UDC 004.832.3

A. V. Skatkov, ScD.,
E. N. Mashchenko, PhD.,
V. I. Shevchenko

A DYNAMIC CLASSIFICATION MODEL FOR SECURE ACCESS CONTROL IN BUSINESS-CRITICAL SYSTEMS

Abstract. *It is proposed a dynamic classification model of software applications, that are part of business critical systems. Software applications were classified on the degree of access security. The information technology was developed, which identifies three classes of safety-critical software regarding applications access. This allows to hold a reengineering of user roles . The information technology was developed, which identifies three classes of safety-critical software regarding applications access. This allows to hold the reengineering of user roles. An example of application of technology and the assessment of its effectiveness were presented.*

Keywords: *business critical system, software applications, cluster analysis, dynamic classification, k-means method, incident, security metric, access control, control model, security access*

А. В. Скатков, д-р техн. наук,
Е. Н. Мащенко, канд. техн. наук,
В. И. Шевченко

МОДЕЛЬ ДИНАМИЧЕСКОЙ КЛАССИФИКАЦИИ ДЛЯ УПРАВЛЕНИЯ УРОВНЕМ БЕЗОПАСНОСТИ ДОСТУПА В БИЗНЕС-КРИТИЧЕСКИХ СИСТЕМАХ

Аннотация. *Предлагается модель динамической классификации программных приложений, входящих в состав бизнес-критической системы по степени безопасности доступа. Разработана информационная технология, позволяющая выделить три класса критичных по безопасности доступа программных приложений с целью проведения ренижиниринга ролей пользователей. Рассмотрен пример применения технологии и оценки ее эффективности.*

Ключевые слова: *бизнес-критическая система, программное приложение, кластерный анализ, динамическая классификация, метод k-средних, инцидент, метрика безопасности, управление доступом, модель управления, безопасность доступа*

О. В. Скатков, д-р техн. наук,
О. М. Мащенко, канд. техн. наук,
В. І. Шевченко

МОДЕЛЬ ДИНАМІЧНОЇ КЛАСИФІКАЦІЇ ДЛЯ УПРАВЛІННЯ РІВНЕМ БЕЗПЕКИ ДОСТУПУ В БІЗНЕС-КРИТИЧНИХ СИСТЕМАХ

Анотація. *Пропонується модель динамічної класифікації програмних додатків, що входять до складу бізнес-критичної системи , за ступенем безпеки доступу. Розроблено інформаційну технологію, що дозволяє виділити три класи критичних з безпеки доступу програмних додатків з метою проведення реніжінірінга ролей користувачів. Розглянуто приклад застосування технології та оцінки її ефективності.*

Ключові слова: *Бізнес-критична система, програмний додаток, кластерний аналіз, динамічна класифікація, метод k-середніх, інцидент, метрика безпеки, управління доступом, модель управління, безпека доступу*

Introduction. Currently the architecture of business critical information systems companies, are ever more complex, including in the area of security. Rest are constantly evolving, the number of sources of information is increasing, and as a result the security event monitoring is not trivial [1]. The constantly growing volume of data and events in an online business-critical object, an increase in the number of users and network devices, significantly complicate the task.

In most companies, as a rule, there is the following situation: implemented a centralized analysis and management of all network incidents running DLP (Data Loss Prevention) system that controls all the leaks of confidential information, as well as a number of isolated highly specialized systems. In such circum-stances, the ability to analyses developments and identifying security incidents severely limited, because there is no consolidation between different systems of protection and there is no possibility to get information about the dynamics and correlation of security events and incidents in the infrastructure as a whole. Identify the relationship between these events generates a large amount of manual data processing of a partly or security systems. In the end, actually caused the incident may not be seen or detected late.

As an approach to address this problem effectively to information technology management secure access based on dynamic classification model software applications [2; 3; 4; 5; 13] and modification of the k-means method, proposed by the authors [6, 7].

