Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 07 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

CLASSIFICATION OF UNPLANNED INTERRUPTIONS DURING IT SERVICE EXECUTION AT INCIDENT LIFECYCLE MANAGEMENT

Rustam G. Asadullaev[1]
Vladimir V. Lomakin[2]
Tatiana A. Lysakova[3]

Abstract: This article focuses on the issue of software incident lifecycle management. It analyzes the standards with incident management instructions. A formal presentation of the corporate information system is performed, which allows to identify an incident location. They develop incident classification algorithm formally presented in multidimensional space. After software update, new incidents may occur that are not listed in the knowledge base. If an incident is represented by isolated cases of "non-standard incident", then it is processed separately. If an incident is often "standard", then an incident model is developed for it. The algorithm presented in the paper takes this feature into account and allows the development of new incident clusters based on the minimum density indicator set by the user. The minimum cluster density index is determined individually for each corporate information system, depending on the approach to incident categorization.

Keywords: incident management, data classification, corporate information system, incident model, data clustering, DBSCAN.

Introduction.

Corporate information systems (CIS) solve the problem of complex automation of organization

[1] Federal State Autonomous Educational Institution of Higher Education - Belgorod National Research University.
[2] Federal State Autonomous Educational Institution of Higher Education - Belgorod National Research University.
[3] Federal State Autonomous Educational Institution of Higher Education - Belgorod National Research University.

business activities under a single management. Business success depends on the efficient use of information technology to support the corporation business processes. CIS consists of subsystems that solve individual tasks of economic activity. As a rule, individual modules of subsystems and subsystem as a whole are geographically dispersed depending on the activities of a company. This imposes additional requirements on the CIS, such as taking into account the specifics of the legislative framework or a system organization for corporate information centralized collection and processing concerning business processes. In particular, the service system is centralized for the entire corporation, and business process support systems depend on the country, region, type of business, and so on. In this regard, questions arise concerning the evaluation of the entire IT structure reliability, as well as the incident management system. The measures ensuring the reliability of software differ from technical support measures. For example, some IT technical elements can be duplicated, which will ensure the system operability in the event of a device failure. Duplication of software will not give a similar result.

All software included in CIS is updated periodically. With software updates, situations are possible in which the system crashes. Errors are an integral part of software development, as hundreds of IT specialists participate in this process, providing support for the infrastructure in the current state through the development of new features, optimization of existing business processes and so on. According to the degree of influence of system failure as a whole, one can distinguish local failures that affect only the functioning of individual modules and subsystems, and global ones that are characterized by a malfunction of the CIS as a whole. In order to minimize the risks of incidents during software updates, some updates are tested on system duplicates. This is a costly undertaking, since it requires virtually the same resources as the original system. At that, restrictions are imposed on the testing time and it

is not clear whether all possible situations of the system were produced. For some systems, such testing is not possible. If there are failures in system updates, some can be fixed or the system can be restored to a state before the update. In this case, it is necessary to identify critical systems to strengthen control in order to minimize the risk of failure. It is worth noting that a certain part of system failures is formed due to incorrect user operation.

The companies distinguish separate subsystems of failure accounting and incident management, which are mainly based on standards [1, 2, 3, 4]. Such systems are designed to support the process of operational incident management in the event of system malfunctions by identifying and classifying an incident, and forming measures for its elimination. At the same time, due to periodic software updates, new failures appear in the CIS, which are not recorded in the knowledge base. During incident management, there may be errors in the classification of failures, which lead to additional time costs in the process of an incident processing and, thus, to financial losses. In this regard, there is a need to develop formal tools for the operational classification of an incident.

Methodology. The issue of incident management is described by various information technology standards. The ITIL (Information Technology Infrastructure Library) forms a concept in which the company IT department provides IT services. ITIL is a set of publications with the recommendations for quality service provision in the form of a set of processes. According to the ITIL an incident is an unplanned interruption of a service or its quality decrease. At that, a malfunction, which at the moment did not affect the service, is also an incident. For example, the lack of user access to email or the slowdown of the application. The process of service restoration for the user with minimization of time costs is an incident management, the essence of which is the management of the life cycle of incidents in order to minimize the negative impact on the business. Incident management allows you to identify and eliminate

