Risks Prediction for Artificial Intelligence Systems Using Monitoring Data

Andrey Kostogryzov
Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences
Moscow, Russia
e-mail: Akostogr@gmail.com

***Abstract*—The approach for cognitive processing of monitored data is proposed. An application for artificial intelligence systems (AIS) allows to use the possibilities of probabilistic modeling. There are described the models and methods for prediction a probability of "success" and/or a risk of "failure", software tools to support them, techniques for solving the problems of rationale preventive measures against threats and effective risk control. The approach means practically a proactive commitment to excellence in uncertainty conditions. A suitability of the proposed models and methods is demonstrated by some practical examples.**

Keywords—analysis, control, model, probability, risk, safety, system

I. INTRODUCTION

Today global trends in the development of modern systems for various functional purposes indicate the need for a radical turn from "manual" control of certain types of safety, based on the implementation of established instructions and expert estimations of emerging situations, to the implementation of proactive measures based on prediction. This allows, on the basis of a prognostic look ahead, to proactively take effective managing actions. This idea runs like a red line through all world concepts and the latest standards of systems engineering. But how to do it remains behind the scenes. There is no universal approach to the implementation of this idea yet. In search – all the leading countries of the world. Special hopes are connected with the use of AIS. Here AIS are understood as systems, operating in uncertainty conditions by logic reasoning on the base of processing the monitored data. In AIS practice there are often used subjective expert estimations (for AIS training), a regression analysis of collected data, a simulation of processes [1-9]. It means, that search of new methods for rationale AIS operation is very important.

Note. System is combination of interacting elements organized to achieve one or more stated purposes (according to ISO/IEC/IEEE 15288).

This paper focuses on applications that are critical from the point of view of safety depending on the structural complexity of systems, formal conditions of uncertainty, implemented methods of countering threats, as well as the conditions of elements operation. Available probabilistic methods in cognitive processing of monitored data are proposed. As a result the predicted probability of "success" or risk of "failure" is produced. The inputs for modeling are monitored data from current and previous states of compound elements.

The proposed ideas, models and methods are designed to implement feedback to rationale requirements and conditions that guarantee the non-exceeding of the specified acceptable risks. The proposed probabilistic approach develops the established probabilistic approaches [10-36], applicable where there is some similar repeatability of events.

II. THE ESSENCE OF THE PROPOSED APPROACH

The monitored system may itself be a system of interest for analysis (for example, a dispatching intelligence center) or may be part of another, more comprehensive system of interest (for example, a complex of functionally oriented robots). To perform the functions of the system, current information is collected and processed. It is proposed to carry out probabilistic prediction of critical processes in order not only to act, but also to compare predictions and their coincidence with subsequent realities, to accumulate and use this knowledge. The cognitive decisions for AIS using monitoring data is in the accumulation, analysis and the use of emerging knowledge about the possible integrity of the system in the future.

When the system is operating in the conditions of heterogeneous threats, the degree of acceptability of events is proposed to be assessed by the probability of "success" and/or "failure" taking into account the consequences (risk of "failure") during a given period of prediction. In each case of modeling, the concept of "success" must be defined in terms of the acceptable state of the system concerned to perform the given or expected functions. The concept of "failure" means no "success".

It is proposed to carry out analytical prediction of risks on the basis of probabilistic modeling. For practical application, methods and models [10-36] are recommended (not an exhaustive list of adequate ones), where subjective weight coefficients are excluded. The proposed models are based on a classically constructed probabilistic space (Ω, B, P) [37-40], where: Ω - is a limited space of elementary events; B – a class of all subspace of Ω-space, satisfied to the properties of σ-algebra; P – is a probability measure on a space of elementary events Ω. Because, $\Omega=\{\omega_k\}$ is limited, there is enough to establish a reflection $\omega_k \rightarrow p_k = P(\omega_k)$ like that $p_k \geq 0$ and $\sum_k p_k = 1$.

