Kostogryzov Andrey

Stepanov Pavel
Federal Research Center "Computer Science and Control", Russian Academy of Sciences, Moscow, Russia

Nistratov Andrey

Nistratov George

Zubarev Igor
Research Institute of Applied Mathematics and Certification, Moscow, Russia

Grigoriev Leonid
The Gubkin Russian State University of Oil and Gas, Moscow, Russia

Analytical modelling operation processes of composed and integrated information systems on the principles of system engineering

Keywords

information, model, probability, quality, risk, safety, system, technology

Abstract

The approach for analytical modelling operation processes of composed and integrated information systems is proposed. It allows to estimate the reliability and timeliness of information producing, the completeness, validity and confidentiality of the used information from users' point of view. In application to composed and integrated systems the existing models are developed by introducing the space of elementary events for operation processes from system engineering point of view. It is intended for systems analysts for any IS. Some effects are demonstrated by examples.

1. Introduction

The founder of cybernetics Norbert Wiener in his treatise "Cybernetics" wrote that all systems are in the main information systems (IS) with feedbacks. In other words, any system may be interpreted as a system for information processing and the results achieved by a system as a consequence of rational use of qualitative output information. Today it may mean that separate or integrated IS plays a role of a brain of any modern system. At the same time in overwhelming number of cases the potential of IS possibilities (and today to them the possibilities of «Smart systems» and the "Internet of things" are added) is used only functionally, for example – continuous gathering of the information about facts, conditions, their analysis and corresponding functional actions. But not about predicted quality of the complex operation processes of composed or/and integrated IS in different conditions. And additional extraction of the numerous latent effects from implemented technologies and the collected information is missed in system life cycle.

Because of the increased complexity a cardinal turn from "manual" optimization of information processes (based on performance of the settled standard instructions and on expert estimations of developing situations) to implementation of scientifically proved balanced preventive measures is needed. It allows on the basis of a probabilistic sight forward preventively to undertake effective preventive measures. Such idea passes through all modern concepts and last standards of system engineering (for example, standard series ISO 9000, 27000, 31000, ISO/IEC 15288, 12207, 16085, 17776, etc.).

Considering, that potential damages and expenses for liquidation of consequences of critical influences on quality and safety exceed essentially expenses for preventive measures, the present researches expand and develop the analytical approaches stated in earlier works [4], [7], [12], in application to composed and integrated information systems.

2. The analysis of threats and general propositions for analytical modelling

Requirements to IS operation in different application domain depend on SYSTEM purposes and general purpose of IS operation, real conditions, including potential threats, available resources, information sources facilities and communication requirements (see *Figure 1*).

The preliminary idea of estimating IS operation quality appeared as a result of studying potential threats to output information (see *Table 1*).

Table 1. Evaluated IS operation quality characteristics against the results of threats realization

The results of threats realization	Evaluated IS operation quality characteristics
To reliability of information producing: Non-produced information for using in consequence of system's unreliability	**Reliability of information producing** is the property causing capability of IS to operate required functions for information producing (or technological operations processing) when operated under specified conditions
To timeliness of information producing: Untimely used information	**Timeliness of information producing** is the property causing capability of IS to operate timely required functions for information producing (or technological operations processing)
To completeness of output information: Incomplete used information	**Completeness of output information** is the used information property to reflect conditions of all real objects of IS application domain according to specified purposes destination. One is composed of a completeness of IS function fulfillment, of a completeness of initial information filling and of IS filling by data as regards a new objects and processes of application domain during operation time.
To validity of output information: Deteriorated used information validity, including:	**Validity of output information** is the used information property to reflect real or estimated objects and processes of IS application domain conditions with the degree of approximation which is acceptable for effective using this information. One is composed of a validity of prepared and stored information, processed before composing, of a faultlessness and actuality of unprocessed input and stored composed information, of processing accuracy by IS software as well as of data transmission validity. **Information faultlessness** is the used information property to be without random errors and hidden distortions, including distortions as a result of unauthorized accesses and viruses influences.
to actuality of faultless information: ● non-actual used information; **to information faultlessness:** ● used information due to random errors missed during checking; ● used information due to random faults of users and staff; ● used information with hidden virus distortions; ● used information with hidden distortions as a result of an unauthorized access	● **actuality of faultless information** is the used faultless information property to correspond to the current conditions of IS application domain objects and processes with the degree of acceptable approximation. One is the property causing natural process when information is becoming antiquated in due course; ● information faultlessness after checking; ● information faultlessness as a result of faultless users and staff actions; ● IS protection against viruses influences; ● IS protection against an authorized access.
To confidentiality of used information: Non-confidential used information	**Confidentiality of used information** is the used information property to be protected within required period from an unauthorized scanning.
Integral (to IS operation processes) from system engineering point of view: The lost system integrity	**System integrity is** such system state when system purposes are achieved with the required quality

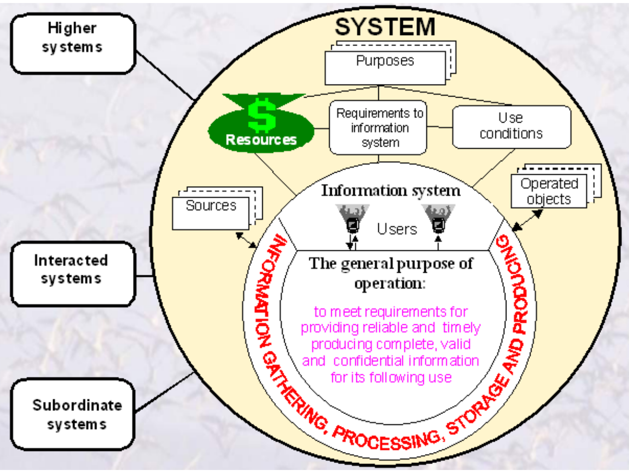

Higher systems
SYSTEM
Purposes
Resources
Requirements to information system
Use conditions
Information system
Sources
Operated objects
Users
Interacted systems
The general purpose of operation:
to meet requirements for providing reliable and timely producing complete, valid and confidential information for its following use
INFORMATION GATHERING, PROCESSING, STORAGE AND PRODUCING
Subordinate systems