The aim of the research is the development of synthesis methods of access control in business critical systems (BCS) model-based dynamic classification. Object of research is the software applications that are part of the BCS. The subject of the research is the process of managing user access. The practical result of the research is to determine the most critical class of software applications in terms of compliance with the limit values of metrics to further security policy priority of reengineering the role-based access control. Role-based access control (Role Based Access Control RBAC) is the development of a policy of selective access control, security management of BCS [8, 9]. Role-based access allows you to implement a flexible, changing dynamically in the operation of the computer system access rules. Roles are created inside the BCS for various job functions. Specific roles are assigned permissions to perform certain operations. Staff members (or to other users of a software application to BCS) are assigned fixed roles, through which they receive the appropriate privileges to perform the fixed system functions [5, 10].

1. Statement of the problem. The model must be developed and information technology clustering software applications for security access that allows for the information from the log files of the BCS, using methods of cluster analysis to form classes of software applications with varying degrees of severity in terms of compliance with the limit values of metrics to further security policy priority of reengineering the role-based access control.

Input: O – the set of software applications of clustering $O = \{o_i \mid i = 1, n\}$. (K) – the set of private access security metrics, $K = \{k_j \mid j = 1, p\}$.

Training set of values of private security access software metrics is:

$$X = \begin{pmatrix} x_1^{(1)} & x_2^{(1)} & \dots & x_n^{(1)} \\ x_1^{(2)} & x_2^{(2)} & \dots & x_n^{(2)} \\ \dots & \dots & \dots & \dots \\ x_1^{(p)} & x_2^{(p)} & \dots & x_n^{(p)} \end{pmatrix} = (X_1, X_2, \dots, X_n)$$

where $x_i^{(j)}$ – the value of the j-th security metrics for the i-th software application; m = 1, M – the number of clusters, m<n; $z_m^{(j)}$ – coordinate of the center of gravity on a metric k_j:

$$z_m^{(j)} = \frac{1}{N_m} \sum_{l=1}^{N_m} x_{i_l}^{(j)}, \qquad (1)$$

where N_m – the number of objects in the m-th cluster.

The distance between objects (o_l, o_h):

$$\rho_E(X_l, X_h) = \left[\sum_{j=1}^{p} \alpha^{(j)} \left(x_l^{(j)} - x_h^{(j)} \right)^2 \right]^{\frac{1}{2}}, \qquad (2)$$

where $\alpha^{(j)}$ – weight coefficient of the metric k_j, defined by individual decision-makers (DM).

The result: partition of the original sample by clusters $O = \{Q^{(1)}, Q^{(2)}, \dots Q^{(M)}\}$, where $Q^{(m)} = \{o_i^{(1)}, o_i^{(2)}, \dots o_i^{(N_m)}\}$.

The criterion of effectiveness of clustering is a minimum of intra-group scattering:

$$f = \sum_{m=1}^{M} \sum_{l=1}^{N_m} \sum_{j=1}^{p} (x_{i_l}^{(j)} - z_m^{(j)}) \qquad (3)$$

2. Modernization of the k-means method

As a part of this technology we have the further development of the k-means cluster analysis that adapts to the task of classification of software applications. Classic k-means method [6, 7] has the following disadvantages:

1) random cluster centers in the early stages of the break;

2) full search options to determine the factor space points to the cluster; 3) DM does not take into account the degree of influence the

clustering of individual parameters for the cluster. The offered modification addresses these shortcomings by introducing and overriding dynamic weights in (2), the initial configuration of the cluster centers, multidimensional optimization techniques.

Based on practical experience in the development of systems for automation of business processes and research described in [11] requires that any software application can have one of three States (S) access security: green zone means that access security metrics correspond to the SLA (Service Level Agreement); yellow zone is medium criticality; the red zone is high criticality.