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 07 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

an incident quickly, increasing the indicator of service availability, organizes the functioning of IT departments depending on company priorities, according to the results of incident analysis, identifies the ways of service improvement, forms additional requirements for IT services through service desks. ITIL identifies an incident model that describes how to deal with an incident of a particular type. The incident model describes the actions and their time limits for an incident elimination, the order of actions, appoints responsible persons, and also describes with whom it is necessary to maintain contact depending on the stage of incident processing. Thus, the incident model allows you to standardize the actions in the incident management process depending on the incident class. Incidents for which a class is not defined are handled separately without using the model [1]. According to ITIL, a separate category of incidents should be distinguished that lead to significant losses for the business. This category of incidents is determined individually for each company. The impact of an incident is assessed depending on such factors as the degree of financial loss; the number of services dependent on an incident; danger to life; probability of violation of law; decline in business reputation.

In ITIL, the incident management process includes the following steps [2]:

- identification and registration of incidents;

- categorization, determination of the incident priority according to the criteria of urgency and influence;

- initial diagnostics, in which the service desk operator tries to determine the cause of an incident on his own and to resolve the incident. Otherwise escalation and the attraction of additional resources for an incident solution takes place;

- research and diagnostics, clarification of information about an incident, the assessment of an incident impact, and so on;

- solution and recovery;

- incident closure, including the check of an incident established category correctness, surveying the satisfaction of users with the service, confirmation of an incident development reason.

Microsoft has also developed

the Microsoft Operations Framework (MOF) methodological model, which consists of a set of guides to achieve the reliability of IT solutions and services. Within the MOF, the Problem Management function (PMF) is singled out as a separate unit. The following stages of work are carried out as the result of SMF operation: incident registration, investigation of the identified problem, and the development of solutions [3].

The business model for the management of enterprise IT "COBIT 2019" consists of management system principle description. In the framework of corporate IT management processes, the process “Provision, service and support” is distinguished separately, which includes “The management of service requests and incidents” [4].

Thus, all standards demonstrate the importance and necessity of an incident stage categorization, which allows by taking into account the existing knowledge, to develop a decision on an incident model application. However, the standards indicate that each company chooses the method of an incident category determination on its own. The paper proposes the approach of breaking incidents into clusters. The description of each cluster by IT department experts will allow the development of incident classes. At that, new incidents will be identified by the description of the service desk operators in multidimensional space, and the class will be determined by proximity to existing classes.

During the classification problem solution, it is necessary to set the degree of similarity between incidents, for example, the Euclidean distance. The developed classification algorithm basically contains the data clustering algorithm, which will allow the development of new classes of incidents during the system operation. Currently, many data clustering algorithms have been developed, the most famous of which are hierarchical clustering [5], k-means and its variant k-medoids method [6, 7, 8], DBSCAN [9, 10] and others. Each type of clustering has customizable parameters and operating features, which, depending on the problem being solved and the initial conditions, can be evaluated both from the positive and negative aspect. In the present work, DBSCAN will be taken as

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 07 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

the basis of the developed algorithm. The DBSCAN algorithm allows you to set the neighborhood radius parameter (ε) between a pair of points in a multidimensional space and the minimum number of neighboring points ($MinPts$) to form a cluster.

Main part. To build an incident classification algorithm, it is necessary to systematize incidents taking into account the location in the CIS structure. This will formalize the knowledge of incident management and the description of measures to eliminate the negative consequences of an incident. CIS enterprises is a multitude of interacting information systems $MCIS$.

$$MCIS = \{MIS_i\}, \qquad i = \overline{1,n}$$

Where MIS_i - the i-th CIS Information System;

n – the number of CIS information systems.

At that, each IS has its own weight coefficient in the interval [0, 1], reflecting its reliability. This coefficient is determined taking into account the multitude of impacts on IS (license validity period, system criticality, update frequency, the possibility of preliminary update check, the dependence on other IS and other factors). Therefore, it is possible to assess the reliability of the CIS as a whole, as an average weighted sum over all IS.

Each MIS covers a block of business processes of the corporation and consists of many modules, which are information systems of a narrower specialization.

$$MIS = \{MMod_j\}, \qquad j = \overline{1,m}$$

where $MMod_j$ - the j-th module of the i-th CIS information system;

m – the number of modules of the information system.

At that, each MMod module of the information system is characterized by a set of functions.

$$MMod = \{f_l\}, \qquad l = \overline{1,s}$$

Where f_l - the l-th function of the j-th module of the i-th CIS information system;

s – the number of functions of the information system module.

