UDC 004.051

DOI: 10.15587/1729-4061.2022.266387

DEVELOPMENT OF REFERENCE INCIDENT MANAGEMENT MODEL

Gulbakyt Sembina
Corresponding author
Candidate of Technical Sciences, Associate Professor*
E-mail: g.sembina@iitu.edu.kz
Karina Mayandinova
Master's Student*
Lyazat Naizabayeva
Doctor of Technical Sciences, Professor*
Saule Sagnayeva
Candidate of Physical and Mathematical Sciences,
Associate Professor
Department of System Analysis and Control
L. N. Gumilyov Eurasian National University
Satpayev str., 2, Astana, Republic of Kazakhstan, 010000
*Department of Information Systems
International Information Technology University
Manas str., 34, Almaty, Republic of Kazakhstan, 050000

One of the most important tasks of improving the information technology infrastructure of an enterprise is to increase the efficiency of the incident management system. The relevance of this study lies in the fact that at present the work of the technical support service in the conditions of a large flow of applications accelerates violation of the deadlines for resolution established by the business. It, in turn, leads to downtime of information systems and financial losses of the enterprise. This article analyzes the feasibility of introducing a third line of technical support to increase the proportion of incidents resolved within the framework of the Service Level Agreement adopted at the enterprise. A comparative analysis of the widely used two-level model with the proposed three-level model in this work is considered, using business process model notation. The effectiveness of the model is confirmed by automated computations using metrics, by calculating the rate and satisfaction coefficients within the framework of two and three levels of the model and then comparing these indicators to establish patterns. Thus, it is possible to track how successfully and timely incidents of information systems are resolved, which in turn directly reflects the availability and correct functioning of systems and the entire company.

The company's practical losses due to system downtime were calculated, as well as the resulting financial losses before and after the adopting of the three-level system, taking into account the associated costs to identify if the initiation of the model is justified and profitable.

Thus, the proposed model can be adopted by organizations in order to improve the quality of services provided by the IT department, to reduce the effect and impact of incidents on the performance and availability of systems that affect the formation of financial statements

Keywords: incident management, service interruption, support line, resolution time, SLA (service level agreement), reference model

Received date 04.10.2022
Accepted date 13.12.2022
Published date 30.12.2022

***How to Cite**: Sembina, G., Mayandinova, K., Naizabayeva, L., Sagnayeva, S. (2022). Development of reference incident management model. Eastern-European Journal of Enterprise Technologies, 6 (2 (120)), 41–50. doi: https://doi.org/10.15587/1729-4061.2022.266387*

1. Introduction

Currently, the technical support service provides support to users in services that will help troubleshoot problems with computer hardware and software. The technical support service is tasked with ensuring the availability of supported information systems and timely resolution of service interruptions. There is a certain model for resolving incidents, but it is not effective enough when many applications are received. On average, every 5th application from the number of received calls is not registered in the system. When managing incidents, many applications are not served on time, there is a problem of violation of the deadlines for resolving the incident. The presence of problems indicates an insufficient degree of efficiency in the functioning of incident management and the absence of a service-oriented approach in its organization. Currently, many enterprises are looking for an efficient and simple way to manage incidents in a quality manner, however, the only solution offered may be ready-made software offered by vendors available for a provision for a large fee and not always suitable for the actual needs of the company. Moreover, the cost of such decisions can be much higher than the financial losses of the company in case of accepting the existing risk. Stakeholders of the company are interested in a quick and convenient solution that offers the restructuring of the organizational structures of the enterprise. The relevance of this particular model is due to the lack of variability in the already existing organizational structure of modern enterprises looking for a quick and effective solution to the problem of ineffective incident management, bypassing the numerous solutions offered by vendors that require large financial costs, time and human resources for customization and adaptation, by distributing the load between the first two lines of support, and the allocation of a third line of specialists to deal with incidents that affect the performance of the entire enterprise and entail a request to change the entire infrastructure, thus using the already existing assets of the company in an optimized way. And, while process automation sounds like a good solution, not all companies can afford to use automated solutions with expensive licenses that are often charged on a per-employee basis. With the introduction of a third line of support, without attracting additional specialists, but with a competent and efficient distribution of employees already in the office, it will be possible to optimize the time for solving incidents and distribute the load evenly. Since the number of incidents is always inversely proportional to their complexity, a large number of incidents are simple user difficulties in their daily tasks: for example, forgetting an account password, being unable to connect to the corporate network, and the like, requiring little knowledge but a large amount of operational work. Also, the first level specialists will be tasked with classifying and prioritizing incidents in accordance with the regulatory matrix. Thus, second-level specialists will always receive requests within their competence and with a priority mark, and second-level specialists, with more in-depth knowledge of individual components of the infrastructure in particular, will be able to start resolving errors immediately. The specialists of the introduced third level of support will deal with incidents, the degree of impact of which is assessed within the entire infrastructure of the company and does not fall under the competence of each individual employee of the second level of support, since it affects more than a few critical infrastructure objects. Level 3 employees will be involved in a small number of complex incidents, the resolution of which requires a lot of time and knowledge. In turn, during and after the resolution of the incident, the third level specialists will be able to update the global knowledge base in such a way that, after an unprecedented event, there is a resolution plan for this incident, or at least initial support, thus, instead of escalation, employees of the third level will be able to delegate the resolution of individual incidents to employees of lower levels.

Therefore, studies that are devoted of a new support architecture are scientific relevance.

2. Literature review and problem statement

The paper [1] presents results of research on the possibility of reducing the incident processing time using machine learning algorithms, thus excluding human involvement in the classification and routing of second-level incidents. The described approach is comprehensive and can be used as a basis for global and long-term studies. But there were unresolved issues related to practical value in the short term and is not an out-of-the-box solution. The work [2] also proposes an automated search and case-based suggestion of solutions to a first-line support worker. However, the main issue is that it only provides a theoretical overview of currently available techniques without offering direct machine-based methods.

The articles [3, 4] describe the methodological aspects of responding to information security incidents can be used as the main directions and setting goals, since they contain a description of many of the best practices and government regulations, but do not offer specific mathematical models and, accordingly, experimental studies.

Mentioned in the papers [5, 6] the incident management model proposed by the world-famous and used ITIL framework will be further used as the basis for the development of the reference model. In contrast, in this article, as in the two previously mentioned, there is no sample of a real dataset for research and presentation of results.

Several of the metrics used to calculate channel occupancy (i.e., the busyness of Service Desk employees) presented in the article [7] were used as a basis for developing alternative metrics (such as response rate) considered in the study. However, in addition to the formulas presented in the article, there is no experimental confirmation of their relevance and applicability.

