate the work of the organization. The results of the inspections are transmitted only to the management and the board of directors so that they can take measures to improve.

The internal audit process begins with planning: auditors decide what to pay attention to. Documents, financial statements, and processes are then reviewed to identify problems and suggest improvements. As a result, a report with recommendations is compiled, after which the auditors monitor how their advice is implemented and how effective they are.

As a result, internal audit helps the bank to work more efficiently, manage risks and avoid fraud. This allows you to identify and correct errors in advance that may affect the operation of the bank.

An external audit is an audit of a bank by a third–party audit company. Independent auditors assess how reliable the bank's financial statements are and whether they comply with legal requirements. This audit is conducted for external stakeholders: investors, customers and regulators.

The main task of the external audit is to confirm that the bank's financial statements are honest and transparent, and the bank itself manages risks and complies with all requirements. Auditors analyze financial data, check documents and procedures to identify possible problems.

Independent audit firms such as KPMG, Deloitte or PwC conduct external audits. These companies must have the appropriate licenses and experience working with financial institutions in order for their reports to be recognized by regulators and investors.

In the process of external audit, the audit company agrees with the bank on the list of documents and processes to be checked, analyzes accounting data, checks sample transactions and, based on the results, draws up a report evaluating the bank's performance.

As part of the study, event logs obtained from various sources of the bank's infrastructure were examined and analyzed in order to identify malicious activity and security incidents. In particular, the integration of ElasticSearch with other SIEM tools was used, as shown in Figure 4, which made it possible to centrally collect and analyze data. Logs, including logs of servers, routers, and security systems, have been carefully checked for anomalies, signs of unauthorized access, and other signs of possible threats, such as vulnerability attempts, DDoS attacks, or malicious activity related to internal or external threats. This process made it possible to effectively identify security incidents and respond to them in real time, increasing the overall protection of the bank's information systems.

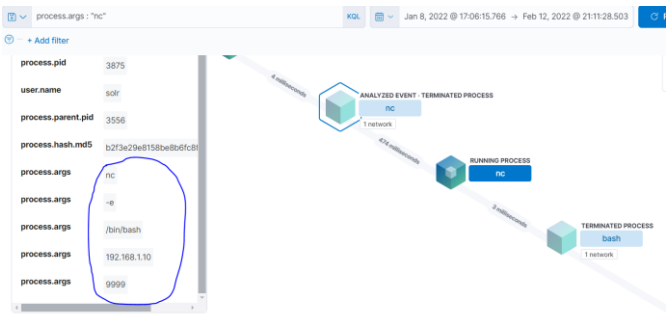

Figure 4. Analysis of logs and process tree using ElasticSearch to detect malicious activity

An external audit is necessary so that outside observers, such as investors or regulators, can trust the bank. He confirms that the bank conducts its activities transparently and complies with financial standards.

Internal audit helps the bank to improve its work from the inside, identifying problems and offering solutions. An external audit confirms that all financial statements are honest and comply with regulatory requirements. The internal audit is carried out by the bank's employees, the external audit is carried out by independent companies. An internal audit can

be an ongoing process, while an external one is conducted once a year for reporting purposes.

When conducting an information security audit in accordance with international and Kazakhstani standards, the process included several key stages covering both documentation and practical aspects of security. The first step was to thoroughly analyze all the information security documentation that exists in the organization. The relevance of internal security policies and regulations was checked, their compliance with standards such as ISO/IEC 27001, as well as harmonized Kazakhstani standards (for example, the requirements of Kazakhstan's Cyber Shield). Special attention was paid to documenting risk management processes, incident response planning, and data backup and recovery policies. It was verified that these documents fully reflect the real situation, and do not exist only on paper, and comply with both internal regulations and external regulations, including the legislative requirements of Kazakhstan.

As shown in Figure 5, the entire organization was audited and all the necessary fields were filled in to evaluate the MSAT security information.

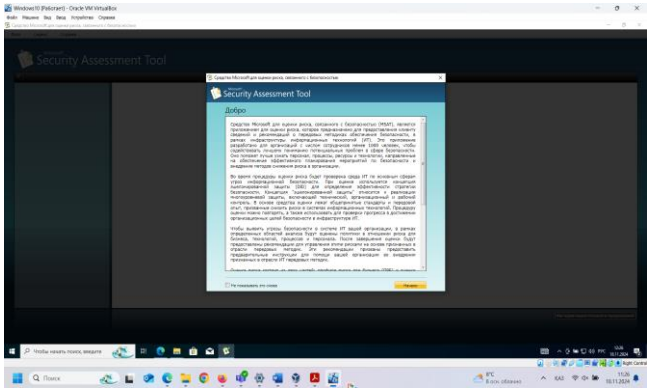

Figure 5. Studying the Microsoft Security Assessment Tool (MSAT)

After analyzing the documentation, the user's access rights to information systems and data were checked. This was an important stage aimed at minimizing risks by limiting access to critical resources. The current structure of access rights was evaluated, it was analyzed which employees had access to various systems, and it was checked whether this access corresponded to their functional responsibilities. The principle of minimum necessary access was applied to ensure that users receive only those rights that are necessary to perform work tasks. Access to critical systems such as servers, databases, and confidential documents was limited and strictly regulated. The processes of auditing user actions were checked, including accounting for attempts to change data, access to confidential information and any changes in access rights.

