UDC 004:336.71
DOI: 10.15587/2312-8372.2018.134981

Baglai R.

RESEARCH OF DEPLOYMENT MODELS OF CLOUD TECHNOLOGIES FOR BANKING INFORMATION SYSTEMS

Об'єктом дослідження є банківські інформаційні технології (надалі ІТ). Одним з найбільш проблемних місць є низька ефективність використання апаратних ресурсів та як наслідок високі витрати часу та бюджету на підтримку та розвиток банківських інформаційних систем (надалі ІС). Застосування хмарних технологій, особливо за умови використання моделі розгортання Public Cloud, дозволяє значно підвищити економічну ефективність банківських ІТ. Крім цього, підвищується відмовостійкість, гнучкість та масштабованість банківських ІТ, а також показник швидкості виводу продуктів на ринок (від англ. time to market). В ході дослідження використовувалися кількісні та якісні показники функціонування банківських ІС.

Проведено аналіз сучасних підходів до побудови сервісно-орієнтованої архітектури банківських ІС на основі хмарних технологій. Приведено опис архітектурного рішення ІТ з впровадження автоматизованих банківських ІС з урахуванням вимог Національного Банку України та Європейських регуляторів. Проаналізовано основні банківські ІС та доцільність застосування до них різних моделей розгортання хмарних технологій.

Отриманий результат в кількісному вираженні показників навантаження на систему дозволяє знайти додаткові резерви для оптимізації часу обробки інформації і підвищення економічної ефективності за рахунок застосування Public Cloud. Найбільшого ефекту можливо досягти, застосувавши цю модель до автоматизованого операційного дня банку (від англ. Core Banking System). Для дотримання вимог та урахування обмежень щодо розміщення клієнтських даних в роботі запропонований механізм деперсоналізації.

Завдяки цьому забезпечується можливість отримання найбільш оптимальних значень показників. У порівнянні з аналогічними відомими сервісами, такими як віртуалізація, це забезпечує перевагу, адже немає необхідності придбання чи оренди обладнання, а обчислювана потужність може масштабуватися в значно ширшому діапазоні.

Ключові слова: *архітектура банку, хмарні технології, банківські інформаційні технології, Core Banking System.*

1. Introduction

Due to the peculiarities of the activity, regulatory requirements and construction of business processes, the system universal banks operate with large volumes of data and have integrated information technologies (IT) of the landscape. The use of cloud technologies can significantly improve the effectiveness of IT in general. In addition, the visibility, flexibility and scalability of banking IT, as well as the rate of output of products to the market (from English, time to market, later TTM), are increasing. However, there are significant regulatory restrictions on the movement of data into the clouds. The study will justify the possibility of obtaining these advantages of cloud technologies without violating regulatory requirements.

Therefore, it is relevant to study the Public Cloud deployment model, because this model allows to obtain the best price offers at the cost of the service, because the data center of the vendors are located in regions with a minimum cost of resources.

2. The object of research and its technological audit

The object of research is banking information technologies.

In the context of European integration, Ukrainian system banks should be ready for radical modernization of client, operational and reporting systems. The introduction of European regulatory requirements is a difficult problem for IT services of any Ukrainian bank. The solution lies in the application of the latest IT technologies, in particular, the building of the IT architecture of the bank, based on cloud services.

The main value of the bank is the data. Knowledge of client data imposes a number of regulatory constraints, such as the General Data Protection Regulation (GDPR), etc. This creates legal and operational risks associated with the fact that the bank at any time must to monitor client data and ensure their confidentiality, integrity and accessibility. The author believes that this is the reason for the majority of regulatory restrictions and prohibitions on the transition to cloud technologies in various legal systems.

3. The aim and objectives of research

The aim of research is studying the promising areas of application of cloud technologies at different IT landscape levels of banking IS, to reduce costs and improve the effectiveness of IT support for business processes of the bank.

To achieve this aim, it is necessary to perform the following tasks:

1. To compose high-level architectural scheme of information technology landscape of the bank.

2. To group the systems, determine their functional purpose, analyze the quantitative and qualitative indicators.

ISSN 2226-3780

4. Research of existing solutions of the problem

The problems of using cloud technologies in various socio-economic spheres are studied in [1].

