Chapter 7

Some Applicable Methods to Analyze and Optimize System Processes in Quality Management

Andrey Kostogryzov, George Nistratov and Andrey Nistratov

Additional information is available at the end of the chapter

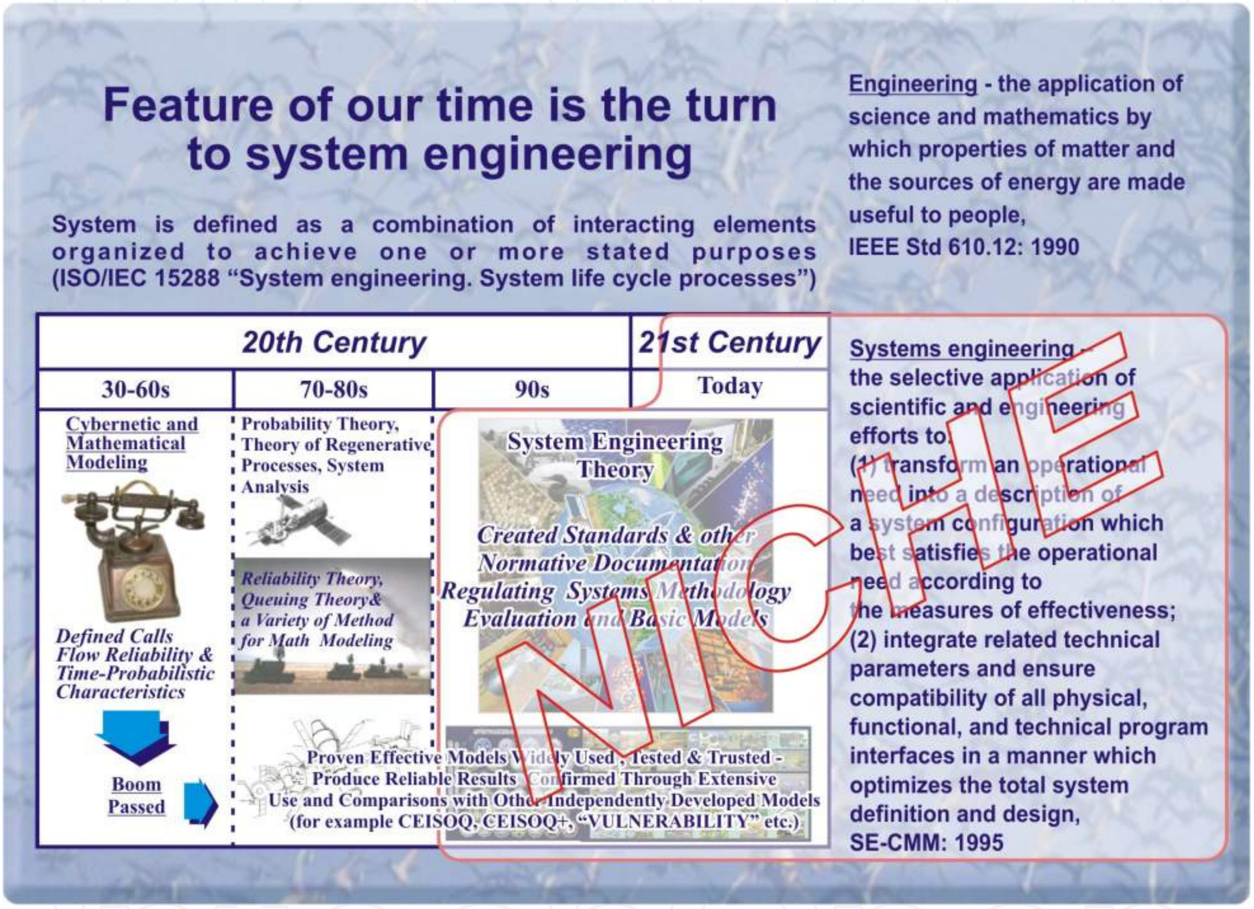
http://dx.doi.org/10.5772/46106

1. Introduction

The complexity of present man-made systems has reached an unprecedented level. In fact any system is grounded on computer technologies in the sense that it contains computer elements or is modeled or supported with the help of computer. This trend resulted in new opportunities and at the same time caused additional difficulties. Shortcomings in integration of scientific, engineering, management, and financial areas, which are used to ensure an effective system development and employment, now become more obvious. Today processes of system life cycle in different conditions and threats are the main objects for forecasting, analysis and optimization. Indeed these objective changes become the main reason for establishing the first system engineering ISO/IEC standard ISO/IEC 15288 “System Engineering - System Life Cycle Processes" (since 2002). Covering systems in industrial, energetic, transport, aerospace, military and other fields, this standard recommends to perform only the actions that were substantiated and not to act in the directions, which were not estimated and justified. It means that feature of our time is the turn to system engineering – see Figure 1.

Up-to-date approach to system maturity refers us to international standards ISO 9001 and 9004, ISO/IEC 15026, 15504, CMMI etc. It is clear without "system analysts" there is not achievable the highest level “Optimizing”, but also a previous “Predictable” level. However many customers and Chief Designers often fail to take quantitative system requirements into consideration, they do so wittingly or through an oversight. From now on these omissions do not conform to the requirements of the international standards. It is only the beginning. What will be the continuation?

Nowadays if comprehensive quantitative system requirements were not established in quality management, the system efficiency and customer satisfaction can not be controlled and confirmed. To great regret in many application areas the system requirements do not allow to understand the true reasons of failures. However the degree of processes influences on a final result should be estimated and often may be managed! Let's consider information system. Standards recommend to propose requirements for system reliability during given period, for the information timeliness, completeness, actuality, faultlessness after checking, correctness of processing, protection against dangerous influences and unauthorized accesses, and if needed information confidentiality. It means that those system requirements should be set that are focused on customer satisfaction according to used information.



Feature of our time is the turn to system engineering

System is defined as a combination of interacting elements organized to achieve one or more stated purposes (ISO/IEC 15288 "System engineering. System life cycle processes")

Engineering - the application of science and mathematics by which properties of matter and the sources of energy are made useful to people, IEEE Std 610.12: 1990

20th Century			21st Century
30-60s	70-80s	90s	Today
Cybernetic and Mathematical Modeling Defined Calls Flow Reliability & Time-Probabilistic Characteristics Boom Passed	Probability Theory, Theory of Regenerative Processes, System Analysis Reliability Theory, Queuing Theory& a Variety of Method for Math Modeling	System Engineering Theory Created Standards & other Normative Documentation Regulating Systems Methodology Evaluation and Basic Models	

Proven Effective Models Widely Used, Tested & Trusted - Produce Reliable Results Confirmed Through Extensive Use and Comparisons with Other Independently Developed Models (for example CEISOQ, CEISOQ+, "VULNERABILITY" etc.)

Systems engineering - the selective application of scientific and engineering efforts to: (1) transform an operational need into a description of a system configuration which best satisfies the operational need according to the measures of effectiveness; (2) integrate related technical parameters and ensure compatibility of all physical, functional, and technical program interfaces in a manner which optimizes the total system definition and design, SE-CMM: 1995

Figure 1. Now applicable models, methods, software tools and technologies support standard system requirements

Unfortunately many graduates from technical colleges and universities do not use the foundations of "system analysis", "operations research", "mathematical modelling" in quality management, they missed the particulars of existing methods and models. And without use of mathematical models they can only dream about deep logical investigation to predict forthcoming effects. That pawns the doubtful base of high risks to the future systems. There is more deeper increasing break between needs for competitive system quality and methodical opportunities of the experts, called these needs to estimate, substantiate and satisfy without wasted expenses. Time has come to make again more popular mathematical models for rational solving the problems of quality management.

The goal of this work is to propose models, methods, and software tools well-tested in practice, for forecasting quality and risks as applied to newly developed and currently operated manufacture, power generation, transport, engineering, information, control and measurement, food storage, quality assurance and security systems. Presented work is devoted to the researches of standard processes for providing effective quality management in systems life cycle. It covers logically closed contour: « system requirements of standards – supporting mathematical models to estimate probabilities of success, risks, profits and damages – ways of rational management». Thereby the reader can substantiate answers on system engineering questions: «How to reach in quality management the level of international standards?», «Is expected quality achievable?», «Can be the system requirements met?», «How much safe are those or others scenarios?», «What about the real risks, profits and possible damages?», «What choice is rational?», «What measures are more effective?», «What rational measures should lead to estimated effect without waste expenses, when, by which controllable and uncontrollable conditions and costs?» and others. The answers may be received before critical events (not only after these events).

While reading this work, the reader will be shipped in logic of standard processes, which can spend resources and be compared on a timeline in different conditions. This implies an understanding of system requirements, strength of mathematical models and optimization methods, i. e. everything that is vitally important but has never been in the focus of attention of either technical specialists or students. Certainly, in the justification of such indifference it is possible to refer to doubts of the famous physicist Albert Einstein. He has spoken, as far as the laws of mathematics refer to reality, they are not certain, and as far as they are certain, they do not refer to reality. But now we are living at the time of innovations! While understanding that this century-old dictum is negative for the chances of our work to be a success, we nevertheless decided not to 'loose' advanced physicists for the sake of their own interests. Thereto 10 practical examples are investigated and explained, the detailed 'hardware' of the work, other hundreds examples and routine comments are gathered at the References of the book and on site *www.mathmodels.net*. These new results are a humble initial contribution of author's to the 'coin-box' of the knowledge base for decision support to improve quality management, boost the efficiency and safety of different systems and/or reduction of nonproductive costs.

And now we can review briefly our own experience. There is an inconceivable ocean of practical problems which are subjects to the decision with use of system forecasting. Existing decisions from one area are far from being always appeared applicable in other areas. As a result in 9 cases from 10 it was necessary to create original mathematical models. Their quantity grew. Further, having analyzed problems and approaches to the decision of system engineering, there was clear uniformity of a train of thought of modern system analysts in various spheres. The logic scheme everywhere is identical: at first the set of destabilizing factors and threats against quality and-or safety is defined, then taking into account available resources the possible measures of neutralization should be chosen or developed. A vulnerability set of system comes to light. Technologies of system control and recovery of broken integrity should be implemented as counteraction against destabilizing factors and threats (there where expediently - continuous monitoring of conditions is used). Thus at every step of system life cycle the development of processes is supported by probabilistic forecasts, criteria of optimization are chosen in depending on the problem purposes. According to these rational decisions are made on the base of mathematical modelling and optimization.

Natural tests of road also are fraught with serious consequences. Therefore mathematical modelling becomes more and more popular. For this reason the described universal scheme of the system analysis has laid down in a basis of the presented below models methods and software tools. Modelling shouldn't be carried out only for modelling itself. If as a result of modelling we get only one value it is not quite clear how we should appreciate it (such a disadvantage is typical for simulation models, which require thousands executions of the same data, what is not made sometimes because of time-shortage; inverse problems solving is almost impossible for such kind of models). That is why the offered software tool suites, which uses only analytical models, is developed in such a way that it is possible in a split second to carry out computations, catch tendencies, reveal stability of processes in case of input data changes in the range –50% +200% and in a few minutes (!) to find admissible solutions of complex inverse synthesis problems. As a result of the offered models use a system analyst gets an ability to sense not a computed point but the whole quality field, which may be appropriate to system at different scenarios of system operation and environment behavior. Why you should trust to evaluating results by the offered models? In other words how models adequacy is substantiated? Though any answer to these questions won't be irrefragable for a certain system we shall try to formulate our arguments (experience readers understand that any model needs in similar arguments).

Argument 1. 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 (Feller, 1971) 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 of the software tools, if computation results are presented by one curved line they are lower estimations. The results reflect pessimistic value for following using.

Argument 2. As a basis of our models we used the probability theory and the theory of regenerative processes (i.e. recurring processes). Proofs of basic theoretical results are received, for example, by (Gnedenko, 1973; Klimov, 1983). If to return in the 70-s of the last century we may remember the boom of mathematical modelling, 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 models of subsections 3.2 – 3.4 are the classical models of the 70-s improved and developed 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.

Argument 3. Skilled analysts know that if a probabilistic analytical model is incorrect then if input data are changed in the range from -∞ to +∞ 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 offered software tools are assigned in the range from -∞ to +∞ (more precisely from 10-8 milliseconds to 108 years). Three-year testing of models including beta testing by fifty different independent companies raise confidence in software tools algorithmic correctness.

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 presented software tools with results of other models use proved their high adequacy (concerning computations of reliability and time-probabilistic characteristics, the other models don’t have analogues).

The offered software tools are an original Russian creation patented. They have been presented at seminars, symposiums, conferences, ISO/IEC working groups and other forums since 2000 in Russia, Australia, Canada, China, Finland, France, Germany, Kuwait, Luxembourg, Poland, Serbia, Ukraine, the USA, etc. The software tools were awarded by the Golden Medal of the International Innovation and Investment Salon and the International Exhibition “Intellectual Robots”, acknowledged on the World's fair of information technologies CeBIT in Germany, noted by diplomas of the Hanover Industrial Exhibition and the Russian exhibitions of software. The offered technology of modelling through the Internet has been acknowledged as the best project-2007 by the National Association of Innovations and Developments of Information Technologies of Russia.

Having analyzed results of long-term our practice, we, authors, have noticed the following. Many scientific researches, practical investigations, implementations and recommendations based on use of our models, methods, and software tools were bringing increasingly deep satisfaction not only to ourselves but, most important:

- to developers, i. e. all of our colleagues involved in the works (since the obtained results can be proved step-by-step and their usefulness checked; forecasts were confirmed in time; and, respectively, the number of profitable orders has been growing),
- to customers (since we managed to convince them that the residual system risks may and should be mitigated proactively; and now they have scientific justification of the

amount of investments adequate to achieved quality and safety levels that may be guaranteed for the allocated money),

- to users (the forecast made in time has mobilized them on the basis of the 'forewarned is forearmed' concept; using our recommendations, in utilization stage they can extract from the system the best effects, that were assumed in concept, design&development and support stages).

This work is purposed for systems analysts from customers, developers, users, as well as investigators and staff of quality and security management, experts of testing laboratories and certification bodies. It can be used in system life cycle to form system requirements, compare different processes, substantiate technical decisions, carrying out tests, adjust technological parameters, estimate quality and risks. The decisions, scientifically proved by the offered models and software tools, can provide purposeful essential improvement of quality and mitigation of risks and decrease expenses for created and operating systems. The spectrum of the explored systems is indeed broad; it includes systems operated by government agencies, manufacturing structures (including enterprises, oil-and-gas and transport facilities, and hazardous production systems), food storage, power generation, financial and business, aviation and space industry, emergency services, municipal economy, military, etc. Moreover, our assessments and forecasts are generated much faster, feature innovations, have invariably high quality and, most important, the expected effects may be easily interpreted (what specifically is the result and how it can be reached) regardless of whether it pertains to increase in gains or reduction in losses. Eventually, having gained experience and being sure that those instruments are of use, we decided to share our knowledge and skills for analyzing and optimizing system processes in quality management. It should be stressed from the very beginning that no one forces you to use these proposed models, methods, and software tools. Any author trusts primarily his/her own models and is suspicious about someone else's if uses them at all. From this perspective we also understand our colleagues from the writers' community, share their doubts and nevertheless invite them... Join us, the esteemed reader. The knowledge that you will gain after even brief acquaintance with the work or just browsing the book and then comprehending its content will not allow you to continue unsystematic life without forecasting quality and risks! You can easily verify this author's forecast.

2. Review of system processes to reveal general engineering problems that are due to be solved by the mathematical modeling

System analysis is an important science intensive process, which is connected with system concept, development, production, utilization and support. As a result of adequate system analysis we extend our knowledge about systems, obtained quality dependency on different system characteristics and about a degree of system purposes achievement. This knowledge allows a customer to formulate substantiated requirements and specifications, a developer - to implement them rationally without wasted expenses, a user – to use system potential in the most effective way. Let's review some system standards - ISO 9001 "Quality

Management Systems - Requirements", ISO/IEC 15288 "System Engineering – System Life Cycle Processes", ISO/IEC 12207 "Information Technology - Software Life Cycle Processes", ISO/IEC 15504 "Information Technology –Process Assessment", ISO/IEC 17799 "Code of Practice for Information Security Management", IEC 60300 «Dependability Management», IEC 61508 "Functional safety of electrical/ electronic/ programmable electronic safety-related systems", CMMI "Capability Maturity Model Integration", "GOST RV 51987 "Information technology. Set of standards for automated system. The typical requirements and metrics for information systems operation quality. General provisions", some standards for use in the oil&gas industry (ISO 10418 "Basic surface safety systems", ISO 13702 "Control & mitigation of fire & explosion", ISO 14224 "Reliability/maintenance data", ISO 15544 "Emergency response", ISO 15663 "Life cycle costing", ISO 17776 "Assessment of hazardous situations" etc. - from the role of system analysis point of view. These are the representative part of the modern system and software engineering standards.