A complex system is decomposed to compound elements to solve problems with respect to each of the elements and

subsystems with the possibility of integrating them into the system as a whole. Each of the elements is represented as a "black box", and various probabilistic models can be applied to it to calculate and construct the desired probability distribution function (PDF) for time between neighboring integrity losses, taking into account heterogeneous threats, the measures taken to control, monitor and integrity recovery. Below are some generalized models "black box" for the risk prediction.

III. THE MODELS PROPOSED

In general case successful system operation (not only AIS) is connected with system counteraction against various dangerous influences on system integrity - these may be counteractions against failures, defects events, "human factors" events, etc. There are proposed the formalization for two general technologies of providing counteraction against threats: periodical diagnostics of system integrity (technology 1, without monitoring between diagnostics) and additionally monitoring between diagnostics (technology 2). As a rule these technologies are implemented by AIS.

Assumptions: for all time characteristic the PDF exists. It is supposed for technologies 1 and 2 that the used diagnostic tools allow to provide necessary system integrity recovery after revealing danger sources penetration into a system or consequences of influences.

The probability of system operation with required safety within the given prognostic period (i.e. probability of "success") may be estimated as a result of modeling. Risk to lose integrity (R) is an addition to 1 for probability of correct system operation (P), i.e. R=1-P considering consequences.

A. *Model for the periodical diagnostics of system integrity*

The model considers periodical diagnostics of system integrity, that is carried out to detect danger sources penetration into a system or consequences of negative influences (see Figure 1).

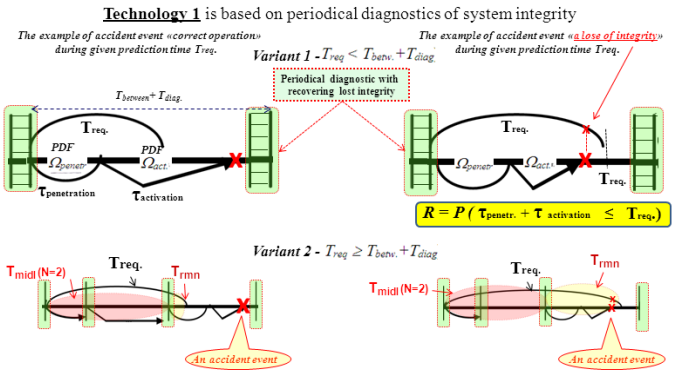

Fig. 1. Some accident events for technology 1 (left – correct operation, right – a lose of integrity during prognostic period)

Dangerous influence on system is acted step-by step: at first a danger source penetrates into a system and then after its activation begins to influence. System integrity can't be lost before a penetrated danger source is activated. A danger is considered to be realized only after a danger source has influenced on a system. The lost system integrity (after an accident event) can be detected only as a result of diagnostics. System recovery is started after detection.

There are possible the next variants for technologies 1 and 2: variant 1 – the given prognostic period T_{req} is less than established period between neighboring diagnostics ($T_{req} < T_{betw.}+T_{diag}$); variant 2 – the prognostic period T_{req} is more than or equals to established period between neighboring diagnostics ($T_{req} \geq T_{betw.}+T_{diag}$). Here $T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic, T_{diag} – is the diagnostic time.

The next formulas for PDF of time between the losses of system integrity are proposed [11, 13, 15, 29, 30].

PDF for the model of technology 1, variant 1: Under the condition of independence for characteristics the probability of providing system integrity for variant 1 is equal to

$$P_{(1)}(T_{req}) = 1 - \Omega_{penetr} * \Omega_{activ}(T_{req}), \quad (1)$$

where $\Omega_{penetr}(t)$ – is the PDF of time between neighboring penetrations of dangers; $\Omega_{activ}(t)$ – is the PDF of activation time of penetrated danger. For different dangers a frequency of dangers for these PDF is the sum of frequencies of every kind of dangers.