The initial time for all security metrics defined boundaries as, where $k_{im}^{(t)н}$ and $k_{im}^{(t)в}$ is the lower and upper bounds of possible change in metric. Thus, unlike the classic k-means method, the first iteration of the centers for a specified number of clusters are determined randomly, and not on the basis of security boundaries for each State of the BCS. The feature of the proposed modification is the use of dynamically changing weights, the calculation of distances (2) from a point-factor space to the center of the cluster. This allows the decision maker (DM) to take into account the significance of private security access criteria and thus manage the risks of global security incidents in the BCS.

A modified clustering algorithm consists of the following four stages:

1. Initialization. The cluster centers are generated $\{Z^{\text{К}},Z^{\text{Ж}},Z^{\text{З}}\}^{t}$

2. Attribution. Object refers to the cluster, the center of which he is closer. $Q_m = \{x^t \mid \rho(x^t, Z_m) = \min_{l=1,N_m} \rho(x^t, Z_l)\}$

3. Adaptation. Recalculation of the cluster centers on (1).

4. Checking the quality of the clustering on criterion (3).

3. Technology description. Figure 1 shows how the dynamic classification of information technology application in UML notation. In accordance with the proposed technology expert BCS determines the composition and the boundary values of the access security settings. It support service, which is responsible for security access control, based on data from monitoring systems software application generates files that contain information about the values of monitored parameters and transmits that information in a decision support system. On the basis of data on limit values for the security settings, the system generates a preset coordinates of cluster centers. DM selects the weighting factors for (2), depending on the importance of security metrics. In the procedure of "attribution" is a split software products on three classes of criticality using selected metric. To expedite the task of the algorithm in step 4 added procedure multidimensional search engine optimization based on the Hooke – Jives, Pattern search – that significantly reduced the speed of decision-making, compared with brute force..

4. Pilot studies. As an illustration of the application of the proposed information technology examines the BCS, which includes 10 software applications to automate financial and economic activity on the Platform 1C. As source data log-log software applications for the year of 2013 received four metrics: value k1 is the number of bugs in the system of open access to electronic documents, outside its competence (Fig. 2, a); K2 is the number system alerts attempts to access the private electronic documents; K3 is the number of emergency shutdowns applications related to unauthorized access; K4 is the average recovery time for user access to a software application after a crash (min) (Fig. 2, b).

In Fig. 2 are a priori boundaries the criticality of software applications for security access.

Table 1 shows the iterative process of dynamic adjustment of clusters, as the security of software applications (the first three iterations).

1. Coordinates of cluster centers by security state for software applications included in the BCS

	t(1)				t(2)				t(3)			
SLA	k_1	k_2	k_3	k_4	k_1	k_2	k_3	k_4	k_1	k_2	k_3	k_4
К	50	100	10	120	50	80	12	120	50	100	12	120
Ж	20	60	5	40	10	30	5	40	10	20	5	60
З	5	10	2	20	5	10	2	20	5	10	2	20