In compliance with ISO 9001 to all processes there can be applied methodology known as "Plan-Do-Check-Act" (PDCA). Plan: from system analysis point of view it means that all parties should understand in equal measure the essence of customer requirements, metrics and admissible level of goals achievement. Do: it implies that implemented processes meet customer requirement on admissible level. Check: there should be used methods and tools for evaluations. Act: used methods should allow appearing dependencies and determining adequately an effective way for expected improvement. For any improvement a documented procedure shall be established to define requirements for determining potential nonconformities and their causes, evaluating the need for action to prevent occurrence of nonconformities, determining and implementing action needed.

In compliance with the standard ISO/IEC 15288 system analysis actions are the main actions for achievement system purposes in life cycle including required propositions in Agreement, Enterprise, Project and Technical Processes. In compliance with the standards ISO/IEC 12207 system analysis problems are to be solved to meet system requirements with resources optimization. The standard ISO/IEC 17799 is used for providing information security purposes. This and others like standards in security area (for example, ISO/IEC 15443, ISO/IEC 13335 etc.) imply that high effectiveness of system protection measures should be evaluated and confirmed quantitatively. It means that any system security evaluations need in an adequate mathematical methodology. The standard IEC 60300 describes the approaches to the risk analysis of technological systems from system analysis point of view. The standard IEC 61508 includes Parts "Examples of methods for the determination of safety integrity levels" and "Overview of techniques and measures" that recommend to evaluate system risks. An application of CMMI allows selecting the order of improvement that best meets the organization's business objectives and mitigates the organization's areas of risk. And these results are also based on system analysis.

To understand the situation with requirements and applicable methods to analize and optimize system processes an existing practices for providing system quality and safety were reviewed. The integral results of safety analysis are presented on Figure 2.

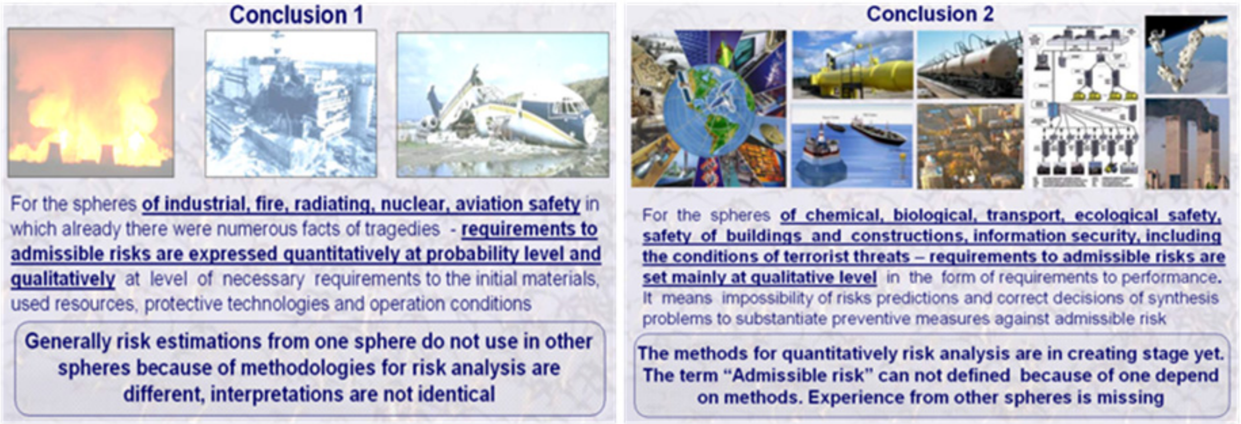
Some situations with modelling of processes for system quality are more wide viewed in this book. According to applicable mathematical models everyone (majority) solves the problems "how can", we can resume: all organizations need quantitative estimations, but only some part from them uses modelling complexes; used models are highly specialized, input and calculated metrics are adhered strongly to specificity of systems; existing modelling complexes have been created within the limits of concrete order for the systems and as a rule are very expensive.

Thus the summary of the analysis of existing approaches is the next.

1. Analysis of quality and risks is carried out mainly at qualitative level with assessments "better or worse". Independent quantitative estimations at probability level are carried out for specially created models.
2. Generally risk estimations from one sphere do not use in other spheres because of methodologies for risk analysis are different, interpretations are not identical. The methods for quantitatively risk analysis and quality analysis (on probability level) are in creating stage yet. The terms "Acceptable quality" and "Admissible risk" in use should be defined on probability scale level only in dependence on corresponding methods. As consequence probability estimations are not comparable for different areas, experience from other spheres is missing, comparisons for systems from different areas, as a rule, are not used, as universal objective scale of measurement is not established yet.
3. In all cases effective risk management for any system is based on: a) uses of materials, resources, protective technologies with more best characteristics from the point of view of safety, including integrity recovery; b) rational use of situation analysis, effective ways of the control and monitoring of conditions and operative recovery of integrity; c) rational use of measures for risk counteraction.
4. It does not allow to solve the main problems of a substantiation of system requirements to parameters of information gathering and analysis, control, monitoring and counteraction measures at restrictions, and also to confirm about efficiency of the prevent measures for providing quality and safety!

Note. System integrity is defined as such system state when system purposes are achieved with the required quality.

In general case system methods for analyzing and optimizing are founded completely on the mathematical modelling of system processes. We understand that any process is a repeated sequence of consuming time and resources for outcome receiving. In general case the moments for any activity beginning and ending are, in mathematical words, random events on time line. Moreover, there exists the general property of all process architectures. It is a repeated performance for majority of timed activities (evaluations, comparisons, selections, controls, analysis etc.) during system life cycle - for example see on Figure 3 the problems that are due to be solved by the mathematical modelling of processes according to ISO/IEC 15288.



Conclusion 1

For the spheres **of industrial, fire, radiating, nuclear, aviation safety** in which already there were numerous facts of tragedies - **requirements to admissible risks are expressed quantitatively at probability level and qualitatively** at level of necessary requirements to the initial materials, used resources, protective technologies and operation conditions

Generally risk estimations from one sphere do not use in other spheres because of methodologies for risk analysis are different, interpretations are not identical

Conclusion 2

For the spheres **of chemical, biological, transport, ecological safety, safety of buildings and constructions, information security, including the conditions of terrorist threats – requirements to admissible risks are set mainly at qualitative level** in the form of requirements to performance. It means impossibility of risks predictions and correct decisions of synthesis problems to substantiate preventive measures against admissible risk

The methods for quantitatively risk analysis are in creating stage yet. The term "Admissible risk" can not defined because of one depend on methods. Experience from other spheres is missing

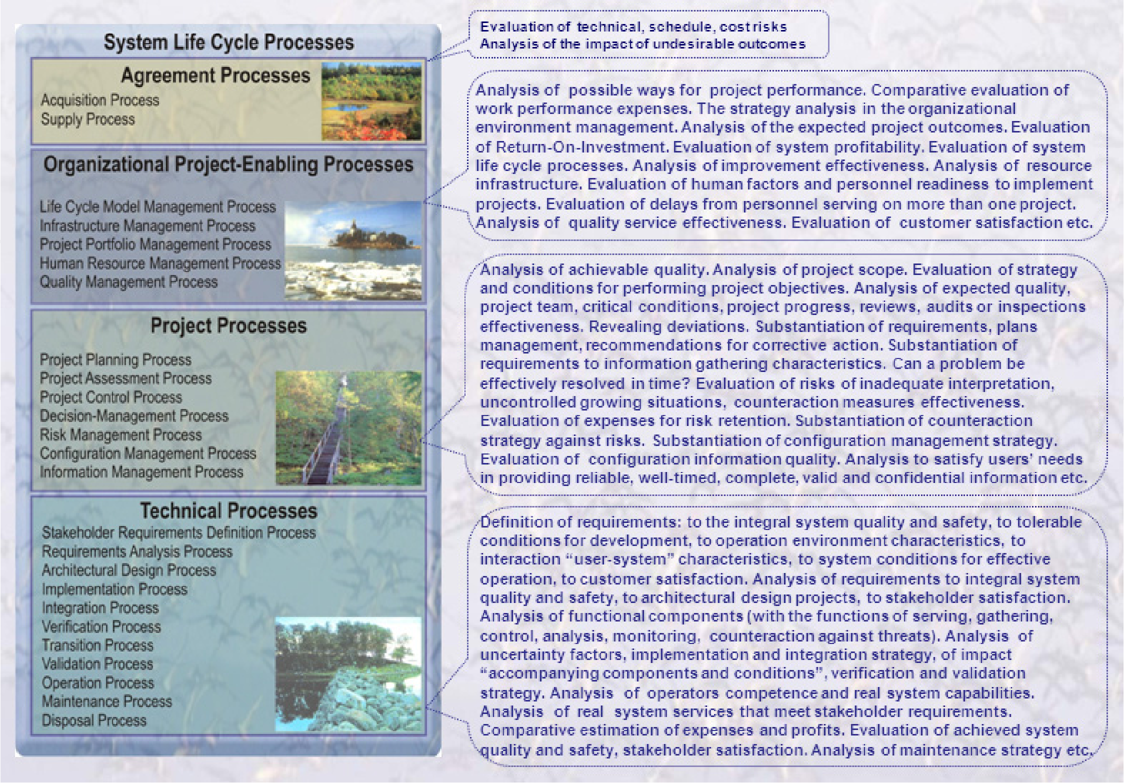
Figure 2. Conclusions of safety analysis

This work focuses on the way for extracting latent system effects from system processes by using universal metrics: probabilities of success or failure during a given period for an element, subsystem, system. Calculation of these metrics within the limits of the offered probability space built on the basis of the theory for random processes, will allow to predict outcomes on an uniform scale, quantitatively to prove levels of acceptable quality and admissible risks, to solve the problems of synthesis, answering preventive a question « What rational measures should lead to estimated effect without waste expenses, when, by which controllable and uncontrollable conditions and costs?».

Below we describe many-sided analysis of quality management. Thus we want to help the reader in solving problems of providing system effectiveness, which depends on both the reviewed system quality parameters and the parameters of pragmatic usefulness in a certain domain. They cover many important engineering problems in a systems life cycle - see Figure 4.

There exist different process-centered methods and integrated tool suites for systems analysis (see for instance Guide to the Software Engineering Body of Knowledge SWEBOK). In sections 3 and 4 we illustrate the original approaches based on mathematical modelling. Many analysis and synthesis problems and their solutions are demonstrated in section 5. However detailed mathematical definition for all problems is omitted not to overload a reader by complicated mathematical propositions, which require deep knowledge of the probability theory, theory of regenerative processes and mathematical analysis. You may find full mathematical models and their proofs (Martin (1972); Gnedenko (1973); Kleinrock (1976), Matweev & Ushakov (1984) etc.).

As a resume we can define the role of analysis and optimization system processes in compliance with modern engineering standards as decisive for rational reaching system operation quality. From analyst's point of view system analysis reduces system uncertainties and provides a quantitative basis to predict and choice in balancing business needs, quality, risks and specified requirements.



System Life Cycle Processes

Agreement Processes

Acquisition Process
Supply Process

Organizational Project-Enabling Processes

Life Cycle Model Management Process
Infrastructure Management Process
Project Portfolio Management Process
Human Resource Management Process
Quality Management Process

Project Processes

Project Planning Process
Project Assessment Process
Project Control Process
Decision-Management Process
Risk Management Process
Configuration Management Process
Information Management Process

Technical Processes

Stakeholder Requirements Definition Process
Requirements Analysis Process
Architectural Design Process
Implementation Process
Integration Process
Verification Process
Transition Process
Validation Process
Operation Process
Maintenance Process
Disposal Process

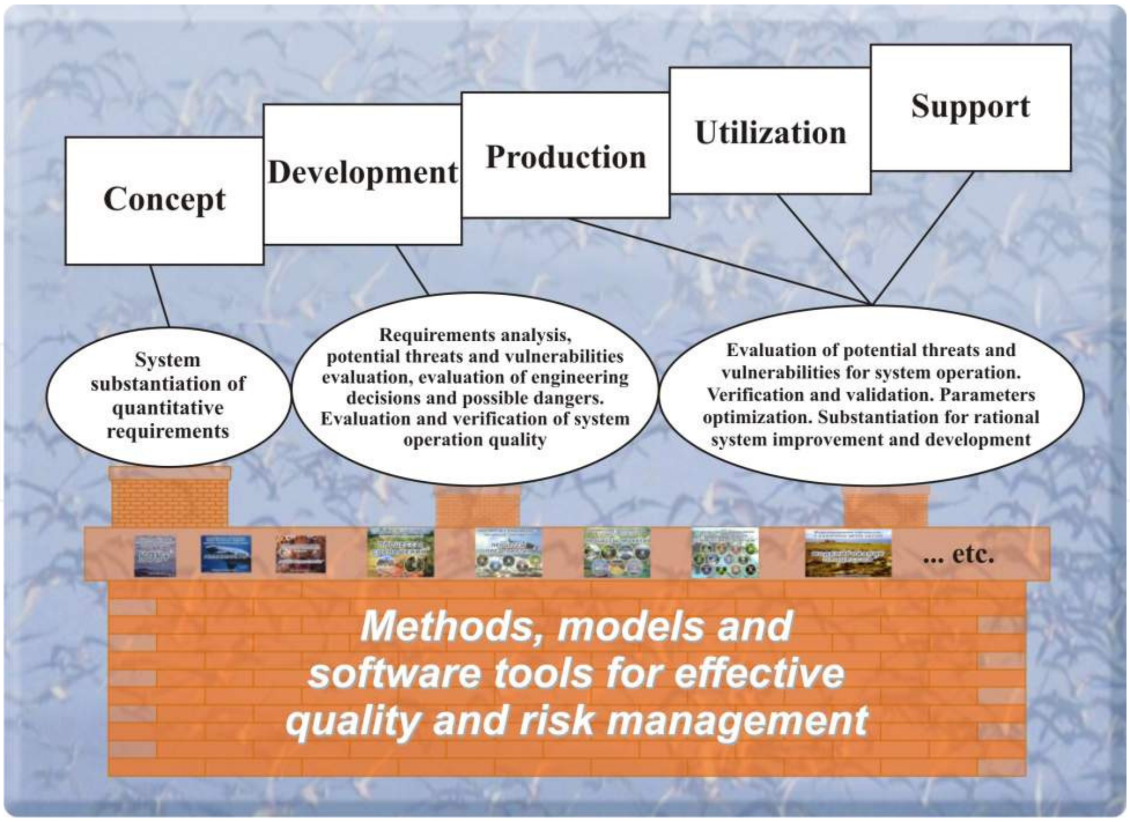
Evaluation of technical, schedule, cost risks
Analysis of the impact of undesirable outcomes

Analysis of possible ways for project performance. Comparative evaluation of work performance expenses. The strategy analysis in the organizational environment management. Analysis of the expected project outcomes. Evaluation of Return-On-Investment. Evaluation of system profitability. Evaluation of system life cycle processes. Analysis of improvement effectiveness. Analysis of resource infrastructure. Evaluation of human factors and personnel readiness to implement projects. Evaluation of delays from personnel serving on more than one project. Analysis of quality service effectiveness. Evaluation of customer satisfaction etc.

Analysis of achievable quality. Analysis of project scope. Evaluation of strategy and conditions for performing project objectives. Analysis of expected quality, project team, critical conditions, project progress, reviews, audits or inspections effectiveness. Revealing deviations. Substantiation of requirements, plans management, recommendations for corrective action. Substantiation of requirements to information gathering characteristics. Can a problem be effectively resolved in time? Evaluation of risks of inadequate interpretation, uncontrolled growing situations, counteraction measures effectiveness. Evaluation of expenses for risk retention. Substantiation of counteraction strategy against risks. Substantiation of configuration management strategy. Evaluation of configuration information quality. Analysis to satisfy users' needs in providing reliable, well-timed, complete, valid and confidential information etc.

Definition of requirements: to the integral system quality and safety, to tolerable conditions for development, to operation environment characteristics, to interaction "user-system" characteristics, to system conditions for effective operation, to customer satisfaction. Analysis of requirements to integral system quality and safety, to architectural design projects, to stakeholder satisfaction. Analysis of functional components (with the functions of serving, gathering, control, analysis, monitoring, counteraction against threats). Analysis of uncertainty factors, implementation and integration strategy, of impact "accompanying components and conditions", verification and validation strategy. Analysis of operators competence and real system capabilities. Analysis of real system services that meet stakeholder requirements. Comparative estimation of expenses and profits. Evaluation of achieved system quality and safety, stakeholder satisfaction. Analysis of maintenance strategy etc.

