ATLANTIS PRESS
Advances in Computer Science Research (ACSR), volume 72
IV International Research Conference "Information Technologies in Science, Management, Social Sphere and Medicine" (ITSMSSM 2017)

Information Technology in Business Continuity

Elena V. Chernova
Power Engineering and Automated Systems Institute
NMSTU
Magnitogorsk, Russia

Andrei S. Dokolin
Magnitogorsk School №28
Magnitogorsk, Russia
a.dokolin@gmail.com

Irina V. Gavrilova
Power Engineering and Automated Systems Institute
NMSTU
Magnitogorsk, Russia

Marina V. Romanova
Power Engineering and Automated Systems Institute
NMSTU
Magnitogorsk, Russia

Abstract – **Ensuring the continuity of business activity is an important competitive advantage of modern companies. Currently separated two approaches of business continuity management, each with a key role for information technology. Information security means lower risks of downtime due to the actions of intruders. Business process management systems allow you to trace the execution of business processes, timely warn of threats, provide an opportunity to improve the work with clients. Cloud technologies, initially supporting continuity of services, provide quality IT-support to start-ups and small businesses. We determined Business Process Management Systems functionality for business continuity. We have studied the practice of applying cloud technologies in companies and provide basic and advanced models of cloud technologies for business continuity**

Keywords – business continuity management; information security; business Process Management; iBPMS

I. INTRODUCTION

The conduct of a successful business and the competitiveness of a modern organization in an information society need optimal and relevant approaches to ensuring the continued operation of key business processes. It "is caused by both universal integration processes and necessity of elaboration of effective management mechanisms" [1]. Obviously, even for large firms short-term failure of the client system leads to financial losses, and for a small company can be fatal. The primary task of the management is the need to organize the business processes of the company in such a way that its functioning does not stop when critical or extraordinary situations occur, or it is resumed as soon as possible.

The business continuity management is "a holistic management process which identifies potential threats to an organization, and identifies possible implications for business operations in the case of the implementation of these threats and create the basis for the organization's ability to recover and effectively respond to incidents that ensures that the interests of key stakeholders, reputation, brand and value creation" [2]. According to the standard BS 25999-1:2006 "Business continuity management. Part 1: a practical guide", the process of continuity management involves managing the recovery and continuation of business activities in case of business normal course violation and managing a total program of business continuity by providing training, exercises, and analysis to maintain plan(s) of business continuity to date [3].

At this time, there are a number of standards in the field of business continuity of the organization, describing best practices, process continuity management and disaster recovery of the company's operations in emergencies, among which the most widely used standards BS 25999-x Business Continuity Management, which became the basis for Russian standards [4]:

- GOST R 53647.1-2009 "Management of business continuity. Part 1. A practical guide";
- GOST R 53647.2-2009 "Management of business continuity. Part 2. Requirements";
- GOST R 53647.3 2010 "Management of business continuity. Part 3. Implementation guide";
- GOST R 53647.4-2011 "Management of business continuity. Part 4. Guidelines on preparedness for incidents and business continuity";
- GOST R 53647.5-2012 "Management of business continuity. Part 5. Willingness to dangerous situations and incidents";
- GOST R 53647.6-2012 "Management of business continuity. Part 6. Requirements for the management of personal information to ensure data protection".

According to Sergey Petrenko, depending on the area of professional development there are two main approaches to business continuity: ensuring the continuity of IT-processes and services performance (IT approach) or support systems in place to ensure key business processes and data into a single reporting forms (business approach) [5]. As we see, in both cases information technology is the main mechanism for ensuring business continuity. The question arises: how to best organize the work of the organization, based on standard technologies, tailored to the needs of continuous maintenance activities, as well as response to possible incidents? In our opinion, at the forefront must be placed the analysis of business processes in terms of their resilience to incidents, among