It is possible to carry out preliminary identification of an incident on the basis of the presented sets characterizing its location. An incident can manifest itself in different ways. For example, an incident related to a system update, a number of system users report various problems, which, as it turns out, are initiated later by the same incident.

The failure of one operation, after the system update manifests itself differently. It is advisable to carry out preliminary testing of software updates in more detail. And there may be many incoherent incidents, which are mainly related to the human factor after the analysis. The recommendation can be expressed in better training of staff or in the simplification of functionality. Therefore, during the description of an incident, in addition to the location, there must be characteristics that can identify it taking into account the descriptions of users. Thus, based on the timely classification of an incident, it will reflect the consequences of the incident (the degree of financial loss, the number of services depending on the incident, the danger to life, the likelihood of law violation, business reputation decrease) and determine the measures of their minimization.

Based on the foregoing, depending on the formal description, an incident can be represented as a point in multidimensional space. Similar incidents are expected to constitute the clusters of points in multidimensional space. Thus, having developed recommendations for the preliminary processing of data received from users, it is possible to represent the incident on a multidimensional numerical plane. Many methods have been developed to solve the classification problem. Periodic software updates lead to new incidents that are not included in the knowledge base and do not have their own classification.

A modified DBSCAN algorithm was developed in [11], which allows preliminary data clustering based on the available data about recorded incidents. At that, the parameters of the neighborhood radius (ε) and the minimum number of neighboring points (MinPts) are set individually. In this modified algorithm, noise clusters are formed for the emission points instead of the single “noise” category. This will allow us to evaluate new incidents for the development of new classes. Thus, on the basis of available data, the modified DBSCAN clustering algorithm allows to form incident clusters, on the basis of which classes and models of incidents are formed to manage them.

Figure 1 presents the developed classification algorithm for incidents, taking into account the assessment of new incident cluster development. The

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 07 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

clusters of various shapes can be formed as the result of the DBSCAN algorithm [11]. The implemented algorithm allows you to review many clusters based on the analysis of newly received incident data. The algorithm performs the following iterations:

1. Input of the initial data $X = \{x_1, x_2, \dots, x_n\}$, where x_i is the incident presented in multidimensional space and the results of partitioning into clusters by a modified DBSCAN (*pK* clusters and *pNK* noise clusters).