Figure 3. The problems that are due to be solved by mathematical modelling of processes



Concept

Development

Production

Utilization

Support

System substantiation of quantitative requirements

Requirements analysis, potential threats and vulnerabilities evaluation, evaluation of engineering decisions and possible dangers. Evaluation and verification of system operation quality

Evaluation of potential threats and vulnerabilities for system operation. Verification and validation. Parameters optimization. Substantiation for rational system improvement and development

... etc.

Methods, models and software tools for effective quality and risk management

Figure 4. System engineering problems which are solved on the base of system analysis in quality management

As the first objects for demonstrating author's original approach to analyze and optimize system processes the information systems (IS) are selected. We will not attract readers' attention listing uncountable features of IS because the effect of their implementations is obvious in all spheres of human activities.

3. Models and software tools to analyze information system processes

3.1. General propositions

On information technology market there is offered a wide choice of engineering solutions that are able to satisfy functional requirements of a customer. You may choose an acceptable variant if you are guided by logical considerations. The thing is that you cannot be sure whether this variant is rational or not if to estimate it from the point of view of integral system operation goals achievement. The answer is likely to be positive if the technological solution is intended for an enterprise system, which goal is to get the highest benefit from goods manufacturing and sale. In this case the criterion for choosing a manufacturing computer system may be the one of upgrading goods quality and increasing the company profits under expenses limitations. And what will be the answer if to speak about IS, which production is output information? The criterion for providing IS high quality is the use of models and methods that allow to estimate, investigate and optimize processes of information gathering, processing, storage and producing. The basis for the functions performance is the integration of computers, software, communications and human capabilities. IS are the most important integral components of financial, transport, energy, customs, military and other SYSTEMS.

It is clear that requirements to IS operation depend on general SYSTEM purposes, use conditions (including potential threats), available resources, information sources facilities and communication requirements (see Figure 5). There is impossible to provide IS operation quality without the help of models and implementation tools. Its use allows to estimate the reliability and timeliness of information producing, the completeness, validity and confidentiality of the used information from users' point of view. This is the logical basis to create universal mathematical models and software tools which could estimate IS operation quality, compare various IS engineering projects, reveal "bottle-necks" and optimize the processes of information gathering, storage and processing. Such original mathematical models have been introduced in processes of IS development, use and maintenance.

The idea of estimating IS operation quality appeared as a result of studying potential threats to output information (see Figure 6). The results of their use to analyze technical solutions in processes of designing, developing, producing, using, supporting and certifying proved their effectiveness and multifunctional capabilities.

The main windows for choosing the mathematical models is illustrated on Figure 7. The modelling software tools complex CEISOQ+ is one of the few scientific and technical masterpieces, which satisfy most of the high requirements of the intellectual market. Moreover, this complex has appeared quite in time. The market requires the quantitative substantiation of engineering solutions and the IS quality validation. It is pleasant that CEISOQ+ developed by those who work in the field of defense reveals a new conceptual approach to quality.

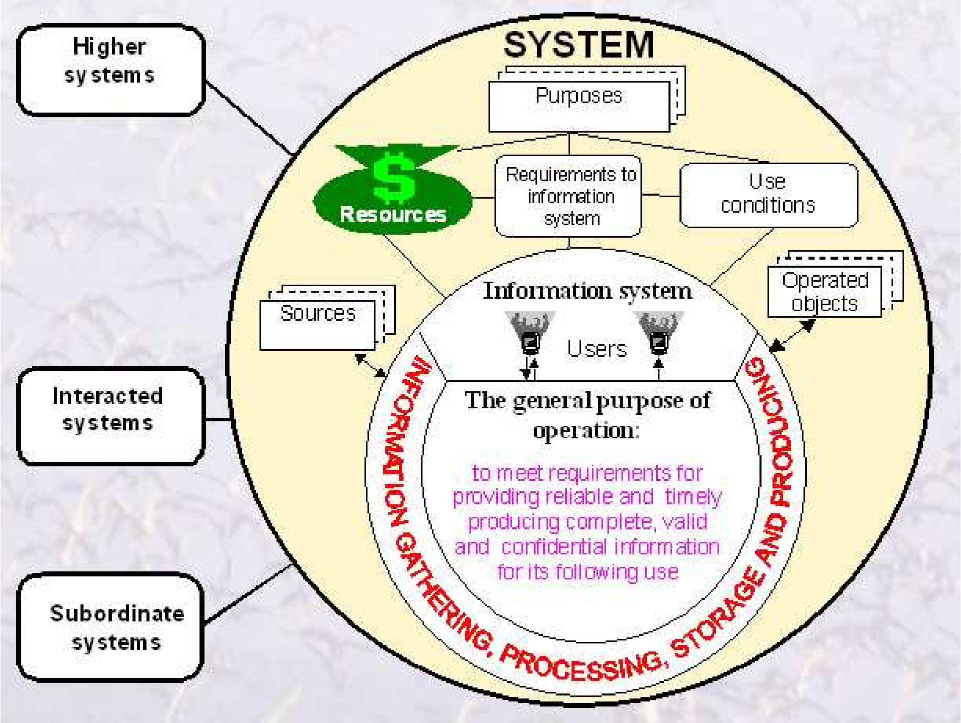

SYSTEM
Higher systems
Interacted systems
Subordinate systems
Purposes
$
Resources
Requirements to information system
Use conditions
Sources
Operated objects
Information system
Users
The general purpose of operation:
to meet requirements for providing reliable and timely producing complete, valid and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

Figure 5. The place and the purpose of information system in a SYSTEM

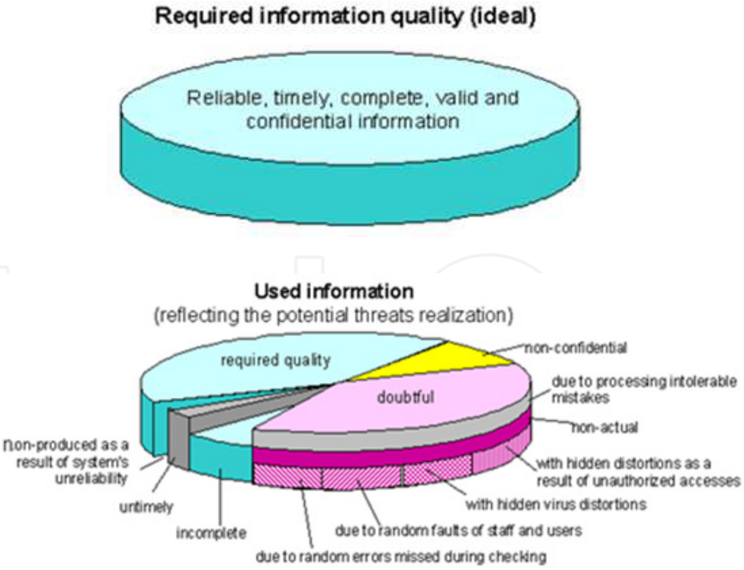


Figure 6. Potential threats to output information according to general purpose of IS operation

The created modelling Complex for Evaluation of Information Systems Operation Quality (CEISOQ+) allows to simplify and to spread the use of the next mathematical models: of functions performance by a system in conditions of unreliability of its components; complex of calls processing; of entering into IS current data concerning new objects of application domain; complex of information gathering from sources; of information analysis; of dangerous influences on a protected system; of an unauthorized access to system resources.

The offered original mathematical models intended for estimating the level of the IS operation purpose achievement are supported by the created software tools CEISOQ+.

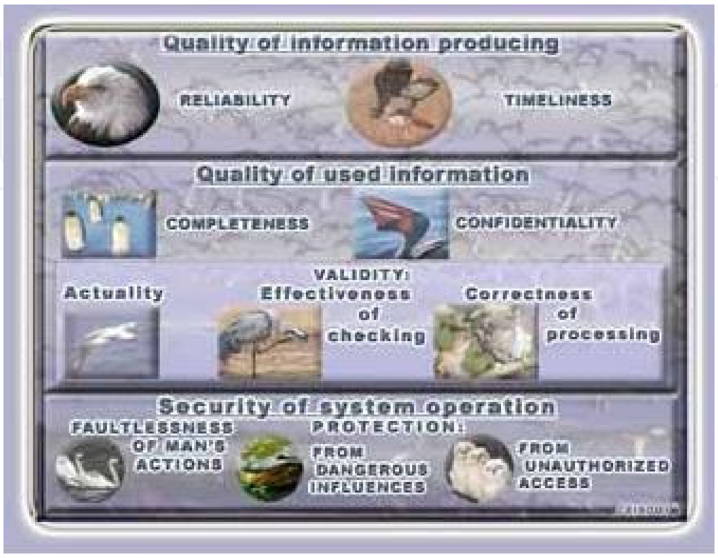

Quality of information producing
RELIABILITY
TIMELINESS
Quality of used information
COMPLETENESS
CONFIDENTIALITY
Actuality
VALIDITY:
Effectiveness of checking
Correctness of processing
Security of system operation
FAULTLESSNESS OF MAN'S ACTIONS
PROTECTION:
FROM DANGEROUS INFLUENCES
FROM UNAUTHORIZED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

Figure 7. The main windows of software tools CEISOQ+

To make the understanding easier we didn't take into detail consideration that information quality depends on kind of input information, on functional tasks to be accomplished and on different users' requirements to conditions of IS operation. These dependencies were studied in a special complex IS operation quality investigation (Kostogryzov et al. (1994, 2000-2002)).

The software tools CEISOQ may be applied for solving such system problems appearing in an information systems 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.

Every system analyst (an IS customer, designer, developer, expert of testing laboratories and certification bodies etc.) may become a user of the software tools CEISOQ+. The CEISOQ+ may also be helpful in training programs for skilled specialists and educational programs of students studying information systems estimation.

The use of models and the software tools CEISOQ+ on different stages of an IS life cycle allows to answer the following questions: what quantitative requirements should be to hardware/software devices operation time between failures and to system repair time? which information operation processes should be duplicated and how? what processing devices and technologies should be chosen to achieve the necessary level of system throughput? what about the system tolerance to data flows changing? what data flows and functional tasks may be considered as the main causes of bottlenecks? what level of preparation, transfer and input productivity and what data gathering technologies can guarantee the completeness and actuality of information? which engineering solutions can provide the actuality of information? what about the quantitative level of information control quality? what qualification quantitative requirements should be for the staff and users? how dangerous are scenarios of environment influences and what protective technologies will provide the required security? how the use of protective technologies will influence on the IS operation quality characteristics? how the use of integrity diagnostics and security monitoring will worsen time-probabilistic characteristics of a system? what protection system effectiveness should be to prevent an unauthorized access? what about quantitative level of information security risks? etc.

This appendix is dedicated to building a probabilistic space (Ω, B, P) for the evaluation of system operation processes, 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 $w_k \rightarrow p_k = P(w_k)$ like that $\mathrm{p}_\mathrm{k} \geq 0$ and $\sum_k p_k = 1$.

Such space (Ω, B, P) is proposed on the base of processes architectures formalization by the limited theorems for regenerative processes (Feller (1971), Gnedenko (1973), Klimov (1983), etc.) and also by using principal propositions of probability theory and theory for random processes. The proofs of the mathematical formulas used by the CEISOQ+, see (Kostogryzov et al. (1994, 2000-2002)).

3.2. Reliability of information producing

Problems of reliability have been solved already as related to technical means and systems but they are extremely urgent concerning. The reliability standards require acknowledgement of these values achievement. It is clear that without modelling acknowledgement of IS reliability, which consists of dozens territorially distributed software resources, may be obtained only as a result of its use. Such a use is a risk and every risk must be substantiated. Indeed there is no choice except modelling.

Modelling of functions performance reliability may be carried out with the help of the next model.

What about the logical idea for modelling processes from the point of view to provide reliability of information producing? From the point of formal reliability any system, subsystem or their components may be in "operable" or in "inoperable" condition during given period Θ. Let an operable condition is identified with the formulated condition "component provides reliable functions performance during period Θ". Period, connected with system repairing after failure, is signed as "system does not provide reliable functions performance during period Θ'. Then both mentioned conditions complete the set of elementary events for stochastic process $\xi_{rel.}(t)$ defining the system condition at the time t and functionality for period Θ after t, i.e.

$$\xi_{\text{rel.}}(\text{t}) = \begin{cases} \text{“system provides reliable functions performance during period}\,\theta\text{,”} \\ \text{if system is in operable condition before moment t and during period}\,\theta\,\text{begun at the moment}\,t; \\ \text{“system does not provide reliable functions performance during period}\,\theta\text{,”} \\ \text{if system is in inoperable condition at the moment}\,t\,\text{or a failure will be during period}\,\theta\,\text{begun at the moment}\,t. \end{cases}$$

The next variants are possible:

a) a virtual moment t has overtaken the system in operable condition and there has not been a failure during period Θ (failure means change from operable in inoperable condition), in this case system operation is characterized by condition “system provides reliable functions performance during period Θ”, i.e. the event of reliable functions performing is going on;

b) a failure has happened during period Θ, in this case system operation is characterized by conditions “system does not provide reliable functions performance during period Θ';

c) system is not capable for functions performing because one is in inoperable conditions at the moment t. Then it is going on the event “system does not provide reliable functions performance during period Θ'.

The next **statement 1** is proposed on the base of introduced formalization.

Statement 1. The limited probability of providing reliable function performance by system during the required time exists under the condition of existence for stationary probability distributions for considered characteristics and their independence. One is equal to

$$P_{rel} = \int_0^\infty \left\{ \int_t^\infty V(\tau - t)\, dN(\tau) \right\} dt \Bigg/ \int_0^\infty t\, d\left[N * W(t) \right], \tag{1}$$

where N(t) - is the probability distribution function (PDF) of time between neighboring failures (T_{MTBFnk} is the mean time); W(t) – is the PDF of repair time ($T_{rep.}$ is the mean time); V(t) – is the required period PDF of permanent system operation when reliability should be provided ($T_{req.}$ is the mean time);* - is the convolution sign.

The proof of this and others statements of the chapter 3 see (Kostogryzov et al. (1994, 2000-2002)) and site www.mathmodels.net.

Convolution of complex system framework into framework for one unit is implemented by usual methods (see, for example subchapter 4). The final clear analytical formulas for modelling are received by Lebesgue – integration (1) expression and convolution of complex system framework in to single-unit system.

The next variants are used in modelling of functions performance reliability: a) period Θ is strict deterministic and equals to $T_{req.}$ (discrete distribution $V(t)$); b) $V(t)=1-exp(-t/T_{req.})$ when period Θ is exponential distributed (i.e. one is variable) and its mean is equal to T_{req} ; c) $W(t)=1-exp(-t/T_{rep.})$. Input: n is the conditional number of a subsystem; k is the conditional number of a unit; *TMTBF nk* is the mean time between hardware/software failures for the *k*-th unit of the *n*-th subsystem;*Trep.* is the mean time of system repair after any unit failure. Customer requirements: *Treq.* is the mean required period of permanent IS operation when reliability should be provided; $P_{adm.}$ is the admissible probability of providing reliable functions performance by IS during the required time $T_{req.}$.

With the subsystem "Reliability" of CEISOQ+ the next reliability metrics may be evaluated: $T_{MTBF\ n}$ – the mean time between failures of the n-th subsystem in an active redundancy mode; $T_{MTBF\ 1..n}$ - is the mean time between failures of a complex composed of 1, 2,…, n subsystems, each of which can perform its functions both in active and passive redundancy modes; $\mathbf{P}_{rel\ n}$ – is the probability of reliable *n*-th subsystem functions performance during the period $\mathbf{T}_{req.}$ both in active and passive redundancy modes; $\mathbf{P}_{rel\ 1..n}$ - is the probability of reliable functions performance by a complex composed of 1, 2,…, n subsystems during the time $\mathbf{T}_{req.}$ when redundant elements are used both in active and passive redundancy modes; $\mathbf{P}_{rel}$ – is the probability of reliable functions performance during the time $\mathbf{T}_{req.}$ when redundant elements are used both in active and passive redundancy modes, $\mathbf{P}_{rel} = \mathbf{P}_{rel\ 1..N}$, where *N* – is the number of subsystems in the modeled system; $\mathbf{K}_{avail.}$ – is the system availability when redundant elements are used both in active and passive redundancy modes, $K_{avail.} = \lim\limits_{T_{req.} \to 0} P_{rel.}(T_{req.})$, i.e. if to set very small $T_{req.}$ (for example 1 millisecond) the evaluated value P_{rel} approximates $K_{avail.}$.