PDF for the model of technology 1 , variant 2. Under the condition of independence for characteristics the probability of providing system integrity for variant 2 is equal to

$$P_{(2)}(T_{req}) = N((T_{betw}+T_{diag})/T_{req})\, P_{(1)}^{N}(T_{betw}+T_{diag}) + (T_{rmn}/T_{req})\, P_{(1)}(T_{rmn}), \quad (2)$$

where $N=[T_{req.}/(T_{betw.}+T_{diag.})]$ – may be real (for PDF) or the integer part (for estimation of deviations), $T_{rmn} = T_{req} - N(T_{betw}+T_{diag})$. The probability of providing system integrity within the given time $P_{(1)}(T_{given})$ is defined by (1).

B. *Model for continuous monitoring between the periodical diagnostics of system integrity*

Technology 2, unlike the previous one, implies that system integrity is continuously monitored between diagnostics by operator (operator functions may be performed by a man or special AIS component or their combination). In case of detecting a danger source an operator recovers system integrity. The ways of integrity recovering are analogous to the ways of technology 1.

Faultless operator's actions provide a neutralization of a danger source trying to penetrate into a system. A penetration of a danger source is possible only if an operator makes an error but a dangerous influence occurs if the danger is activated before the next diagnostic. Otherwise the source will be detected and neutralized during the next diagnostic.

The next formulas for PDF of time between the losses of system integrity are proposed [11, 13, 15, 29, 30].

PDF for the model of technology 2, variant 1. Under the condition of independence for characteristics the probability of providing system integrity is equal to

$$P_{(1)}(T_{req}) = 1 - \int_{0}^{T_{req.}} dA(\tau) \int_{\tau}^{T_{req.}} d\,\Omega_{penetr} * \Omega_{act.}(\theta) \quad . \quad (3)$$

Here $A(\tau)$ is the PDF of time between operator's error.

PDF for the model of technology 2, variant 2. Under the condition of independence of characteristics the probability of providing system integrity is equal to

$$P_{(2)}(T_{req}) = N((T_{betw}+T_{diag})/T_{req})\, P_{(1)}{}^{N}(T_{betw}+T_{diag}) + +(T_{rmn}/T_{req})\, P_{(1)}(T_{rmn}), \quad (4)$$

where the probability of providing system integrity within the given time $P_{(1)}(T_{req.})$ is defined by (3).

The final clear analytical formulas for modeling are received by Lebesque-integration of (3) expression.

C. *About a generation of probabilistic models for complex system*

The basic ideas of correct integration of probability metrics are based on a combination and development of models. For a complex systems with parallel or serial structure described there are proposed the method to generate adequate probabilistic models described in [11, 13, 15, 29, 30]. Considering the importance to rationale the generation of new probabilistic models for complex system, the approach is described below. Let's consider the elementary structure from two independent parallel or series elements. Let's PDF of time between losses of i-th element integrity is $B_i(t) = P(\tau_i \leq t)$, then:

1) time between losses of integrity for system combined from series connected independent elements is equal to a minimum from two times τ_i: failure of 1st or 2nd elements (i.e. the system goes into a state of lost integrity when either 1st, or 2nd element integrity is lost). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P[\min(\tau_1,\tau_2)\leq t] = 1 - P[\min(\tau_1,\tau_2) > t] = 1 - P(\tau_1 > t)P(\tau_2 > t) = 1 - [1-B_1(t)]\,[1-B_2(t)], \quad (4)$$

2) time between losses of integrity for system combined from parallel connected independent elements (hot reservation) is equal to a maximum from two times τ_i: failure of 1st and 2nd elements (i.e. the system goes into a state of lost integrity when both 1st and 2nd elements have lost integrity). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P[\max(\tau_1,\tau_2)\leq t] = P(\tau_1 \leq t)P(\tau_2 \leq t) = B_1(t)B_2(t). \quad (5)$$

Applying recurrently expressions (4) – (5), it is possible to build PDF of time between losses of integrity for any complex system with parallel and/or series structure and theirs combinations.

Analytical modeling of complex systems is supported by the software tools "Mathematical modeling of system life cycle processes" – "know how" (registered by Rospatent №2004610858), "Complex for evaluating quality of production processes" (registered by Rospatent №2010614145) and others [31-36].

IV Modeling to the Rationale of Preventive Measures. Examples

The proposed practical way to forming input for modeling is explained in application to a parameter conditions.

