MATHEMATICAL MODELS AND SOFTWARE TOOLS FOR QUALITY AND RISK MANAGEMENT ACCORDING STANDARD REQUIREMENTS

Prof. **Andrey Kostogryzov**
Director of the Research Institute of Applied Mathematics and Certification,
1-st Miasnikovskaja Ul., Vl. 3, Moscow, Russia,107564, tel. +7(495) 795-8524,
e-mail: akostogr@gmail.com

Abstract

The offered mathematical models and supporting them software tools complexes (M&STC) are purposed for a systems analysts from customers, designers, developers, users, experts of testing laboratories and certification bodies, as well as a staff of quality maintenance for any complex system etc. M&STC are focused on providing system standard requirements on the base of modeling random processes that exist for the life cycle of any complex system. Models implement original author's mathematical methodology based on probability theory, theory for regenerating processes and methods for system analysis. M&STC may be also used in training and education for specializations "System engineering", "Software engineering", "System safety and security", "Information systems".

1. Introduction

According to standard ISO/IEC 15288 system is defined as a combination of interacting elements organized to achieve one or more stated purposes. An application of offered methodology uses to evaluate probabilities of "success", cost, time and quality risks and related profitability and expenses. This helps to solve on the scientific basis the next practical problems in system life cycle: analysis of quality management systems for enterprises, substantiation of quantitative system requirements to hardware, software, users, staff, technologies; requirements analysis, the evaluation of project engineering decisions; investigation of problems concerning potential threats to system operation including information security and protection against terrorists; evaluation of system operation quality, substantiation of recommendations for rational system use and optimization etc.

2. Focusing on rational management

All complexes are offered for providing rational management. Management is a purposeful changing of an object state, a process or a system. Management is based on choosing one among a set of alternatives. Rational management is a management leading to the objective achievement according to the criterion of a chosen parameter extreme (minimum or maximum) under the set limitations. Classical examples of rational management are usually either maximization of a profit (an income, a degree of quality or security, etc.) under limitations on expenses or expenses minimization under limitations on an admissible quality and/or security level. It is clear that criterion and limitations may vary throughout the system life.

For rational management of processes it is necessary to know and plan their behaviour at various influences. For this purpose we offer for using about 100 the mathematical models [1,2]. As criterion parameters there are used the quantity measures (objective functions) characterizing a possibility of object achievement at different stages of a system life cycle. For example, an investor's criterion is the maximum income from the project implementation under limitations on the production process and product quality. For the enterprise it is important to organize a quality management system properly – so that in the form of criterion it can choose the probability of qualified work performance, i.e. in time and without defects or the maximum probability of success for quality management policy concerning work complexes. A security service must provide safety of an object, a process or a system up to the mark. In this case there may be used the criterion of expenses minimum under limitations on the admissible level of dangerous influence risk taking countermeasures into account or minimum of a dangerous influence risk at limitations on expenses. The customer and the developer are interested in the final result – in this case as an integrated parameter there may be used such criterion as the maximum part of functional operations carried out with the admissible quality or the relative degree of customer satisfaction with the limitations on quality or expenses.

The first from the offered models is Complex for Evaluation of Information Systems Operation Quality (CEISOQ) [1-2,5-6]. The development of CEISOQ was based on the general purpose for all information systems (see Fig. 1 and 2).

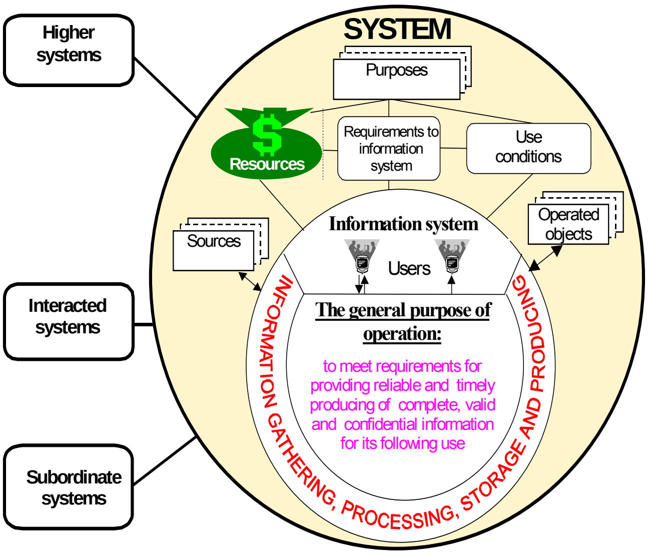

Higher systems
SYSTEM
Purposes
Resources
Requirements to information system
Use conditions
Sources
Information system
Operated objects
Users
Interacted systems
The general purpose of operation:
to meet requirements for providing reliable and timely producing of complete, valid and confidential information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