3.3. Timeliness of information producing

Data circulated in a system, resources spent by process performer, queries for operator processing, output as a result of input flows for transforming into outputs may be formally calls for processing in a queue system. To estimate timeliness of required calls processing by process architectures let's examine existing approaches to their formalization. According to researches various methods of the queuing theory provide rather high degree of adequacy for calls processing modelling. There may be quite a few processing technologies: priority and unpriority processing by one or several servers, multiphase processing, time-sharing processing etc. Now there are some methodical approaches to estimation of some technologies under various conditions including the ones to analysis of computing systems and networks. As applied to queueing systems the term "processing technology" means the same with the term "processing mode, order or discipline", determining an order of call selection from a queue buffer for further processing. For example in accordance to information systems these calls are not only the ones on receiving of output documents but also on files transfer or information entering into a database, as well as technological calls on control of a computing process, access administration, information security providing.

It is proposed to formalize processes of users' information servicing as processing of Poisson flows by reliable singleserver or multiserver queuing system with a buffer of an infinite size. In practice process architectures for calls processing are formalized often as processing of Poisson calls flows by single-server or multi-server queuing system with a buffer of an infinite size. A supposition concerning Poisson calls flows may be substantiated by the fact that among Palma type flows a Poisson flow puts the queuing system in the most hard conditions and for queuing time metrics gives upper estimations. Moreover, calls flows of the same type as a rule constitute a compound flow from different sources. In practice, each flow intensity is very low in comparison with the compound flow. In such a situation theorem (Grigolionis (1963)) is applicable, according to which the compound flow is a Poisson flow. All the cited considerations as well as statistical researches results prove a possibility of assumption concerning Poisson calls flows. On the analogy with this a supposition concerning an exponential law of calls processing time distribution also allows to get pessimistic estimation of system response time.

There are several approaches to an analytical estimation of calls processing timeliness in queuing systems. The simplest is the one allowing a distribution function of system response on a call. It is necessary to note that an explicit distribution function may be got only for simplest systems without priorities, for example, for system M/M/1/∞ (Gnedenko (1973)). There is another approach to estimation of systems for which distribution functions of system response time are expressed in terms of various Laplace-Stielies transformations (Gnedenko (1973)). For the wide range of priority systems M/G/1/∞ with different processing technologies time-probabilistic characteristics are drawn in such a form. The expressions of joint distribution of a queue length and waiting queue time are drawn in the form of a functional dependency in terms of various Laplace-Stielties transformations and productive (generating) functions. They give an idea of mathematical complexity of models. In this case the desired probability may be computed on the basis of invert Laplace-Stielties transformations. Though there are some applied ways of such invert transformations practical computations require not only additional programming on a high level but also essential time expenses. Such conditions complicate a work of a system analyst. That’s why in practice there often used approaches providing approximate estimations of the desired probability. The most popular way of approximate estimation consists in an approximation of a response distribution function with the help of the incomplete gamma-function. J.Martin’s studies of some priority processing technologies proved rather high engineering accuracy of such an approximation (Martin (1972)). This approach is used by the CEISOQ+.

A supposition concerning infinite number of queuing buffer in practice means allotment for storage of calls, input and output data such system memory sizes that guarantee in case of right system use absence of information losses caused by possible buffer’s overflow. Though last years we can trace a stable tendency of main storage and external storage memory size expansion together with its price reduction. Problems with lack of memory for information systems appear more seldom and it seems they won’t cause any troubles in the nearest future. Taking into account all the abovementioned the supposition concerning infinite number of queuing buffer seems to be acceptable for many cases.

The core of formalization is: modelling by means of priority and unpriority queuing systems M/G/1/∞ is possible (Gnedenko (1973); Kleinrock (1976), Matweev & Ushakov (1984) etc.**)**.

The offered models and software tools CEISOQ+ allow to estimate and to compare effectiveness of the next dispatcher technologies:

- technology 1 for apriority calls processing: in a consecutive order for single-tasking processing mode (regime ”Singletasking”); in a time-sharing order for multitasking processing mode (regime ”Multitasking”);
- priority technologies of consecutive calls processing 2-5:
- technology 2 for calls processing with relative priorities in the order “first in - first out” FIFO;
- technology 3 for calls processing with absolute priorities in the order FIFO;
- technology 4 for batch calls processing (with relative priorities and in the order FIFO inside a batch) (Kostogryzov (1987));
- technology 5 is a combination of technologies 2, 3, 4 see (Kostogryzov (1987, 1992)).

In case of technology 1, single-tasking processing mode allows to process calls in the consecutive order FIFO. In case of multitasking processing mode if there are n calls they are all processed simultaneously but each call is processed n times as slower as it had been processed alone in the system. According to technology 2 calls with higher priority are processed earlier. If calls are of the same priority they are processed in the consecutive order. There is no interruption of begun call processing by another call of higher priority appeared. Unlike technology 2, technology 3 allows an interruption of processing if a priority of the coming call is higher than a priority of the processed call. Processing of interrupted calls continues from the interrupted place. In the case of technology 4, the first call, coming to an off-line system, forms the first batch. The next batch is formed by calls, which come during the previous batch processing time, and is processed immediately after all the calls of previous batch have been processed. In the processed batch all calls are processed according to technology 2 with the exception that the processing cannot be interrupted. Finally, for technology 5, all calls are divided into n groups. Calls of the g-th group have higher priority than calls of the e-th group if g<e (e, g = 1,…, n). Calls of one group have their own relative priorities that are actual only within this group.

Estimation of system operation time-probabilistic characteristics may be made with the help of the CEISOQ+ subsystem “TIMELINESS” (Kostogryzov et al. (2000-2002)). The models use allows to choose between the calls timeliness criterions: the mean processing time criterion 1; the probability criterion 2 of well-timed processing.

Criterion 1. An output information of the *i*–th type is considered to be well-timed according to the criterion of calls mean processing time if response time $T_{full\ i}$ is no less than required admissible time $T_{req.i}$: $T_{full\ i} \leq T_{req.i}$

Criterion 2. An output information of the *i*–th type is considered to be well-timed according to the probabilistic criterion if $P_{tim.i} = P(t_{full\ i} \leq T_{req.i.}) \geq P_{req.i}$, where $t_{full\ i}$ is the processing time, including queueing time and run time, $T_{full\ i}$ is the mean response time.

Note. The CEISOQ+ use proved the revealed analytical regularity for Technology 4: ratio of mean waiting time in a calls queue of low priority to mean waiting time of high priority calls doesn't exceed 3 units no matter what the system throughput is. At the same time for Technologies 2 and 3 this ratio may be measured in dozens or hundreds (other things being equal it is much greater for Technology 3 than for Technology 2). This very regularity is used for increasing the processing effectiveness owing to a combination of Technologies 2, 3 and 4 (see Technology 5).

The CEISOQ+ subsystem "TIMELINESS" use allows to estimate the next metrics: the mean wait time in a queue $\boldsymbol{T_{queue\ i}}$; the mean processing time, including the wait time (it names also the mean response time) $\boldsymbol{T_{full\ i}}$; the probability of well-timed processing during the required term $T_{req.r}$ ($\boldsymbol{P_{tim.i}}$); the relative portion of all well-timed processed calls (S); the relative portion of well-timed processed calls of those types for which the customer requirements are met (C). For all technologies the probability function of well-timed calls processing is approximated by incomplete gamma-distribution:

$$P_{tim..i} = P\left(t_{full.i} \le T_{req.i}\right) = \frac{\int\limits_{0}^{\gamma_i^2 T_{req.i} / T_{full.i}} t^{\gamma_i - 1} e^{-t} dt}{\int\limits_{0}^{\infty} t^{\gamma_i - 1} e^{-t} dt}, \ where \gamma_i = \frac{T_{full.i}}{\sqrt{T_{full.i2} - T_{full.i}^2}}.$$

$$S = \frac{\sum\limits_{i=1}^{I} \lambda_i P_{tim.i}}{\sum\limits_{i=1}^{I} \lambda_i}, C = \frac{\sum\limits_{i=1}^{I} \lambda_i P_{tim.i}\left[Ind(_{\alpha_1}) + Ind(_{\alpha_2})\right]}{\sum\limits_{i=1}^{I} \lambda_i}, \ Ind\left(\alpha\right) = \begin{cases} 0, \text{ if } \ \alpha = true \\ 1, \text{ if } \ \alpha = false' \end{cases}$$

a_1=(there is used criterion 1 and $T_{full\ i}$£$T_{req.\ i}$); a_2=(there is used criterion 2 and $P_{tim.i} \geq P_{req.i}$.

3.4. Completeness of output information

A system will work in user's interest only after necessary initial input data concerning objects of its application domain have been entered. In the operational process there may be entered 2 types of current information sources:

- information concerning new objects which is firstly entered into a system;
- information concerning objects, which has already been stored in a system and is purposed for updating.

From the moment of information of the 1st appearance till the moment of its entering into a system is considered as incomplete as respects this information. In reality this information exists, characterizes states of new objects, which must be registered by system, but is not reflected in the system and therefore can't be taken into account by a system because he doesn't know about it. Concerning this information we may speak about its completeness only after its operational representation in system, after which a formal state of incompleteness disappears. Estimation of completeness level may be carried out with the help of the model of entering into system current data concerning new objects of application domain (below described), the CEISOQ+ subsystem “Completeness”.

For both types of information the next question is reasonable: how actual is the information represented in the system at the moment of its use? The answer may be found in the next subchapter 3.5, where the models complex of information gathering from sources and the subsystem “Actuality” of the CEISOQ+ are used. In this chapter we pay attention to modelling process architectures for providing completeness of entering into system current data concerning new objects of application domain, i.e. of the first type of information. It is important to note that a theoretical solution of applied analysis and synthesis problems does not mean simplicity of its practical implementation. Though problems of data transfer and input into a system present no difficulties, problems of required information gathering and identification are still a stumbling block. As a result many systems are obliged to operate in conditions of information incompleteness because a scientific conception of required information gathering system characteristics does not provide practical possibilities of its implementation.

An analysis of system operation reveals that solving some problems it is often necessary to account a variety of objects and events, which occurrence is of a stochastic character. There may be considered some tasks of airport system, aircraft global positioning receiver system, tasks of reconnaissance, tracking of an area state in conditions of radioactive contamination, loads accounting by the customs etc. we shall consider output information complete if it represents all real objects and events necessary for system staff to perform their functions. In an automatic control system there is always represented only complete output information. All information circulating in an automatic control system is strictly determined and processed automatically, i.e. occurrence of new objects influencing on technological operations is eliminated. And vice versa any system is always operating in information incompleteness according to terrorist threats conditions. At the same time, we’ll distinguish completeness and validity of represented information: the completeness concerns only that objects which appear, and validity concerns both new and stored information. In consequence, information may be complete, but not actual.

The essence of information incompleteness influence on decision-making consists in the impossibility of registration of all objects and events (OE), describing formal state of reality and influencing on decisions. As a logic result of decision-making may turn out to be inadequate to the situation, i.e. a decision turns out to be incorrect. A system contains information about states of all real objects and coincides if the number of occupied server for system M/G/∞ is equal to zero.

Let's assume that appearance of new objects or events essential for a solution of a specific task occurs at random moments (we shall call them “causing”). Periods between these moments are also random, their duration is distributed by the exponential law with the parameter *l*. In a causing moment with the probability q_m there appear m new objects and events $\sum_m q_m = 1$. A generating function of appearing objects and events number at a causing moment we shall notate as *Φ(z)*. In practice appearance of several objects and events is explained by their common origin: for example, as a result of a catastrophe on a chemical plant appears a set of zones of ecological contamination. After their appearance there is organized a message preparing during mean time w_1 with a distribution function $B_1(t)$. Then the message is transferred for its loading into an IS during mean time d_i with a distribution function $B_2(t)$. There may be a delay in receiving of the message (for example, for a visual check of the data), then the message is loaded into an is within b_i with a distribution function $B_3(t)$. Thus, the loaded information allows to use classic results for queuing systems with an infinite number of servers $M/G/\infty$.

The probability that IS contains information about states of all real object and coincides with the probability that number of occupied server for system $M/G/\infty$ is equal to zero. It mails calculated by formula (Matweev & Ushakov (1984)). If with the probability q_m m new objects appear in random intervals exponentially distributed with parameter *l*, then the found probability:

$$P_{comp.} = exp\left\{-\lambda\int_0^\infty \left[1-\Phi\left(\mathrm{B}(t)\right)\right] dt\right\}, \tag{2}$$

where $\Phi(z)=\sum_{m>0} q_m z^m$ -is productive (generating) function; *B(t)* – is the PDF of time for new information revealing and preparing $B_1(t)$, transfer $B_2(t)$ and entering into IS $B_3(t)$. $B(t)=B_1{*}B_2{*}B_3(t)$.

The next variants are used by the CEISOQ+: *Φ(z)=z; B(t)* is exponentially distributed.

The final clear analytical formulas for modelling are received by integration (2) expression.

With the subsystem "Completeness" of the CEISOQ+ use the probability that IS contains information about states of all real object and coincides may be estimated.

3.5. Actuality of input information from using point of view

After information has been entered into a system it gains a property of actuality. It is clear that for real systems output information is received after it has been structured, formally processed and mixed with other information, which is gathered from different sources and is characterized by different significant state changes frequency of considered objects. Output information is a "mixture" of various input data elements with different actuality. As an analogue to actuality there may be product freshness by the moment of cooking. For example fresh fish has its useful life (a period between significant changes of consumer properties) equal to several hours, fruits life equals to several days, wine's – several years. Output information is also a product to be used by a man, that is why it should be "fresh" (in our terms – actual) for problems solving. As a stale ingredient spoils all food a non-actual part of output information may spoil information quality. The same information may be actual for solving one problem and non-actual for another one.

IS users usually use "anonymous" output documents received as a result of their calls processing by a computer. It would be ideal an output document were marked by the date by which the values included in it would have been actual. It would be completely similar with sold food on packages of which there are indicated its expiry date. However, in a reality it is wide from the truth. In practice the objects state changes are entered into an IS with some delay and for the different data delays are different. Moreover, the same information may be actual for a solution of one problem and turn out to be completely irrelevant for another one. In other words, in an output document under a date of its creation data of a different actuality degree may be represented. Thus, for problem solving there is used output information different from the real one because of its changes in the course of time. If this difference is essential, use of such information may cause errors. Therefore, substantiating engineering solutions of providing an actual condition of used information an engineer has to solve a problem of quantitative estimation of achieved actuality for different technologies of information gathering and bringing it to the notice of users.

Without any limitation we consider process architectures for items gathering on the examples of providing information actuality. According the offered below models complex of information gathering from sources the next statement for evaluation information actuality is proposed.

Statement 2. The limited probability of information actuality on the moment of its use exists under conditions of existence for stationary probability distribution for considered characteristics and their independence.

One is equal to:

a. for the mode D_1 when information is gathered in order “immediately after an essential object state change:

$$P_{act} = \frac{1}{\xi} \int_{0}^{\infty} B(t)[1-C(t)]dt, \tag{3}$$

b. for the mode D_2 when information is gathered without any dependencies on changes of objects current states (including regulated information gathering)

$$P_{act.} = \frac{1}{q} \int_{0}^{\infty} \left\{ [1-Q(t)][1-\int_{0}^{\infty} C(t+\tau)dB(\tau)] \right\} dt, \tag{4}$$

where $C(t)$ is the PDF of time between essential changes of object states, ξ – is the mean time; $B(t)$ is the PDF of time for information gathering and preparing $B_1(t)$, transfer $B_2(t)$ and entering into IS $B_3(t)$; $B(t)=B1*B2*B3(t)$; $Q(t)$ is the PDF of time interval between information updating, q is the mean time (only for mode D_2).

The final clear analytical formulas for modelling are received by Lebesque-integration of (3) and (4) expressions.

Introduction of admissible limits of item suitable values changes is connected with a concept of an essential change of real characteristics of objects and events. We'll call a change of an object's characteristic essential for a solution of a certain problem, if well-timed representation of faultless information about this change to a user influences logic or result of the solution. Fully similar situation is peculiar not only to information process architectures but also to many other gathered items (inputs, system elements or components for a project in life cycle, required products or system operation outputs for an user, for instance, information, etc.).

With the subsystem "Actuality" of the CEISOQ+ use the probability of information actuality on the moment of its use may be estimated.

