CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
http://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 03 Issue: 02 | Feb 2022 ISSN: 2660-5309

Information Security in the Financial and Banking System of the Republic of Uzbekistan

Bekbaev Gamzatdin Aleuatdinovich
Associate Professor of the Department of Social, Humanitarian and Exact Sciences, Tashkent State University of Economics

Yalgasheva Shirinkhol Usarovna
Department of Social, Humanitarian and Exact Sciences, Tashkent State University of Economics

Annotation:
This article examines the main provisions and essence of information security of the banking system of the Republic of Uzbekistan. Management of the information security system is an integral part of the management of any organization, regardless of its scope, size, etc. The paper describes the main stages of the creation of an information security system, examines the main approaches to building an information security system and the conduct of an effective information policy that specifies the specific features and differences of the information banking system from the information systems of other organizations, based on the requirements of the latest domestic Bank of Uzbekistan Standard for ensuring information security of organizations of the banking system of the Republic of Uzbekistan

ARTICLEINFO

Article history:
Received 26 jan 2022
Revised form 28 Jan 2022
Accepted 2 Feb 2022

Key words: Information Security, Bank of Uzbekistan, Banking System.

At the current stage of information technology development, it is becoming clear that for the development of reliable information technologies, banking services products and services exists necessity in providing appropriate level their information system safety. The development of the global economic space expands the opportunities for banking activities. at the current stage of economic development, the banking system plays a key role in the functioning of economic systems. institutions and in the life of every person, which means that it is subject to an increased risk of information security. The problem of studying and effective management of information security in the banking system has become particularly important sharpness in modern ones terms and conditions, what explained by next reasons for [1]:

- cutting height scale up development email address infrastructure bank card number the system;
- significant increase impacts intensive developing company email address infrastructure bank card number the system on all sides economic life activities in as a result use cases electronic devices payment systems systems;

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

- structural features changes, ongoing events in bank card number system, associated with fast development financial services organizations with new ones appearing banking services products and services, by globalization financial services markets and etc.

To ensure information security, you should accurately assess the risks and introduce the necessary systems security features. Provision information system safety in banks — this system level process, requiring developments a set of measures that will be aimed at reducing losses to a minimum level and that will reduce probability of occurrence of the risk in the future.[2] Expanding the range and increasing the volume of banking services requires the availability of common approaches, common terminology and common criteria for assessing the state of information security of banks in the Russian Federation. at the level of national standards – only in these conditions is it possible to ensure the necessary level of sustainability bank card number the system.

Factors, which should be considered by providing information system safety banks:

1. The information stored and processed in banks is real money. In case of unsafe access to this one for more information threats information system safety submit essential danger: through tools computing power technicians can open up loans, produced by different payouts, but also get translated significant amounts of money without of your knowledge owner's name this account. Obviously, what is illegal manipulation? with information will result in to losses varying degrees.
2. If information related to the banking sector concerns a large number of people and organizations, then there is clients banks. Bank must to provide acceptable level information system safety, what is priority its task is activities.
3. It depends on how convenient it is for the client to work with the bank, as well as on the wide range of services provided to them the bank's competitiveness directly depends on it. That is why the bank should provide the opportunity to quickly and efficiently hassle-free orders in cash by other means. However similar ease of use access points to in cash assets and increases the number of intruders, which show interest to bank account systems.
4. The Bank is obliged to ensure high reliability of its information systems. systems even in in case of an incident information security, because the bank, unlike most companies, is responsible not only for its own funds tools, but and behind your own money clients.
5. The bank stores important information about its customers, which expands the range of potential intruders, interested parties in theft or worse such information. In goals security features interests from threats, related products with information system security of the banking system of the Republic of Uzbekistan, domestic standards for information security of the banking system of the Republic of Uzbekistan were created. safety.

The main one by document is standard Pot Of Uzbekistan "Software information system safety organizations bank card number the system Of the Republic of Uzbekistan. Common provisions", where scheduled events requirements international organizations standards in the field of information system safety based on features modern bank card number the system Uzbekistan.

The logic of the standard consists in describing the following stages of creating an information security system: safety (figure 1).

1. Forming policies information system safety - preparation documents and standards, defining features purposes, tasks and requirements policies information system safety, formulation on their to the database the main ones provisions, regulations, instructions for each one regions activities pot (questions management an antivirus program security features, provision information security on stages life cycle of the cycle ABS).

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

2. Defining the scope of the information security management system - it should be identified system boundaries, for which you should use to be secured mode information system security based on the organization's structure, information resources, and automated systems, and as well as data processing technologies and application software. Based on the results of this stage, the following documents should be drawn up: instructions, reflective elements the borders the system, list resources information system the system, subjects protection.
3. Evaluation and processing risks information system safety – task evaluations risks consists of in definition indicators risks information system the system and her resources (drawing 2). By total evaluations risks compiled by documents, describing parameters threats safety, vulnerabilities and possible ones results negative content impacts; becomes possible choose tools, providing services desired one level information system safety organizations.