Among the main directions of solving the problem of application of the Public Cloud and Hybrid Cloud deployment models, identified in the resources of the world scientific periodical, publications [2–4] can be singled out. These publications take into account the specifics of securing information that constitutes banking secrecy, but there are no proposals for data depersonalization. In particular, work [5] is devoted to solving the problem of confidentiality of data by encryption, but this imposes significant restrictions on data processing.

The work of other scientists [5–7] does not fully take into account the specifics of IT security provision for banking institutions.

Works [8–10] contain proposals on the use of cloud technologies, but do not contain a comprehensive analysis of the architecture of banking information systems (further IS) based on cloud technologies, taking into account regulatory constraints.

Thus, the results of the analysis allow us to conclude that the introduction of cloud technologies in the IT landscape of Ukrainian banks must meet regulatory requirements. In particular, the regulatory acts of the National Bank of Ukraine [11], the European Central Bank [12], the Basel Committee on Banking Supervision, the Council of Security Standards for payment cards and other institutions. Such features determine the specifics of the IT architecture and the organization of the security system that determines the need to study the mechanisms for ensuring operational efficiency and protection against IT security threats for banks.

5. Methods of research

The following scientific methods are used in research:
– graphical method – when studying IS architectural schemes;
– system classification method – when determining the priority directions of application of different models of cloud technologies deployment;
– quantitative analysis method – when studying non-functional requirements for banking IS;
– synthesis method – when forming a sample of systems that carry the greatest load and are critical for business continuity.

6. Research results

According to the explanation of the National Bank of Ukraine (NBU), the use of cloud technologies in the activities of Ukrainian banking institutions is possible provided that the data is located on servers located on the territory of Ukraine. This corresponds to the Private Cloud deployment model. Let's consider deployment models for On-Premise, Private Cloud, Public Cloud and Hybrid Cloud in more detail.

Public Cloud. According to this deployment model, the cloud service provider, for example, Amazon Web Services (AWS) or Microsoft Azure, has computing resources and supports them, giving customers access via the Internet. Resources are shared and shared among all users. This model is also known as the multi-tenant environment. By saving the scale of the location of data centers in places with a minimum cost of resources, cloud service providers can provide resources at a much lower price than the cost of maintaining their own infrastructure.

Private Cloud. According to this deployment model, the bank creates and maintains a cloud infrastructure in its own data center or leased facilities. The main difference from the Public Cloud is that the bank is the only user who owns and uses the resources of a private cloud. This deployment model is known as a single-tenant environment. Private Cloud does not have such advantages in terms of cost savings as Public Cloud, but it still allows to use the functional advantages of cloud services to improve the efficiency of the business processes of the bank.

Hybrid Cloud. The hybrid deployment model combines cloud technologies of Public and Private Cloud to take advantage of both models. The author believes that such model will allow to secure the data as much as possible while simultaneously acquiring advantages of the economic efficiency of the Public Cloud.

On-Premise is a deployment model in which information assets (data, software, processes) placed on the bank's own physical servers. In this model, the bank carries the maximum costs – capital investment, operating costs for support and utility payments, depreciation. This model provides for the functional benefits of cloud services.

Let's consider the main types of architectural landscapes of banking IS:

Monolithic architecture is a comprehensive IT solution, which includes the front end, an automated banking system, a general ledger, subsystems for setting up banking products, and storing data from one vendor. Usually leads to total dependence on the supplier (from the English Vendor lock in situation), a decrease in flexibility in meeting the needs of the bank and the deterioration of TTM.

Modular architecture is an IT solution based on a large number of software modules from different vendors and internal developers that are integrated among themselves through enterprise data buses, in accordance with the principles of service-oriented architecture. The disadvantage of such architecture is usually the high cost of resources to support and develop a complex integrated IT landscape, which slows TTM. In addition, this creates the need to create and develop internal competence centers that implement changes at the corporate data bus level.