The paper [8] implies improving the incident management process based on the case-based approach. This study can only be used if there is a certain knowledge base and accompanying software for quick access of employees is used in the company. Even so, it cannot be applied in small businesses, since an infrastructure downtime may entail less losses than the cost of its implementation due to cost part.

Also offered for consideration are the features and functions of information security incident response systems [9]. However, the above-mentioned applications, although they offer detection and resolution algorithms, are of a very narrow focus, and mainly address incidents because of cyber-attacks on the main elements of the network infrastructure. As well, the work [10] focuses on the study of computer incidents (i. e., failures subject to automatic detection). The main impractical part of it is that it may not be applicable to improving the service of applications of end business users.

In this article [11] optimization methods are considered by introducing an information security incident monitoring system, in which a block developed by the authors for assessing the reliability of information protection tools based on current operation data is introduced. The performance of the monitoring system is evaluated before and after the start of using the improved subsystem for ensuring operability. The main disadvantage of this article is that the developed algorithm is based on implementation in ABS (automated banking systems) and may not always be applicable to the systems of enterprises in other fields of activity due to the limited field of the study.

Incident Management process model must meet the following requirements:

– ensuring the availability of channels for processing requests, excluding their loss;

– continuous maintenance of the knowledge base in up to date;

– transfer of a complex incident for further processing to an additional line support;

– exclusion of exceeding the established incident processing time (according to SLA).

All this suggests that it is advisable to conduct a study on development of the reference incident management model and related metrics to evaluate its effectiveness, that could be an ‘out-of-the-box’ solution for most enterprises, thus offloading specialists first line of support, assigning only operational work, not distracting them with non-unprecedented incidents, as well as entrusting the classification and prioritization of individual tickets, the initial collection of information from the business user, and not getting stuck on those types of tickets that require great competence and understanding of the global infrastructure and enterprise processes. A second line support person, with more in-depth knowledge of the area, will be assigned as responsible for the incident, operating exactly within their area, to which the incident will be assigned precisely through classification, and also work according to the priority assigned by the first line person. The third line support employee will deal with incidents that caused the entire system to fail and for which there will be no possibility of correction through the operational work of the first line or the basic knowledge of the second. After the incident is resolved by the third line employee, the knowledge base will be updated by it, introducing the relevant document, the wild narrative and the procedures necessary for resolving, so that in subsequent incidents the problem can be solved by the first and second line specialists. The analysis of the shortcomings of the existing model made it possible to formulate the requirements for building a three-level model of the incident management process.

3. The aim and objectives of the study

The aim of the study is improving the quality of the incident management process through the implementation of a new reference model.

To achieve this aim, the following objectives are accomplished:

– to develop of support architecture with the recommendations and best practices described in widely used standards and frameworks;

– to confirm the relevance and effectiveness of the proposed model experimentally, using programming platform MATLAB and sampling of incidents with associated attributes using the considered metrics.

4. Materials and methods

The object of the study is the incident management. The hypothesis of the study is the assumption that by changing the architecture of the incident management process, it is possible to improve the quality of it. It will increase the correctness of the operability and availability of the system, thereby reducing the risks of incurring losses.

To simplify the work, some tools were adopted to help in the analysis and calculations. These tools were BPMN notation, which contributes to the visual representation and accurate understanding of a business process in a company. Additionally, with the use of MATLAB it was possible to create a computation code and eliminate manual calculations of a large amount of data.

In this study, the business process modeling methodology, namely the BPMN notation is used, which allows to design the company's business processes and provides the capability of understanding their business procedures in a graphical. Its purpose is to model ways to improve efficiency, account for new circumstances or gain competitive advantage. The approach of building processes' functional models of AS-IS and TO-BE is used. Analysis of AS-IS functional model gives opportunity to understand where the weakest points are, what will be the advantages of new business processes. The shortcomings found in the AS-IS model can be corrected by creating the TO-BE model – a model of a new organization of business processes. The TO-BE model is needed to assess the impact of implementing an information system and analyze alternative ways of doing work and documenting how the system will function in the future. The AS-IS model is an "as is" model, i. e. model of an already existing process. The construction of a functional AS-IS model allows to clearly fix what information objects are used when performing functions of various levels of detail. Based on the analysis of the current processes of the information training system, the following AS-IS model was created, which allows to identify and systematize the processes that occur in this system during its operation. It should be noted that the TO-BE model reflects those useful features that will allow to successfully implement and organize the process.

To check the adequacy of the model, using the MATLAB tool and its standard libraries, a program code was written that contains variables reflecting the proposed metrics to study the relevance of the proposed solution. The MATLAB environment allowed to do calculations for a large volume of input data, eliminating the possibility of making manual errors.

The resolution was simulated in the AS IS and TO BE models, on the same set of input data, which contains the parameters of the considered incidents.

Theoretical research methods, such as analysis and comparison, were also used to evaluate the result obtained. Thus, the coefficients that determine the effectiveness of the proposed solution i.e. models were measured before and after its theoretical implementation in the business processes of the enterprise, i.e. a comparative analysis of the indicators of the AS IS and TO BE models was carried out.

To evaluate the effectiveness of the resulting structure, let's provide metrics based on the speed and time of incident resolution, which is relevant, compared to the reference dictated by the SLA (that is, the requirements of business users regarding what downtime or inefficient system operation they consider acceptable). Further, for the subsequent evaluation and interpretation of the obtained results, it is possible to guide by the ITIL standards library, which indicates that in a company whose incident management process can be called effective, more than 80 % of incidents were resolved successfully and in a timely manner. In this case, it is possible to conclude that the proposed model is effective and has not only theoretical, but also practical benefits.

5. Results of theoretical and experimental research

5. 1. Development of a three-level incident management model

One of the most important tasks of improving the IT infrastructure of an enterprise is to increase the efficiency of the incident management system. In addition, the work of the technical support service is organized using various automated systems.

Automation of the technical support service currently consists in receiving many requests from various sources: e-mail, web forms from sites, receiving and registering calls by phone, receiving memos, through the user's personal account and using the self-service portal.

All received appeals are made out by the operator in applications. Work with applications is carried out according to a certain algorithm, which is generally the same in all technical support services.

When analyzing the incident management reference model (Fig. 1), the following shortcomings were identified:

– formation of a queue on the line with a large flow of calls (applications);

– limited time for consultation and processing of calls by operators, registration and classification of calls takes a lot of time;

– insufficient number of operators with a large flow of applications, workload of operators;

– unstructured Knowledge Base and its untimely updating. When trying to provide initial support, it is extremely difficult to navigate the unstructured Knowledge Base on the subject of consultation;

–transfer of the incident to the 2^{nd} level of support without its resolution at the 1^{st} level.