Fig.1 The purpose of information system in a SYSTEM

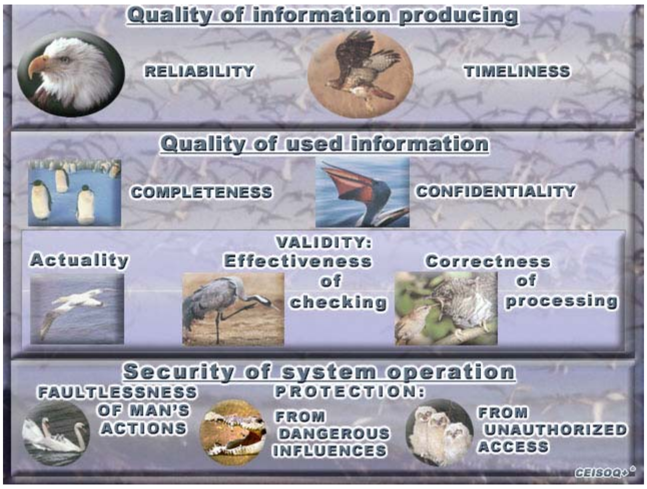

Quality of information producing
RELIABILITY
TIMELINESS
Quality of used information
COMPLETENESS
CONFIDENTIALITY
Actuality
VALIDITY:
Effectiveness of checking
Correctness of processing
Security of system operation
FAULTLESSNESS OF MAN'S ACTIONS
PROTECTION:
FROM DANGEROUS INFLUENCES
FROM UNAUTHORIZED ACCESS
CEISOQ

Fig. 2 The main CEISOQ window for choosing the model

The problems connected with usual computation of parameters are called direct operation research problems or analysis problems. The problems directed on a choice of variants maximizing or minimizing values of objective functions under limitations are called inverse operation research problems or synthesis problems. The offered models and supporting software tools allow to solve both direct and inverse operation research problems.

3. Abstract formalization

This formalization is used to building a probabilistic space (Ω, B, P), 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 [3];
P – a probability measure on a space of elementary events Ω.

Because, $\Omega=\{\omega_k\}$ is limited, there is enough to establish a reflection $\omega_k \rightarrow p_k = P(\omega_k)$ 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 [3-4] 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 mathematical models to support an assessment of standard system processes.

4. Example of created mathematical model

Nowadays at system development and utilization an essential part of funds is spent on providing system protection from various dangerous influences able to violate system integrity. Under system integrity it means such system state when system purposes are achieved with the required quality under specified conditions of use. Such examples of dangerous influences are terrorists attacks, viruses or ‘violators’ influences, software defects events etc. As this problem wasn’t studied carefully dangerous influences often reach their aims.

There are examined three typical technologies of providing protection from dangerous influences. In this paper it is illustrated only technology 1 that is based on preventive diagnostics of system integrity. Diagnostics is carried out periodically. It is assumed that except diagnostics means there are also included means of necessary integrity recovery after revealing of danger sources penetration into a system or consequences of negative influences. Integrity violations detecting is possible only as a result of diagnostics, after which system recovery is started. Dangerous influences on a system are acted step-by step: at first a danger source penetrates into a system and then after its activation begins to influence. System integrity is considered to be violated only after a danger source has influenced on a system. If to compare a system with a man technology 1 reminds a periodical diagnostics of a man’s health state. If diagnostics results have revealed symptoms of health worsening a man is cured (and integrity is considered as recovered). Between diagnostics an infection penetrated into a man’s body brings a man into an unhealthy state (a dangerous influence is realized and integrity is violated)–see Fig. 3.