Copyright © 2017, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

which, first and foremost, you must identify the most critical to the business and then group them relative to IT processes and services. According to Business Continuity Management, the first step for policy development business continuity is "the first analysis of the impact on the business, BIA – Business Impact Analysis, the purpose of which is the ranking of business processes and it services of the enterprise according to the degree of criticality and the generation of primary, general enough assessment of the likely loss to business in case of violation of the functioning of these processes and services" [3]. According to experts, conducting a BIA is a critical point for developing functional BCM programs as data BIA give management an understanding of what and the extent to which needs protection and special treatment. Standards BCM recommend starting BIA with the design of business processes and the main information flows of the organization. Simultaneously, it is necessary to calculate the extent of losses from the disruption of critical business processes and to analyze the main information services and their relationship to business processes and information flows of the organization.

Let us formulate the main internal threats to business:

- leakage or loss valuable information (trade secrets, information about clients and suppliers, economic information);
- disruption of the production cycle (cessation or delay of provision of services, stop or delay the creation/provision of product, delay of documentation support services/products);
- internal management organization problems (delay relevant information, problems of control, operational coordination of different structures, speed decision-making by different departments, etc.).

Based on the foregoing, it can be noted that all of the selected threats are somehow connected with the used information technologies and thus the organization at any level has a critical reference to contemporary information technologies, systems and services.

II. INFORMATION SECURITY IN ORGANIZATION

The current realities of doing business are such that it is impossible to separate the process of managing the continuity of the organization's activities from the process of ensuring the information security of the organization. “In the context of globalization of society and development of modern info-communicative technologies the thread of a new form of extremism – electronic extremism as it is called cyber extremism – is increasing.” [6]. Safety of functioning of any business depends on the level of understanding by management of the importance of implementation of activities in the company of it solutions related to information protection and information security.

It is undeniable that the cost and scale software to support information security will be different for organizations of different levels and different areas, however, it is possible to identify necessary and recommended set of software products that are unique to any business. The main object should be the system of differentiation of access according to the staff levels of confidential information. Password protection should be natural for workers in any capacity, and they must understand the responsibility for infringements of work with the access system. The use of such a system will reduce the risks of information leakage and facilitate control over user actions with the information.[7]

Next in importance to become the backup system and the rules for their inclusion in the activities of the organization. Backup – the process of creating a copy of the information object on the independent media. Common issues include temporary periods of backup information, storing the backup on the server with the original information and maintaining backups during working hours. The third most important to distinguish anti-virus protection. Modern malware can infiltrate on the workstations even when there is no Internet connection or ban to download and upload files from the network, their diversity and the mechanisms are changing with such speed that a normal user may not be prepared for self-counteraction and protection from infection. Update the virus databases is required, otherwise out-of-date antivirus is not able to provide complete data protection for workstation and servers.

III. BUSINESS PROCESS MANAGEMENT SYSTEMS

Business process management systems include a methodology (most often workflow-notation, eEPC, BPMN) for modeling business processes and software for their automation.

Any business process management system contains the following modules [8]:

- graphic tools that are designed to describe and analyze processes;
- workflow server - the main server on which the described processes run, while the server monitors the status of each process and business event within the process;
- operational tools for making changes during the execution of the process, for example, when managing task lists and working priorities;
- monitoring and management tools that show how the process is carried out or at what stage it is under, under what conditions.

The development and integration intelligent technologies into software products has expanded the functionality of business process management systems and led to the emergence of a new class of systems - iBPMS (intellectual Business Process Systems), which, in addition to the components listed above, include:

- additional methods for analyzing the implementation of business processes, ensuring the continuity of the company's business processes: real-time business analysis, interactive control panels, alerts in exceptional situations;
- more powerful business rules tools;
- social tools that allow you to connect as many external sources as possible, which include expert assessments and customer testimonials;

- tools for working with unstructured information, including video, audio and social flows;
- tools for integration with various analytical tools;
- support for mobile devices that allow access to business processes 24 hours a day;
- access tools based on roles, skills, and interaction patterns.