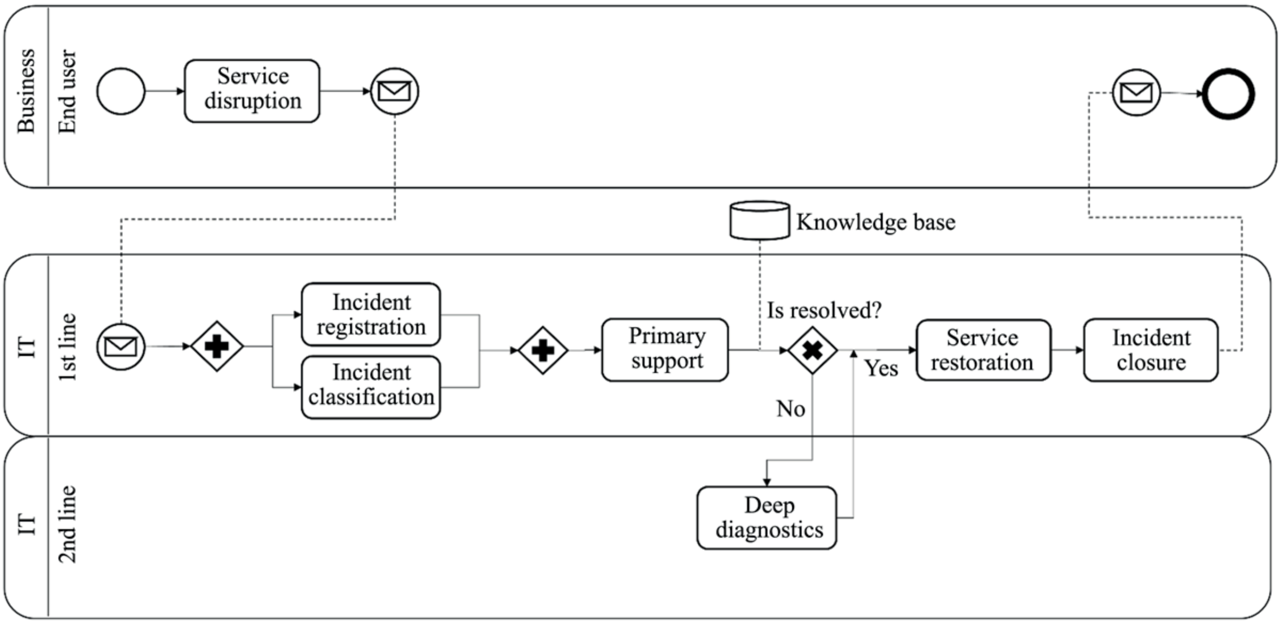


Fig. 1. 'AS-IS' incident management model

In most cases, the problem of routing most calls to the second line is due to the limited time to search for an answer in an unstructured Knowledge Base. The emergence of a queue of unhandled incidents on the 2nd support line. A large percentage of incidents directed to the 2nd line is a negative and extremely low indicator of the quality of the work of the first line of support, which should close at least 80 % of all incoming calls.

A fairly large number of studies have been devoted to the problem of improving the efficiency of the incident management process.

Thus, in the work, a set of models, algorithms and software tools based on the ITIL library is proposed, which provide an increase in the efficiency of processing requests received by the technical support service due to the rational distribution of personnel for work and prioritization of user requests.

The issues of improving the quality of incident resolution are analyzed, mathematical models and methods of incident management are presented a mathematical model that describes the dependence of the number of calls on the number of jobs served.

To assess and control the quality of IT services, it is proposed to consider service performance indicators, such as the percentage of missed calls for the period, the percentage of resolved incidents for the period, the average number of applications for the second support line for the period and the average number of applications for the period for one employee of the second support line. Analysis of the results of research in the field of incident management in the enterprise information system showed that the existing models of the incident management process do not fully meet the requirements.

The BPMN-notation of the typical incident management model (Fig. 1) is based on a two-level incident processing system, including the 1st support line, on which the incident is registered, the problem is classified, and the initial support stage is implemented. If the issue is resolved during initial support, then the incident is closed. If it is impossible to resolve the incident within the first line of support, the incident is sent to the second line of support. The second line engineers investigate the problem more deeply, diagnose the malfunctions and send the result to the first line for closure. If the problem could not be solved on the second line of technical support, then the problem is sent for a deeper investigation and diagnostics, and the first line informs the user about this [7].

Thus, in the incident management model, the output is a message to the user about the restoration of the service, a record of the incident and a record of the problem that has occurred are saved. At the same time, statistics are accumulated in the knowledge base: the number of open incidents sorted by priority, by elapsed time, by working groups; the number of incidents resolved on each support line; average time to resolve an incident in a working group; average service recovery time, the percentage of incidents resolved within the deadline, etc.

In view of the foregoing, the task of developing a model of the incident management process has been formulated, which should ensure an increase in its effectiveness. For this purpose, the necessity of using a set of relevant metrics is justified, such as the speed of eliminating incidents; user satisfaction with the quality of IT support; the level of availability of call processing channels. To provide a more flexible incident handling process, the developed incident management process model includes an additional support line that provides processing of complex incident, which imply requests for infrastructure changes and communication with software and hardware vendors i.e. failures that have critical and blocking priorities, which can result in large financial risks, a drop in the level of service, availability, and operability service.

The incident and user request management process are the most mature management practice in many modern IT organizations. For many managers, it is one of the main sources of numerical information about the quality of user support, the quality of services provided, and the workload of staff and resources.

The purpose of the process is to ensure the quality of IT services by resolving incidents as quickly as possible and responding to service requests in a timely manner.

The main feature of the incident and user request management process, which directly and quite significantly affects its measurement, is functional escalation. Functional escalation is the transfer of a certain task from one functional group to another, which has a higher competence, technical or other capabilities to solve this problem. Within the framework of the process under consideration, such tasks, of course, are incidents and user requests. This means that one incident or request can be processed sequentially by several teams, and the final success is the sum of the actions of many specialists.

Tidying up almost always involves the creation of a system of metrics and indicators aimed at measuring and controlling the management processes, the services provided and the IT systems that underlie these services.

3 measurement problems – obsession with measurements, poor quality of measurement and evaluation systems, as well as the lack of a unified system, "patchwork" evaluation. It does not allow drawing conclusions about the operation of a complex of processes, does not give an idea about the health of the IT service.

Measurement is the quantified reduction in uncertainty based on one or more observations. A metric is a technically or procedurally measured value that characterizes the control object. IT processes enable the efficient use of information technology to meet customer needs. Efficiency here means that: information technology creates value for customers (delivers value by increasing the productivity of business processes and/or reducing the constraints on these processes), the costs of information technology are rational and controlled, and the risks associated with the use of information technology are also controlled and reduced to an acceptable level.