Micro-service architecture is based on micro services that use events that are generated by software applications, including them into processes that support the execution of business logic scenarios by applying standardized mechanisms and API functions. This architecture is the most innovative, because it allows to fully use the potential of cloud technologies, significantly reducing the TTM indicator for banking institutions.

It is proposed to consider a conditional bank, in the architectural landscape of which the second and third types of architecture are combined. In order to determine the quantitative and qualitative parameters that will be taken as a basis for determining functional and non-functional

requirements for banking IS, the following scenario is proposed:

– bank is licensed by the NBU and operates in all client segments of the business – servicing individuals and legal entities, international corporations, the public sector, provides treasury services;
– client base has up to 15 million customers;
– the number of branches is 2 thousand (up to 10 employees working simultaneously on one department at rush hour);
– the number of transactions is 50 million per day, half per hour peak;
– the number of client accounts is 25 million.

The high-level architectural scheme of the IT landscape of the bank (Fig. 1) consists of the following functional blocks of applications:

1. Client IS/public-access hardware/software complexes of public channels).
2. Customer relationship management systems (CRM).
3. Ensuring intersystem interaction, integration layer (Integration layer).
4. Back end systems).
5. Enterprise data management.

Let's consider these blocks in more detail:

1. *Client IS/software and hardware public access complexes* include software applications and hardware for interaction with bank customers, individuals and legal entities. These systems carry a heavy load in terms of the number of users, while simultaneously using the functional (the number of active user sessions). In addition, access from public networks increases the risk of integrity violations due to external attacks. To authenticate the payment transactions, an electronic digital signature (EDS) must be used. The availability of these systems directly results in business continuity, therefore the recovery time of these systems should be minimal.

2. *Customer relationship management systems* include software applications for the input, processing and analysis of client data, carried out by the bank's employees. These systems carry significantly less load, in terms of the number of users and usually do not have interfaces for accessing public networks. EDS must be used to confirm the authenticity of payment transactions. The availability of these systems has less impact on business continuity, therefore Service Level Agreement (SLA) may provide for a longer recovery time than for the systems of the functional unit No. 1 and No. 3.

3. *Ensuring intersystem interaction, the integration layer* includes systems that enable the exchange and transformation of data between applications. These systems bear a heavy load in terms of the number of Online Transaction Processing (OLTP) from integrated systems, often playing the role of transport or data sources for all other systems. In some cases, access from public networks may be provided, increasing the risk of integrity violation due to external attacks. The availability of these systems directly results in business continuity, so the recovery time of these systems should be minimal.

4. *Operating banking systems include* document processing systems for accounting and reporting on bank operations, processing of events generated by the systems of functional blocks No. 1–3 and displaying the result of these events in the bank's balance sheet. Separate systems, in particular the Core Banking System, (CBS), carry a large peak load during Online Analytical Processing (OLAP) to perform scheduled settlement closing processes operational day and the formation of daily reporting. In some cases, access from public networks may be provided, increasing the risk of integrity violation due to external attacks. The availability of these systems greatly influences business continuity, therefore the recovery time of these systems should be close to the minimum.

5. *Data management systems include* Data Warehousing (DWH) and Data Lake and Business Intelligence Tools (BI tools) for analysis, visualization of data for the formation of regulatory and management reporting and decision-making. Access from public networks is not provided. The availability of these systems does not affect the continuity of the business, therefore the recovery SLA may provide for a longer recovery time than for the systems of functional unit No. 1–4. However, it should be noted that these systems are often a source for regulatory reporting, including in accordance with International Financial Reporting Standards, so their inaccessibility for more than a day will affect the timeliness of reporting to the NBU and European regulators.