Example 1. For each critical parameter (for which prognostic estimations are needed to do actions) the ranges of acceptable conditions can be established. The traced conditions of monitored parameters are data about a condition before and on the current moment of time. For example, the ranges of possible values of conditions may be established: "Working range inside of norm", "Out of working range, but inside of norm", "Abnormality" for each separate critical parameter. If the parameter ranges of acceptable conditions are not established in explicit form than for modeling purpose the may be implied and can be expressed in the form of average time value. These time values are used as input for probabilistic modeling. For example, for coal mine some of many dozens heterogeneous parameters are: for ventilation equipment - temperature of rotor and engine bearings, a current on phases and voltage of stator; for modular decontamination equipment - vacuum in the pipeline, the expense and temperature of a metano-air mix in the pipeline before equipment, pressure in system of compressed air, etc. It may be interpreted similarly by light signals – "green", "yellow", "red" - see Fig.2 and following Example 2.

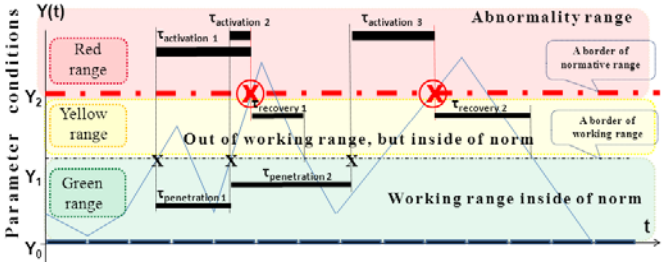

Fig. 2. An example of universal elementary ranges for monitored data about events and conditions

Example 2. For avoiding the possible crossing a border of "Abnormality" a prediction of residual time, which is available for preventive measures, according to gathered data about parameter condition fluctuations considering ranges should be carried out. For prediction it is proposed: 1) a choice of probabilistic models for construction PDF of time before the next abnormality for one element ("black box"), 2) development of the algorithm of generation PDF of time before the next abnormality for complex system, 3) formalization of calculative methods of estimating the mean residual time before the next parameters abnormalities for monitored critical system.

The method allows to estimate residual time before the next parameter abnormality state (i.e. time before first next coming into "red" range) $T_{resid(1)}$ for a given admissible risk $R_{adm.}(T_{req})$ to lose integrity. The estimated $T_{resid(1)}$ is the solution t_0 of equation:

$$R(T_{penetr}, t, T_{betw}, T_{diag}, T_{err.}, T_{req.}) = R_{adm.}(T_{req}) \quad (6)$$

concerning of unknown parameter t, i.e. $T_{resid(1)} = t_0$.

Here $R(T_{penetr}, t, T_{betw}, T_{diag}, T_{err.}, T_{req.})$ is risk to lose integrity, it is addition to 1 for probability $P(T_{req})$ of providing system integrity ("probability of success"), for calculations the formulas (1)–(3), (6) are used. T_{penetr} is the mathematical expectation of PDF $\Omega_{penetr}(\tau)$, it is defined by parameter statistics of transition from "green" into "yellow" range (see Fig.2). The others parameters T_{betw}, T_{diag} in (6) are known. The main practical questions are: what about $T_{req.}$ and what about a given admissible risk $R_{adm.}(T_{req})$? For answering we

can use the properties of function $R(T_{penetr}, t, T_{betw}, T_{diag}, T_{err.}, T_{req.})$:

- if parameter t increases from 0 to ∞ for the same another parameters, the function R(…, t, …) is monotonously decreasing from 1 to 0, i.e. if the mean activation time of occurred danger (threat - from the 1-st input at the "yellow" range to the 1-st input in the "red" range) is bigger to lose integrity is less;
- if parameter T_{req} increases from 0 to ∞ for the same another parameters, the function $R(…,T_{req})$ is monotonously increasing from 0 to 1, i.e. for large T_{req} risk approaches to 1.