Figure 1. The place and the purpose of different information system operating in a SYSTEM

This is the logical source of probabilistic modelling to estimate the reliability and timeliness of information producing, the completeness, validity and confidentiality of the used information from users' point of view. In application to composed and integrated systems the existing models [4], [7], [12] are developed by introducing the space of elementary events for operation processes ("correct operation" and "a lose of integrity") from system engineering point of view.

3. Probabilistic modelling to estimate information system processes

3.1 General

In general case a probabilistic space (Ω, B, P) for an evaluation of system operation processes is proposed, 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 - a probability measure on a space of elementary events Ω.

Because, $\Omega = \{\omega_k\}$ is limited, there is enough to establish a reflection $\omega_k \to p_k = P(\omega_k)$ like that $p_k \geq 0$ and $\sum_k p_k = 1$. Such space (Ω, B, P) is built by the limited theorems for regenerative processes [1]-[2] and also by using principal propositions of probability theory and well famous results for single and multi-units queuing systems.

This probabilistic space (Ω, B, P) is the essence of the proposed mathematical models for studying IS processes according to general proposition above.

3.2 Modelling from users' point of view

The abstract users' point of view on used information is demonstrated by *Figure 2*.

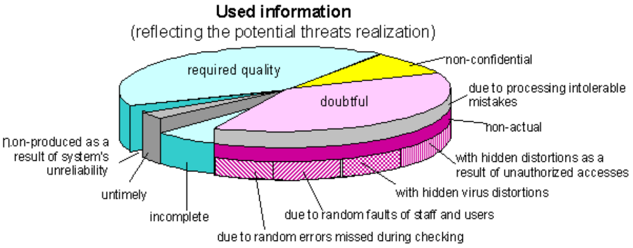


Figure 2. Potential threats to output information according to general purpose of IS operation

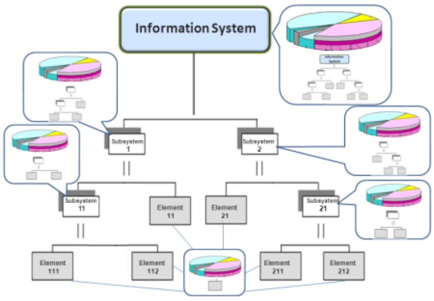


Figure 3. Decomposition of complex system upto subsystems and elements

The proposed analytical models and calculated measures are the next [5]-[6], [8]-[11], [13]-[14]:

"The model of functions performance by a complex system in conditions of unreliability of its components" (the measures: T_{MTBF} - the mean time between failures; P_{MTBF} - the probability of reliable operation of IS, composed by subsystems and system elements, during the given period; P_{man} - the probability of providing faultless man's actions during the given period);

"The models complex of calls processing (the measures for the different dispatcher technologies (for unpriority calls processing in a consecutive order for singletasking processing mode, in a time-sharing order for multitasking processing mode; for priority technologies of consecutive calls processing with relative and absolute priorities; for batch calls processing; for combination of technologies above): the mean wait time in a queue; the mean full processing time, including the wait time; P_{tim} - the probability of well-timed processing during the given time; the relative portion of all well-timed processed calls; the relative portion of well-timed processed calls of those types for which the customer requirements are met);

"The model of entering into IS current data concerning new objects of application domain" (the measure: P_{compl} - the probability that IS contains complete current information about states of all objects and events);

"The model of information gathering" (the measure: $P_{actual.}$ - the probability of IS information actuality on the moment of its use);

"The model of information analysis" (the measures: P_{check} is the probability of errors absence after checking; the fraction of errors in information after checking; $P_{process}$ - the probability of correct analysis results obtaining; the fraction of unaccounted essential information);

"The models complex of dangerous influences on a protected system" (the measures: $P_{infl.}$ - the probability of required counteraction to dangerous influences from threats during the given period);

"The models complex of an authorized access to system resources" (the measures: P_{prot} - the probability of providing system protection from an unauthorized access by means of barriers; $P_{conf.}$ - the probability of providing information confidentiality by means of all barriers during the given period)[1].

These models, supported by different versions of software Complex for Evaluation of Information Systems Operation Quality, patented by Rospatent №2000610272 (CEISOQ+), may be applied for solving such system problems in IS life cycle as: substantiation of quantitative system requirements to hardware, software, users, staff, technologies; requirements analysis; estimation of project engineering decisions and possible danger; detection of bottle-necks; investigation of problems concerning potential threats to system operation and information security; testing, verification and validation of IS operation quality; rational optimization of IS technological parameters; substantiation of plans, projects and directions for effective system utilization, improvement and development.

3.3 System engineering point of view

According to definition of ISO/IEC/IEEE 15288-2014 "System engineering is interdisciplinary approach governing the total technical and managerial effort required to transform a set of stakeholder needs, expectations, and constraints into a solution and to support that solution throughout its life". It means also a use of scientific efforts for rational creation and effective application of complex systems. The modern systems consist a set of compound subsystems and system elements (their number may be tens- hundreds-thousand and more), and for each generally should be solved identical problems of estimation and optimization information processes – see *Figure 3*. The measures of predicted

[1] Note: For simplifying the indexes of measures details are not reflected.

quality and risks should be commensurable and should allow the decision of analysis and synthesis problems by criteria "safety-efficiency-cost" in life cycle of system elements and systems.