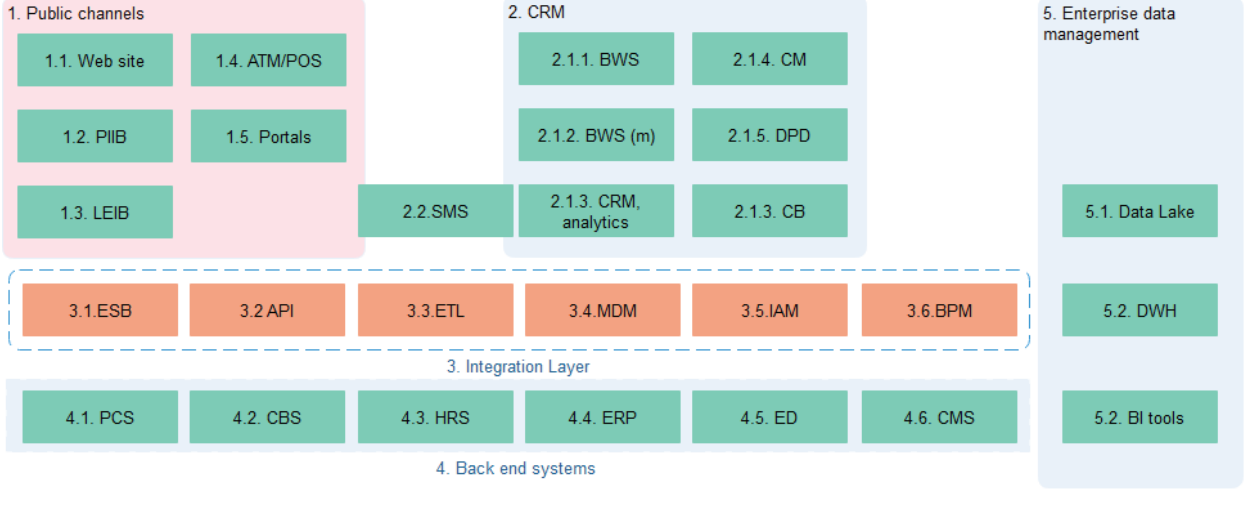

Fig. 1. High-level architectural scheme of information technologies of the bank landscape

ISSN 2226-3780

Functionality of banking IS. Let's briefly define the functional purpose of each of the systems included in the above-mentioned functional blocks.

1. Client IS/public-access hardware-software complexes (Public channels):

1.1. Web page of the bank/Contact center (Web site). It is designed to place structured content on the products of the bank with the possibility of an interactive chat with contact center employees for the bank's customers.

1.2. Private individuals Internet banking (PIIB). It is designed to manage your own accounts and cards for bank customers, individuals.

1.3. Legal Entities Internet Banking (LEIB). It is intended for management of own accounts, credit lines, salary projects for bank customers, legal entities.

1.4. Automated teller machines, Point of sale terminal (ATM, POS). Are intended for realization of settlement operations with payment cards for clients of bank.

1.5. Partner portals. Are intended for rendering of payment services for clients of bank.

2. Customer Relationship Management System (CRM) is designed for comprehensive customer service, analysis of client data and development of solutions for bank product offerings that meet the needs of customers, based on customer profile analysis, risk rating, bank policies.

2.1.1. Branch work station (BWS) of the branch employee. It is intended for opening accounts, issuing and registering payment cards, cash payment transactions, currency operations, maintaining a customer questionnaire, financial monitoring.

2.1.2. BWS-mobile application. It is intended for registration of salary projects, consumer loans for managing the electronic queue of a branch for mobile bankers, establishment of client loan applications.

2.1.3. Customer relationship management and analytics system. It is designed to analyze the customer profile, based on the risk rating, credit limits calculations, proposals for cross sales of products for the bank's clients.

2.1.4. Collateral management system (CM). It is designed for registration and storage of photo data of fixation and assessment of collateral for the risk management units of the bank.

2.1.5. Customer debt management system (Days past due system (DPDS)). It is designed to automatically calculate days of overdue debt for risk management units of the bank.

2.1.6. Credit bureau, CB) – database of problem borrowers for risk management divisions of the bank.

2.2. The system of automated delivery of messages to customers (Short message system (SMS). It is intended for delivery of information messages about campaigns of promotional offers of individual conditions of service for bank customers.