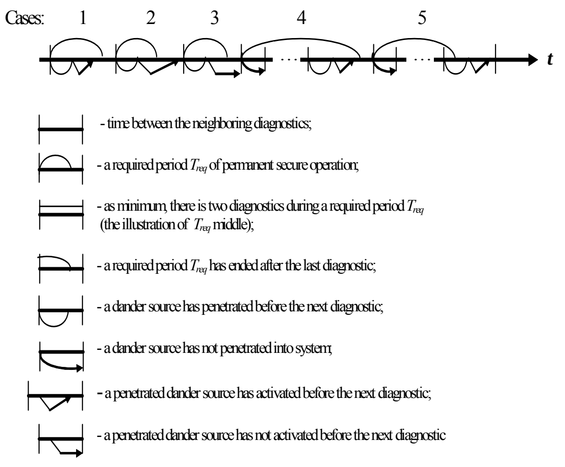

Cases: 1 2 3 4 5
t
- time between the neighboring diagnostics;
- a required period T_{req} of permanent secure operation;
- as minimum, there is two diagnostics during a required period T_{req} (the illustration of T_{req} middle);
- a required period T_{req} has ended after the last diagnostic;
- a dander source has penetrated before the next diagnostic;
- a dander source has not penetrated into system;
- a penetrated dander source has activated before the next diagnostic;
- a penetrated dander source has not activated before the next diagnostic

Fig. 3 The illustration of system resources protection against dangerous influences by technology 1

The availability of means of danger sources total-lot detecting and existence of ways of violated system integrity total-lot recovery is obligatory requirement. The offered models are supported by software tools CEISOQ.

Te system protection from dangerous influences may be evaluated if the next characteristics are known: frequency of influences for penetrating a danger source into a system (σ) ; mean activation time of a penetrated danger source (β); time between the end of diagnostic and the beginning of the next one ($T_{betw.}$); diagnostic time including the time of system integrity recovery ($T_{diag.}$); a required period of system operation ($T_{req.}$) for investigation. There are possible the next variants:

variant 1 – the assigned 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 ($T_{req} \geq T_{betw.}+T_{diag}$).

Statement 1. Under the condition of independence of considered characteristics the probability of dangerous influence absence for variant 1 is equal to

$$P_{infl.(1)}(T_{req}) = 1 - B_{penetr} * B_{activ}(T_{req}), \qquad (1)$$

where * - is convolution sign, $B_{penetr}(t)$ is the probability distribution function (PDF) of time between neighboring influences for penetrating a danger source, $B_{activ}(t)$ is the PDF of activation time of a penetrated danger source, for modeling $B_{penetr.}(t)=1-e^{-\sigma t}$, $B_{activ}(t)=1-e^{-t/\beta.}$

Note. This formula (1) is used also for the evaluation of security for system operation without diagnostics. There is supposed that before the beginning of period T_{req} system integrity is provided.

Statement 2. Under the condition of independence for considered characteristics the probability of dangerous influence absence for variant 2 is equal to

$$P_{infl.(2)}=P_{mdl}+P_{end} \qquad (2),$$

where P_{mdl} – is the probability of dangerous influence absence within the period T_{req} since beginning to the last diagnostic, P_{end} – is the probability of dangerous influence absence within the period T_{req} after the last diagnostic, i.e. in the last remainder $T_{rmn}=T_{req}$ -N(T_{betw}+ T_{diag}), N is the number of periods between diagnostics placed wholly within assigned period T_{req},

N = [T_{req}/(T_{betw} + T_{diag})] – is integer part;

$P_{wholly(1)}$ =$P_{infl.(1)}$(T_{betw} +$T_{diag.}$), is calculated by formula (1),

$$P_{mdl} = \frac{N\left(T_{betw.} + T_{diag.}\right)}{T_{req.}} \cdot P_{wholly(1)}{}^{N}, \qquad P_{end} = \frac{T_{rmn}}{T_{req.}} \cdot P_{\mathbf{inf}\, l.(1)}(T_{rmn}). \qquad (3)$$

The mathematical proof is in [1,2]. This is one from more than 100 mathematical models offered to support an assessment of standard system processes.