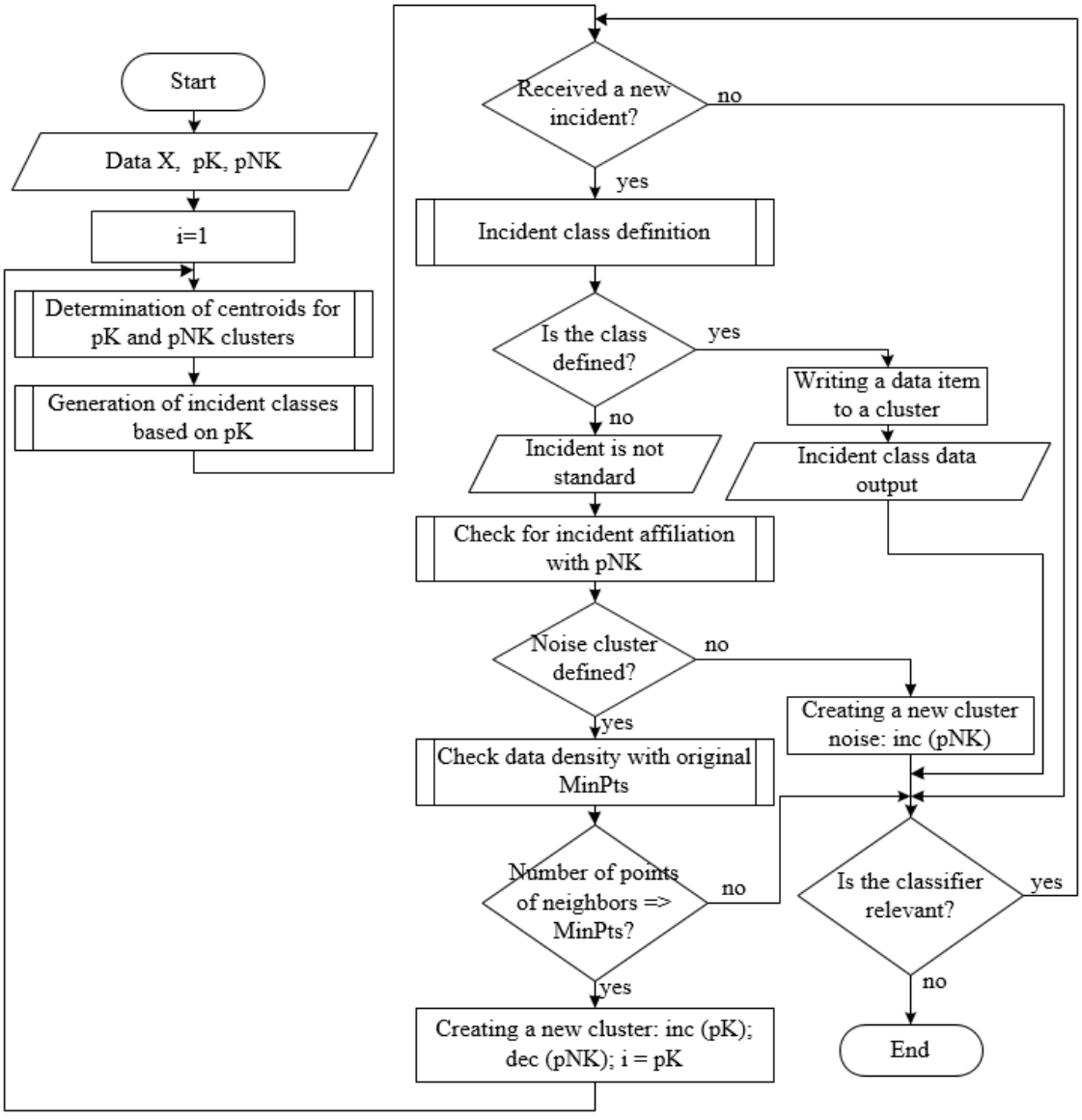

Fig. 1. Incident classification algorithm

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 07 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

2. The centroid Ci is determined for each pK cluster. The subprogram for centroid determination is shown on Fig. 2. 4. Then the incident classes are generated based on pK.

3. Next, a continuous classification of new incidents is carried out until their processing is relevant to the system. For incoming incident data, a check is made for belonging to known incident classes. If the class is defined, then the output of the incident class data is implemented. Otherwise, the incident is not standard and no model has been developed to handle it.

4. If an incident is not standard, then a check is made for belonging to the noise cluster. If the noise cluster is not defined, a new noise cluster record is generated. Otherwise, its data density is checked.

5. If the data density in the vicinity of the centroid is less than MinPts, then the transition to the processing of new incidents is carried out. Otherwise, a new cluster is created for which the centroid is determined. After that, a new class of incidents is formed, for which an incident model is being developed.

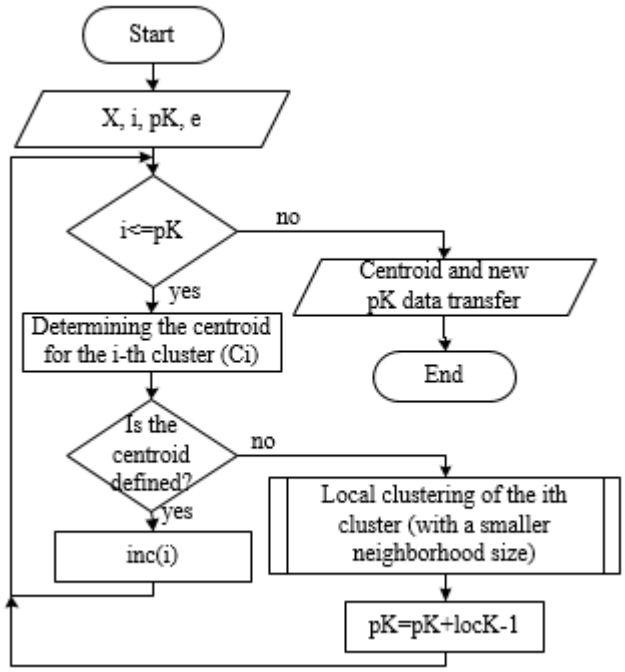

Fig. 2. Algorithm for cluster centroid determination

Figure 2 presents the subprogram operation algorithm to determine cluster centroids. The specifics of the DBSCAN algorithm allows to obtain the clusters of various shapes (ribbon-shaped, spiral, elongated, and so on). Such forms of clusters are not acceptable for the development of incident management models, since the elongated form of a cluster probably indicates the need for different management decisions for two extreme points. Moreover, the cent of the cluster is not determined for irregularly shaped centroids. In this regard, the mechanism for local clustering of clusters with a smaller radius of the neighborhood is implemented in the centroid determination program. This allows us to determine centroids for irregularly shaped clusters. After local clustering, the i-th cluster transforms locK of new smaller clusters, for which the procedure of central point determination is also used.