3. Ensuring intersystem interaction, integration layer:

3.1. Enterprise service bus (ESB) is designed to provide inter-system integration and interoperability of banking IS.

3.2. API programming interface (API) is intended to provide open APIs for integration with external systems including portals that provide payment services to clients.

3.3. Extract, Transform, Load (ETL) system is designed to synchronize large data sets of directories for the IS bank.

3.4. Master Data Management (MDM) system is the only source of reference data about bank customers and online synchronization with other bank systems that contain client data.

3.5. Identity and Access Management (IAM) system is intended for providing strong authentication for external and internal users of banking IS, dynamic management of their access rights.

3.6. Business process management (BPM) system is designed to manage, automate and robotize the bank's internal processes for operational service units.

4. Operating banking systems:

4.1. Product catalog system (PCS) is intended to serve as the only source of reference data for the bank's products and for synchronization with other bank systems that contain the bank's products.

4.2. Core banking day (CBS) is designed to perform the function of the general ledger, acting as a source of data on assets and liabilities and the bank's daily balance sheet for the NBU.

4.3. Human Resources System is designed to manage the mode of work and pay for the personnel of the bank's human resources department.

4.4. Enterprise Resource Planning (ERP) system is designed to manage the accounting of fixed assets, IBE and other bank assets for the financial vertical units of the bank.

4.5. Electronic Document flow (ED) is designed for storing, processing and approval of electronic documents of bank customers.

4.6. Card management system (CMS) is designed for managing a network of POS terminals, ATMs, calculating commissions and coverage, managing the life cycle of plastic cards for employees of the bank's operational service.

4.7. Other separate food systems (other) are designed to account for treasury operations, documentary services, custody operations, deposit box leases, sales of coins and precious metals, and the like.

5. Data management systems:

5.1. Data Warehouse is designed to store structured data from data source systems and data enrichment to form accounting, management, statistical and operational reporting. Users are units of analysis of bank data.

5.2. Data Lake is a storage for storing both structured and non-structured data (images, emails, video, audio data, etc.) to manage the bank's data in a broad sense, from financial statements to marketing campaigns.

5.3. Tools for data transformation and analysis (BI tools) are designed for analysis, transformation, visualization of data for the formation of regulatory and management reporting and decision-making.

Non-functional requirements for banking IS. The author proposes to divide non-functional requirements into blocks corresponding to the following qualities of information:

– confidentiality of data;
– data integrity;
– authenticity;
– data availability (including IP performance).

Confidentiality means that data, especially those that make up bank secrecy, must be protected from unauthorized opening. The GDPR regulates the requirements for the protection of personal data and the possibility of their removal from all bank systems, at the request of the client [7]. Under the Public Cloud model, the bank does not own or dispose of resources, and the resources used to store, process and transfer files are shared among other users. This conflicts with these requirements.

To solve this problem, the data placed in the cloud is necessary to maximize depersonalize. Data can be depersonalized by placing all the data that constitutes bank secrecy using the Private Cloud deployment model, and when inter-system interaction with the Public Cloud is exchanged exclusively with the unique secret identifier of the client. This identifier can be linked to the international bank account number (IBAN) in combination with the unique client ID of the master data management system (MDM).

This approach will also eliminate the risk of unauthorized use of data by cloud service providers. After all, there is a hypothesis that global IT corporations, having seized data from bank customers and obtained licenses for financial activities, may pose a threat to the existence of financial institutions. The latter will not be able to compete with them in a technological aspect. Integrity means that IT assets can only be changed by authorized parties in an authorized way, refers to data, software and hardware. In particular, to protect the «session level» of the interaction of open information systems of the NBU, the use of the cryptographic protection protocol at the transport level version 1.2 (Transport Layer Security (TLS) is regulated to ensure the integrity and confidentiality of information [6].

Authenticity means that only authorized users can access information resources and system functionality. Management of credentials and user access based on cloud services (Identity as a Service, IDaaS) that provides strong user authentication and minimizes the risks associated with attacks aimed at interfering with the session and stealing credentials. In the IT market, there are comprehensive solutions from leading suppliers. Such solutions include two-factor authentication of users, dynamic management of user access based on the template-role model, federated scenarios for different security domains, audit of access events and other opportunities. Functionality is able to fully meet the needs of banking institutions.