5. Software tools to support an assessment of standard system processes

35 created software tools complexes implementing original mathematical models [1-2,5-6] consist complexes created in 2001-2005: for the Evaluation of Information Systems Operations Quality (CEISOQ, CEISOQ+); for Evaluation of System Vulnerability including Conditions of Terrorist Threats ("VULNERABILITY"); for complex analysis of system security ("ANALYSIS OF SYSTEM SECURITY"), for Modeling of System Life Cycle Processes "MODELING OF PROCESSES". The last complex "MODELING OF PROCESSES" includes multi-functional complexes for evaluation of Agreement (models and software tools "ACQUISITION", "SUPPLY"), Enterprise (models and software tools "ENVIRONMENT MANAGEMENT", "INVESTMENT MANAGEMENT", "LIFE CYCLE MANAGEMENT", "RESOURCE MANAGEMENT", "QUALITY MANAGEMENT") and Project (models and software tools "PROJECT PLANNING", "PROJECT ASSESSMENT", "PROJECT CONTROL", "DECISION-MAKING", "RISK MANAGEMENT", "CONFIGURATION MANAGEMENT", "INFORMATION MANAGEMENT") Processes Modeling and also for Technical Processes Modeling (models and software tools "REQUIREMENTS DEFINITION", "REQUIREMENTS ANALYSIS", "ARCHITECTURAL DESIGN", "HUMAN FACTOR", "IMPLEMENTATION", "INTEGRATION", "VERIFICATION", "TRANSITION", "VALIDATION", "OPERATION", "MAINTENANCE", "DISPOSAL").

The models created have undergone extensive testing in an operational environment and the results have been compared with the results of other independent models (if such exist). This comparison has provided documented evidence that the models implemented in these tool suites are realistic, including the reality of the calculations and the time&probabilistic characteristics. Created software tools are an original Russian creation patented by Rospatent, certified, have been presented at seminars, working groups, symposiums, conferences and forums since 2000 in Russia, Australia , the USA, Canada, France, Germany, Kuwait. In 2001 the CEISOQ [1-2,5-6] was awarded be the Golden Medal of the International Innovation and Investment Salon, in 2004-2005 the software tools "RISK MANAGEMENT", "HUMAN FACTOR" and "ARCHITECTURAL DESIGN" also were awarded by the Golden Medal of the International Exhibition "Intellectual Robots" and acknowledged as the software products of the year.

How these models adequacy may be conformed? Though any answer to these questions won't be irrefragable for a certain system we shall try to formulate our arguments.

Argument 1. The M&STC uses mathematical models formalizing standard processes on time line. Majority of dependencies gives upper and lower estimations. The fact is that while shaping models all mathematical results are initially drawn in the integral form. As input data are somehow connected with time after choosing distribution functions characterizing these data there were selected the gamma – distribution and the Erlang's distribution. Mathematicians know that these distributions approximate sums of positively distributed random variables well. Every temporary data are as a matter of fact such a sum of compound time expenses. Studies of regularities have shown that extremes are achieved on bounds of these distributions, i.e. of exponential and deterministic (discrete) distributions. Thus, real values will be somewhere between lower and upper estimations calculated by the software tools.

Argument 2. As a basis of models there is used the probability theory and the theory of regenerative processes. Proofs of basic theoretical results are cited in [1-2]. If to return in the 70-s of the last century we may remember the boom of mathematical modeling, defining calls flow reliable and time-probabilistic characteristics. The boom passed and appeared the reliability theory, the queuing theory and a variety of models, which proved themselves to be effective. There are created standards and other normative documents regulating system methodical evaluations on the basis of these models. Nowadays these models are widely used and trusted because they produce reliable results confirmed in the course of time. It is worth to remind that these created theories and models are based on the probability theory and the theory of regenerative processes. The several offered models "The model of functions performance by a system in conditions of unreliability of its components", "The models complex of calls processing", "The model of entering into system data current concerning new objects of application domain" are the classical adapted models of the 80-s improved to meet the requirements of the present time. The other models are created on the basis of the limit theorem for regenerative processes developed in the 70-80-s in Moscow State University on the faculty of computing mathematics and cybernetics by professor Klimov's school [4]. Three-year testing of M&STC including beta-testing by fifty different companies raise confidence in models algorithmic correctness.

Argument 3. Skilled analysts know that if a probabilistic analytical model is incorrect then if input data are changed in the range from $-\infty$ to $+\infty$ there are always errors appearing either in infraction the probability theory laws or in illogic of dependencies behavior (most probably on the bounds of possible values) or in impossibility of obtained effects physical explanation. Bounds of input data in the M&STC are assigned in the range from $-\infty$ to $+\infty$ or to be more exact from 10^{-8} milliseconds to 10^{8} years.

Argument 4. As far as possible any designer tends to use several models of different authors. If results of different models use are not divergent a designer begins to trust not only to results but also to the models. Comparison of results of the M&STC use with results of other models use proved its high adequacy (concerning computations of reliability and time-probabilistic characteristics, the other models don't have analogues).