3.6. Information foultlessness after checking

Problems of item content analysis are everywhere in system life cycle. It may be nondestructive defects control for some objects safety checking, documentation or drawings checking, hardware or software testing against potential errors, information analysis for making decision etc. In any case there exist some objects, may be latent or suspicious for revealing and their following analysis. It is clear that more often item content analysis quality depends on system's application domain and used analysis methods. In a general case methods of analysis and decision-making may contain elements of both creative work and guessing. Nonetheless, any analysis is based on logical positions. Logic implies argumentation based on essential information use. The way of logical information use is an algorithm of given information analysis. In practice this algorithm is implemented by either a man or an applied software. Both of them we shall mean under the term "analyst". The cited sequence of positions concerning logicality of item analysis algorithm allowed us to formalize a process architectures for item content analysis according to the offered model. To apply this concept to information architectures, let's assume that in a system there are provided gathered information completeness and actuality and there is confidence in software/hardware tools correct operation. Is it enough for providing validity of output information? No, it is far from being enough. The person, from his/her date of birth, lives in conditions of information incompleteness, that is why modern IS are oriented on all possible ways of gathering complete information. One of the modern IS advantages is that they are developed to solve principal problems of information actuality owing to quick consumers informing. If it is not possible to use "the freshest" information then a man may use less fresh information to estimate the current and predict future states of considered objects. Incompleteness and non-actuality of information are the unavoidable properties of natural human environment. The main danger is in insufficient effectiveness of information gathering.

The problem concerning information faultlessness is completely different. In practice it is very difficult to provide information faultlessness. The fact lies not only in technological complexity but also in the term "error" and in man's physical inability of not making errors. So let's review the term "error" and the term "distortion" which is close to the first one.

Despite seeming simplicity these terms concerning information circulating in an IS are not fully the same. A syntax error in spelling, which does not influence sense of input or output documents, does not have a deteriorative influence upon information validity. Moreover, if quantitative deviation of considered objects characteristics is considered significant if it is more than 10% (for instance) an appeared deviation in parts of percent cannot be characterized as an error. It is only degree of information correctness, which is taken into account by those who make decisions. From the other hand the term "to distort" is interpreted as "to show smth in the false color". The term "distortion" itself means inadmissibility of further use. Below we shall use the term "error" for accidental data deviations. In cases implying premeditation we shall use the term "distortion". To define these terms for IS let's assume that information gathering and processing is carried out instantly and during storage before its use accounted objects do not change their states (if they change them the information is instantly updated). Then under an information error or distortion in such idealized IS we mean such data changes which in case of correct information processing may cause paralysis and/or changes in results of system operation. Thus use of these terms we shall connect with information quality inadmissibility for its further efficient use. In fact data updating does not happen instantly but after a certain period of information transferring. In this case to errors and distortions are added non-actuality and other natural and artificial influences deteriorating information quality.

This subchapter is dedicated to studying faultlessness estimated with the help of the next model of items analysis. The core of modelling is illustrated by Figure 8 (for information checking application domain).

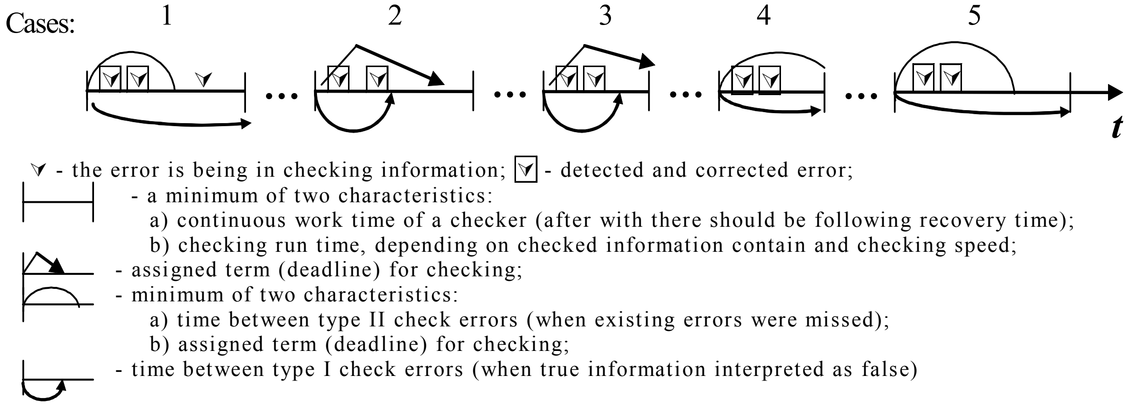

Cases:
1
2
3
4
5
t
- the error is being in checking information;
- detected and corrected error;
- a minimum of two characteristics:
a) continuous work time of a checker (after with there should be following recovery time);
b) checking run time, depending on checked information contain and checking speed;
- assigned term (deadline) for checking;
- minimum of two characteristics:
a) time between type II check errors (when existing errors were missed);
b) assigned term (deadline) for checking;
- time between type I check errors (when true information interpreted as false)

Figure 8. The illustration of processes for information analysis

On an example for visual checking, the cases 1, 2, 3 characterize presence if only of one errors, the cases 4, 5 and any other characterize that faultlessness after checking is provided.

It is not always possible in practice to draw a logical bound for admissible deviations. Often even an insignificant deviation may become important for system functions performance. At the same time it is undisputable that required data faultlessness should be set taking into consideration effects of system operation, damage caused by errors and also errors preventing and negative consequences elimination expenses. If to put an end to the above mentioned it turns out that for a user understanding of an "error" depends on information purpose and methods of its processing. Information processing implies: syntax and semantic information control to detect and eliminate errors; various processes (generalization, arithmetical and logical operations etc.) and as a final result – pragmatic information filtering and analysis and logical making decision with the purpose of its further use.

In real systems we always have to solve a problem of a balance between input information content and quality of its processing within the assigned period. If an input information content is big the number of errors increases what may cause a control action time waste. To be on schedule it is necessary to optimize the information content and to develop more rational information processing and representing technologies.

The model is used for evaluation of information foultlessness after checking and information processing correctness.

Definition 1. Information after checking is considered as faultless if all data errors were detected and corrected and no new errors were made. *Definition 2.* Information processing is considered as correct analysis if all essential information was faultless analyzed and no algorithmic errors was made.

There are possible the four variants of correlations between the characteristics.

Variant 1. An assigned term for analysis is no less than the real analysis time ($T_{real} \leq T_{req.}$) and the content of analyzed information is such small that it is required only one continuous analyst's work period ($T_{real} \leq T_{cont.}$).

There is proposed the next Statement 3.

Statement 3. Under the condition of independence for considered characteristics the probability of information faultlessness (for problems of checking) or processing correctness (for problems of analysis) during the required term is equal to:

$$P_{after(1)}(V,\mu,\nu,n,T_{MTBF},T_{cont.},T_{req.}) = \left[1-\hat{N}(V/\nu)\right]\left\{\int_{0}^{V/\nu} dA(\tau)[1-M(V/\nu-\tau)] + \int_{V/\nu}^{\infty} dA(t)\right\} \quad (5)$$

where N(t) is the PDF of time between type I analysis errors, η^{1} is the mean time, for example, N(t) = $1 - exp(-t\times\eta)$; $M(t)$ is the PDF of time between the neighboring errors in checked information, for example $M(t) = 1 - exp(-t\times\mu\times\nu)$; $A(t)$ is the PDF of analyzed type II errors, T_{MTBF} is the mean time; μ is the relative fraction of errors in information content (destined for problems of checking) or the relative fraction of information essential for analysis (destined for problems of analysis); $T_{real}= V/\nu$ - is the real time for complete information analysis; V – is a content of analyzed information; ν - is an analyzed speed; $T_{cont.}$ - is time of continuous analyst's work; $T_{req.}$ - is an assigned term (deadline) for analysis.

V, ν, $T_{cont.}$ and $T_{req.}$ are assigned as deterministic values. The probability that there are not errors without checking is $P_{no}(V) = e^{-\mu V}$.

The final clear analytical formulas for modelling are received by Lebesque-integration of (5) expression.

Variant 2. An assigned term for analysis is no less than the real analysis time (i.e. $T_{real} \leq T_{req.}$). But the content of analyzed information is comparatively large, i.e. $T_{real}>T_{cont.}$.

Statement 4. Under the condition of independence for considered characteristics the probability of information faultlessness (for problems of checking) or processing correctness (for problems of analysis) during the required term may be estimated by following:

$$P_{after(2)} = \left\{ P_{after(1)}\left(V_{part(2)},,,n,T_{MTBF},T_{cont.},\tau_{part(2)} \right) \right\}^{N}, \tag{6}$$

where $N = V/(\nu \mathrm{T}_{cont.}), V_{part(2)} = V/N, \tau_{part(2)} = \mathrm{T}_{req.}/N$.

Variant 3. An assigned term for analysis is less than the real analysis time ($T_{real}>T_{req.}$) and the content of analyzed information is such small that it is required only one continuous analyst's work period ($Treal \leq Tcont.$)..

Statement 5. Under the condition of independence of considered characteristics the probability of information faultlessness (for problems of checking) or processing correctness (for problems of analysis) during the required term may be estimated by following:

$$P_{after(3)} = \left(V_{part(3)} / V \right) \times P_{after(1)}\left(V_{part(3)},,,n,T_{MTBF},T_{cont.},T_{req.} \right) + \left[\left(V - V_{part(3)} \right) / V \right] \times P_{without}, \tag{7}$$

where $V_{part(3)} = T_{req.}, P_{without} = e^{-\left(V - V_{part(3)}\right)}$.

Variant 4. An assigned term for analysis is no less than the real analysis time (i.e. $T_{real}>T_{req.}$). But the content of analyzed information is comparatively large, i.e. $T_{real}>T_{cont.}$.

Statement 6. Under the condition of independence of considered characteristics the probability of information faultlessness (for problems of checking) or processing correctness (for problems of analysis) during the required term may be estimated by following:

$$P_{after(4)} = \begin{cases} \left[\dfrac{V_{part(4)}}{V} \right] P_{after(1)}\left(V_{part(4)},,,,T_{MTBF}.,T_{cont}.,T_{req}. \right) \\ \quad + [(V - V_{part(4)})/V] e^{-\left(V - V_{part(4)}\right)}, if\ T_{real} \leq T_{cont.}; \\ \left[\dfrac{V_{part(4)}}{V} \right] \left\{ P_{after(1)}\left(V_{part(4.2)},,,,T_{MTBF},T_{cont},_{part(4.2)} \right) \right\}^{N} + \\ \quad + \left[V - \dfrac{V_{part(4)}}{V} \right] e^{-\left(V - V_{part(4)}\right)}, if\ T_{real} > T_{cont.}. \end{cases} \tag{8}$$

where $V_{part(4)} = T_{req.}$, $V_{part(4.2)} = \frac{V_{part(4)}}{N}$, $t_{part(4.2)} = T_{req} / N, N = \frac{V_{part(4)}}{Tcont.}$.

The fraction of errors in information after checking equals to $\mu_{after} = \mu \times \left(1 - P_{after}\right)$.

The final clear analytical formulas for modelling are received by integration (5) and using (6)-(8).

With the subsystem "Effectiveness of checking" of CEISOQ+ use the probability of errors absence after checking and the fraction of errors in information after checking may be estimated.

3.7. Correctness of information processing

The mathematical model of items analysis (subchapter 3.6) is recommended to be used also for estimating correctness of information processing. With the subsystem "Correctness of processing" of the CEISOQ+ the probability of correct analysis results obtaining may be estimated.

3.8. Faultless operation of staff and users

A man is an unavoidable element of an IS as its user and staff, providing system's functionality. How does this element influence achievement of system operation purposes? To answer this question the CEISOQ+ subsystem "Faultlessness man's actions" may be used. As the subsystem is completely analogous to the subsystem **"RELIABILITY"** (see subchapter 3.2) we'll use the minimum problem definitions and illustrating examples. The next metrics may be estimated: the mean time between errors for a complex composed of functional groups; the probability faultless operation of a complex composed of functional groups 1,…,n during the period $T_{req.}$

3.9. Protection against dangerous influences

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 including information integrity. Under information integrity we mean such information state which provides the required operation quality of a used IS.

Such dangerous influences on IS are program defects events, virus influences, influences of software bugs, violators' influences, terrorists attacks (in the information field), psychological influences on men by means of ordered radio and TV programs etc.

There are examined two technologies of providing protection from dangerous influences: proactive diagnostic of system integrity (technology 1) and security monitoring when system integrity is checked at every shift change of operators (technology 2).

Technology 1 is based on proactive diagnostics of system integrity. Diagnostics are 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 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 not considered to be violated before a penetrated danger source is activated. A danger is considered to be realized only after a danger source has influenced on a system. If to compare an IS 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 (integrity is recovered). Between diagnostics an infection penetrated into a man's body brings a man into an unhealthy state (a dangerous influence is realized). The essence of protecting process architecture for the first technology is illustrated by Figure 9. The cases 1, 4 illustrate dangerous influences. The cases 2, 3, 5 illustrate secure system operation during a period T_{req}.

Note. It is supposed that used diagnostic tools allow to provide necessary system integrity recovery after revealing of danger sources penetration into a system or consequences of negative influences.

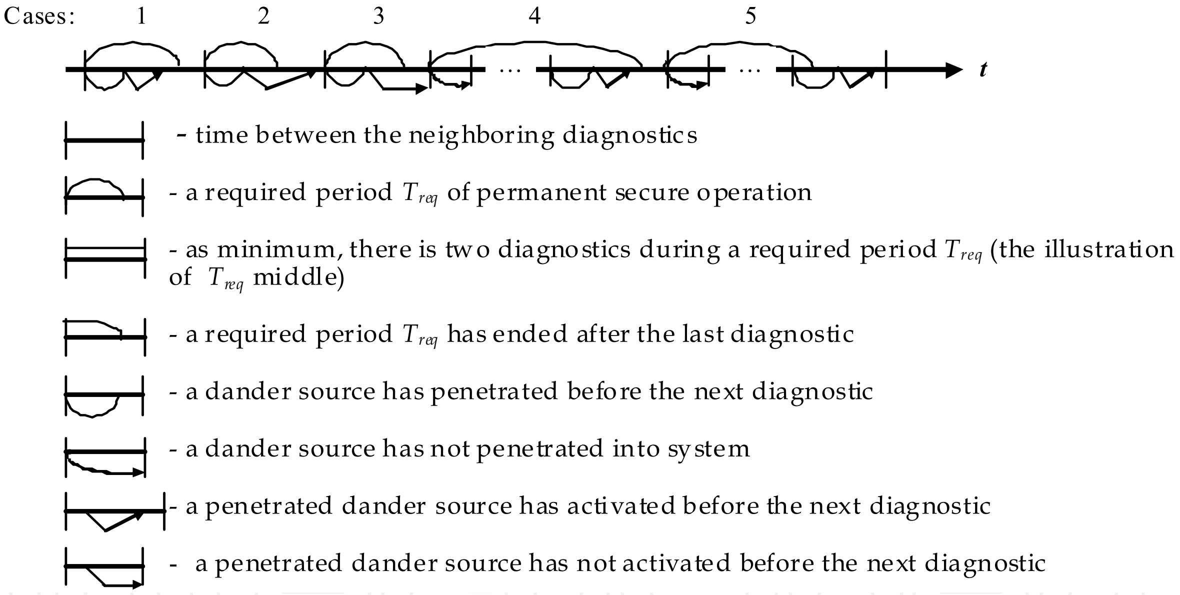

Cases: 1 2 3 4 5
t
- time between the neighboring diagnostics
- a required period T_{req} of permanent secure operation
- as minimum, there is two diagnostics during a required period T_{req} (the illustration of T_{req} middle)
- a required period T_{req} has ended after the last diagnostic
- a dander 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

Figure 9. The illustration of processes for protecting system resources against dangerous influences by technology 1

Technology 2, unlike the previous one, implies that operators alternating each other trace system integrity between diagnostics. In case of detecting a danger source an operator is supposed to remove it recovering system integrity (ways of danger sources removing are analogous to the ways of technology 1. A penetration of a danger source into a system and its activation is possible only if an operator makes an error. Faultless operator's actions provide a neutralization of a danger source trying to penetrate into a system. When operators alternate a complex diagnostics 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.

Thus in comparison with a man technology 2 reminds a continuous staying in a hospital when between rare diagnostics a patient is permanently under medical observation of operator. A dangerous infection penetrates into a man's body only because of a doctor's fault while it may be discovered later as a result of either an exacerbation of a latent illness or the next diagnostic.

For all technologies availability of means of danger sources total-lot detecting and existence of ways of violated system integrity total-lot recovery may seem to be a very high requirement. Nonetheless, a system which can't check and recover its integrity is a very vulnerable and knowingly doomed system.

With the subsystem "Protection from dangerous influences" of CEISOQ+ the probability of secure system operation within the assigned period may be estimated as a result of use the next mathematical models.