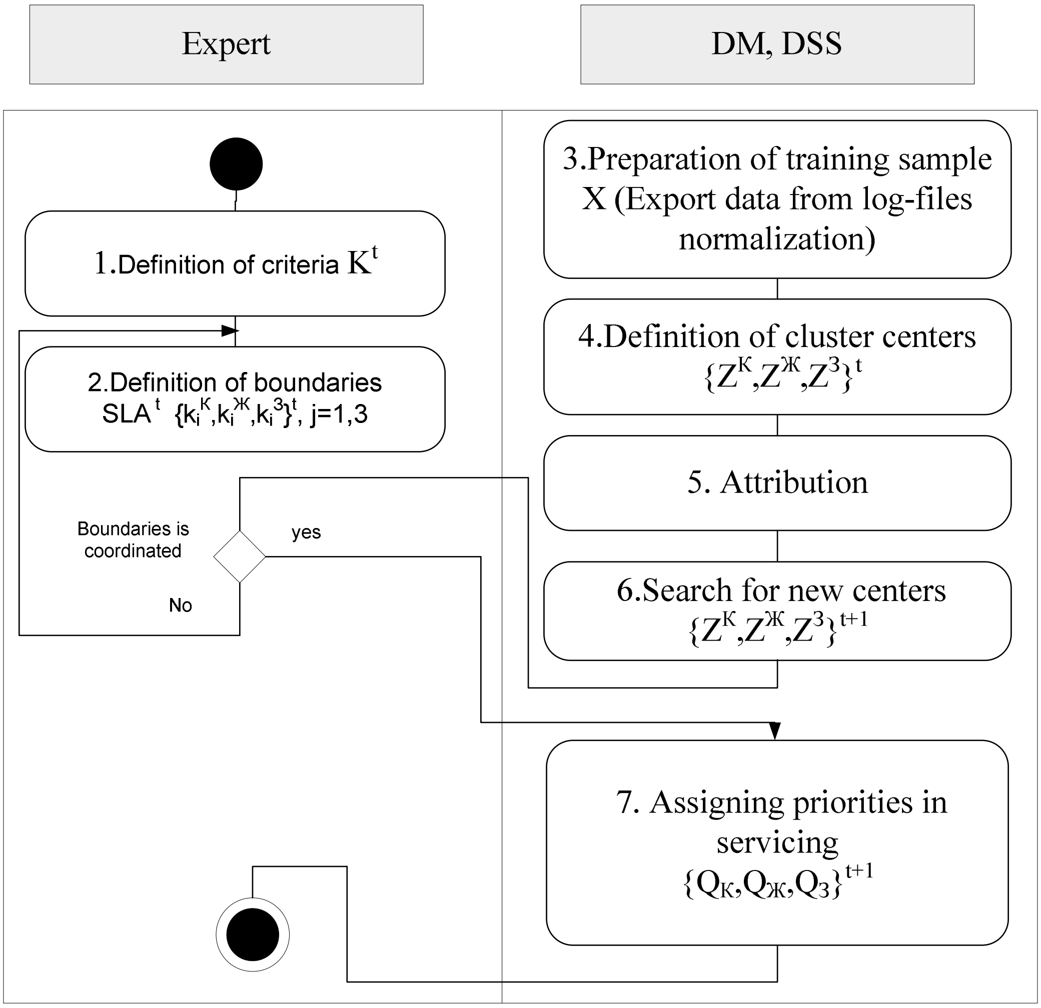
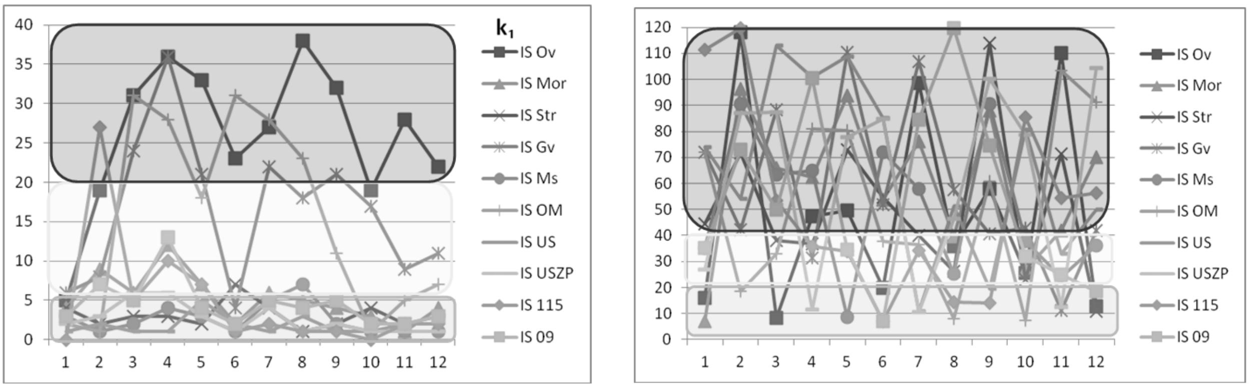