6. Examples of software tools application

The offered M&STC have been and are applied for solving the problems of:

information security and reliability for banks, transport systems, protected and military objects etc.;

rational protection for oil and gas systems in conditions of terrorist threats;

quality and reliability for cosmic robot systems and heat supply etc.;

risk analysis for dangerous coal mine and manufactures;

system certification;

education in the field of system analysis.

Below there are demonstrated some capabilities of the software tools "RISK MANAGEMENT".

Example 1 for demonstration the capabilities of subsystem "Evaluation of counteraction measures effectiveness". Let 10 barriers be installed in order to protect valuable resources of a system from unauthorized access. In table there are shown prospective characteristics of barriers (as counteraction measures) and the mean time of their possible overcoming by a specially prepared violator (as the time of keeping measure effectiveness). Real values of similar characteristics may be received as a result of natural experiments or application of other special models.

It is required to evaluate the risk of dangerous influence on a system in spite of counteraction measures during a week. The minimal admissible risk shouldn't be more than 0.0001. The initial data for calculations are shown in the Table.

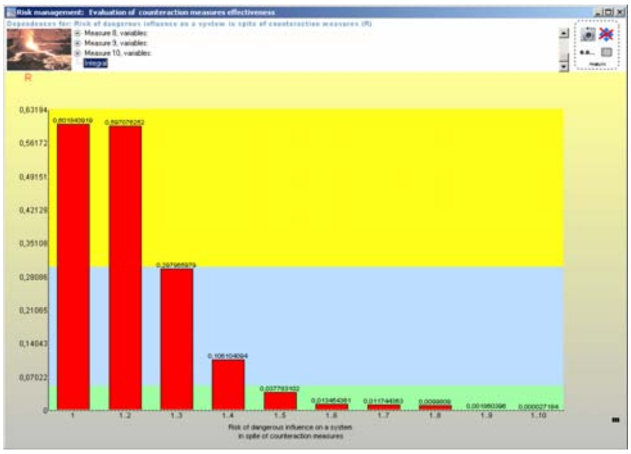
Table

Characteristics of the threat scenario and the protection system

Barrier	***Change frequency of the barrier parameter value as time to the next strenthening of the measure***	***Mean time of barrier overco-ming by a violator***	***Possible way of barrier overcoming***
1. External guards	*Change of guards every 24 hours*	*10 hours*	*Latent penetration*
2. System of passes to the system with a change of security services	*Change of guards every 24 hours*	*10 minutes*	*Documents falsification, conspiracy, fraud*
3.The electronic key to get to the control unit	*5 years (time between changes)*	*1 week*	*Theft, forcible key withdrawal, conspiracy*
4. The password to enter the automated system	*1 month*	*10 days*	*Spying, compulsory questioning, conspiracy, selection of a password*
5. The password to get access to software devices	*1 month*	*10 days*	—//—
6. The password to get access to the required information	*1 month.*	*10 days*	—//—
7. The registered external information carrier with write access	*1 year*	*24 hours*	*Theft, forced registration, conspiracy*
8. Confirmation of a user identity, during a session of work with the computer	*1 month.*	*24 hours*	*Spying, compulsory questioning, conspiracy*
9. Telemonitoring	*Time between changes of software devices – 5 years*	*1 month*	*Simulation of a failure, false films, dressing up as employees, conspiracy*
10. Encoding of the most important information	*Change of keys every month*	*1 year*	*Decoding, conspiracy*

<u>Solution.</u> The analysis of the withdrawn calculated dependences has shown the following (see Fig. 4).

The first 3 barriers as counteraction measures are overcome with the probability about 0.34. Use of alternating passwords once a month for the 4th, 5th and 6th barriers allows to decrease the risk from 0.34 to 0.14. However, the general system protection after the introduction of the first six barriers remains rather weak. The 7th and 8th counteraction measures are practically useless. Use of telemonitoring means allows to decrease risk of dangerous influence on a system in spite of counteraction measures to 0.002 what also doesn't meet the stated requirements. The use of all 10 counteraction measures provides the required system protection.