There are possible the next variants for technology 1: 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 $\left(T_{req} \geq T_{betw.} + T_{diag}\right)$.. Here $T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic, T_{diag} – is the diagnostic time.

Statement 7. Under the condition of independence of considered characteristics the probability of dangerous influence absence for variant 1 is equal to

$$P_{infl.(1)}\left(T_{req}\right)=1\text{-}\Omega_{penetr}{}^{*}\Omega_{activ}\left(T_{req}\right), \tag{9}$$

where $\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source, for example $\Omega_{penetr}(t) = 1\text{-}e^{-st}$, s - is the frequency of influences for penetrating; $\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source, for example $\Omega_{activ}(t)=1\text{-}e^{-t/b}$, b – is the mean activation time; $\boldsymbol{T_{req}}$ – is the required period of permanent secure system operation.

Statement 8. Under the condition of independence for considered characteristics the probability of dangerous influence absence for variant 2 is equal to

$$P_{\inf l.(2)} = \frac{N\left(T_{betw.}+T_{diag.}\right)}{T_{req.}} \cdot P_{\inf l.(1)}{}^{N}\left(T_{betw.}+T_{diag.}\right) + \frac{T_{req.}-N\left(T_{betw.}+T_{diag.}\right)}{T_{req.}} P_{infl.(1)}\left(T_{rmn}\right), \tag{10}$$

where N=**[** $T_{req.}/(T_{betw}+T_{diag})$**]** – is the integer part, the remainder time $T_{rmn} = T_{req}\text{-}N(T_{betw}+T_{diag})$.

Statement 9. Under the condition of independence for considered characteristics the probability of dangerous influence absence for variant 1 is equal to

$$P_{\inf.(1)}(T_{req.}) = 1 - \int_{0}^{T_{req.}} dA(\tau) \int_{0}^{T_{req.}-\tau} d\Omega_{penetr.} * \Omega_{act.}(\theta). \tag{11}$$

Here $\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source, $\Omega_{penetr.}(t)=1\text{-}e^{-st}$, s - is the frequency of influences for penetrating; $\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source, $\Omega_{activ}(t)=1\text{-}e^{-t/b}$, b – is the mean activation time;

$T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic ($T_{betw.}$*=const*); *A(t)* is the PDF of time between operator's error, T_{MTBF} is the mean time, *A(t)=1-exp(-t/*T_{MTBF}*)*. T_{diag} – is the diagnostic time ($T_{diag.}$*=const*); T_{req} – is the required period of permanent secure system operation.

Statement 10. Under the condition of independence of considered characteristics the probability of dangerous influence absence for variant 2 is equal to

$$P_{\inf.(2)}(T_{req.}) = \frac{N\left(T_{betw.} + T_{diag.}\right)}{T_{req.}} \cdot P_{wholly}{}^{N} + \frac{T_{rmn}}{T_{req.}} \cdot P_{\inf l.(1)}(T_{rmn}), \tag{12}$$

P_{wholly} – is the probability of dangerous influence absence within the assigned period $T_{req.}$:

$$P_{wholly} = 1 - \int\limits_{0}^{T_{betw.}+T_{req.}} dA(\tau) \int\limits_{0}^{T_{betw.}+T_{req.}-\tau} d\Omega_{penetr.} * \Omega_{activ.}(\theta), \tag{13}$$

and $P_{infl.(1)}(T)$ is defined above, but one is calculated not for all period T_{req}, only for the remainder time $T_{rmn} = T_{req} - N(T_{betw} + T_{diag})$.

The final clear analytical formulas for modelling by the CEISOQ+ are received after Lebesque-integration of (11), (13) expressions with due regard to Statements (7)-(10).

3.10. Protection from an unauthorized access

At all times a particular attention was paid to the problem of effective system resources (facilities, valuables, information, software etc.) protection from an unauthorized access (UAA). None clever solutions didn't guarantee complete protection from UAA to complex systems. As we have made sure there is also impossible to provide total-lot system reliability, information timeliness, actuality, faultlessness, correctness, and system protection from dangerous influences. Now we shall pay some attention to common regulations of providing protection from UAA in applications to IS.

Results of UAA may be the next: a dangerous influence on a secure system operation(on a subsystem of access control, a subsystem of account, a subsystem of integrity providing); a physical influence on system items (destroying, power supply failures, interceptions of electromagnetic radiation); an unauthorized withdrawing, acquaintance, use or dangerous influences on stored, processed, transferred and represented information (theft, fraud, insertion of spurious information, deleting, i.e. any violation of information integrity); an unauthorized use or change of system content, structure and functionality (including changes of configuration parameters, an introduction of bugs, viruses); hardware/software failures and malfunction; violating of network interconnection etc.

It should be formulated system security policy. The protected batch should create a virtual system operation environment, model potential threats, reveal vulnerabilities of a system, estimate potential risks and damage, compare expenses on the whole system operation and the subsystem of providing IS security. However we should remember that security provision mustn't hinder from real objectives achievement for the sake of which these systems are created.

To understand ways of overcoming protective barriers by a violator it is worth citing some examples of bottlenecks in existing information security systems:

- authenticating users a security service doesn't always have an ability to make sure of a user's authenticity. The particular ways of authentication (on the basis of a fingerprint or an eye retina analysis) have not been widely distributed yet;
- access delimitation to computer resources is not insuperable. The majority of systems does not support a mandatory access control, a cryptography information protection is not always introduced (sometimes such disregard of a cryptography information protection is justified if to take into account a required IS throughput but in other cases it is unjustified), a password access to the most relevant resources is not executed etc.;
- many protective systems do not prevent an unauthorized start of executable software files including a remote start of access procedures to resources of other computers;
- protection from viruses and bugs is still problematical (see the examples of this chapter);
- speed of crypto-transformations is not high enough, what often causes users' refusals of encoding;
- a control of a protection system operation correctness is quite often ignored, signaling functions are not performed;
- a required security of a network transfer is not provided (authenticity, capabilities of interception, insertion of spurious message are not checked and there is no keys distribution between network nodes);
- functions of substantiated information redundancy are often not realized. For example, a used background redundancy does not provide an information recovery owing to both failures of soft/hardware means and unauthorized actions;
- there are possible errors of network administrator (configuration, access to network resources and recovery control) and in control of a protection system operation correctness;
- weaknesses of used a cryptographic algorithms (absence of short and trivial passwords check, use of secret functions of overcoming cryptographic protection etc.);
- unfounded periodicity and order of tuned parameters changes (identifiers and authorities of the users, passwords and key information, frequency of resources integrity control etc);
- failures to meet requirements to the protocol of information intercommunication, correctness and completeness (there are possible interception of the transferred data, their thefts, changes and readdressing, unauthorized mailing on behalf of another user, a denial of data authenticity, etc). For example, an interception is possible if a violator synthetically connects to an unauthorized router network with readdressing of a messages flow;
- an IS elements malfunction (failures or an essential slowdown of executed operations), which can be as a result of a network overload, critical data deleting and performance of critical functions etc.

Thus the above-mentioned positions of information protection and overcoming of protective measures are to promote a better understanding of process architectures for protecting system resources from an UAA.

If to represent such a system from the point of view of its operation logics the process architecture for system resource protection is a complex of sequential obstacle barriers. A user is taught how to overcome these barriers to get an access to resources. A violator has to overcome these barriers trying to find system vulnerabilities (see Figure 10). A security service controls system operation thus reducing system vulnerability.

A probabilistic space for estimating of influences absence after UAA is created in the supposition that in a system there are realized protective measures from a potential violator. To get access to resources stored in a system there is a set of barriers known to an authorized user. A violator is a tool or person who does or doesn't know how protective barriers work. Somehow breaking an algorithm of barriers overcoming a violator may easily get access to system resources. We examine the most difficult mode of security system operation in conditions of the constant threat of its breaking. A violator is able to penetrate into a system only if: 1) he finds out how that part of the protection system works which is needed for his/her purposes achievement; 2) he gets access to information and/or software resources before this protective system will be changed (in this case the violator will have to overcome the new barriers). In modelling actions of "clever" violator equipped with high-tech means of system breaking are described by a greater speed of barriers overcoming.

The formalized process architectures for protecting system resources is fair for security estimating without and with considering objective period when resources value is high (see Figure 10b)). Often in practice this period is essentially limited. As an Air Transport System example there may be information resources used for performance of one passenger transportation or a certain task. After the task fulfillment the objective value of these resources comes to zero (is actual only archive value). The second example concerns a flight control system of an aircraft which operating lever are located in a cockpit. From the point of view of a flight security in conditions of terrorist threats a period of objective value of these resources coincides with a flight time or if an airplane is high-jacked it coincides with the period of its capture. As the third example there may be cash financial or gold-value resources in a bank after their receipt for storage. In this case from the point of view of the bank's security system the period of objective value of resources coincides with the period of their keeping in depositories of bank.

As a rule information has a certain period of its objective value (POV), which influences on the system protection from UAA. In the offered subchapter on the basis of use the model of unauthorized access to system resources taking into account POV of information resources, there is estimated confidentiality of used information. Estimations are based on a use of the CEISOQ+ subsystem "CONFIDENTIALITY". Thus the period of objective information confidentiality in a system is POV concerning information resources.

Thus, a period of objective value (POV) of a resource is time appropriate for the resource after expiring of which the resource loses its value and objectively does not need any protection from UAA. For the present model taking into account POV resources are considered to be protected from UAA if as a result of UAA after their POV has finished there is no penetration to them. The core of more general process architecture with due regard to resources value for one barrier is illustrated by Figure 10b)). Unauthorized access during objective period, when resources value is high, went through barrier in cases 1 and 4. Resources are protected in other cases 2,3,5.

With the subsystem "Protection from unauthorized access" of CEISOQ+ the probability of providing system protection from UAA by means of barriers 1st, 2nd..., mth and by means of all barriers may be estimated as a result of use the next mathematical model.

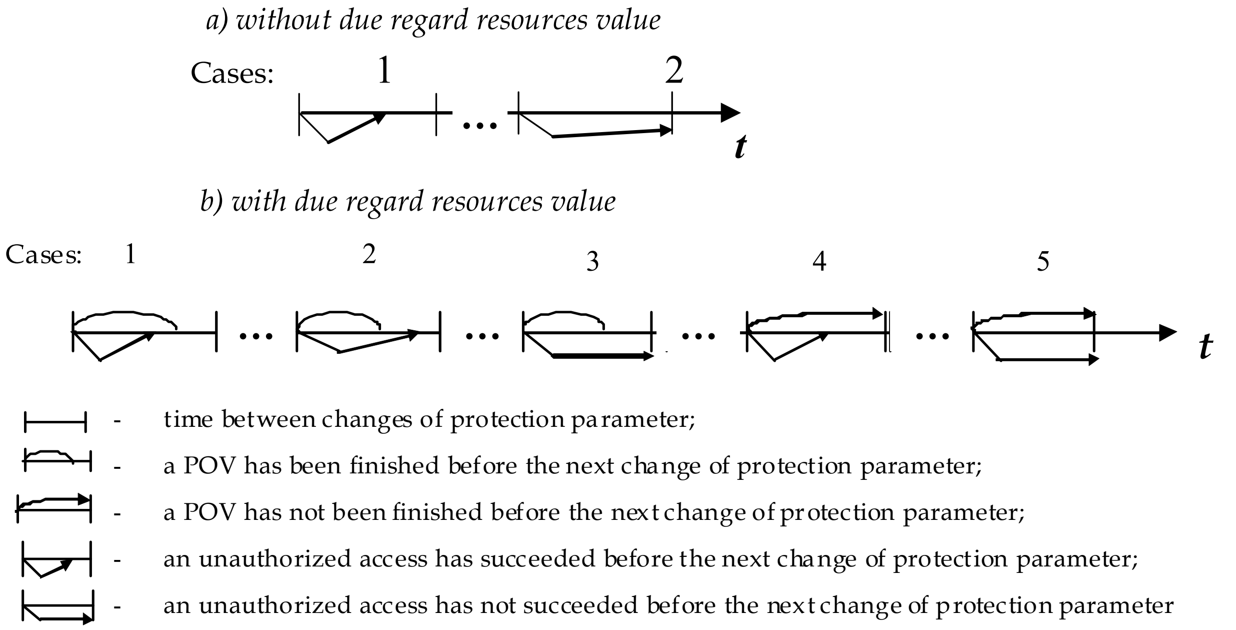

a) without due regard resources value
Cases:
1
2
t
b) with due regard resources value
Cases:
1
2
3
4
5
t
- time between changes of protection parameter;
- a POV has been finished before the next change of protection parameter;
- a POV has not been finished before the next change of protection parameter;
- an unauthorized access has succeeded before the next change of protection parameter;
- an unauthorized access has not succeeded before the next change of protection parameter

Figure 10. The illustration of processes for protecting system in application to a) UAA and b) information confidentially for an one barrier

As the model without considering objective period when resources value is high there is proposed the next Statement 11 for evaluation system resources protection against unauthorized access.

Statement 11. The limited probability of system protection against unauthorized access exists under the condition of existence for stationary probability distributions for considered characteristics and their independence.

One is equal to

$$P_{prot} = 1 - \prod_{m=1}^{M} P_{over\ m}, \tag{14}$$

where M is the conditional number of a barriers against an unauthorized access; $P_{over\ m}$ – is the probability of overcoming the m-th barrier by violator,

$$P_{over\,m} = \frac{1}{f_m} \int_0^{\infty} [1 - F_m(t)] U_m(t) dt; \tag{15}$$

where $F_m(t)$ is the PDF of time between changes of the m-th barrier with regulated parameter, f_m is the mean time;

$U_m(t)$ is the PDF of possible time of overcoming the m-th barrier, u_m – the mean time of a barrier overcoming.

The final clear analytical formulas for modelling by the subsystem "Protection from unauthorized access" of CEISOQ+ are received after Lebesque-integration of (15) expression with due regard to Statement (11).

3.11. Confidentiality of used information

The model taking into account a period of resources objective value is the next. With the subsystem "CONFIDENTIALITY" of the CEISOQ and CEISOQ+ the probabilities of providing information confidentiality by means of barriers 1st, 2nd..., mth from UAA and by means of all barriers may be estimated.

There is proposed the next Statement 12 for evaluation system protection against unauthorized access during objective period, when resources value is high.

Statement 12. The limited probability of system protection against unauthorized access during objective period, when resources value is high, exists under the condition of existence for stationary probability distributions for considered characteristics and their independence. One is equal to

$$P_{value} = 1 - \prod_{m=1}^{M} P_{over.m}, \tag{16}$$

where M is the conditional number of a barriers against an unauthorized access; $P_{over\ m}$ – is the risk of overcoming the m-th barrier by violator during objective period when resources value is high,

$$P_{over} = \frac{1}{f_m} \int_0^{\infty} dt \int_t^{\infty} dF_m(\tau) \int_0^{t} dU_m(\theta) \left[1 - H(\theta)\right], \tag{17}$$

where $F_m(t)$ is the PDF of time between changes of the m-th barrier parameters; $U_m(t)$ is the PDF of parameters decoding time of the m-th security system barrier, u_m – the mean time of a barrier overcoming; $H(t)$ – is the PDF of objective period, when resources value is high.

The final clear analytical formulas for modelling by the subsystem "CONFIDENTIALITY"of CEISOQ+ are received after Lebesque-integration of (17) expression with due regard to Statement (12).

4. Models, software tools and methods to analyze and optimize system processes

4.1. General approach to mathematical modelling standard processes

The offered below mathematical models and supporting them dozens software tools complexes are focused on providing system standard requirements (ISO/IEC 15288 “System Engineering – System Life Cycle Processes”, ISO 9001 “Quality Management Systems - Requirements” etc.) on the base of mathematical modelling random processes that exist for any complex system in its life cycle. The basic idea of the models develops the idea used for information systems - see subsection 3.1. At the beginning there were created the models of complex CEISOQ and CEISOQ+, after that - the other models.

The idea of mathematical modelling consists in the following. Any process represents set of the works which are carried out with any productivity at limitations for resources and conditions. This amount of works is characterized by expenses of resources (cost, material, human), accordingly works can be executed for different time with various quality. And conditions are characterized by set of the random factors influencing processes. It can be natural, technical, time, social factors, factors of the market and scientific and technical progress, say, all that is capable to affect processes. From the point of view of probability theory and the theory of regenerating processes it is possible to put formally, that all processes on macro-and micro-levels are cyclically repeated. If to assume, that number of recurrences of such processes is very large it is theoretically we can speak about probability of any events which can occur. The elementary example is a frequency loss of "heads" and «tails» at tossing up coins. If to enter conditions on a site (for example, on edge of gorge), on weather (a snow, a rain, a wind and so forth), on hardness of a ground it is possible to speak already not only about events of "heads" and «tails», and about other events falls, for example, that a wind will carry it away and coins will be lost. Actually course of complex system processes in life cycle from the mathematical point of view can be formalized absolutely similarly formalizations of tossing up coins process for the complicated conditions. In other words, the same as a matter of fact mathematical models can appear rather effective at their carry to other area of the practical applications. For example, the queueing theory which has arisen for calculations in a telephony, is used with success and for estimations at strikes on antiaircraft installations, and for estimations of time delays in networks of the computer systems, and for estimations of throughput of motorways etc.