It means the such maximal x exists when t=x and $T_{req.}$=x and $0<R(T_{penetr}, x, T_{betw}, T_{diag}, T_{err.}, x)<1$. The residual time before the next parameter abnormality (i.e. time before first next coming into "red" range) is equal to defined x with confidence level of admissible risk $R(T_{penetr}, x, T_{betw}, T_{diag}, T_{err.}, x)$. The implementation see on Fig. 3 [20, 29].

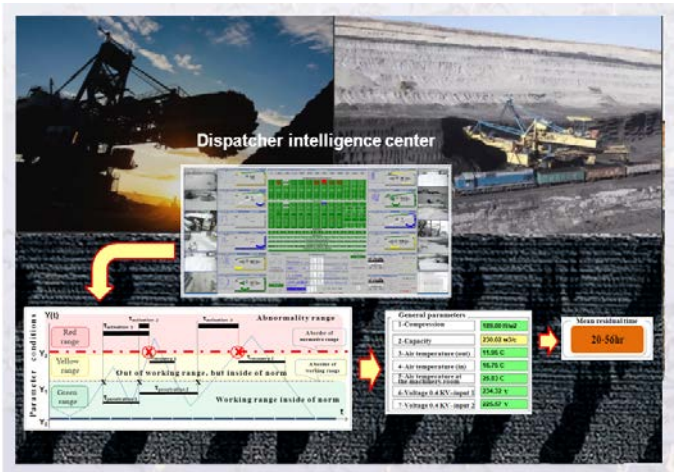

Fig. 3. Example of a prognozed residual time before the next parameter abnormality state

V THE POSSIBLE PRAGMATIC EFFECTS

Author of this article took part in creation of the Complex of supporting technogenic safety on the systems of oil&gas transportation and distribution and have been awarded for it by the Award of the Government of the Russian Federation in the field of a science and technics. The AIS is a part of the created peripheral posts are equipped additionally by means of Complex to feel vibration, a fire, the flooding, unauthorized access, hurricane, and also intellectual means of the reaction, capable to recognize, identify and predict a development of extreme situations – see engineering decisions on Fig. 4.

The applications of this Complex for 200 objects in several regions of Russia during the period 2009-2014 have already provided economy about 8,5 Billions of Roubles. The economy is reached at the expense of effective implementation of the functions of risks prediction and processes optimization [17].

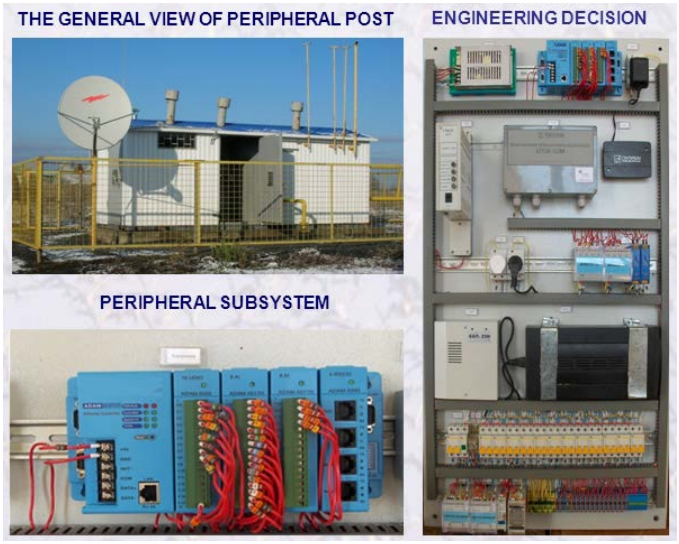

Fig. 4. The AIS as a hard-software part to support technogenic safety on the objects of oil&gas distribution

CONCLUSION

The proposed approach for cognitive processing of monitored data develops the existing approaches to risk prediction, ensuring and improving the safety of systems with AIS. Probabilistic models and methods that allow predicting the probability of "success" and/or the risk of "failure", supporting their software tools, methods for solving practical problems are presented. Application of the proposed approach allows to counteract threats by rationale preventive actions. A suitability of the approach is illustrated by practical examples.