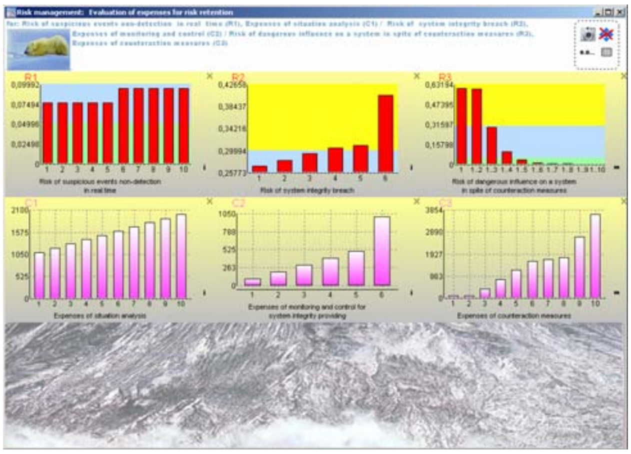


Risk management: Evaluation of counteraction measures effectiveness

Dependences for: Risk of dangerous influence on a system in spite of counteraction measures (R)

Fig. 4 *Results of computation for example 1*

The use of subsystem “Evaluation of expenses for risk retention” allows to define expenses against risks (see calculation results on Fig. 5). It is the capability to optimizing by criterion “risk-expenses”.



Risk management: Evaluation of expenses for risk retention

for: Risk of suspicious events non-detection in real time (R1), Expenses of situation analysis (C1) / Risk of system integrity breach (R2), Expenses of monitoring and control (C2) / Risk of dangerous influence on a system in spite of counteraction measures (R3), Expenses of counteraction measures (C3)

R1
0,09992
0,07494
0,04996
0,02498
0
1 2 3 4 5 6 7 8 9 10
Risk of suspicious events non-detection in real time
R2
0,42658
0,38437
0,34216
0,29994
0,25773
1 2 3 4 5 6
Risk of system integrity breach
R3
0,63194
0,47395
0,31597
0,15798
0
1 1.2 1.3 1.4 1.5 1.6 1.7 1.8 1.9 1.10
Risk of dangerous influence on a system in spite of counteraction measures
C1
2100
1575
1050
525
0
1 2 3 4 5 6 7 8 9 10
Expenses of situation analysis
C2
1050
788
525
263
0
1 2 3 4 5 6
Expenses of monitoring and control for system integrity providing
C3
3854
2890
1927
963
0
1 2 3 4 5 6 7 8 9 10
Expenses of counteraction measures

Fig. 5 *Results of computation by the subsystem “Evaluation of expenses for risk retention”*

The use of subsystem “Substantiation of counteraction strategy against risks” allows to evaluate different damages and expenses against risks for the given scenario.

The last complex “ANALYSIS OF SYSTEM SECURITY” allows to evaluate the integral security for the system consisting of any number of components. The condition is the components are united in parallel and/or consecutive order. The structure may be any degree of complexity. The strength of every measure (component) is approximated by exponential low.

Example 2 for demonstration the capabilities of subsystem “Analysis of integral security”. Let the system contains 3 level of interacted subsystems: higher subsystem, interim subsystem and subordinate subsystem (see Fig.1). It may be territorially distributed enterprise or bank with the branches etc. Every subsystem have the valuable resources protected by the counteraction measures from the table (see example 1). The system structure, constructed by software tools for modeling, is on Fig.6. The frequency of threats source appearance is 10 times in a year by qualified violator, the mean time for system recovery is 1 hour.