In other words, business continuity is one of the essential functions of iBPMS.

Every year Gardner Group analyzes the market IBPM systems, grouping software solutions using the "Magic square". Comparison and analysis of squares revealed the following trends in the iBPMS market. (http://bpm-in-ua.com/article_id/27.html)

1. Over the last five years the leading position is occupied by the products Pegasystem, Appian and IBM, while the observed lag of the latter from its competitors.

2. Despite the ongoing consolidation in the BPMS market, the square of Gartner's regularly updated with new vendors. It is worth noting two categories of newcomers: 1) vendors that focus on your BPMS solution and neutral to the rest of the it environment (Bizagi, Auraportal, Axon Ivy); 2) vendors that are focused on tight integration with Microsoft products (K2, AgilePoint), which will allow to cost-effectively manage business continuity in organizations information infrastructure which is built on the it solutions of Microsoft.

3. Increasing demands of the market for BPMS solutions are forcing developers to constantly improve their products.

However, the use of iBPMS can afford only companies which have successfully implemented the process approach to management: isolated and regulated business processes, identified key roles, describes the environment of the business processes. The scope of the company it does not matter. In that case, if the processes were not clearly defined, or the process approach is not applicable in General, the effect of the implementation of such systems will not – and this means that the organization business continuity will be implemented on the basis of standard office packages, antivirus software, computer workstations and Internet solutions. [10]

IV. CLOUD TECHNOLOGIES

According to the CNews magazine, about 90% of organizations use cloud technologies in their activities - a powerful tool for ensuring business continuity by ensuring data and application security on the side of the service provider. Cloud tools have successfully integrated into the activities of companies due to the diversity and availability of services covering all business needs: from office programs, e-mail, payment systems and to software development. It is important to note that using cloud technologies effectively eliminates the need for organizations to manage business continuity, and this is especially important for small companies or start-ups [11].

There are three basic cloud delivery model tools: 1) infrastructure as a service (Infrastructure as a service), where clients are provided with computer infrastructure (network virtual platform or computers), which the organization sets up independently to solve their business problems; 2) platform as a service (Platform as a service), which is passed to the client platform with an installed system and application software; 3) software as a service (Software as a service), in which the client receives access to license versions of required it software. It is obvious that all these models can be used together.

The variety of business environment needs has led to the emergence of additional models[12]:

1) everything as a service (Everything as a Service) – organizations, in the presence of access to the Internet, receive a completely information infrastructure, including specialized corporate information systems that support the management of business processes;

2) hardware as a service (Hardware as a Service) – in fact, rental of computer equipment without software;

3) the workstation as a service (Workplace as a service): In this model, a cloud-based client provides automated workstations for its employees with all the necessary software; This model is often used to organize the work of remote offices;

4) data as the service (data as a service) – the model provides clients with disk space that it can use to store large amounts of information; The model is very common among individuals who are users of the global network;

5) security as a service (security as a service), a model whose main ideas are to ensure the security of your company's information technology and services.

It is important to note that the use of cloud technology does not always obviate the need for the organization to manage business continuity, because even a very large and reliable provider is likely to be denied service Cloud technology. For this reason, there is a need to consider strategies for the use of alternative suppliers, as well as for the preservation of confidential data that constitute a commercial secret. At the same time, for small companies or start-ups, the level and volume of cloud technology is often sufficient and, more importantly, financially available.

V. CONCLUSION

So, despite the fact that the problem of the continuity of the organization's activities is considered long enough (the concept of continuous production appeared in the XIX century or, perhaps, earlier), in the IT-context, this problem is dealt with for the past twenty years. The result was a distinguished two basic approaches to business continuity management of companies: IT-approach ensure the operability of the supporting business information technology and business approach associated with the implementation of control systems for business processes. For each approach, created a high performance IT-tools which are improving, allows

organizations to actively work and develop in the conditions of crisis of the domestic economy.