Considering heterogeneous threats and specific methods of control, monitoring and integrity recovery in application to integrated IS the next proposed general analytical approach is used for modelling operation processes from system engineering point of view.

3.4 Preliminary modelling before integration

There are proposed two general technologies of providing protection from critical influences on IS quality or/and safety: technology 1 - periodical diagnostics of system integrity (without the continuous monitoring between diagnostics) and technology 2 - continuous monitoring between periodical diagnostics is added to technology 1 - see *Figure 4*.

Technology 1 is based on periodical diagnostics of system integrity, that are carried out to detect danger sources penetration from threats (destabilizing factors) into a system or consequences of negative influences. The lost system integrity can be detect only as a result of diagnostics, after which system recovery is started. 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 from threats (destabilizing factors) is considered to be realized only after a danger source has influenced on a system.

Technology 2, unlike the previous one, implies that operators alternating each other trace system integrity between diagnostics (operator may be a man or special device 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. When operators alternate a complex diagnostic is held. 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.

It is supposed for technologies 1 and 2 that the used diagnostic allows to provide necessary system integrity recovery after revealing danger sources penetration into a system or consequences of influences. Assumption: for all time input characteristic the PDF exists. Thus the probability of correct system operation within the given prognostic period (i.e. probability of success) may be computed as a result of use the models. For the identical damages risk to lose integrity is an addition to 1 for probability of correct system operation $R = 1 – P$.

There are possible the next variants for technology 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 assigned 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.

For the given period for prediction ($T_{req.}$) the next statements are proposed.

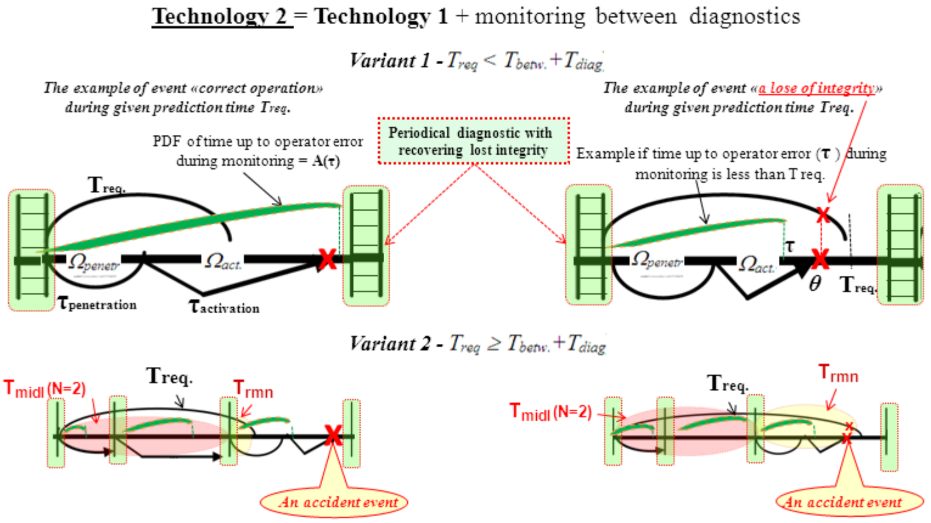

Technology 2 = Technology 1 + monitoring between diagnostics
Variant 1 - $T_{req} < T_{betw.} + T_{diag}$
The example of event «correct operation» during given prediction time Treq.
The example of event «a lose of integrity» during given prediction time Treq.
Periodical diagnostic with recovering lost integrity
PDF of time up to operator error during monitoring = A(τ)
Example if time up to operator error (τ) during monitoring is less than T req.
Treq.
Ω_{penetr}
$\Omega_{act.}$
τpenetration
τactivation
τ
θ
Treq.
Variant 2 - $T_{req} \geq T_{betw.} + T_{diag}$
Tmidl (N=2)
Treq.
Trmn
An accident event
Tmidl (N=2)
Treq.
Trmn
An accident event

Figure 4. Some accident events for technology 2 (left – “correct operation”, right – “a loss of integrity” during the given period of prediction $T_{req.}$)

Statement 1 (for technology 2). Under the condition of independence for considered characteristics the probability of correct system operation for variant 1 is equal to

$$P_{(1)}(T_{req}) = 1 - \int_0^{Treq} dA(\tau) \int_\tau^{Treq} d\Omega_{\text{penetr}} * \Omega_{\text{activ}}(\theta) \quad (1)$$

where $\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source; $\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source, $A(t)$ is the PDF of time from the last finish of diagnostic time up to the first operator error.

Statement 2 (for technology 2). Under the condition of independence of considered characteristics the probability of correct system operation for variant 2 may be equal to:

- measure a)

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

where

$N = [T_{req.}/(T_{betw.}+ T_{diag.})]$ – is the integer part,

$T_{rmn} = T_{req.} – N(T_{betw.} + T_{diag.})$;

- measure b)

$$P_{(2)}(T_{req}) = P_{(1)}{}^N (T_{betw} + T_{diag})P_{(1)}(T_{rmn}), \quad (3)$$

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

For technology 1 the formulas to evaluate the measures P and R are the same (see (1)-(3)), considering that the time from the last finish of diagnostic time up to the first operator error is equal to 0, i.e.

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

The final clear analytical formulas for modelling are received by Lebesque-integration of (1) expression with due regard to Statements 1-2.

Comment: The measure a) allows to perform latent knowledge mining in the possibilities and impacts of every control because N is integer part. The measure b) allows to mine latent knowledge by average value of probability on the level of classical PDF.