Availability means the property of the system to provide the input of an authorized user and the smooth operation of the functionality according to its needs.

To achieve maximum economic effect, cloud services are advisable to apply to systems with high load. Among the criteria: the number of simultaneous users or a large peak load during online analytical processing that requires a lot of processing power. Cloud technologies also make it possible to achieve the maximum level of availability of computing resources (i. e., the absence of failures that cause the shutdown of the business process) for systems that stop working in the most dangerous in terms of operational risks of the bank.

To determine such systems, the author suggests applying the following parameters (Table 1) in the context of availability:

– availability 24/7 – the value of the yes/no option means the possibility of round-the-clock access for the bank's customers to the IS bank in the on-line mode;
– RPO (Recovery point objective) – means a point in time, on which it is possible to recover data in case of stopping the business process as a result of a malfunction in the IS, in minutes;
– RTO (Recovery time objective) is SLA for restoring a business process after a shutdown due to a malfunction in the IS, in minutes.

In the context of productivity:
– Data Base size is the size of the IS database in terabytes.
– OLTP1 – the number of active client sessions, that is, simultaneously working users online in thousands.
– OLTP2 – the number of requests in thousands of units per system and responses from other ISs, are processed per hour.
– OLAP – the interval of updating the system data by data of other systems in minutes.

Table 1

Bank systems with maximum peak loads

№ of system	24/7	RPO	RTO	DB size	OLTP 1	OLTP 2	OLAP
3.1	Yes	0	60	<1	<1	5000	–
3.5	Yes	240	60	<1	200	5000	240
1.2	Yes	5	60	2-4	50	1500	240
1.5	Yes	5	60	<1	50	1500	240
3.2	Yes	0	60	<1	<1	1500	–
3.4	Yes	5	60	>10	10	1000	240
4.6	Yes	5	60	2–4	50	1000	240
1.3	Yes	5	60	2–4	10	300	240

Based on the analysis of the sample shown in Table 1 the author believes that the following systems are the most burdensome and critical for business continuity and SLA to restore work:

3.1. Enterprise service bus.
3.5. Identity and access management system.
1.2. Private individuals Internet banking.
1.5. Partner portals.
3.2. API programming interface.
3.4. Master data management.
4.6. Card management system.
1.3. Legal entities Internet banking.

7. SWOT analysis of research results

Strengths. The use of the Public Cloud deployment model would maximize economic efficiency, reduce costs and operational stability. After all, providing such parameters requires a significant investment in hardware resources that the bank bears when applying the Public Cloud and On-Premise models.

Weaknesses. Separate systems, in particular, the automated banking day (in the architectural scheme 4.2.CBS), carry a large peak OLAP load during the execution of scheduled settlement processes of closing the operational day and the formation of daily reporting. At the same time, in the daytime, the hardware resources are actually under-utilized, and are used inefficiently.

Opportunities. One of the most promising areas of application of Hybrid Cloud and Public Cloud is an automated banking day. Deployment of two instances of this system – Private Cloud for client data and Public cloud for the depersonalized client data.

Data can be depersonalized by placing all the data that constitutes bank secrecy using the Private Cloud deployment model, and when inter-system interaction with the

ISSN 2226-3780

Public Cloud is exchanged exclusively with the unique secret identifier of the client. Such an identifier can be linked to the international bank account number IBAN in combination with the unique identifier of the client of the MDM system.

Research results can be used in the banking system of any country in the world.

Threats. The use of the Public Cloud model without depersonalizing data is impossible because it violates the requirements of the GDPR and the NBU. De-personalizing data and applying the Public Cloud model for complex online interaction processes is a very difficult task for practical implementation.

8. Conclusions

1. A high-level architectural scheme of the IT landscape of the bank is drawn up and functional blocks of applications are defined, of which it consists. For each of the blocks, the requirements of confidentiality, integrity and authenticity of the data are generalized. This formed the basis for determining the priority areas of application of different models of cloud technologies deployment.