Measurement and evaluation of IT processes is carried out in the interests of two main stakeholder groups – Investors, customers, senior management, external regulators are interested in the extent to which the IT management system solves the set tasks (effectiveness), whether and how management mechanisms are provided to ensure the proper level of control and system changes in response to new requirements (compliance), IT managers is interested in the current state of processes in terms of the content and results of activities, as well as the amount of work (productivity) and the rationality of the use of resources (rationality).

Efficiency shows how a given process (or a group of interrelated processes) meets its purpose and achieves its goals. The purpose determines the role of processes in the management system, that is, the answer to the question "why is this process needed, what is it responsible for." The purpose of the process, as a rule, is universal, that is, it changes little from company to company. The formulations can be found in standards and codes of knowledge (COBIT, ITIL, ISO 20000).

The effectiveness of the processes is ensured through the use of the organization's resources spent on the execution of processes and the provision of control. Rationality metrics characterize the number of errors that occur during the execution of the process, as well as the use of various cost reduction mechanisms. The basic principle of ensuring and evaluating the rationality of the management system: the cost of owning the management system and its control should not exceed the value generated as a result of the operation of this system, taking into account-controlled risks.

Productivity metrics characterize the amount of work on the execution and control of the process. For example, when designing a change management process, it is important to understand what kind of change flow is expected before writing into a process schedule. For example, an increase in the flow of incidents due to the unsuccessful implementation of a new IT system can significantly reduce the value of a performance metric.

Compliance metrics, primarily of interest to stakeholders external to the process, also often include an assessment of the implementation of the purpose and key practices of the process. The maturity of the IT management system is usually assessed. It is expressed, first, in the levels of formalization and control that apply to a particular activity. It is important to note that a certain level of maturity characterizes not the activity itself, but the management practice that applies to it: process maturity is a characteristic that allows to assess how carefully and formally the activities included in the process are controlled; the maturity of the management system or the maturity of the organization characterizes the control practices operating in the organization in relation to processes.

The measurement allows: to ensure the reliability of the assessment of the current state of the control object; increase the reliability of the forecast of possible improvements; monitor the implementation of decisions made; more accurately and comprehensively evaluate the effect of the implementation of the decisions taken. Measurement, however, is not capable of drawing conclusions and making decisions. The measurement results are not valuable in themselves, but only provide information for processing. And if the report intended for decision-making, in addition to the measurement results, does not contain analysis, conclusions and suggestions.

To improve the efficiency of the incident management process in accordance with the COBIT methodology and the ITIL library, various metrics are used, which must comply with the principles of SMART (that is, be specific, measurable, achievable, relevant and tied to a certain interval of time. Metrics, which are quantitative measures of the degree of achievement by processes their goals, allow to evaluate the quality of the incident management process, the ability to achieve planned results and, as a result, evaluate their effectiveness.

The papers consider the classification of metrics with reference to the components of the information system. An analysis of the metrics presented in the COBIT methodology and the ITIL library showed that many of the existing metrics correspond to the following main classes of information system objects: infrastructure, processes, and services. In accordance with this classification, they distinguish technological (metrics of components and applications, such as performance, availability, etc.), process (reflect the efficiency of the functioning of internal IT processes) and service metrics (reflect the quality-of-service provision, parameter values agreed in SLA).

To build a model of the incident management process and determine the most significant (relevant) metrics of the process under consideration, the fact is taken into account that the goal of the incident management process is the guaranteed reactive elimination of the latter, an important indicator of which is the speed of response to the incident. It allows to quantify the time spent on the first and second line of support during registration, classification, consulting, routing, detailed analysis of the incident, access to the knowledge base, etc.

In addition, one of the important indicators is the timeliness of processing requests from users (this is especially important for the end customer of an IT service). As an indicator of the quality of service on the part of the user, a metric is used – an assessment of user satisfaction with the quality of IT support. This metric allows to quantify how convenient and fast the assistance was provided to the end user – the customer of the service.

The incident management process model should meet the following requirements:

– ensuring the availability of channels for processing requests, excluding their loss;

– continuous maintenance of the knowledge base up to date;

– transfer of a complex incident for further processing to an additional support line;

– exclusion of exceeding the established deadlines for processing an incident.

The 3rd support line was introduced into the architecture of the model for unloading specialists of the 1st and 2nd support lines, which provides the solution of complex incidents that require additional resources for this. This is shown in Fig. 2.

The input data in the model are user requests about service interruptions and failures. Appeals come to the first line of support, which receives, registers, classifies, prioritizes incidents, and provides initial consultation. Channels through which requests are received on the first line: phone, voice message, email, social networks, instant messengers, feedback forms through the website or through the mobile application.

Support lines use a single knowledge base that is updated in real time. In the absence of a solution in a single knowledge base and the impossibility of providing an initial consultation, the first line routes incidents to the second line of support.

On the second line of support, incidents are resolved, and their detailed analysis is carried out. New solutions obtained during the analysis of the incident are added to a single knowledge base and are available to all support lines for subsequent consultations on similar incidents. If an incident cannot be resolved at the level of the second line of support, it is routed to the third line of support.

The third line of support is monitoring errors, processing complex incidents, failures that have critical and blocking priorities, which can lead to large financial risks, and a drop in the level of serviceability.

5. 2. Experimental confirmation of the relevance and effectiveness of the proposed model

Under the conditions of a sufficiently large flow of requests from users, considering the failures that occur, it is necessary to ensure the guaranteed availability of the channels for processing requests, or to minimize (reduce) the probability of denial of service using the metric of the same name [9].

The property of the incident management process is such that all participants in the incident handling process contribute to the speed of solving the incident.

Metric coefficient K_1 calculated as follows:

– if the incident is handled in a timely manner, R_{ij} and W_{ij} are equal to 1;

– if the incident is overdue, and the j-th line processed it longer than the full processing time T_i, rating R_{ij}=0, weight W_{ij} more than 1 is proportional to the processing time in the line;

– if the incident is overdue, but the j-th line processed it, for example, within half the time, weight W_{ij}=1, rating R_{ij}=0.5;

– if any line processed the overdue incident within a short time and, therefore, is unlikely to significantly affect its delay, the coefficient K_1 for this line will be very small.

To measure this metric, taking into account number of support levels (1) is used:

$$K_1 = \sum_i \left(W_{ij} \times R_{ij}\right) / \sum_i W_{ij}, \tag{1}$$

where R_{ij} – processing rate of the i-th incident in the j-th line, determined by the (2):

$$R_{ij} = \begin{cases} 1, \text{ if the incident is processed on time,} \\ 1 - \dfrac{t_{ij}}{T_i}, \text{ if the incident is overdue.} \end{cases} \tag{2}$$

Thus, the more incidents were resolved on time, the closer the value of the variable is to 1, and the more time spent on resolving the incidents, relative to the set by the business, the closer the value of R_{ij} to 0.