The results of the study allowed to draw the following conclusions:

1. We found that main Russian standards of business continuity management enacted in 2009 are based on standards BS 25999-x Business Continuity Management.

2. We determined Business Process Management Systems functionality for business continuity. Modern iBPMS are developed to provide business continuity.

3. We have studied the practice of applying cloud technologies in companies and provide basic and advanced models of cloud technologies for business continuity

We plan to continue the study of business continuous management with information technologies tools.

REFERENCES

[1] Ovchinnikova I. G., Kurzaeva L.V., Solomatina N.B., Chusavitina G. N., et al. (2016) Elaboration of a Frame Model for Intensification and Managing Requirements to Learning Outcomes in Regional Systems of Continuing Professional Education International Review of Management and Marketing, 2016, vol. 6, no. 2S, pp. 190-197. Available at: http://www.econjournals.com/index.php/irmm/issue/view/71 (Accessed 18 October 2017).

[2] Musatov K. Business continuity. Approaches and solutions. Jet Info 5 N, 2007.

[3] Standard BS 25999-1:2006 "Business continuity management. Part 1: Code of practice".

[4] Chernova Ye.V. (2016) Professional'nye kompetencii magistrov biznes-informatiki v kurse «Upravlenie nepreryvnost'yu biznesa» [Professional competences of masters of Business Informatics in the course "Business continuity management"]. Ivanovo: OOO Nauchnyj Mir, pp. 22-27.

[5] Petrenko S.A., Belyaev A.V. (2011) Upravlenie nepreryvnostyu biznesa. Vash biznes budet prodolzhatsya. Informatsionnye tekhnologii dlya inzhenerov [Business continuity management. Your business will continue. Information technology for engineers]. Moscow: DMK Press. Moscow: Kompaniya AyTi, P. 400.

[6] Chusavitina G. N., Zerkina N.N. (2015) Mery profilaktiki kiberekstremizma v podgotovke budushchikh uchitelei [Cyber Extremism Preventive Measures in Training of Future Teachers]. SGEM2015 Conference Proceedings, Book 1, Vol 2, pp. 275 - 280. DOI: 10.5593/SGEMSOCIAL2015/B12/S3.035

[7] Folkers, A. (2017). Continuity and catastrophe: business continuity management and the security of financial operations. Economy and Society, 46(1), 103–127. doi:10.1080/03085147.2017.1307650

[8] Gavrilova I.V. (2011) Svobodnoe programmnoe obespechenie dlya upravleniya biznes-processami [Open source for Business Process Management] Proceedings of the Teoriya i praktika primeneniya svobodnogo programmnogo obespecheniya Sbornik trudov uchastnikov Vserossijskoj molodezhnoj konferencii s ehlementami nauchnoj shkoly. Magnitogorsk, 2011, pp. 144-147.

[9] Spitsin, V., Mikhalchuk, A., Spitsina, L., Shabaldina, N., Novoseltseva, D., & Shinkeev, M. (2016). Product Innovation Efficiency of Russian Electronic Industry: DEA Approach and Cluster Analysis. Proceedings of the 2016 2nd International Conference on Social Science and Higher Education. doi:10.2991/icsshe-16.2016.20

[10] Bajgoric, N. (n.d.). Information Architectures for Business Continuity. Continuous Computing Technologies for Enhancing Business Continuity, 60–78. doi:10.4018/978-1-60566-160-5.ch004

[11] Saleem, M. (2017). Cloud Computing and Its Technologies: A Survey. IJARCCE, 6(6), 355–357. doi:10.17148/ijarcce.2017.6663

[12] Dhawan, G. (2017). Conceptualization of Cloud Computing and its Security Threats, Challenges, Technologies and Application. International Journal for Research in Applied Science and Engineering Technology, V(IV), 629–635. doi:10.22214/ijraset.2017.4112