In each of the offered models time characteristics of processes, frequency characteristics of any events and characteristics, connected in due course (for example, the set amount of works at known speed of their performance will give representation about mean time of performance of these works) are used as input. As final or intermediate result probabilities of "success" during a given time of forecasting or risks of failures as an addition to 1. They are used as evaluated output. So, at formalization of concept «customer satisfaction» estimations were under construction for the general case of following reasons. The customer expects performance of the certain amount of works with the acceptable quality and/or admissible risks for given time and money. In a reality the amount of works can appear other, the degree of quality essentially depends on applied technologies and management actions, time of performance and an expenses can undergo changes. As a result it is possible to speak about a degree of satisfaction in probability terms of performance of the set amount of works with the admissible quality for given time and money, and also about an expected and real part of the functional operations which are carried out with acceptable quality and/or admissible risks and expected and real expenses of the customer.

Thus the main proposition, implemented in the offered models, concludes the next: all amounts of works, characteristics of their performance, possible events and other inputs are interpreted as expense of time which can be reflected on a timeline. Probability metrics on the introduced limited space of elementary events are calculated by the rule of the probability theory (see section 3).

The basic ideas of correct integration of probability metrics are based on a combination and development of models, above presented, and consist in the following.

1st idea. As models are mathematical, the use of the same mathematical models is possible by a semantic redefinition of input and output of modelling. The idea is mentioned only for understanding the further logic in construction of modeled system, subsystems, elements and corresponding metrics on the basis of integrated modules.

2nd idea. For a complex estimation of the systems with parallel or consecutive structure existing models can be developed by usual methods of probability theory. For this purpose it is necessary to know a mean time between violations of integrity for each of element (similarly MTBF in reliability, but in application to violation of quality, safety etc.). Further taking into account idea 1 concept of a mean time between violations of an element integrity may be logically connected (for example, redefined) in concepts of a frequency of influences for penetrating into an element and a mean activation time of a penetrated danger source. The last concepts mean characteristics of threats.

Note. As logic element a subsystem, compound object or separate indicator from a complex of product indicators can be used.

Let's consider the elementary structure from two independent elements connected consecutively that means logic connection "AND" (Figure 11, left), or in parallel that means logic connection "OR" (Fig. 11, right).

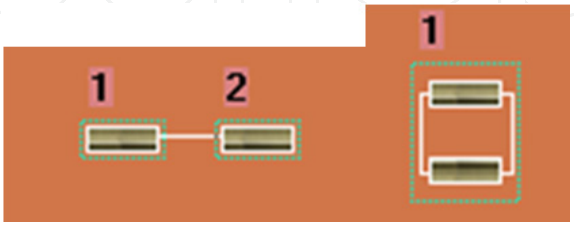


Figure 11. Illustration of system, combined from consecutively (left) or parallel (right) connected elements

Let’s designate PDF of time between violations of i-th element integrity as $B_i(t)$ =P ($\tau_i \leq$ t), then:

1. time between violations of integrity for system combined from consecutively 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 violated integrity when either 1st, or 2nd element integrity will be violated). For this case the PDF of time between violations of system integrity is defined by expression

$$B(t) = P(\min(\tau_1, \tau_2) \le t)=1- P(\min(\tau_1, \tau_2) > t)=1-P(\tau_1 > t)P(\tau_2 > t)= 1 - [1-B_1(t)]\ [1- B_2(t)]. \quad (18)$$

For exponential approximations: $B(t)=1-[1-B_1(t)][1-B_2(t)]=1-\exp(-t/T_{MTBF1})\exp(-t/T_{MTBF2})$.

Mean time between violations of integrity may be calculated by expression $T_{MTBF} = 1/(1/ T_{MTBF1}+1/ T_{MTBF2})$;

2. time between violations 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 or 2nd elements (i.e. the system goes into a state of violated integrity when both 1st and 2nd element integrity will be violated). For this case the PDF of time between violations of system integrity is defined by expression

$$B(t) = P(\max(\tau_1, \tau_2) \le t)= P(\tau_1 \le t)P(\tau_2 \le t)= B_1(t)B_2(t). \quad (19)$$

For exponential approximations: $B(t)=B_1(t)B_2(t)=[1-\exp(-t/T_{MTBF1})]\ [1-\exp(-t/T_{MTBF2})]$. Mean time between violations of integrity may be calculated by expression $T_{MTBF}= T_{MTBF1}+T_{MTBF2} - 1/(1/ T_{MTBF1}+1/ T_{MTBF2})$.

Applying recurrently expressions (18) – (19), it is possible to receive PDF of time between violations of integrity for any complex system with parallel and/or consecutive structure. The illustration of threats, periodic control, monitoring and recovery of integrity for combined subsystems of estimated system is reflected on Figure 12.

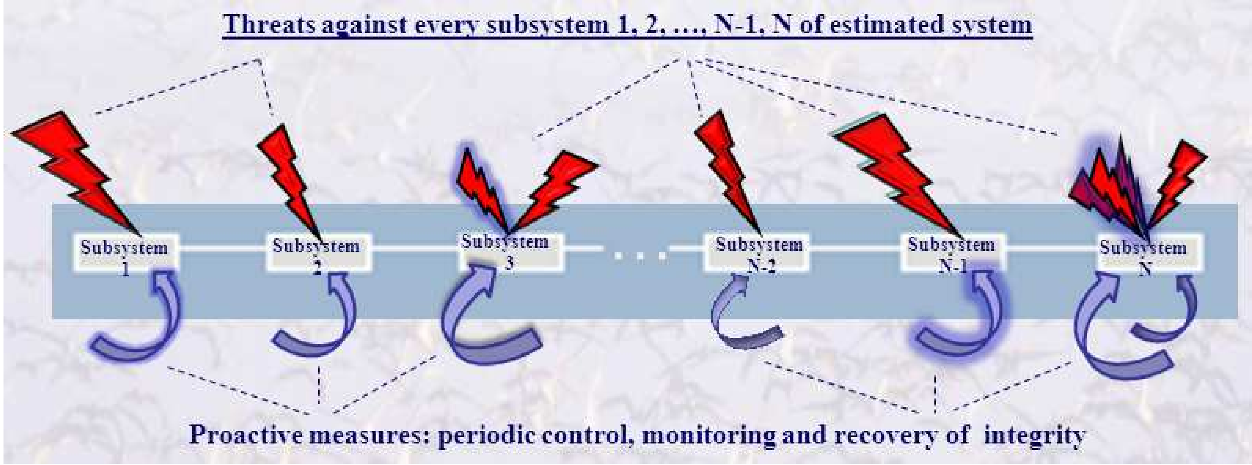

Threats against every subsystem 1, 2, …, N-1, N of estimated system
Subsystem 1
Subsystem 2
Subsystem 3
. . .
Subsystem N-2
Subsystem N-1
Subsystem N
Proactive measures: periodic control, monitoring and recovery of integrity

Figure 12. The illustration of threats, periodic control, monitoring and recovery of integrity for combined subsystems

3rd idea. Mean recovery time for system combined from consecutively connected independent elements may be calculated by expression $T_{rec.} = T_{rec.1}\ ((1/T_{MTBF1})/\ (1/T_{MTBF1}+$

$1/T_{MTBF2}))+T_{rec.2}$ $((1/T_{MTBF2})/$ $(1/T_{MTBF1}+$ $1/T_{MTBF2}))$, for system combined from parallel connected independent elements $T_{rec.}$ = $T_{rec.1}$ $((1/T_{MTBF2})/$ $(1/T_{MTBF1}+$ $1/T_{MTBF2}))+T_{rec.2}$ $((1/T_{MTBF1})/$ $(1/T_{MTBF1}+$ $1/T_{MTBF2}))$. Applying recurrently these expressions, it is possible to receive mean recovery time for any complex system with parallel and/or consecutive structure.

4th idea. If integrity violations are absent then diagnostic time for each element is equal on the average $T_{diag.}$. At the same time, if results of diagnostics require additional measures of integrity recovery this time increases. Thus mean time of diagnostics can be calculated iteratively with the given accuracy ε:

1-st iteration: $T_{diag.}{}^{(1)}$ = $T_{diag.}$ that is given by input for modelling. I.e. for 1st iteration at detection of violation it is supposed instant recovery of integrity. Risk to lose required integrity $R^{(1)}$ is calculated (for example, by the models of subsection 3.9). Here recovery time is not considered; 2-nd iteration: $T_{diag.}{}^{(2)} = T_{diag.}{}^{(1)}$ $(1 - R^{(1)}) + T_{rec.}$ $R^{(1)}$, where $R_{.}{}^{(1)}$ is risk to lose required integrity for input $T_{diag.}{}^{(1)}$. Optimistic risk to lose required integrity $R^{(2)}$ is calculated; …, n-th iteration is carried out after calculating risk $R_{.}{}^{(n-1)}$ for input $T_{diag.}{}^{(n-1)}$: $T_{diag.}{}^{(n)} = T_{diag.}{}^{(n-1)}$ $(1 - R^{(n-1)}) + T_{rec.}$ $R^{(n-1)}$, where $R_{.}{}^{(n-1)}$ is risk to lose required integrity for input $T_{diag.}{}^{(n-1)}$. Here recovery time is considering with the frequency aspiring to real, hence risk $R_{.}{}^{(n-1)\,)}$ will aspire to the real.

The last iteration is when the given condition is satisfied: $|R^{(n)} - R^{(n-1)}| \leq$ ε.

5th idea. Existing models of section 3 are applicable to the system presented as one element. The main output of such system modelling is probability of providing system integrity or violation of system integrity during the given period of time. If a probability for all points $T_{given.}$ from 0 to ∞ will be calculated, a trajectory of the PDF for each combined element depending on threats, periodic control, monitoring and recovery of integrity is automatically synthesized. The known kind of this PDF allows to define mean time of providing integrity or between violations of system integrity for every system element by traditional methods of mathematical statistics. And taking into account ideas 2-4 it gives necessary initial input for integration.

Thus, applying ideas 1-5, there is possible an integration of metrics on the level of a PDF of time of providing system integrity or violation of system integrity. And it is the base for forecasting quality and risks.

Note. Ideas 2-5 are implemented in the supporting software tools (Kostogryzov, Nistratov at al. (2004-2011)) - see, for example, the "Complex for evaluating quality of production processes" (patented by Rospatent №2010614145) - Figure 13.

Thus models implement original author's mathematical methodology based on probability theory, theory for regenerating processes and methods for system analysis. An application of offered methodology uses to evaluate probabilities of "success", risks and related profitability and expenses. This helps to solve well-reasonly the next practical problems in system life cycle:

- analysis of system use expediency and profitability, selecting a suitable suppliers, substantiation of quality management systems for enterprises, substantiation of quantitative system requirements to hardware, software, users, staff, technologies;
- requirements analysis, evaluation of project engineering decisions, substantiation of plans, projects and directions for effective system utilization, improvement and development;
- evaluation of customer satisfaction in system design&development and possible dangers, detection of bottle-necks;
- investigation of problems concerning potential threats to system operation including protection against terrorists and information security;
- verification and validation system operation quality, investigation rational conditions for system use and ways for optimization etc.

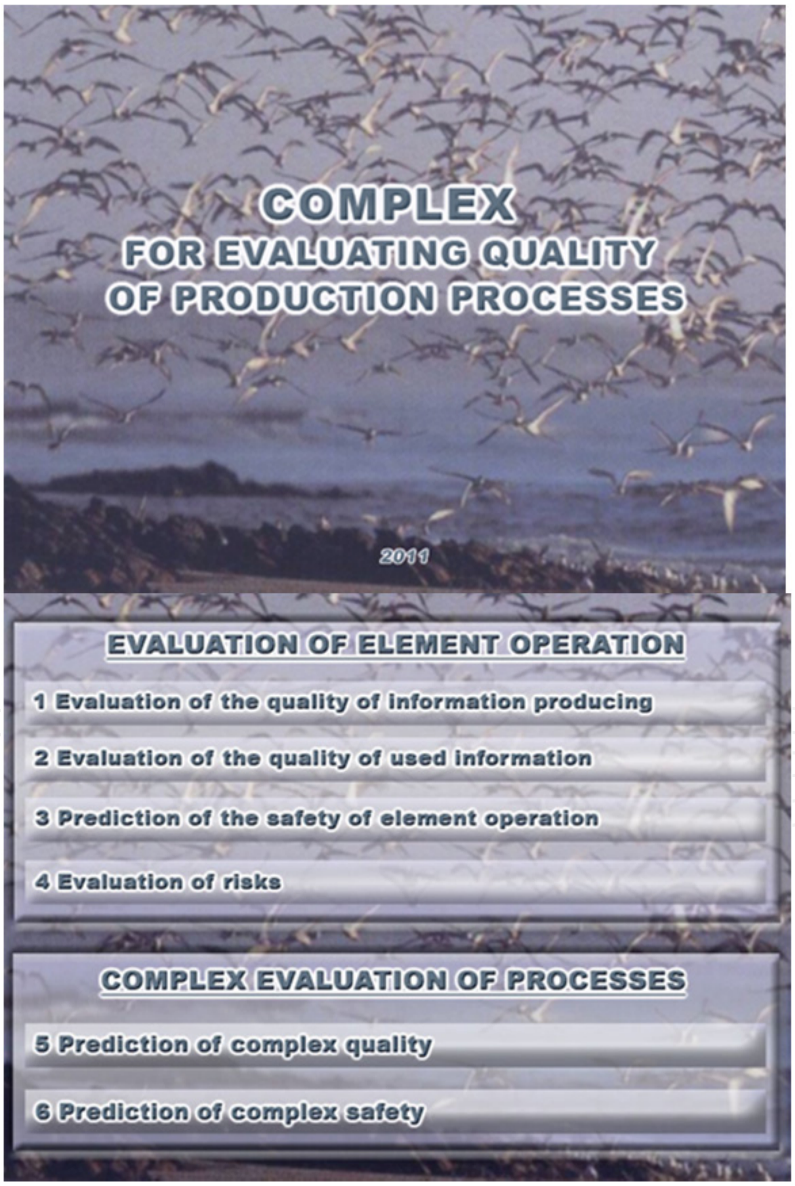

COMPLEX
FOR EVALUATING QUALITY
OF PRODUCTION PROCESSES
2011
EVALUATION OF ELEMENT OPERATION
1 Evaluation of the quality of information producing
2 Evaluation of the quality of used information
3 Prediction of the safety of element operation
4 Evaluation of risks
COMPLEX EVALUATION OF PROCESSES
5 Prediction of complex quality
6 Prediction of complex safety

Figure 13. Subsystems of the "Complex for evaluating quality of production processes"

The next complex for modelling of system life cycle processes "MODELLING OF PROCESSES" includes multi-functional software tools 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"), Project (models and software tools "Project Planning", "Project Assessment", "Project Control", "decision-making", "risk management", "configuration management", "information management") and Technical Processes Modelling (models and software tools "Requirements Definition", "requirements analysis", "architectural design", "human factor ", "implementation", "integration", "verification", "transition", "validation", "operation", "maintenance", "disposal" tools) – see Figures 14-17 (one separate box is an implementation of one or more mathematical models) (Kostogryzov, Nistratov at al. (2004-2011)).