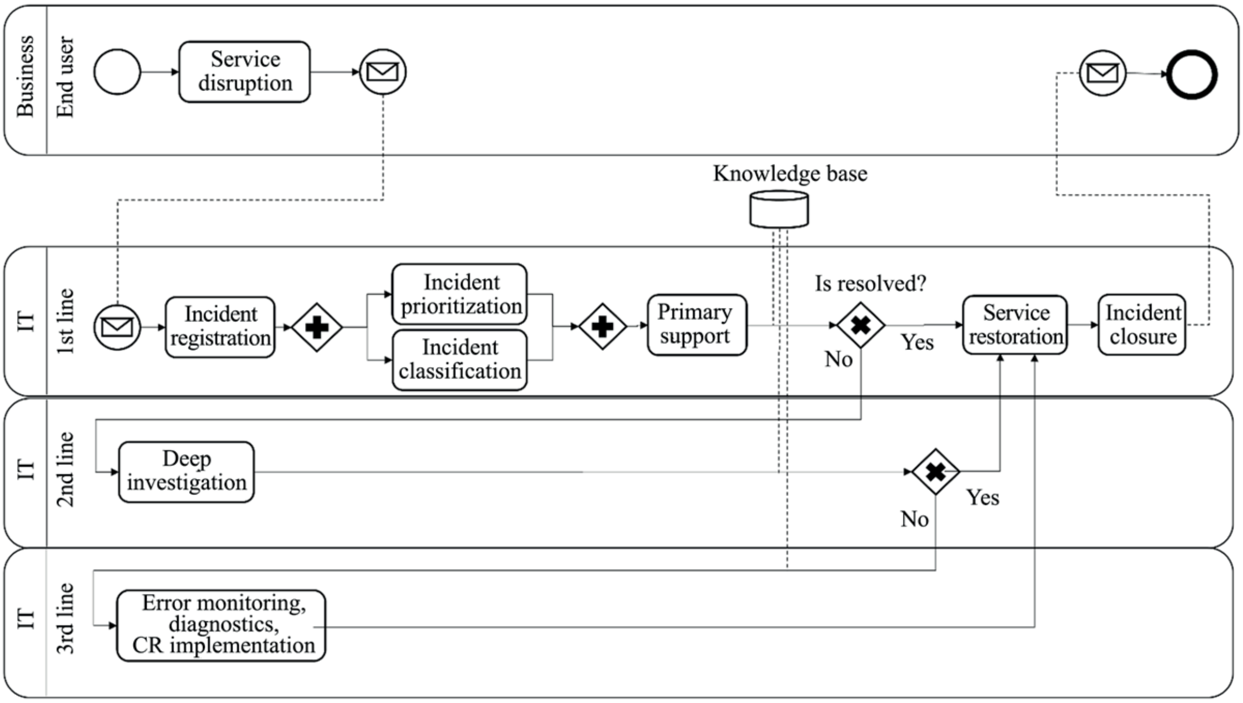


Fig. 2. 'TO BE' three-level incident management model

W_{ij} – the weight of the i-th incident in the j-th line, determined by the (3):

$$W_{ij}=\begin{cases}1, \text{ if } t_{ij}\le T_i,\\ \left(\dfrac{t_{ij}}{T_i}\right)^n, \text{ if } t_{ij}>T_i.\end{cases} \qquad (3)$$

In (2), (3) t_{ij} – processing time of the i-th incident in the j-th line, T_i – maximum processing time of the i-th incident determined by SLA requirements, n is a natural parameter of the algorithm, usually equal to 1.

To measure user satisfaction with the quality of IT support, satisfaction is assessed immediately before the closure of the resolved incident, as a rule, it is provided by means of the web interface of the ITSM process automation system or by phone – the user is asked to rate how satisfied it is with the support provided to it on some point scale.

It is convenient to present a numerical assessment of user responses (obtained both when closing their incidents and as a result of conducting a survey) on an arbitrary integer scale as follows, using (4):

$$K_2=\frac{M-M_{\min}}{M_{\max}-M_{\min}}, \qquad (4)$$

where M – average score for customer responses, $M_{\max}$ and $M_{\min}$ – minimum and maximum scores on a rating scale (for a 5-point scale $M_{\max}$=5 and $M_{\min}$=1).

The approach considered in the paper is used to determine the accessibility metric for call processing channels. The process of users contacting the technical support service can be represented by a queuing model that allows to determine the minimum number of channels for processing calls, in which the probability of denial of service does not exceed a given value. The quantitative assessment of the probability of denial of service is determined by the (5):

$$P_{den.}=\frac{p^i}{i!}\times p_0; i=1,2,\ldots n, \qquad (5)$$

where $P_{den.}$ – the probability of denial of service of the call, $p^{\,i}$– the load factor of the channels for receiving calls, determines the average number of incoming calls coming for the average service time of one call, i – number of calls, p_0 – denial of service probability when the system is in states S_1, S_2, ..., S_i. Probability p_0 can be calculated using the (6):

$$p_0=\left(1+p+\frac{p^2}{2!}+\ldots+\frac{p^i}{i!}\right)^{-1}; \; i=1,2,\ldots n. \qquad (6)$$

The analysis of the shortcomings of the existing model made it possible to formulate the requirements for building a three-level model of the incident management process.

The metrics discussed above made it possible to obtain objective comparative estimates of the performance indicators of the incident handling process at all stages of its life cycle using the existing and developed model.

Using the MATLAB compiler, the following algorithm was written using the formula given in the section above. The input data is the sample of incidents registered in a business enterprise, that can be provided upon special request.

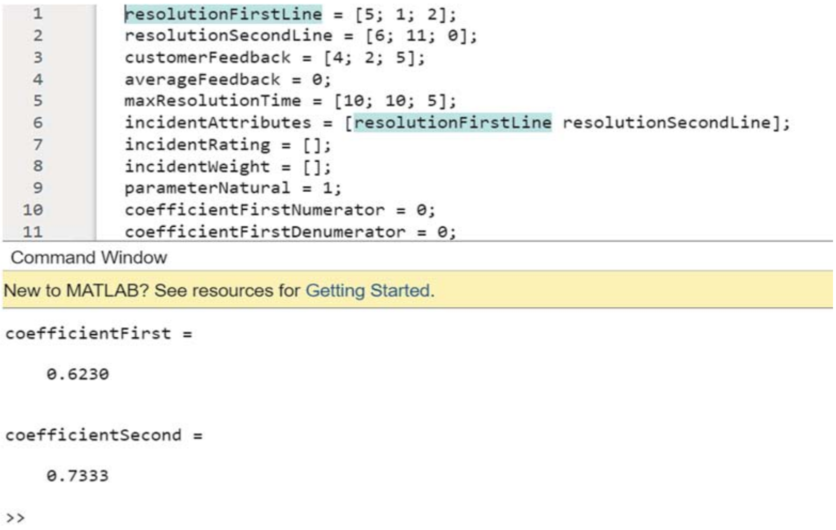
In this example, the variables resolutionFirstLine and resolutionSecondLine are used, symbolizing the resolution time of three incidents in hours for the first and second lines.