REFERENCES

[1] Alan Turing, Computing Machinery and Intelligence, Mind, vol. LIX, no. 236, October 1950, pp. 433—460.
[2] Experimental Robotics. Springer, 2016, 913 p.
[3] Robotics Research. Springer, 2017, 646 p.
[4] Cybernetics Approaches in Intelligent Systems. Computational Methods in Systems and Software, vol. 1, Springer, 2017, 405 p.
[5] Applied Computational Intelligence and Mathematical Methods. Computational Methods in Systems and Software, vol. 2, Springer, 2017, 393p.
[6] R. Valencia, J. Andrade-Cetto, Mapping, Planning and Exploration with Pose SLAM, Springer, 2018, 124 p.
[7] The DARPA Robotics Challenge Finals: Humanoid Robots To The Rescue, Springer, 2018, 692 p.
[8] Cognitive Reasoning for Compliant Robot Manipulation, Springer, 2019, 190p.
[9] S. Tadokoro, Disaster Robotics, Springer, 2019, 532 p.
[10] Kostogryzov, A.I. Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ). Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, USA, Dallas, 2000, pp.63-70.
[11] Kostogryzov A., Nistratov G.: Standardization, mathematical modelling, rational management and certification in the field of system and software engineering. Armament.Policy.Conversion, Moscow, 2004.
[12] Zio En.: An Introduction to the Basics of Reliability and Risk Analysis, World Scientific Publishing Co.Pte.Ltd. , 2006.
[13] Kostogryzov A.I., Stepanov P.V.: Innovative management of quality and risks in systems life cycle (modern standards and ideas of system engineering, mathematical models, methods, techniques and software tools complexes for system analysis, including modelling through Internet, 100 examples with an explanation of logic of the reached