The analysis of the organization's network settings and infrastructure included checking the configuration of firewalls, routing settings, and the use of secure communication channels such as VPNs to access internal resources. Attention was paid to data transmission: it was analyzed whether they are encrypted during transmission over the network, and how reliable the encryption algorithms used are. The use of up-to-date and secure protocols for data transmission, such as TLS 1.2 and higher, was checked in order to exclude the transmission of confidential information through unsafe channels.

Vulnerability testing included analyzing the configuration of servers, databases, and other critical systems for configuration errors that could lead to vulnerabilities. Both manual analysis methods and automated tools (for example, vulnerability scanners) were used, which made it possible to identify potential entry points for attackers and suggest ways to eliminate them.

Data protection during storage and backup was evaluated. It analyzed how data encryption on disks is organized, how reliable the security methods used are, as well as data backup and recovery procedures. It was checked how regularly backups are performed, where they are stored and how quickly they can be restored if necessary. Special attention was paid to controlling access to backups.

3. Results and discussion

3.1. Quality Assurance

Incident management and response procedures were evaluated in terms of their compliance with standards and best practices. The effectiveness of actions in case of data leakage, attacks on infrastructure or other incidents was checked. The efficiency of identifying and eliminating incidents was analyzed, as well as reporting on each case.

The audit made it possible to identify current weaknesses in the organization's security system, assess compliance with international and national standards and offer specific recommendations for improving protection.

A detailed report was compiled indicating the vulnerabilities found, problem areas and recommendations for their elimination. Vulnerabilities related to incorrect configuration of servers and network equipment have been identified in the network of second-tier banks. This included outdated software versions vulnerable to known exploits, and misconfigured firewalls. Insufficient network segmentation allowed intruders to quickly spread through the bank's internal network.

3.2. The process of auditing information security in banks

To eliminate these problems, it was proposed to upgrade all critical systems to the latest versions with installed security patches, optimize network configuration, implement stricter firewall rules and network segmentation to isolate critical resources.

Access control was assessed considering the risk of insider threats. Cases of excessive user rights were identified, which increased the likelihood of data leaks and errors. The application of the principle of minimum necessary access has made it possible to limit access to critical resources.

The analysis showed that data encryption was either not used during storage and transmission, or outdated algorithms were used. It is recommended to implement modern encryption protocols, such as TLS 1.3, and ensure complete encryption of confidential information.

The bank's web applications turned out to be vulnerable to SQL injections and XSS attacks. The conducted penetration testing revealed insufficient filtering of the input data. Strict validation and filtering mechanisms are proposed to enhance protection.

The incident management system has shown poor preparedness to respond to cyber-attacks. It is recommended to develop a detailed incident response plan and implement monitoring systems for rapid threat detection.

As a result of the analysis and elimination of vulnerabilities, the second-tier bank's network has become significantly more secure from possible cyber-attacks, the risks of data leaks and unauthorized access to critical systems have been minimized.

3.3. Recommendations for strengthening the bank's security

The developed methodology for identifying and eliminating vulnerabilities structured the security audit process, minimizing risks at all levels of the bank's information system.

It is important to take into account several aspects related to information security in the context of the layout of the bank building. First of all, you should pay attention to the placement of server and data warehouses. These premises should be isolated and equipped with a security system, and access to them should be restricted only to authorized employees. It is also important to consider the risks associated with unauthorized access through the physical environment. Areas with increased risks, such as archives with confidential data or workplaces where sensitive information is processed, should be under additional control. Office workplaces and open access areas should also be designed in such a way as to minimize the likelihood of data privacy violations. In addition, it is necessary to ensure the availability of video surveillance, access control and alarm systems that integrate with the bank's information systems and the protection system against physical threats such as fire or intrusion. It is also important to take care of protecting communication channels, such as telephone and network connections, from eavesdropping and interference with transmitted data. In the case of remote work, it is necessary to provide secure data transmission channels and the possibility of centralized control. The bank's offices should be properly allocated jobs, taking into account the principle of minimizing the visibility of confidential information, especially if the area is open to visits by customers or other third parties. Thus, the design and layout of the bank's space should take into account various aspects of information security, including physical protection, data protection and monitoring systems, which significantly reduces the risks of information leaks and other threats.