As a result of the calculations, it was obtained that the coefficient K_1, which is the response rate to the incident is 0.62, and K_2, the degree of satisfaction of the employees who asked for help is 0.73 within the framework of the application of the two-level help desk model. This is shown in Fig. 3.

To adapt this algorithm to a three-level model, the variable resolutionThirdLine was introduced, which symbolizes the time of resolution of the incident at the third level of the support service. The following part of the code has also been changed to consider the new variable in the denominator of the formula for calculating the first evaluation coefficient.

The resolution time at the second level as an experiment was equally divided into the second and third lines.

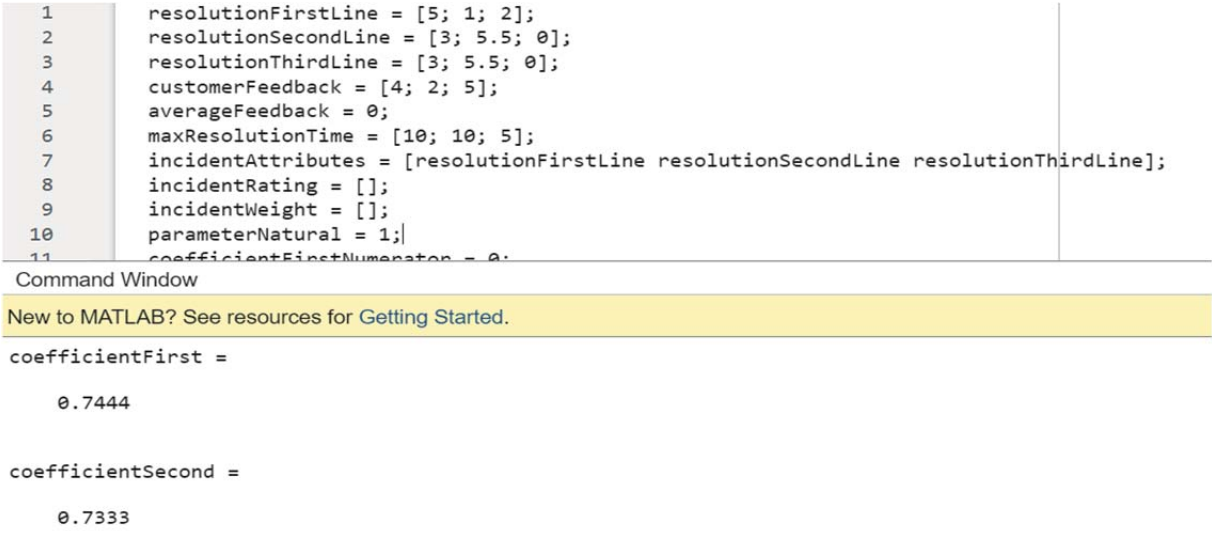
As a result of the calculations, it was determined that coefficient K_2 has not changed (due to saving the input data and the algorithm), and the coefficient K_1 which is the rate of response to an incident increased to 0.74 (increased by 12 %) as part of the application of a three-level help desk model. This is shown in Fig. 4.



```
resolutionFirstLine = [5; 1; 2];
resolutionSecondLine = [6; 11; 0];
customerFeedback = [4; 2; 5];
averageFeedback = 0;
maxResolutionTime = [10; 10; 5];
incidentAttributes = [resolutionFirstLine resolutionSecondLine];
incidentRating = [];
incidentWeight = [];
parameterNatural = 1;
coefficientFirstNumerator = 0;
coefficientFirstDenumerator = 0;
```

```
coefficientFirst =

    0.6230


coefficientSecond =

    0.7333

>>
```

Fig. 3. Calculation of coefficients of response rate and degree of satisfaction in a two-level model



```
resolutionFirstLine = [5; 1; 2];
resolutionSecondLine = [3; 5.5; 0];
resolutionThirdLine = [3; 5.5; 0];
customerFeedback = [4; 2; 5];
averageFeedback = 0;
maxResolutionTime = [10; 10; 5];
incidentAttributes = [resolutionFirstLine resolutionSecondLine resolutionThirdLine];
incidentRating = [];
incidentWeight = [];
parameterNatural = 1;
coefficientFirstNumerator = 0;
```

Command Window

New to MATLAB? See resources for Getting Started.

```
coefficientFirst =

    0.7444


coefficientSecond =

    0.7333
```

Fig. 4. Calculation of coefficients of response rate and degree of satisfaction in a three-level model, given that resolution time is evenly distributed between 2nd and 3rd line

Also, calculations were made for data in a situation where the third support line was introduced; however, the incident was prematurely resolved at the second support level. In this case, the resolution time at the second level remains equal to the initial data, and on the third line it is equal to zero:

– resolutionSecondLine=[6; 11; 0];

– resolutionThirdLine=zeros(3,1).

In this case, by the comparison of the coefficient K_1 obtained in Fig. 4 and Fig. 5, it can be determined that it has changed slightly, by 0.03 and also remained equal to 0.74, meaning the model proposed is also applicable for non-complex incidents.

For further research, a larger number of incidents, namely 15 cases, was taken. The aim was to study how the coefficient K_1 varies depending on the total number of cases considered, since when applying this algorithm in a productive environment of an enterprise system, the input data would be a huge number of rows – registered incidents.

For the test within the two-level model, 15 incidents were taken with the following resolution attributes:

– resolutionFirstLine=[6; 1; 6; 8; 1; 0; 0; 4; 4; 8; 2; 3; 1; 1; 0];

– resolutionSecondLine=[4; 5; 0; 3; 0; 2; 2; 1; 4; 5; 2; 6; 2; 0; 3].