results, useful practical recommendations). Armament.Policy.Conversion, Moscow, 2008.
[14] Kolowrocki K., Soszynska-Budny J.: Reliability and Safety of Complex Technical Systems and Processes, Springer-Verlag London Ltd., 2011.
[15] Kostogryzov A., Nistratov G. and Nistratov A.: Some Applicable Methods to Analyze and Optimize System Processes in Quality Management. Total Quality Management and Six Sigma, InTech, 2012: 127-196.
[16] Grigoriev L., Guseinov Ch., Kershenbaum V., Kostogryzov A. The methodological approach, based on the risks analysis and optimization, to research variants for developing hydrocarbon deposits of Arctic regions. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars, Volume 5, Number1-2, 2014: 71-78.
[17] Akimov V., Kostogryzov A., Mahutov N. at al. Security of Russia. Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety. Under the editorship of Mahutov N.A. Znanie, Moscow, 2015.
[18] Kostogryzov A., Nistratov A., Zubarev I., Stepanov P., Grigoriev L. About accuracy of risks prediction and importance of increasing adequacy of used adequacy of used probabilistic models. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars, Volume 6, Numbers 2, 2015: 71-80.
[19] Eid, M. and Rosato, V. Critical Infrastructure Disruption Scenarios Analyses via Simulation. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, 2016: 43-62.
[20] Artemyev V., Kostogryzov A., Rudenko Ju., Kurpatov O., Nistratov G., Nistratov A.: Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. In: Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, 2017: 368-373.
[21] Kostogryzov A., Stepanov P., Nistratov A., Nistratov G., Klimov S., Grigoriev L.: The method of rational dispatching a sequence of heterogeneous repair works. Energetica. Vol.63, No 4, 2017: 154-162.
[22] Kostogryzov A., Stepanov P., Nistratov A., Atakishchev O.: About Probabilistic Risks Analysis During Longtime Grain Storage. In: Proceedings of the 2nd Internationale Conference on the Social Science and Teaching Research (ACSS-SSTR), Volume 18 of Advances in Social and Behavioral Science. Edited by Harry Zhang. Singapore Management and Sports Science Institute, PTE.Ltd. , 2017: 3-8 .
[23] Kostogryzov A., Stepanov P., Grigoriev L., Atakishchev O., Nistratov A., Nistratov G.: Improvement of Existing Risks Control Concept for Complex Systems by the Automatic Combination and Generation of Probabilistic Models and Forming the Storehouse of Risks Predictions Knowledge. In: Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM), Phuket, Thailand. DEStech Publications, Inc., 2017: 279-283.
[24] Kostogryzov A., Atakishchev O., Stepanov P., Nistratov A., Nistratov G., Grigoriev L.: Probabilistic modelling processes of mutual monitoring operators actions for transport systems. In: Proceedings of the 4th International Conference on Transportation Information and Safety (ICTIS), Canada, Banff, 2017: 865-871.
[25] Kostogryzov A., Panov V., Stepanov P., Grigoriev L., Nistratov A., Nistratov G.: Optimization of sequence of performing heterogeneous repair work for transport systems by criteria of timeliness. In: Proceedings of the 4th International Conference on Transportation Information and Safety (ICTIS), Canada, Banff, 2017: 872-876.
[26] Kostogryzov A., Nistratov A., Nistratov G., Atakishchev O., Golovin S., Grigoriev L.: The probabilistic analysis of the possibilities to keep “organism integrity” by continuous monitoring. In: Proceedings of the International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA), Chengdu, China. Atlantis Press, Advances in Intelligent Systems Research, volume 159, 2018: 432-435.
[27] Kostogryzov A., Grigoriev L., Golovin S., Nistratov A., Nistratov G., Klimov S.: Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. In: Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI), Beijing, China. DEStech Publications, Inc., 2018: 298-303.
[28] Kostogryzov A., Grigoriev L., Kanygin P., Golovin S., Nistratov A., Nistratov G.: The Experience of Probabilistic Modeling and Optimization of a Centralized Heat Supply System Which is an Object for Modernization. International Conference on Physics, Computing and Mathematical Modeling (PCMM), Shanghai, DEStech Publications, Inc., 2018: 93-97.
[29] Artemyev V., Rudenko Ju., Nistratov G.: Probabilistic modeling in system engineering. Probabilistic methods and technologies of risks prediction and rationale of preventive measures by using “smart systems”. Applications to coal branch for increasing Industrial safety of enterprises. Edited by Andrey Kostogryzov, IntechOpen, 2018: 23-51.
[30] Kershenbaum V., Grigoriev L., Kanygin P., Nistratov A.: Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. Edited by Andrey Kostogryzov, IntechOpen, 2018: 55-79.
[31] Kostogryzov A.I., Bezkorovainy M.M., Lvov V.M., Nistratova E.N., Bezkorovainaya I.V. Complex for Evaluation of Information Systems Operation Quality – “know-how” (CEISOQ), registered by Rospatent №2000610272.
[32] Kostogryzov A.I., Nistratov G.A., Nistratova E.N., Nistratov A.A. Mathematical modeling of system life cycle processes – “know-how”, registered by Rospatent №2004610858.
[33] Kostogryzov A.I., Nistratov G.A., Nistratova E.N., Nistratov A.A. Complex for evaluating quality of production processes, registered by Rospatent №2010614145
[34] Kostogryzov A.I., Nistratov G.A., Nistratov A.A. Remote analytical support of informing about the probabilistic and time measures of operating system and its elements for risk-based approach, registered by Rospatent №2018617949.
[35] Kostogryzov A.I., Nistratov G.A., Nistratov A.A. Remote rationale of requirements to means and conditions for providing "smart" systems operation quality, registered by Rospatent №2018618572.
[36] Kostogryzov A.I., Nistratov G.A., Nistratov A.A. Remote probabilistic prediction of informatized systems operation quality, registered by Rospatent №2018618686.
[37] Feller W. An Introduction to Probability Theory and Its Applications. Vol. II, Willy, 1971.
[38] Martin J. (1972) System Analysis for Data Transmission. V. II, IBM System Research Institute. Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1972.
[39] Gnedenko B.V. et al. Priority queueing systems, MSU, Moscow, 448p., 1973
[40] Probabilistic Modeling in System Engineering / by ed. A. Kostogryzov. – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.