The PDF of time between neighboring influences for penetrating a danger source $\Omega_{penetr}(t)$ should consider the results of users' point of view IS operation modelling (calculated in time line from 0 to ∞) including the probability of reliable operation of IS, composed by subsystems and system elements, during the given period (P_{MTBF}); the probability of providing faultless man's actions during the given period (P_{man}), the probability of well-timed processing during the given time (P_{tim}), the probability that IS contains complete current information about states of all objects and events (P_{compl}), the probability of IS information actuality on the moment of its use (P_{actual}), the probability of errors absence after checking (P_{check}), the probability of correct analysis results obtaining ($P_{process}$), the probability of providing information confidentiality (P_{conf}). The PDF of activation time of a penetrated danger source $\Omega_{activ}(t)$ should consider the results of users' point of view IS operation modelling the probability of providing system protection from an unauthorized access by means of barriers (P_{prot}). And the PDF of time from the last finish of diagnostic time up to the first operator error A(t) should consider the results of users' point of view, focused on the probability of reliable operation of IS (P_{MTBF}), the probability of providing faultless man's actions during the given period (P_{man}) and the probability of correct analysis ($P_{process}$).

As a results of preliminary modelling before integration for every compound element the probability of correct operation during the given period (P_{integr}) and risk to lose required integrity (R_{integr})[2].

3.5. Integration modelling from system engineering point of view

The main output of integration modelling for each element is probability of correct system operation or risk to lose system integrity during the given period of time. If probabilities for all points $T_{req.}$ from 0 to ∞ are computed, it means a trajectory of the PDF depending on characteristics of threats, periodic control, monitoring and recovery. And the building of PDF is the real base to prediction measures P and R for given time T_{req}. In analogy with reliability it is important to know a mean time between neighboring losses of integrity like mean time between neighboring failures in reliability (MTBF), but in application to quality, safety etc.

For complex systems with parallel or serial structure existing models with known PDF can be developed by usual methods of probability theory [1]-[3], [9], [12]-[13], [15]. Let's consider the elementary structure from two independent parallel or series

[2] Note: For simplifying the indexes of measures details are not reflected.

elements. Let's PDF of time between losses of i-th element integrity is $B_i(t)$, i.e. $B_i(t) = P(\tau_i \leq t)$, 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[3]

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

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.

For example for system, combined from different IS (*Figure 5*) the formula (4) should be used. The correct operation of this system of system during the given period (P_{integr}) means: during this period of prediction both the 1-st and the 2-nd IS will operate correctly.

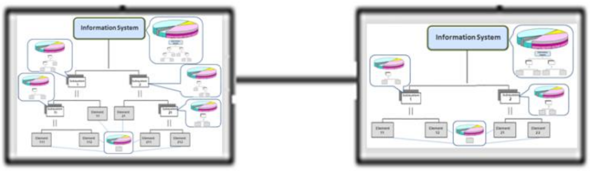


Figure 5. System of two different IS (serial combination) for integration modelling

All these ideas for analytical modelling operation processes are supported by the software tools "Mathematical modelling of system life cycle processes" – "know how" (registered by Rospatent №2004610858), "Complex for evaluating quality of production processes" (registered by Rospatent №2010614145) and others.

4. What latent effects can be discovered by the proposed approach?

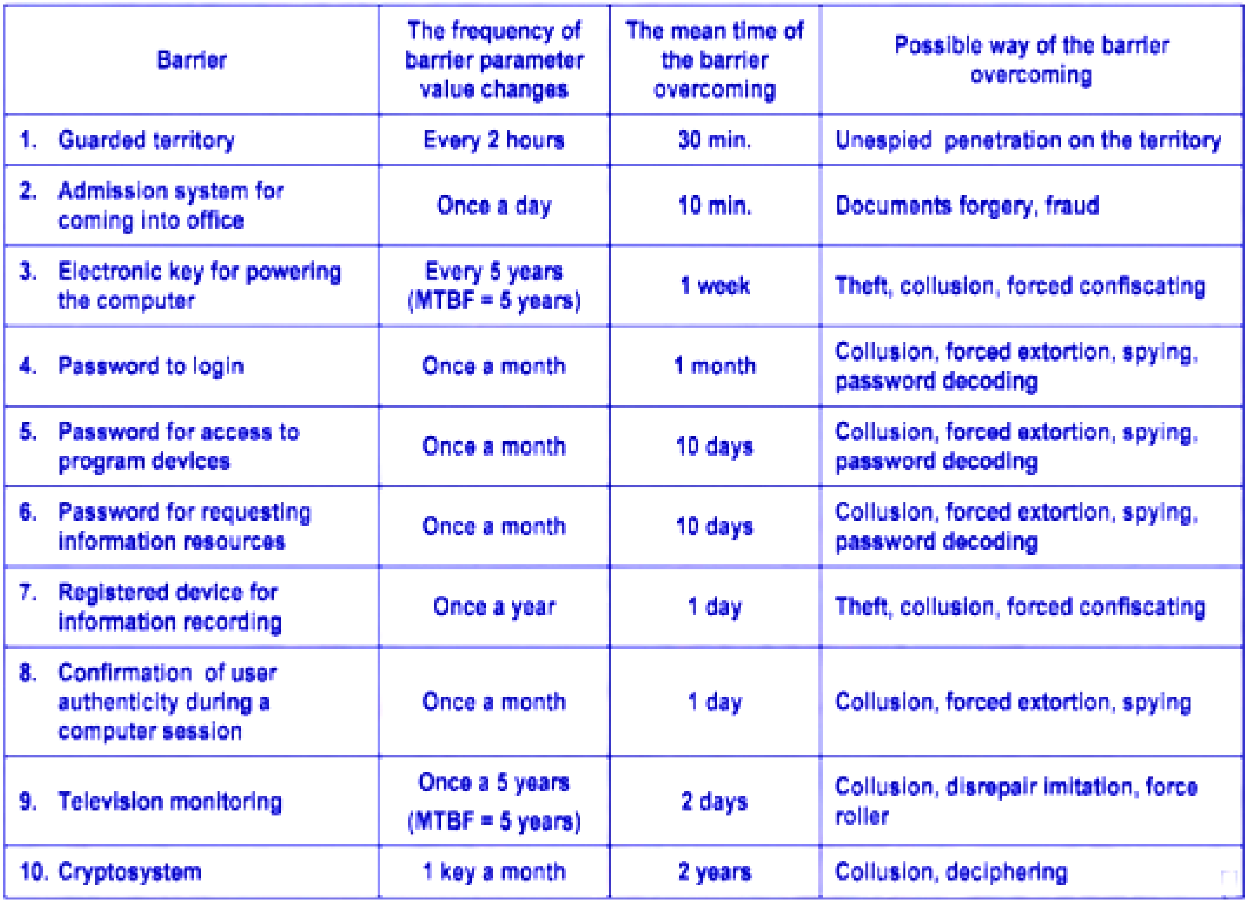
Example 1 (About Internet). It is clear for every enlightened person that the Internet is valuable because it allows to discover new knowledge from a global human intellect and provide data mining from huge information warehouse located in it. It is beyond man's capacity and it is rather difficult for a group of people united by a common goal. What would be if to entrust information filtering and data mining from Internet to a special electronic analyzer, which is never tired and able to work around the clock? The use of proposed models discovers that in comparison with the most experienced man an analyzer allows to derive really useful information from huge amount of information "trash" dozens or even hundreds times as much. Owing to the rational Internet use a man's capacity may be increased greatly. These figures characterize the potentially achieved global informatization efficiency from the data mining point of view.