And for the test within the framework of the three-level model, the following are:

– resolutionFirstLine=[6; 1; 6; 8; 1; 0; 0; 4; 4; 8; 2; 3; 1; 1; 0];

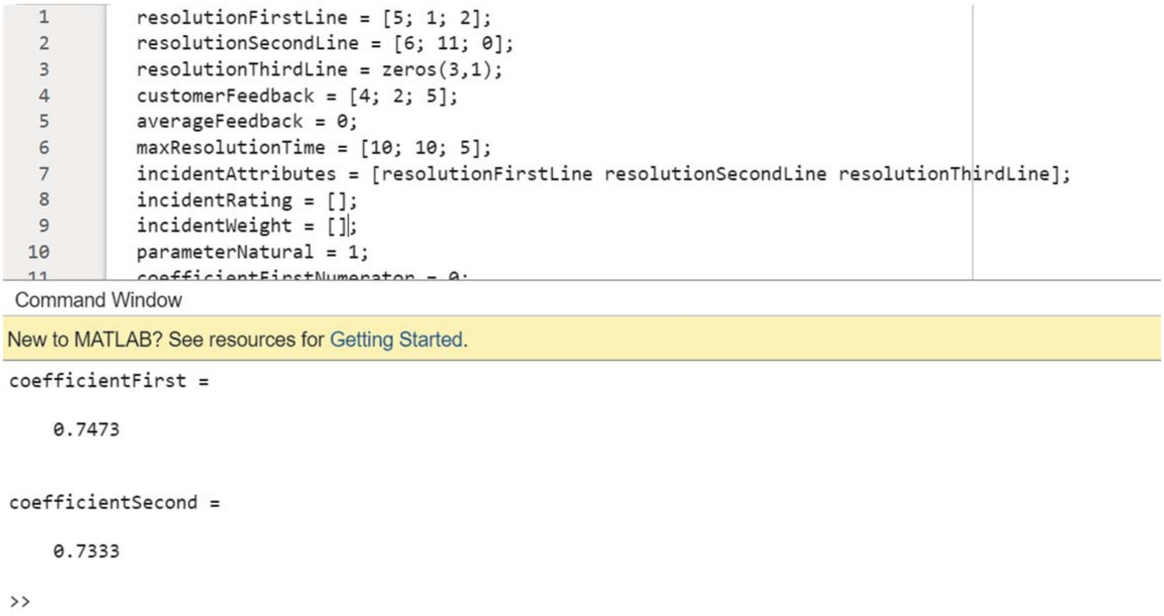
– resolutionSecondLine=[2; 2.5; 0; 1.5; 0; 1; 1; 0.5; 2; 2.5; 1; 3; 1; 0; 1.5];

– resolutionThirdLine=[2; 2.5; 0; 1.5; 0; 1; 1; 0.5; 2; 2.5; 1; 3; 1; 0; 1.5].

Or:

– resolutionSecondLine=[4; 5; 0; 3; 0; 2; 2; 1; 4; 5; 2; 6; 2; 0; 3];

– resolutionThirdLine=zeros(15,1).



```
resolutionFirstLine = [5; 1; 2];
resolutionSecondLine = [6; 11; 0];
resolutionThirdLine = zeros(3,1);
customerFeedback = [4; 2; 5];
averageFeedback = 0;
maxResolutionTime = [10; 10; 5];
incidentAttributes = [resolutionFirstLine resolutionSecondLine resolutionThirdLine];
incidentRating = [];
incidentWeight = [];
parameterNatural = 1;
coefficientFirstNumerator = 0;
```

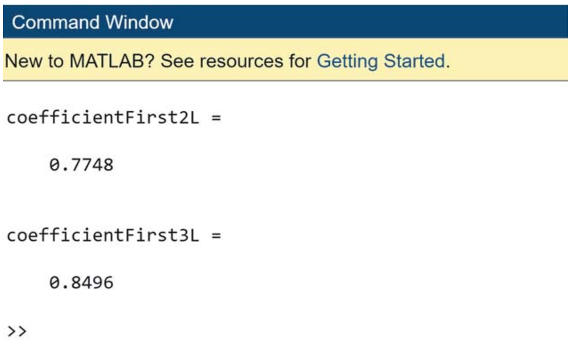
Command Window

New to MATLAB? See resources for Getting Started.

```
coefficientFirst =

    0.7473


coefficientSecond =

    0.7333

>>
```

Fig. 5. Calculation of coefficients of response rate and degree of satisfaction in a three-level model, given that resolution time is not evenly distributed between 2nd and 3rd line

According to the results of the calculations, in the first case K_1 equals to 0.7748 (i. e. 77 %) and in the second case, regardless of the uniformity of the resolution time distribution between the existing second and proposed third support lines, it increased by 0.0748, (i. e. 7.5 %) and is equal to 0.8496 (i. e. 85 %) (Fig. 6).



Command Window

New to MATLAB? See resources for Getting Started.

```
coefficientFirst2L =

    0.7748


coefficientFirst3L =

    0.8496

>>
```

Fig. 6. Comparison of response rate values in a two- and three level incident management models

Since the company suffers multimillion-dollar losses due to downtime of financial reporting systems [11], let's calculate the company's expenses according to the following formula (7):

$$D=(Y/B)*I*H, \tag{7}$$

where Y – gross annual income, B – total business hours per year, I – percentage impact (as a decimal), H – number of idle hours.

Let's took the following values, obtained by special request, which are actual indicators of the company in 2021: gross annual income is 984 893 578 Kazakhstani Tenge, total business hours are 1968, percentage impact as a decimal is 0.01 (1 % as stated in SLA requirements of the company).

For H in two cases (as 2-level and 3-level support architecture model), let's use the formula (8):

$$H=D*(1-K_1) \tag{8}$$

where D – maximum possible downtime of systems, K_1 – incident response late.

Since the D for the company is equal to 200 hours, the H_{2L} for a two-level model (K_1=77 %) will be equal to 46, and H_{3L} for a three-level model (K_1=85 %) will be equal to 30. Using our initial formula (7), it is possible to calculate losses the company incurred in case of loss during the implementation of a two-level models is 23 114 849 and when implementing a three-level 15 074 901.

Also, let's took into account the increase in salaries for employees providing third-level technical support. Let's took the average hourly rate for first- and second-line support employees, as indicated in online job search resources (1000 tenge per hour for 1st line employee and 1500 tenge per hour for 2nd line employee), as well as the average rate for employees with 6+ years of experience as employees with deep knowledge, i.e. possible third line support staff (3200 tenge per hour). Since the company already has 8 employees of the first line and 6 employees of the second line, let's calculate that the amount of their salaries per year will be 44 100 000. Since the number of support employees decreases by about 2 times compared to the previous level of support, let's divide 6 employees for 4 employees of the second line of support and 2 employees of the third line of support, whose salary will be increased accordingly. Thus, the sum of their salaries will be 49,784,000.

Summing up company losses as downtime and payroll costs for first- and second-line support employees in a two-tier incident management model (67,214,849) will always be greater than company losses and payroll costs in a three-tier model (64 858 901), regardless of the change in SLA and downtime hours, and the additional profit will be equal to 2 355 948 tenge.