As shown in Figure 6, a plan of the bank's office premises is presented, which can be used to assess potential risks associated with information security.

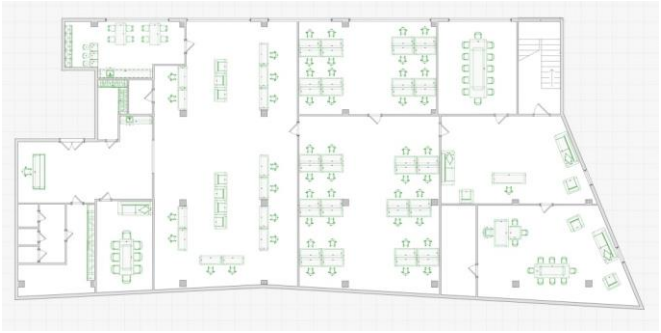

Figure 6. Layout of the bank's office premises taking into account information security risks

The main stages of the methodology:

1. At the preliminary analysis stage, data was collected on the existing infrastructure, current security measures, network hardware and software configuration. To do this, interviews with technical specialists were conducted, network diagrams and server configurations were analyzed, access rights management processes and security policies were documented.

2. Penetration testing included checking systems for vulnerabilities using tools such as Burp Suite and Metasploit. SQL injections, XSS and configuration errors were identified. For example, testing has shown that some servers and web applications are susceptible to attacks on input data.

3. The analysis of access rights was aimed at verifying the correctness of the distribution of rights and their compliance with the duties of employees. The role model of access, accounts with elevated privileges and user actions were studied. The effectiveness of data encryption during transmission and storage was also evaluated. An analysis of network devices and the protocols used revealed the use of outdated protocols, which led to the recommendation of switching to TLS 1.3.

4. At the stage of analyzing the incident response policy, existing cyberattack action plans were studied, incident response regulations and monitoring systems were checked.

Based on the results of the audit, recommendations were developed. All critical systems have been updated to the latest versions to eliminate known vulnerabilities. The roles and rights of users have been revised, the principle of minimum necessary access has been introduced, and control over the actions of users with elevated privileges has been strengthened. The internal network has been segmented to limit access to critical resources. Encryption of confidential data using TLS 1 is provided.3. Security policies have also been improved and monitoring tools have been introduced.

The final report included a detailed description of the identified vulnerabilities, proposed solutions and recommendations for improving the security system. The audit strengthened data and infrastructure protection, brought processes and documentation in line with international and national standards, and provided the bank with methodologies for future audits and improvements.

3.4. Analysis Results

As part of the study devoted to the analysis of vulnerabilities in the network of second-tier banks of the Republic of Kazakhstan and the development of a methodology for their identification and elimination, extensive work has been done covering all stages of studying, testing and implementing solutions to improve information security.

First of all, an analysis of the current state of information security in second-tier banks was carried out. This included a study of their network infrastructure, software components, and technologies used. The main types of vulnerabilities that are most often found in banking systems have been identified, such as insufficiently protected web applications, errors in server configuration, the use of outdated software versions and insufficient protection of data transmission channels.

In the process, vulnerabilities specific to the banking sector were checked, including threats related to phishing, SQL injections, cross-site scripting (XSS), denial of service attacks (DDoS), as well as brute force for password selection. Special attention was paid to the analysis of internal security, including access control, account and privilege management, as well as monitoring user activity.

At the next stage, the systems were audited using both automated and manual methods. Automated tools such as Nessus

and Acunetix were used to quickly scan and identify known vulnerabilities, while manual penetration testing helped to detect more complex flaws that could have gone unnoticed. These methods allowed not only to identify critical vulnerabilities, but also to understand how they can be exploited.

In addition, many hidden vulnerabilities have been discovered related to incorrect system configuration or lack of regular software updates. Problems with an insufficient level of data encryption were also identified, which posed a threat of interception and unauthorized access.

A methodology has been developed that includes a step-by-step process for assessing, identifying and eliminating vulnerabilities. It is based on the principles of threat modeling, such as STRIDE and DREAD, which allowed not only to assess current risks, but also to prioritize them according to the degree of criticality. The methodology also provided for regular security audits, which helps to maintain a high level of protection in the long term.

To verify the proposed solutions, tests were conducted in conditions as close as possible to real ones. Attack simulations were used to test the stability of banking systems to various types of threats. These tests confirmed that the proposed methods can significantly reduce the likelihood of a successful attack.