Example 2 (Protection against an unauthorized access). We will consider the approach to an estimation of IS protection against an unauthorized access (UAA) and information confidentiality. A resources protection from UAA is a sequence of barriers. If a violator overcomes these barriers he gets access to IS information and/or software resources. In the *Table 2* there are shown supposed characteristics of barriers and mean time of their overcoming by a specially trained violator (real values of such characteristics may be drawn as a result of actual tests or use of other models). It is required to estimate IS protection against UAA.

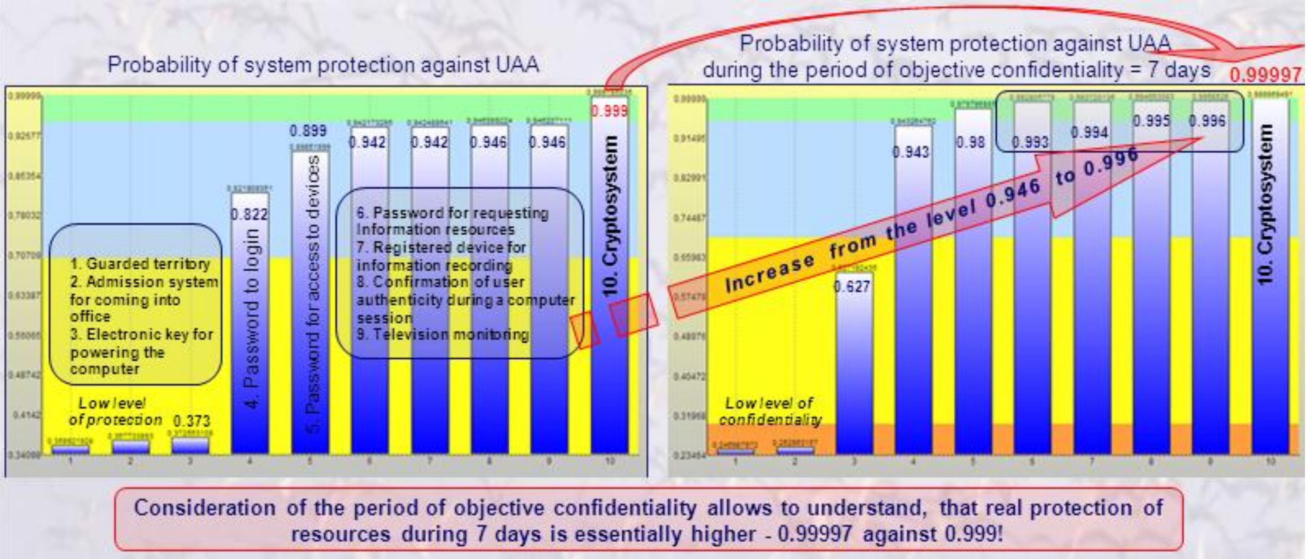
Approach to the solution. The analysis of computed dependencies (see *Figure 6* left) shows the next. The barriers 1-3 will be overcome with the probability equal to 0.63. However, monthly password changing for barriers 4-6 allows to increase the protection probability from 0.37 to 0.94 but the level of IS protection (the first six barriers) is still low. The introducing of 7-9 barriers is useless because it does not practically increase the level of IS protection. The use of cryptography allows to increase the level of IS protection to 0.999. This is probability for all time of IS operation (i.e. about 20-30 years). It is possible to establish a conclusion, that with the use of cryptographic devices the achieved protection level exceeds similar level of reliability and safety for processes from examples above. But according to "precedent" principle this level of protection can't be recommended as high for every case.

[3] Note. The same approach is studied also by Prof. E. Ventcel (Russia) in 80^{th}, she has formulated the trying tasks for students.