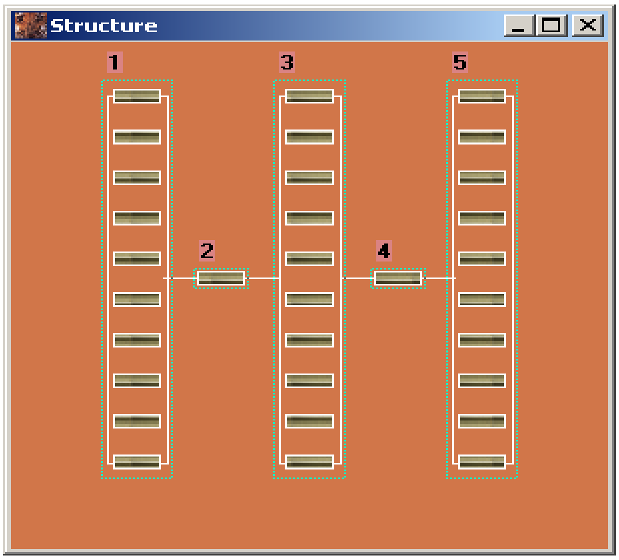
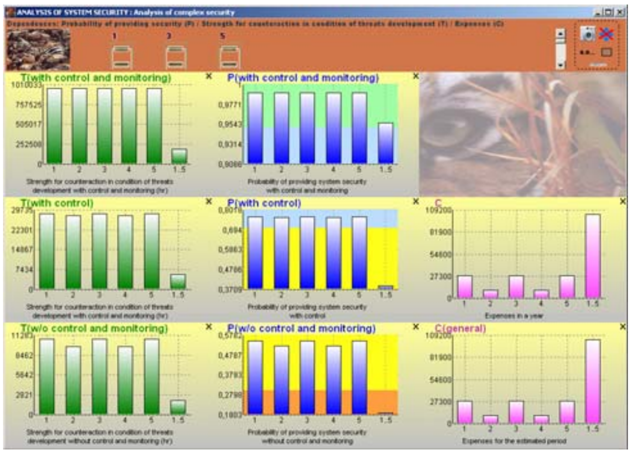


Fig. 6 System structure for modeling

It is required to evaluate the probability of providing system security in a year for the given scenario of threats.

<u>Solution.</u> The integral analysis of the withdrawn calculated dependences has shown the following (see Fig. 7). The probability of providing system security without control and monitoring is about 0.19, with periodic control (without permanent monitoring for the 9-th and 10-th barriers) - 0.39. The use of all 10 counteraction measures (including permanent monitoring for the 9-th and 10-th barriers) provides system security with the probability more than 0.95 against general expenses 104000 conditional units .



ANALYSIS OF SYSTEM SECURITY : Analysis of complex security

Dependences: Probability of providing security (P) / Strength for counteraction in condition of threats development (T) / Expenses (C)

1
3
5
T(with control and monitoring)
1010033
757525
505017
252508
0
1 2 3 4 5 1..5
Strength for counteraction in condition of threats development with control and monitoring (hr)
P(with control and monitoring)
1
0,9771
0,9543
0,9314
0,9086
1 2 3 4 5 1..5
Probability of providing system security with control and monitoring
T(with control)
29735
22301
14867
7434
0
1 2 3 4 5 1..5
Strength for counteraction in condition of threats development with control and monitoring (hr)
P(with control)
0,8018
0,694
0,5863
0,4786
0,3709
1 2 3 4 5 1..5
Probability of providing system security with control
C
109200
81900
54600
27300
0
1 2 3 4 5 1..5
Expenses in a year
T(w/o control and monitoring)
11283
8462
5642
2821
0
1 2 3 4 5 1..5
Strength for counteraction in condition of threats development without control and monitoring (hr)
P(w/o control and monitoring)
0,5782
0,4787
0,3793
0,2798
0,1803
1 2 3 4 5 1..5
Probability of providing system security without control and monitoring
C(general)
109200
81900
54600
27300
0
1 2 3 4 5 1..5
Expenses for the estimated period

Fig. 7 Results of computation by the subsystem
“Analysis of integral security”

7. Conclusion

Expected pragmatic effect from application is the next. It is possible to provide essential system quality and security rise and/or avoid wasted expenses in system life cycle on the base of processes modeling by the offered mathematical models and software tools complexes.

8. References

[1] M.M. Bezkorovainy, A.I. Kostogryzov, V.M. Lvov *Modeling Software Complex for Evaluation of Information System Operation Quality CEISOQ. 150 problems of analysis and synthesis and examples for their solutions,* Moscow: Armament.Policy.Conversion, 2001, 222p.

[2] A.I. Kostogryzov, G.A. Nistratov *Standardization, mathematical modeling, rational management and certification in the field of system and software engineering,* Moscow: Armament.Policy.Conversion, 2004, 395p. (in Russian)

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

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

[5] A.I. Kostogryzov *"Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ)"*. Proceedings of the 34-th Annual Event (25-29 September 2000) of the Government Electronics and Information Association (GEIA), 2000 Engineering and Technical Management Symposium, 2000, 63-70.

[6] A.I. Kostogryzov *"Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ)"*. Information assurance in computer networks: methods, models and arhitectures for Network Security, Proceedings/ International Workshop MMM ACNS 2001, St.Peterburg, Russia, May 21-23 2001, LNCS (2001), 90-101.