Expert
DM, DSS
1.Definition of criteria K^t
2.Definition of boundaries SLA ^{t} $\{k_i^К,k_i^Ж,k_i^З\}^t$, j=1,3
Boundaries is coordinated
yes
No
3.Preparation of training sample X (Export data from log-files normalization)
4.Definition of cluster centers $\{Z^К,Z^Ж,Z^З\}^t$
5. Attribution
6.Search for new centers $\{Z^К,Z^Ж,Z^З\}^{t+1}$
7. Assigning priorities in servicing $\{Q_К,Q_Ж,Q_З\}^{t+1}$

Fig. 1. Dynamic information technology, Classification Scheme of software applications



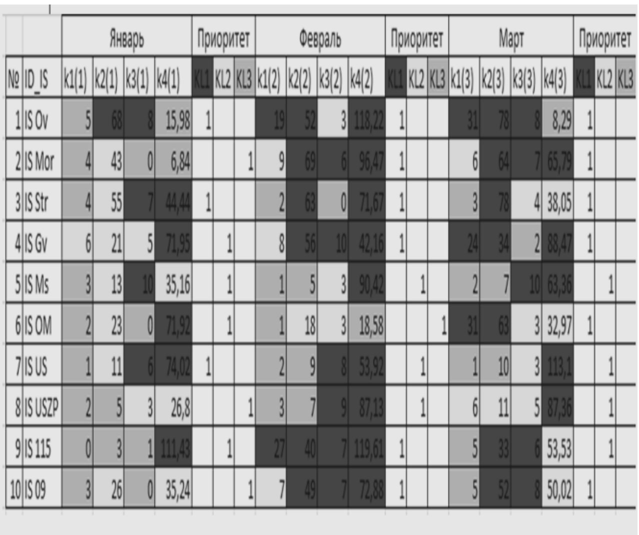
a b

Fig. 2. Piece numerical identification of private security criteria

Adjust values in the cluster centers, took place in accordance with the update of data on the characteristics of the BCS, the update data on a log-log software applications was one month.

Table 2 shows the results of the classification of software applications for degree of safety on the basis of the proposed information technology with highlighted priorities for reengineering the role-based access control.

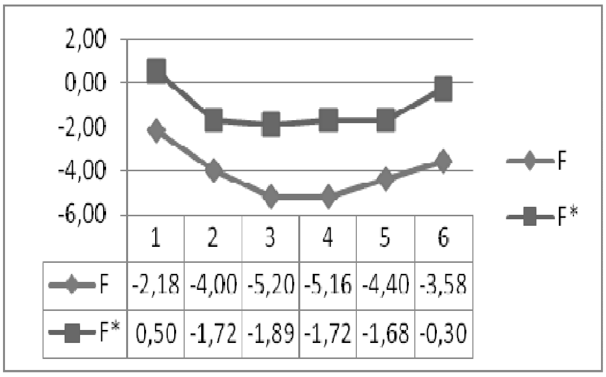
2. Classification results Snippet software applications for security