Table 2. Input for modelling

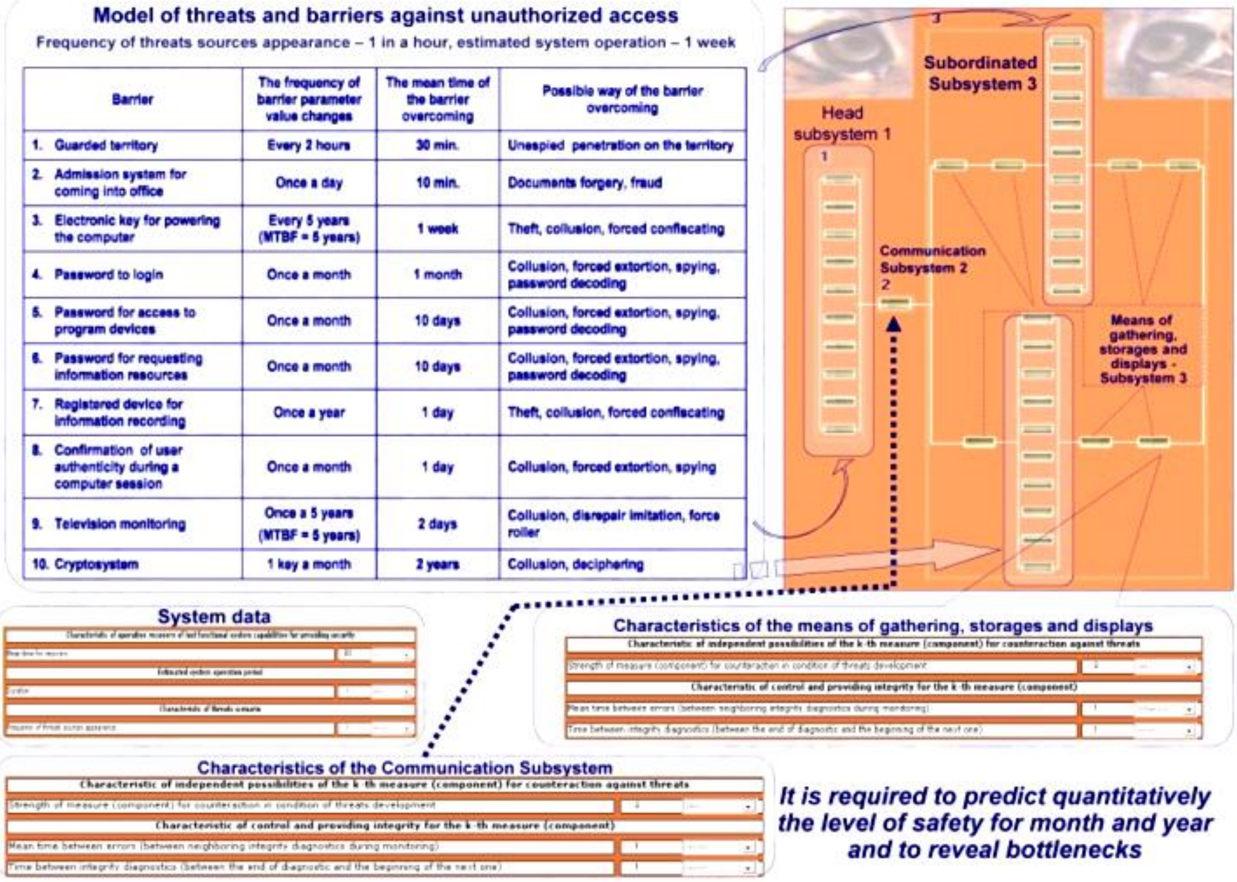


Barrier	The frequency of barrier parameter value changes	The mean time of the barrier overcoming	Possible way of the barrier overcoming
1. Guarded territory	Every 2 hours	30 min.	Unespied penetration on the territory
2. Admission system for coming into office	Once a day	10 min.	Documents forgery, fraud
3. Electronic key for powering the computer	Every 5 years (MTBF = 5 years)	1 week	Theft, collusion, forced confiscating
4. Password to login	Once a month	1 month	Collusion, forced extortion, spying, password decoding
5. Password for access to program devices	Once a month	10 days	Collusion, forced extortion, spying, password decoding
6. Password for requesting information resources	Once a month	10 days	Collusion, forced extortion, spying, password decoding
7. Registered device for information recording	Once a year	1 day	Theft, collusion, forced confiscating
8. Confirmation of user authenticity during a computer session	Once a month	1 day	Collusion, forced extortion, spying
9. Television monitoring	Once a 5 years (MTBF = 5 years)	2 days	Collusion, disrepair imitation, force roller
10. Cryptosystem	1 key a month	2 years	Collusion, deciphering



Consideration of the period of objective confidentiality allows to understand, that real protection of resources during 7 days is essentially higher - 0.99997 against 0.999!