Summary. The proposed incident classification algorithm makes it possible to determine the class of an incident described in multidimensional space. Classes are formed according to the results of the modified DBSCAN clustering algorithm. Moreover, the clusters of irregular shape are divided into smaller ones in the algorithm for centroid determination. Non-standard incidents for which a class is not defined are tested for belonging to noise clusters. The developed algorithm allows you to create new classes based on the analysis of new non-standard incidents through the processing of noise clusters.

Conclusions.

Thus, an incident classification algorithm has been developed to determine the class of an identified incident. An algorithm is the combination of data classification and clustering procedures. If an identified incident is standard, that is, the system has a control model, then the algorithm displays the incident class. If an incident is not standard, the algorithm analyzes it for belonging to the identified noise clusters, or forms a new noise cluster. Noise clusters are the clusters of incidents in a multidimensional space of insufficient density to form a class. Such a mechanism makes it possible to accumulate knowledge about incidents and evaluate their accumulations in a multidimensional space in order to form

a new class of incidents and develop an appropriate incident management model.

A formal description of incidents will make it possible to implement predictive incident management based on machine learning methods. In this paper, we developed an algorithm to classify an incident upon its occurrence. The problem in predictive management model development for software incidents is the difficulty of a set of tagged data collection that would characterize the occurrence of an incident. Thus, a possible way out is to systematize the chronology of incident identification based on complaints from the system users.

Acknowledgements.

The study has been performed as part of the implementation of a comprehensive project on creation of high-tech production "Development of methodology and tools for creating applications supporting the life cycle of information technology provision and decision-making for the effective implementation of administrative and managerial processes within the framework of established powers", coded as "2017-218-09 -187"; Decree of the Government of the Russian Federation dated April 9, 2010. №218.

References

AXELOS. ITIL - IT Service Management. Date Views 12.08.2019 https://www.axelos.com/best-practice-solutions/itil.
Free ITIL, 2016. YeSSoft.

Microsoft Operations Framework 4.0. Date Views 12.08.2019 https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc506049%28v%3dtechnet.10%29.

ISACA. COBIT 2019. Date Views 12.08.2019 http://www.isaca.org/COBIT/Pages/default.aspx.

Alam, S., Dobbie, G. and Rehman, S.U., 2015. Analysis of Particle Swarm Optimization Based Hierarchical Data Clustering Approaches. Journal Swarm and Evolutionary Computation, 25: 36–51.

Jain, A.K., 2010. Data Clustering: 50 Years Beyond K-means. Journal Pattern Recognition Letters, 31: 651 – 666.

Rejito, J., Retantyo, W., Hartati, S. and Harjoko, A. 2012. Optimization CBIR Using K-Means Clustering for Image Database. International Journal of Computer Science and Information Technologies, 3(4): 4789-4793.

Niknam, T., Amiri, B., 2010. An Efficient Hybrid Approach Based on PSO, ACO and k-means for Cluster Analysis. Journal Applied Soft Computing, Elsevier, 10: 183-197.

Kailing, K., Kriegel, H.-P. and Kröger, P., 2014. Density-Connected Subspace Clustering for High-Dimensional Data. In Proceedings of the 2004 SIAM International Conference on Data Mining, pp: 246-256.

Thang, V.V., Pantiukhin, D.V. and Galushkin, A.I., 2015. Hybrid Clustering FastDBSCAN Algorithm. Proceedings of MIPT, 3(7): 77-81.

Asadullaev, R.G., Konstatinov, I.S. and Lomakin, V.V., 2018. Algorithm for Clustering Multidimensional Data in Decision Making Under the Conditions of Cluster Variation. Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 10-Special Issue. Date Views 12.08.2019 https://www.rmlconsultores.com/revista/index.php/crv/article/view/1966