6. Discussion of experimental results of development a three-level support architecture model

As part of the aim of the study, a reference incident management model (Fig. 2) was developed that meets the requirements of the ITIL (library of books on IT infrastructure best practices and related activities to promote, certify and apply these practices). These practices are:

– ensuring the availability of channels for processing requests, excluding their loss;

– keeping the knowledge base up to date;

– transfer of a complex incident for subsequent processing to an additional support line;

– exclusion of exceeding the established deadlines for processing the incident.

Accordingly, the constructed model complies with the above recommendations, which indicates the effectiveness of its implementation within the enterprise.

The proportion of incidents resolved within the time limits established by the SLA was obtained. Based on the results obtained (Fig. 6), it is possible to prove that the incident resolution rate was increased when simulating in the three-level model (85 %). Compared to the speed in the two-tier model (77 %), the score increased by 8 %, and exceeded the response rate, set by ITIL (80 %). In this case the company's incident management process is considered to be business-friendly and effective. Additionally, the practical benefit was calculated of a company that suffered less losses due to system's downtime in three level model (64,858,901 tenge), compared to two level model (67,214,849 tenge). It was achieved as a result of the implementation of the new proposed model, and company's expenses in the incident management process decreased by 2 355 948 tenge.

Thus, a rational distribution of resources is possible, separating the third line of support, those who are responsible for incidents involving changes in infrastructure and communication with vendors. As a result, the first and second lines of support are freed from tasks in which they are not competent specialists. And with the successful resolution of an unprecedented incident, the database is updated and the resolution is delegated to more junior specialists in the future.

The limitations of the study are dictated by the model used as the initial one, which was presented as a collective image of those processes that are used in most enterprises of our time, but is not and cannot be unified, due to the diversity of business areas of different enterprises, so the proposed three-level model cannot be a solution for those enterprises that do not use the two-level model taken as the source. The disadvantages of this study are conditioned by the metrics used. In addition to resolution time and end user evaluation, incident attributes can also be the severity and extent of the incident, and some others that are not used in the set of input data and are not considered in this study. The scientific community can also base their further research on the proposed model by, for example, adding additional layers of support or incorporating into the model a knowledge base using machine learning algorithms to further increase the speed of processing incidents, or classification and prioritization algorithms with elimination of necessity of the first level of support and so on. The main difficulties that can be encountered is the heterogeneity of the system for logging incidents and their attributes, in order to build a single, consolidated and applicable to all cases incident resolution model.

7. Conclusions

1. The new architecture was proposed, adding a third level of incident resolution, which allowed to allocate an additional type of resources for addressing the most complex incidents. Thus, the first two levels of support were eliminated from handling problems that cannot be quickly resolved in an adequate time frame and leaving them the responsibility to perform operational work.

2. Time and labor costs were reduced, namely: the overall rate of response to an incident increased by 8 %, following the commissioning of the third support line. Since the values of the obtained response rate coefficients after applying the three-level model eliminated the gap (from 77 % to 85 %), it is possible to conclude that the proposal about the performance of the solution is correct, and the model has practical value. Since the resulting value (85 %) exceeds the requirements (80 %) of the ITIL standard library for the incident management process, the quality of incident management was improved by increasing the speed of incident resolution. It was achieved without introducing automation and attracting new employees, but by optimally distributing tasks in accordance with responsibilities and competencies among existing specialists. Additionally, the economic effect has been determined with third level implementation according to the reference model, as the company’s expenses suffered less losses.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed without financial support.

Data availability

Data used to conduct the experiment is a sample of incidents registered by the enterprise technical support service and can be provided upon special request.

References

1. Nikulin, V., Shibaikin, S., Sokolova, M. S. (2022). Application of machine learning techniques for automated classification and routing in ITIL library. Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics, 2022 (1), 42–52. doi: https://doi.org/10.24143/2073-5529-2022-1-42-52
2. Blinnikova, A. V., Nesterova, Ju. O. (2020). Incident management in ITSM using artificial intelligence. Vestnik Universiteta, 6, 36–40. doi: https://doi.org/10.26425/1816-4277-2020-6-36-40
3. Loginova, A. (2021). An overview of regulatory sources and practices of information security incidents management. The Herald of the Siberian State University of Telecommunications and Informatics, 1, 50–59. doi: https://doi.org/10.55648/1998-6920-2021-15-1-50-59
4. Mayorova, E. V. (2020). Methodological Aspects of Responding to Information Security Incidents in the Digital Economy. Petersburg Economic Journal, 1, 155–164. doi: https://doi.org/10.25631/PEJ.2020.1.155.162
5. Palilingan, V. R., Batmetan, J. R. (2018). Incident Management in Academic Information System using ITIL Framework. IOP Conference Series: Materials Science and Engineering, 306, 012110. doi: https://doi.org/10.1088/1757-899x/306/1/012110
6. Serikbayeva, S., Tussupov, J., Sambetbayeva, M., Yerimbetova, A., Sadirmekova, Z., Tungatarova, A. et al. (2021). Development of a model and technology of access to documents in scientific and educational activities. Eastern-European Journal of Enterprise Technologies, 6 (2 (114)), 44–58. doi: https://doi.org/10.15587/1729-4061.2021.248506
7. Sembina, G. (2022). Building a Scoring Model Using the Adaboost Ensemble Model. 2022 International Conference on Smart Information Systems and Technologies (SIST). doi: https://doi.org/10.1109/sist54437.2022.9945713
8. Ocheredko, A. R., Bachmanov, D. A., Putyato, M. M., Makaryan, A. S. (2021). Research of IRP systems based on the analysis of mechanisms of response to information security incidents. CASPIAN JOURNAL: Control and High Technologies, 53 (1), 74–82. doi: https://doi.org/10.21672/2074-1707.2021.53.1.074-082
9. Avramenko, V. S., Malikov, A. V. (2020). Procedure of diagnosis security computer incidents in automated special purpose systems. H&ES Research, 12 (1), 44–52. doi: https://doi.org/10.36724/2409-5419-2020-12-1-44-52
10. Muromtsev, D. Yu., Popov, S. V., Shamkin, V. N. (2020). Improvement of the Information Security Subsystem in the Bank Information Security Monitoring System. Vestnik Tambovskogo Gosudarstvennogo Tehnicheskogo Universiteta, 26 (2), 176–187. doi: https://doi.org/10.17277/vestnik.2020.02.pp.176-187
11. Understanding the Cost of IT System Failure to Your Business. Available at: https://blog.power-net.com.au/blog/understanding-the-cost-of-it-system-failure-to-your-business