Figure 6. Comparison of protection levels



Model of threats and barriers against unauthorized access

Frequency of threats sources appearance – 1 in a hour, estimated system operation – 1 week

Barrier	The frequency of barrier parameter value changes	The mean time of the barrier overcoming	Possible way of the barrier overcoming
1. Guarded territory	Every 2 hours	30 min.	Unespied penetration on the territory
2. Admission system for coming into office	Once a day	10 min.	Documents forgery, fraud
3. Electronic key for powering the computer	Every 5 years (MTBF = 5 years)	1 week	Theft, collusion, forced confiscating
4. Password to login	Once a month	1 month	Collusion, forced extortion, spying, password decoding
5. Password for access to program devices	Once a month	10 days	Collusion, forced extortion, spying, password decoding
6. Password for requesting information resources	Once a month	10 days	Collusion, forced extortion, spying, password decoding
7. Registered device for information recording	Once a year	1 day	Theft, collusion, forced confiscating
8. Confirmation of user authenticity during a computer session	Once a month	1 day	Collusion, forced extortion, spying
9. Television monitoring	Once a 5 years (MTBF = 5 years)	2 days	Collusion, disrepair imitation, force roller
10. Cryptosystem	1 key a month	2 years	Collusion, deciphering

Subordinated Subsystem 3
3
Head subsystem 1
1
Communication Subsystem 2
2
Means of gathering, storages and displays - Subsystem 3

System data

Characteristic of operation measures of tool functional system capabilities for providing security

Reaction time for measures

Estimated system operation period

Duration

Characteristic of threats scenario

Frequency of threats sources appearance

Characteristics of the means of gathering, storages and displays

Characteristic of independent possibilities of the k-th measure (component) for counteraction against threats

Strength of measure (component) for counteraction in condition of threats development

Characteristic of control and providing integrity for the k-th measure (component)

Mean time between errors (between neighboring integrity diagnostics during monitoring) 1

Time between integrity diagnostics (between the end of diagnostic and the beginning of the next one) 1

Characteristics of the Communication Subsystem

Characteristic of independent possibilities of the k-th measure (component) for counteraction against threats

Strength of measure (component) for counteraction in condition of threats development

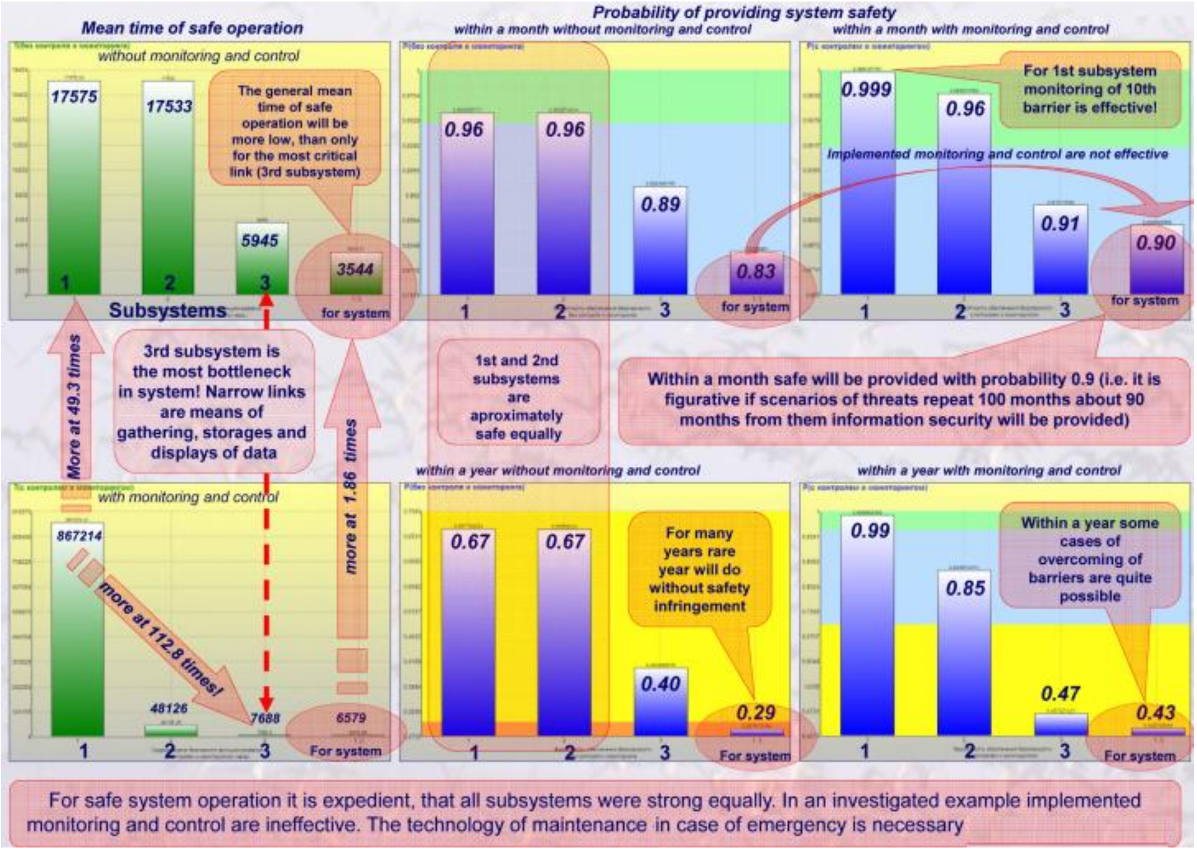
Characteristic of control and providing integrity for the k-th measure (component)

Mean time between errors (between neighboring integrity diagnostics during monitoring) 1

Time between integrity diagnostics (between the end of diagnostic and the beginning of the next one) 1

It is required to predict quantitatively the level of safety for month and year and to reveal bottlenecks

Figure 7. Input for modelling complex safety



The general mean time of safe operation will be more low, than only for the most critical link (3rd subsystem)

3rd subsystem is the most bottleneck in system! Narrow links are means of gathering, storages and displays of data

1st and 2nd subsystems are aproximately safe equally

For 1st subsystem monitoring of 10th barrier is effective!