		Январь				Приоритет			Февраль				Приоритет			Март				Приоритет		
№	ID_IS	k1(1)	k2(1)	k3(1)	k4(1)	KL1	KL2	KL3	k1(2)	k2(2)	k3(2)	k4(2)	KL1	KL2	KL3	k1(3)	k2(3)	k3(3)	k4(3)	KL1	KL2	KL3
1	IS Ov	5	68	8	15,98	1			19	52	3	118,22	1			31	78	8	8,29	1		
2	IS Mor	4	43	0	6,84			1	9	69	6	96,47	1			6	64	7	65,79	1		
3	IS Str	4	55	7	44,44	1			2	63	0	71,67	1			3	78	4	38,05	1		
4	IS Gv	6	21	5	71,95		1		8	56	10	42,16	1			24	34	2	88,47	1		
5	IS Ms	3	13	10	35,16		1		1	5	3	90,42		1		2	7	10	63,36		1	
6	IS OM	2	23	0	71,92		1		1	18	3	18,58			1	31	63	3	32,97	1		
7	IS US	1	11	6	74,02	1			2	9	8	53,92		1		1	10	3	113,1		1	
8	IS USZP	2	5	3	26,8			1	3	7	9	87,13		1		6	11	5	87,36		1	
9	IS 115	0	3	1	111,43		1		27	40	7	119,61	1			5	33	6	53,53		1	
10	IS 09	3	26	0	35,24			1	7	49	7	72,88	1			5	52	8	50,02	1		

Table 2 shows that the various grounds are one and the same application may relate to different security groups. The proposed technology lets you break down your application to 3 Group and thus select the most critical applications in terms of security policy, as the priority for reengineering.

Fig. 3 shows the research of integrated access control quality score in the BCS for this technology. Embedded quality score is based on linear convolution additive metric access control, according to [12].



	1	2	3	4	5	6
F	-2,18	-4,00	-5,20	-5,16	-4,40	-3,58
F*	0,50	-1,72	-1,89	-1,72	-1,68	-0,30

Fig. 3. Comparison of integrated access control to the quality score of (F) and after (F *)

Conclusions. Studies have shown that the application of the technology of the dynamic tuning of cluster centers group application to BCS on criticality levels provides improved access to 23 % for individual groups of user roles. Analytical assessment of this indicator is generally impossible owing to the absence of a priori information. Value is determined by the particular situation in the BCS and the levels of disturbance, for this reason, the proposed technology dynamically adjust cluster centers DM allows an adequate analysis of the situation.

Thus, as a result of the research, based on the data and log files of the BCS on the State of software applications and applied information technology, dynamic clustering of the data, received aggregated groups of software applications.

Areas for further research. It is intended to extend the classes of models and methods, as well as studies of other access control methods in business-critical systems. This approach to controlling access to BCS allowed:

1) improve access to BCS policy reengineering;

2) reduce the number of vulnerabilities and conflict situations resulting from an incorrect definition of user access level;

3) organize DSS, which allows the DM adaptively adjusts user access profiles for the effective management of security policies in the BCS. Work is supported by the Russian Foundation for basic research (grant No. 14-47-01047).

References

1. Smirnov N., Yadro Besopasnosti [Security Kernel], (2013), *Chief Information Officer CIO.ru,* No. 3. Available at: url: http: //www.osp.ru/cio/2013/03/13034655/ (accessed 22.11.2014) (In Russian).

2. Lugovskaya L.P., Skatkov I.A., and Shevchenko V.I., Dinamicheskaya klasterizatsiya informatsionnyih potokov [Dynamic Clustering of Information Flows], (2011), *Journal Informatika, Elektronika, Svyas,* Sevastopol, Vol. 114, pp. 14 – 20 (In Russian), url: http://www.nbuv.gov.ua/old_jrn/natural/Vsntu/informat/2011_114/2011_114/114_03.pdf.

3. Mashchenko E.N., and. Shevchenko V.I., (2012), Issledovanie kriticheskih situatsiy v IT-infrastrukturah metodami klasternogo analiza [Research of Critical Situations in IT-Infrastructures of Cluster Analysis Methods], *Journal Electronic and Computer Systems*, Kharkov, Ukraine, Vol. 5 (57), pp. 191 – 196. url:
http://nbuv.gov.ua/j-pdf/recs_2012_5_36.pdf.