Management information system by security - generated by comprehensive system security features information system safety, including in myself standards and requirements to functioning services information security, detection and response to system vulnerabilities [4]. Information Management by security – very important ones problems in bank card number the system. Bank card system subject to various risks and uncertainties and is a very complex structure. In such an atmosphere, it is very difficult to initiate the system assessments and simulations the main ones risks.

Monitoring the achievement of information security policy goals – the process of verifying compliance installed ones requirements by providing information system safety by to other funds audit results information system safety, conducting an event self-assessments and analysis functioning the system security features information system security, decision-making on tactical and strategic improvements to the information security system. safety.

Information availability indicates whether information users can exercise their access rights. Integrity data source shows their immutability by when executing operations with with them, be that broadcast, usage or storage for more information [3]. Privacy Policy for more information presents by yourself prohibition on her disclosure unauthorized persons without the prior consent of the parties. Information security affects stability resources and the quality of services provided. In the modern banking business, it is the quality of services that is one of the most important factors. the main ones factors success. Low quality, in volume including by the reason unsatisfactory security features It is a source of operational, financial and reputational risks for the bank. Digital interaction between by the user bank accounts services and financial by an organization must to be safe, comfortable and accessible by the price.

The task of implementing an information security process in an organization must meet the following requirements: level her organizational level and technological equipment development. Provision privacy policy, integrity issues and availability for more information may with with confidence assign it to to necessary conditions continuities a business. Requirements to improving the system and implementations measures by providing information system safety formulated by on based on definitions level maturity levels these processes in organizations. For implementations policies information system safety process groups in the form of a cyclic Deming model are used to maintain it at the appropriate level: «.. – planning-implementation – validation-improvement-planning -..", which is the basis of the model management system standards characteristics gost R ISO 9001 and Information Security System ISO/IEC IS 27001-2005. Model maturity levels processes management information security of the organization in this standard is based on the maturity model defined by by standard Cobit 5, where the following are entered maturity levels processes [5]:

Level zero - incomplete process - this process has not yet been implemented or is not capable of at least partially correspond to its purpose, there are no processes within the organization's activities information security management. The problem of ensuring information security is considered managing it organizations

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

how exclusively technical information. Separate services information system safety no. Organizational matters measures to maintain the necessary security level missing items.

First level - completed process - the process is implemented and meets its intended purpose, but available ones processes security features and management information system by security not they are standardized. Importance ensuring information security by an organization is understood and considered as an interconnected complex organizational issues and technical services measures.

Second level - managed process - implemented process of the previous - first one - level up now managed (i.e. planned, tracked, and adjusted). The company's management approved the concept and information security policy, protection plan, and other regulatory and methodological materials and job descriptions instructions.

The third level is an established process-a managed process that able to bring expected results results, characterized by that, what processes standardized, documented and completed before staff members through training. Methods of information security risk analysis that meet the basic level of information security risk analysis have been developed. level security features information system the system. Defined structure and structure services information system safety.

Fourth level-Predictable process-the established process now gets results in the following conditions: specified values restrictions, processes management information system by security are located in stages continuous improvements and are based on good practice. At this level, actions are aimed at development and improvement methods detections and response time on attacks. Also must prevention methods should be implemented.

Fifth level-optimized process-security measures are used in an organization in a comprehensive manner, creating and maintaining a stable environment. providing. The organization can to fast adaptations by changes in the environment and business.

In foreign practice, in contrast to Uzbek, the use of the maturity model for process management ensuring information security is widespread. An example of this is a series of standards ISO27000, which regulates information security management issues. Obviously, before the organization, implementing company activity by management information system by security, early or It's late gets up question about volume, how meet these requirements, to what extent and at what level of detail, etc. These and other questions can be answered by to help model maturity levels, on based on which one will be held estimation maturity level processes.

List used by literatures:

1. Johan Balillon. Current trends in regions information system safety banks // Banking. 2014. № 10. pp. 60-63.
2. Mardanov R. H., Ilyin I. V. Standards information system safety in bank card number the system // Vestnik Ufa Region state-owned enterprise aviation technical university. 2013. Vol. 17. № 7. P. 55-60.
3. Pushchilin V. Evolution IT systems — influence to a bank account business // Bank accounts technologies. 2015. № 4.
4. Revenkov P. V. Management risk management in terms of electronic banking services. M.: ID NUMBER "Economic newspaper", 2011.
5. Serdyuk V. Role standards Pot Of Uzbekistan in providing information system safety credit and financial institutions organizations // Accounting and banks. 2008. № 3.

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/