Implemented monitoring and control are not effective

Within a month safe will be provided with probability 0.9 (i.e. it is figurative if scenarios of threats repeat 100 months about 90 months from them information security will be provided)

For many years rare year will do without safety infringement

Within a year some cases of overcoming of barriers are quite possible

For safe system operation it is expedient, that all subsystems were strong equally. In an investigated example implemented monitoring and control are ineffective. The technology of maintenance in case of emergency is necessary

Figure 8. The results of prediction and analysis

Let's look on example condition more widely. The violator is interested in certain IS resources during a given period of time. This period is called the period of objective confidentiality. Let’s information confidentiality should be provided within 7 days. *Figure 6* (right) shows how this period influences on protection:

in comparison with the results above the use of the first 5 barriers provides confidentiality during 7 days on the level 0.98 which is more higher than protection by the 9 barriers (0.946 – see *Figure 6* left);

the use of all the 10 barriers provides the required confidentiality on the level 0.99997. It eliminates the customer’s risk in providing system protection. It explains the role of a considered period of objective confidentiality. Its consideration allows to understand, that real protection of resources during 7 days is essentially higher - 0.99997 against 0.999!

Example 3 (What about safety of complex system?). Let’s an IS includes head subsystem and two used subsystems 2 and 3 (see *Figure 7*). A frequency of threats is no more than 1 time at hour, average time for system recovery is no more than 30 minutes. It is required to predict quantitatively the level of safety within month and year system operation and to reveal its bottlenecks.

Results of modelling are reflected on Figure 8. With monitoring and control within a month all barriers are overcame with probability 0.9, and within a year – with probability 0.43. Without monitoring and control these probabilities decrease to level 0.83 and 0.29 accordingly. Monitoring is ineffective for example conditions.

Following recommendations are obvious: for safe system operation it is expedient, that all subsystems are strong equally. The technology of safety maintenance in emergency case is necessary. Recommendations are supported by the analytical modelling.

Example 4 (What about the possible pragmatic effects?). Authors of this article took part in creation of the Complex of supporting technogenic safety on the objects of oil & gas distribution and have been awarded for it by Award of the Government of the Russian Federation in the field of a science and techniques for 2014. The created peripheral posts are equipped additionally by means of monitoring 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. The applications of 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 [3].

5. Conclusion

An application of the proposed approach, based on the principles of system engineering, appears new potentiality for system analysts (from customers, designers, developers, users, experts of testing laboratories and certification bodies, as well as a staff of quality maintenance etc.). It is useful for solving such system problems in a life cycle of composed and integrated information systems as: substantiation of quantitative system requirements to hardware, software, users, staff, technologies; requirements analysis; estimation of project engineering decisions and possible danger; detection of bottle-necks; investigation of problems concerning potential threats to system operation and information security; testing, verification and validation of IS operation quality; rational optimization of IS technological parameters; substantiation of plans, projects and directions for effective system utilization, improvement and development etc. Owing to preventive measures, recommended by using the results of the analytical modelling operation processes, the risks in IS life cycle may be mitigated and a level of IS quality and safety - increased.

References

[1] Feller, W. (1971). *An Introduction to Probability Theory and Its Applications*, Vol. II, Willy.

[2] Klimov, G. P. (1983). *Probability theory and mathematical statistics*. Moscow State University, Moscow, 328.

[3] Kolowrocki, K. & Soszynska-Budny, J. (2011) *Reliability and Safety of Complex Technical Systems and Processes*, DOI:10.1007/978-0-85729-694-8, Springer-Verlag London Limited, 405.

[4] Kostogryzov, A. (2000) 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, 25-29 September, 2000, 63-70.

[5] Kostogryzov, A. I. et al. (2014) *The Foundations of Counteremergency Stability for Coal Enterprises*. V. 6 “Industrial safety”. Book 11. - Moscow: “Gornoje delo” Kimmerijsky Center Ltd., 336.

[6] Kostogryzov, A. I. et al. (2015) *Security of Russia. Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific*

Foundations of Technogenic Safety / Edited by N.Machutov – Moscow: «Znanie», 936.

[7] Kostogryzov, A. I., Petuhov, A. V. & Scherbina, A. M. (1994) *Foundations for evaluation, providing and increasing output information quality in application to automatized systems.* Moscow: "Armament. Policy. Conversion", 278.

[8] Kostogryzov, A. I., Stepanov, P. V, Nistratov, G. A. et al. (2015) *Innovative Management Based on Risks Prediction*, Information Engineering and Education Science – Zheng (Ed.). Taylor & Francis Group, London, ISBN 978-1-138-02655-1. 159-166.

[9] Kostogryzov, A. I. & Stepanov, P. V. (2008). Innovative management of quality and risks in systems life cycle, *Armament. Policy. Conversion*, Moscow, 404. (in Russian)

[10] Kostogryzov, A., Nistratov, A. & Nistratov, G. (2012). Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars*, Gdańsk/Sopot, Poland, 3, 1, 1-14.

[11] Kostogryzov, A., Grigoriev, L., Nistratov, G. et al. (2013). Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes, *American Journal of Operations Research. Special Issue* 3, 1A, 217-244, [available at: http://www.scirp.org/journal/ajor/].Kostogryzov, A. & Nistratov, G. (2004). Standardization, mathematical modelling, rational management and certification in the field of system and software engineering, *Armament Policy Conversion*, Moscow, 395. (in Russian)

[13] Kostogryzov, A., Nistratov, G. & Nistratov, A. (2012). Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, *Total Quality Management and Six Sigma*, InTech. 127-196, [available at: http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management].

[14] Kostogryzov, A., Nistratov, G. & Nistratov, A. (2013). The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields. *International Journal of Engineering and Innovative Technology (IJEIT)* 3, 3, 146-155, [available at: http://www.ijeit.com/archive.php].Zio E. (2006) *An Introduction to the Basics of Reliability and Risk Analysis*, World Scientific, 222.