4. Mashchenko E.N., and Shevchenko V.I., Issledovanie protsessov upravleniya kachestvom IT-servisov dlya biznes-kriticheskih sistem metodami klasternogo analiza [Research of Quality Control Processes for IT Services in Business-Critical Systems of Cluster Analysis Methods], (2013), *System Analysis and Information Technologies, 15-th International Conference SAIT* 2013, Kiev, Ukraine, May 27-31, 2013, 301 p. (In Russian).

5. Mashchenko E.N. Model upravleniya dostupom v biznes-kriticheskoy sisteme na osnove ispolzovaniya tehnologiy upravleniya informatsiey i sobyitiyami bezopasnosti i metoda agregatsii roley polzovateley. [Access Control Model in Business-Critical System Based on the use of Technology for Information Management and Security Event and Aggregation Method user Roles], (2014), *Modern Problems of Applied Mathematics, Computer Science, of Automation and Managemen, Materials of the 4th Scientific and Technical Workshop. 23–27 September 2014 in Sevastopol,* Moscow, Russian Federation, 181 p.; pp. 94 – 100 (In Russian).

6. Bendjamin S. Duran, and Patrick L. Odell, (1974), Claster Analysis a survey. Springer-Verlag-Berlin-Heydelberg-New York. 198 p. (In English).

7. Mandel I.D., (1988), Klasternyiy Analiz, Moscow, Russian Federation, *Finansyi i Statistic Publ.*, 176 p. (In Russian).

8. Ferraiolo D.F., Kuhn D.R.. (1992), Role Based Access Control, *15th National Computer Security Conference*, Baltimore MD, October 1992, p. 554 – 563 (In English).

9. Sandhu R., Coyne E. J., Feinstein H. L., Youman C. E., (1996), Role-Based Access Control Models. *IEEE Computer (IEEE Press)* volume 29 Number 2, pp. 38 – 47. (In English).

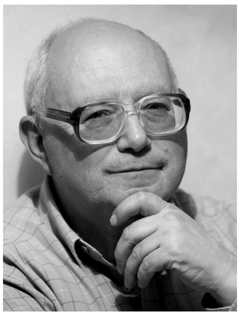
10. Mashchenko E.N.,and Shevchenko V.I., (2013), Upravlenie dostupom v biznes-kriticheskoy sisteme na osnove agregatsii roley polzovateley [Access Control in the Business-Critical System Based on the Aggregation of user Roles], (2013), *Materials of the International Scientific-practical Conference "Institute of Information Technology and Information Security tion in Science, Technology, and Education" Infotech 2013* September 9-13, 2013, Sevastopol, 117 p.; p. 18 – 19 (In Russian).

11. Rolik A.I., (2013), Kontseptsiya upravleniya korporativnoy IT-infrastrukturoy [The Concept of Management by Corporate IT Infrastructure], (2012), *Journal Informatika, Elektronika,, Upravlenie i Vyichislitelnaya Tehnika,* Kiev, Ukraine, No. 56, pp. 31– 55 (In Russian).

12. Skatkov A.V., and Shevchenko V.I., (2014), Optimizatsiya upravleniya protsessami podderzhki IT-servisov [Optimization of Management Process of IT Services Support], (2014), *Journal Optimization of Production Processes,* Sevastopol, Vol. 15, p.p. 97 – 102 (In Russian).

13. Skatkov A.V. (ed.), (2012), Information Technology for Critical Infrastructures: *monograph, SevNTU*, Sevastopol, 306 p. (In Russian).

Received 05.10.2014



Skatkov
Alexandr Vladimirovich,
ScD., professor of Cybernetics and Computer Technology, Sevastopol National Technical University.
E-mail:
kvt.sevntu@gmail.com

Mashchenko
Elena Nicolaevna,
PhD., associate professor of Cybernetics and Computer Technology, Sevastopol National Technical University.
E-mail:
kvt.sevntu@gmail.com

Shevchenko
Victoria Igorevna,
Senior lecturer of Cybernetics and Computer Technology, Sevastopol National Technical University.
E-mail:
kvt.sevntu@gmail.com