In addition, the study made it possible to make a number of discoveries in the field of improving the effectiveness of protection of banking networks. For example, it has been found that using a multi-layered approach that combines monitoring, analysis and intrusion prevention tools provides a higher level of security. It is also confirmed that regular updating and testing of systems plays a key role in preventing threats.

As a result, the developed methodologies and recommendations made it possible to improve the security of second-tier banks, minimize risks and increase the resilience of their systems to modern cyber-attacks. The work has contributed to the development of strategies for protecting financial structures, and its results can be used to further improve information security in the banking sector.

Acknowledgements

Author would like to express my sincere and deep gratitude to Alimseitova Zhuldyz Keneskhanovna, Associate Professor at K. Satpayev Kazakh National Research Technical University, for her invaluable guidance and comprehensive support at all stages of this research. Her professionalism, valuable recommendations and meaningful feedback had a key impact on the successful completion of the work.

Author would like to express my special gratitude to KazNTU named after K. Satpayev in Almaty, Kazakhstan, for the resources, infrastructure and equipment provided that made the implementation of this project possible.

Author would like to note separately that this study was conducted without attracting special grants or financial support from government, commercial or non-profit organizations.

References

[1] ISO/IEC 27001:2022. Information Security Management Systems – Requirements. *International Organization for Standardization*

[2] Gosudarstvennye standarty Respubliki Kazahstan: Obshhie trebovanija k zashhite informacii. (2021). *Astana*

[3] Ministerstvo cifrovogo razvitija, innovacij i ajerokos-micheskoj promyshlennosti Respubliki Kazahstan. (2021). Kibershhit Kazahstana: osnovnye polozhenija i trebovanija. *Astana*

[4] Martynov, P.A. (2022). Audit informacionnyh sistem: instrumenty i metody. *Moskva: Izdatel'stvo Piter*

[5] Kiselev, S.A. (2020). Informacionnaja bezopasnost': metodologija i praktika. *Moskva: Infra-M*

[6] Gorbunov, V.V. (2021). Upravlenie riskami informacion-noj bezopasnosti v finansovyh strukturah. *Moskva: Al'-pina Pablisher*

[7] Ministerstvo cifrovogo razvitija Kazahstana. (2024). Kibershhit Kazahstana. *Retrieved from:* https://digital.gov.kz/ru/articles/cybershield

[8] Nacional'nye standarty Respubliki Kazahstan v oblasti informacionnoj bezopasnosti. (2024). *Retrieved from:* http://gosstandart.kz/documents/standarts2021.pdf

[9] NIST SP 800-53 Revision 5. (2020). Security and Privacy Controls for Information Systems and Organizations. *National Institute of Standards and Technology*

[10] Sidorov, A.V. (2022). Informacionnaja bezopasnost' v bankovskoj sfere. *Moskva: Finansy i Kredit*

Екінші деңгейдегі банктер желісіндегі осалдықтарды талдау және оларды анықтау және жою әдістемесін әзірлеу

Р. Құланбаев*

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: kulanbaev.ramazan@gmail.com*

Аңдатпа. Бұл есепте екінші деңгейдегі банктердің ақпараттық жүйелерінің осалдықтары талданады, оларды қорғаудың әлсіз жақтарын анықтауға және жоюға баса назар аударылады. Негізгі назар қолданыстағы қауіпсіздік жүйелерінің аудитіне және банк мекемелерінің жұмысына әсер ететін негізгі қауіптерге аударылады. Анықталған осалдықтарды жою әдістемесі, сондай-ақ ақпараттық жүйелердің кибершабуылдарға төзімділігін арттыруға бағытталған қауіпсіздік процедуралары мен ұйымдастырушылық шараларды жетілдіру бойынша ұсыныстар берілген.

Негізгі сөздер: *ақпараттық қауіпсіздік, банк жүйелері, аудит, осалдықтар, киберқауіптер, қорғау әдістері, қауіпсіздік жүйелері, ұйымдастырушылық шаралар.*

Анализ уязвимостей в сети банков второго уровня и разработка методологии их выявления и устранения

Р. Куланбаев*

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: kulanbaev.ramazan@gmail.com*

Аннотация. В данном отчете анализируются уязвимости информационных систем банков второго уровня с акцентом на выявление и устранение слабых мест в их защите. Основное внимание уделено аудиту существующих систем безопасности и ключевым угрозам, влияющим на работу банковских учреждений. Представлена методология устранения выявленных уязвимостей, а также рекомендации по совершенствованию процедур обеспечения безопасности и организационных мер, направленных на повышение устойчивости информационных систем к кибератакам.

Ключевые слова: *информационная безопасность, банковские системы, аудит, уязвимости, киберугрозы, методы защиты, системы безопасности, организационные меры*.

Received: 19 January 2024
Accepted: 15 June 2024
Available online: 30 June 2024