2. The functional purpose of each of the main IT landscape systems of the bank, their functional purpose was determined, quantitative and qualitative indicators, in particular, non-functional requirements for banking IS, were analyzed.

The obtained result in quantitative expression of load indicators on the system allows to find additional reserves for optimization of information processing time and increase of economic efficiency due to application of Public Cloud. The greatest effect can be achieved by applying this model to English Core Banking System. The mechanism of depersonalization is proposed to meet the requirements and take into account the restrictions on the placement of client data.

References

1. Zissis D., Lekkas D. Addressing cloud computing security issues // Future Generation Computer Systems. 2012. Vol. 28, No. 3. P. 583–592. doi: http://doi.org/10.1016/j.future.2010.12.006
2. Apostu A., Rednic E., Puican F. Modeling Cloud Architecture in Banking Systems // Procedia Economics and Finance. 2012. Vol. 3. P. 543–548. doi: http://doi.org/10.1016/s2212-5671(12)00193-1
3. Nagaty K. A Framework for Secure Online Bank System Based on Hybrid Cloud Architecture // Journal of Electronic Banking Systems. 2015. Vol. 1–13. doi: http://doi.org/10.5171/2015.614386
4. Rahman M., Qi X. Core Banking Software(CBS) Implementation Challenges of e-Banking: An Exploratory Study on Bangladeshi Banks // Journal of Administrative and Business Studies. 2016. Vol. 2, No. 4. P. 208–215. doi: http://doi.org/10.20474/jabs-2.4.6
5. Ambodo B. S., Suryanto R., Sofyani H. Testing of Technology Acceptance Model on Core Banking System: A Perspective on Mandatory Use // Jurnal Dinamika Akuntansi. 2018. Vol. 9, No. 1. P. 11–22. doi: http://doi.org/10.15294/jda.v9i1.12006
6. Reeshma K. Challenges of Core Banking Systems // Mediterranean Journal of Social Sciences. 2015. Vol. 6, No. 5. P. 24–27. doi: http://doi.org/10.5901/mjss.2015.v6n5p24
7. Personalized Security Approaches in E-banking Employing Flask Architecture over Cloud Environment / Hamidi N. A. et al. // Procedia Computer Science. 2013. Vol. 21. P. 18–24. doi: http://doi.org/10.1016/j.procs.2013.09.005
8. Karthigainathan M. Cloud Computing for Rural Banking // International Journal Of Engineering And Computer Science. 2016. Vol. 5, No. 9. P. 17880–17884. doi: http://doi.org/10.18535/ijecs/v5i9.15
9. Grivas S., Schurch R., Giovanoli C. How Cloud Will Transform the Retail Banking Industry // Proceedings of the 6th International Conference on Cloud Computing and Services Science. 2016. Vol. 1. P. 302–309. doi: http://doi.org/10.5220/0005910903020309
10. Bobyl V. V., Dron M. A. «Khmarni» tekhnolohii yak faktor zbilshennia operatsiinoho ryzyku banku // Bankivska sprava. 2014. No. 11–12. P. 47–62. URL: http://lib.sumdu.edu.ua/library/DocDescription?doc_id=441341 (Last accessed: 24.12.2017).
11. Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky v bankivskii systemi Ukrainy: Resolution of the Board of the National Bank of Ukraine No. 95 from 28.09.2017 // Baza danykh «Zakonodavstvo Ukrainy» VR Ukrainy. URL: http://zakon2.rada.gov.ua/laws/show/v0095500-17 (Last accessed: 24.12.2017).
12. General Data Protection Regulation: Directive of European Parliament and of the Council of 27.04.2016 No. 95/46 // European Union Law data base. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (Last accessed: 24.12.2017).

Baglai Roman, *Postgraduate Student, Department of Cybernetics and System Analysis, Kyiv National University of Trade and Economics, Kyiv, Ukraine, e-mail: romanbaglai@gmail.com, ORCID: http://orcid.org/0000-0002-4067-4929*