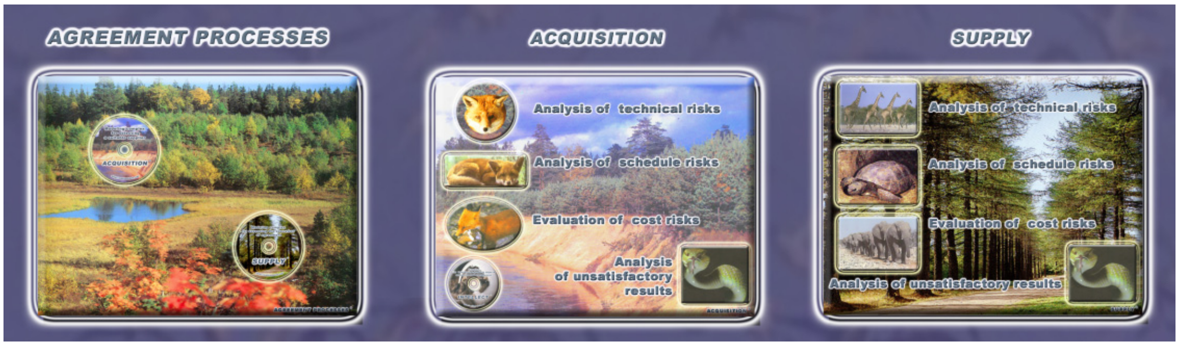

AGREEMENT PROCESSES
ACQUISITION
SUPPLY
ACQUISITION
SUPPLY
Analysis of technical risks
Analysis of schedule risks
Evaluation of cost risks
Analysis of unsatisfactory results
Analysis of technical risks
Analysis of schedule risks
Evaluation of cost risks
Analysis of unsatisfactory results

Figure 14. Software tools for evaluation of Agreement Processes

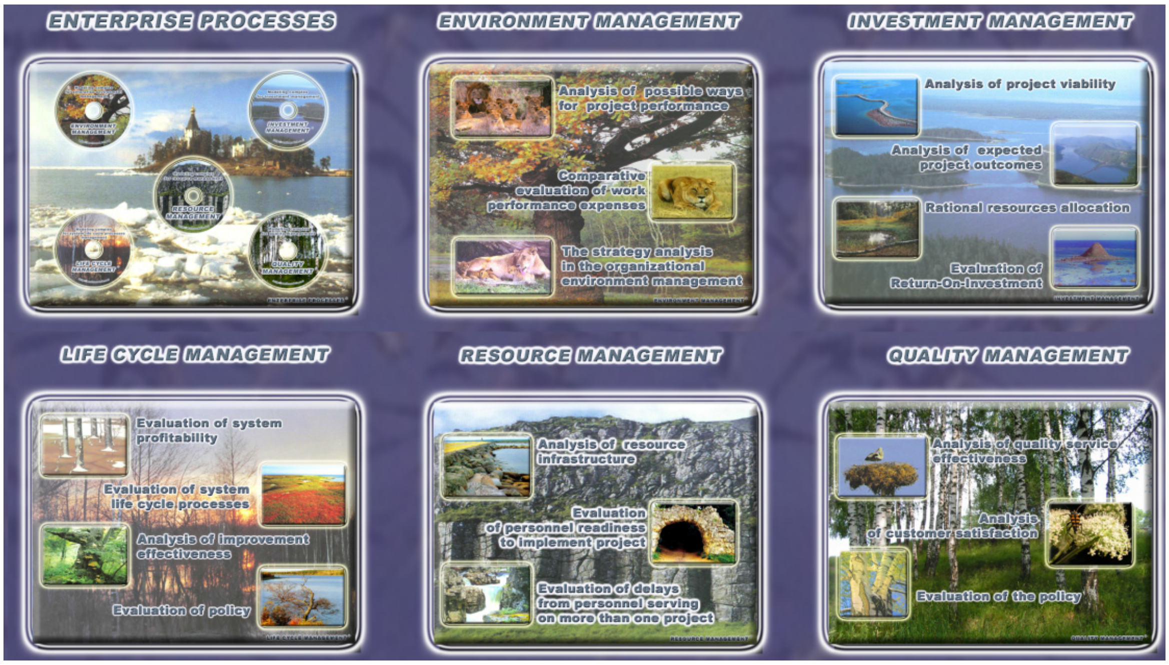

ENTERPRISE PROCESSES
ENVIRONMENT MANAGEMENT
INVESTMENT MANAGEMENT
ENVIRONMENT MANAGEMENT
INVESTMENT MANAGEMENT
RESOURCE MANAGEMENT
LIFE CYCLE MANAGEMENT
QUALITY MANAGEMENT
Analysis of possible ways for project performance
Comparative evaluation of work performance expenses
The strategy analysis in the organizational environment management
Analysis of project viability
Analysis of expected project outcomes
Rational resources allocation
Evaluation of Return-On-Investment
LIFE CYCLE MANAGEMENT
RESOURCE MANAGEMENT
QUALITY MANAGEMENT
Evaluation of system profitability
Evaluation of system life cycle processes
Analysis of improvement effectiveness
Evaluation of policy
Analysis of resource infrastructure
Evaluation of personnel readiness to implement project
Evaluation of delays from personnel serving on more than one project
Analysis of quality service effectiveness
Analysis of customer satisfaction
Evaluation of the policy

Figure 15. Software tools for evaluation of Enterprise Processes

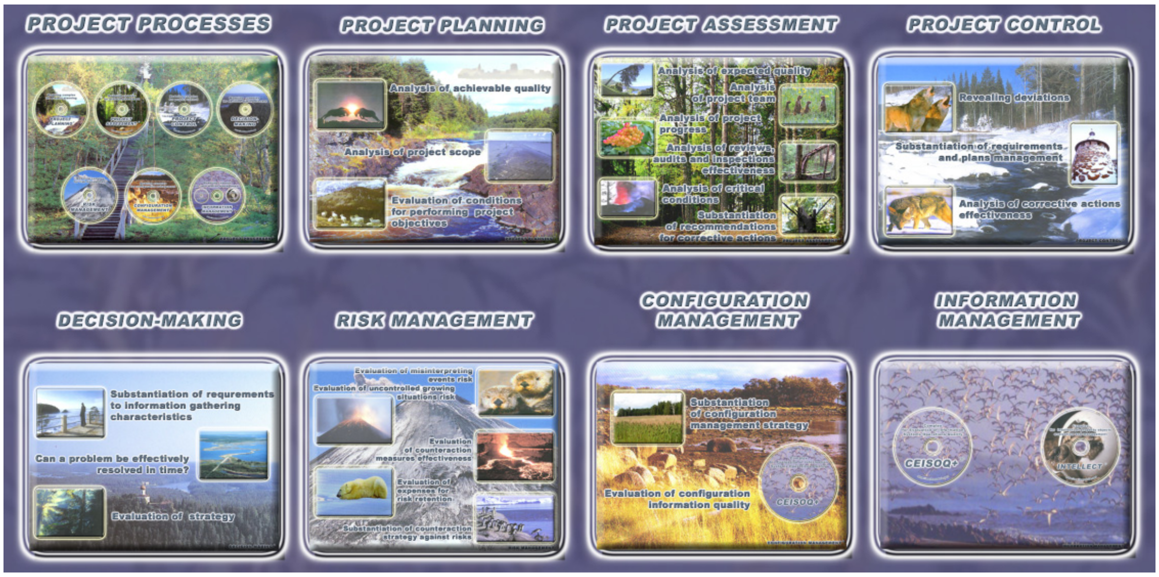

PROJECT PROCESSES
PROJECT PLANNING
Analysis of achievable quality
Analysis of project scope
Evaluation of conditions for performing project objectives
PROJECT ASSESSMENT
Analysis of expected quality
Analysis of project team
Analysis of project progress
Analysis of reviews, audits and inspections effectiveness
Analysis of critical conditions
Substantiation of recommendations for corrective actions
PROJECT CONTROL
Revealing deviations
Substantiation of requirements and plans management
Analysis of corrective actions effectiveness
DECISION-MAKING
Substantiation of requrements to information gathering characteristics
Can a problem be effectively resolved in time?
Evaluation of strategy
RISK MANAGEMENT
Evaluation of misinterpreting events risk
Evaluation of uncontrolled growing situations risk
Evaluation of counteraction measures effectiveness
Evaluation of expenses for risk retention
Substantiation of counteraction strategy against risks
CONFIGURATION MANAGEMENT
Substantiation of configuration management strategy
Evaluation of configuration information quality
CEISOQ+
INFORMATION MANAGEMENT
CEISOQ+
INTELLECT

Figure 16. Software tools for evaluation of Project Processes

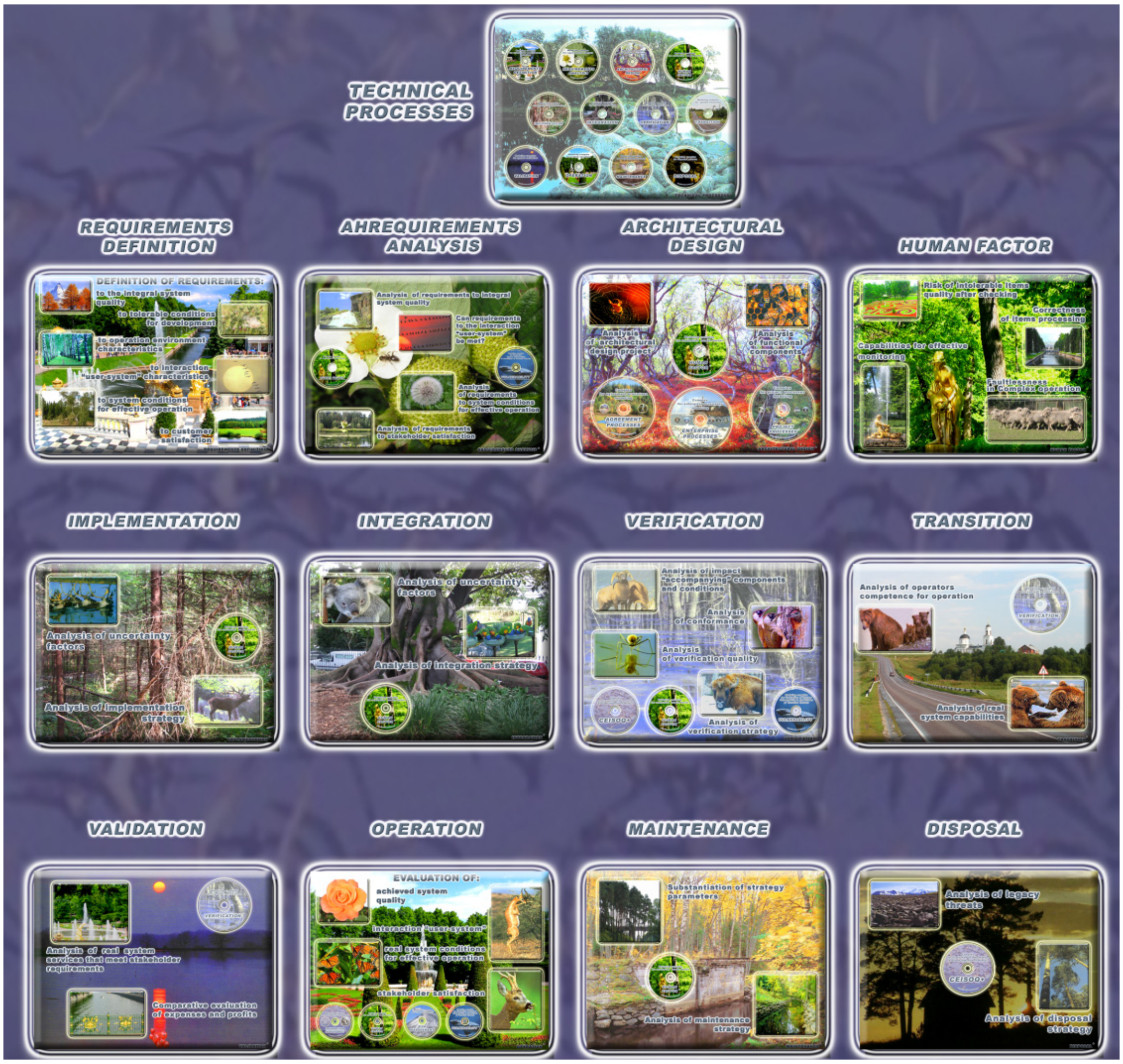

TECHNICAL PROCESSES
REQUIREMENTS DEFINITION
DEFINITION OF REQUIREMENTS:
to the integral system quality
to tolerable conditions for development
to operation environment characteristics
to interaction "user-system" characteristics
to system conditions for effective operation
to customer satisfaction
AHREQUIREMENTS ANALYSIS
Analysis of requirements to integral system quality
Can requirements to the interaction "user-system" be met?
Analysis of requirements to system conditions for effective operation
Analysis of requirements to stakeholder satisfaction
ARCHITECTURAL DESIGN
Analysis of architectural design project
Analysis of functional components
AGREEMENT PROCESSES
ENTERPRISE PROCESSES
PROJECT PROCESSES
HUMAN FACTOR
Risk of intolerable items quality after checking
Correctness of items processing
Capabilities for effective monitoring
Faultlessness in Complex operation
IMPLEMENTATION
Analysis of uncertainty factors
Analysis of implementation strategy
INTEGRATION
Analysis of uncertainty factors
Analysis of integration strategy
VERIFICATION
Analysis of impact "accompanying" components and conditions
Analysis of conformance
Analysis of verification quality
CEISOQ+
Analysis of verification strategy
TRANSITION
Analysis of operators competence for operation
VERIFICATION
Analysis of real system capabilities
VALIDATION
VERIFICATION
Analysis of real system services that meet stakeholder requirements
Comparative evaluation of expenses and profits
OPERATION
EVALUATION OF:
achieved system quality
interaction "user-system"
real system conditions for effective operation
stakeholder satisfaction
MAINTENANCE
Substantiation of strategy parameters
Analysis of maintenance strategy
DISPOSAL
Analysis of legacy threats
CEISOQ+
Analysis of disposal strategy

Figure 17. Software tools for evaluation of Technical Processes

4.2. The formal statement of problems for system analysis and optimization

According to ISO 9000 management is defined as coordinated activities to direct and control an organization. In general case control is considered as the process of comparing actual performance with planned performance, analyzing variances, evaluating possible alternatives, and taking appropriate corrective action as needed (PMBOK). From system analysis point of view the main function of management is a purposeful change of a condition of process, object or system. Thus the process, object or system considered as managed if among all changes there is available one by means of which the purpose can be achieved. Management is based on a choice of one of set of any alternatives. Rational management is the management leading achievement of the purpose by criterion of an extremum (a minimum or a maximum) the chosen parameter at a set of limitations. Classical examples of rational management generally are maximization of a prize (profit, a degree of quality or safety, etc.) at limitations on expenses or minimization of expenses at limitations on a admissible level of quality and-or safety.

It is clear, that in life cycle of systems criteria and limitations vary. We shall consider briefly an essence popular today «process approach» for design, development and improvement of systems management quality according to ISO 9001. For successful operation the organization should define and carry out management of the interconnected kinds of activities. The activity using resources and performed with the purpose of transformation inputs in purposeful outputs, actually represents process. Thus, "process approach» means the application of system processes in view of their identification and interaction. The model of system management quality, based on «process approach», is directed finally to meet customer satisfaction. For rational management of processes it is necessary to know and predict their behaviour at various influences. For this purpose it is offered to use the mathematical models including models offered in this book. The metrics entered in these models, or their combination may be used as criteria metrics. Actually they are the quantitative measure (criterion function) describing degree of achievement of a purpose in view of management at various stages of system life cycle. For the enterprise there is important, for example, to optimize system management quality. A maximum of the probability of qualified work performance (i.e. in time and without any defects) or the probability of successful life-cycle processes running on condition that the competitiveness of each product type is retained can be used as criterion with corresponding limitations. For security services it is necessary to provide safety of object, process or system up to the mark. In this case the criterion of a minimum of expenses at limitations on an admissible risk level of dangerous influence on system contrary to counteraction measures or a minimum of risk of dangerous influence at limitations on expenses are possible. For the customer and the developer of the project the end result is important. In this case the criterion of a maximum of a relative quantity of system functions which are carried out with admissible quality or a relative level of customer satisfaction can be used as the integrated measure. The statement of problems for system analysis includes definition of conditions, threats and estimation a level of critical measures.

Thus the final choice of integrated measures is allocated on a payoff to the customer in view of specificity of created or maintained system. As probability parameters give higher guarantees in estimations of a degree of achieving purposes in comparison with average value at a choice it is recommended to use probability (i.e. on a degree of system quality operation - probability of providing admissible function performance quality during the given period of time) as the cores. And evaluated time characteristics (for example the mean time between violations of admissible system operation quality) are offered as auxiliary.

For example, there are applicable the next general formal statements of problems for system optimization:

1. on the stages of system concept, development, production and support:

system parameters, software, technical and management measures (Q) are the most rational for the given period if on them the minimum of expenses ($Z_{dev.}$) for creation of system is reached:

$$Z_{dev.}(Q_{rational}) = \min_{Q} Z_{dev.}(Q),$$

at limitations on probability of an admissible level of quality $P_{quality}$ (Q) ≥ $P_{adm.}$ and expenses for operation

$C_{oper.}$ (Q) ≤ $C_{\ adm.}$ and under other development, operation or maintenance conditions;

2. on operation stage :

system parameters, software, technical and management measures (Q) are the most rational for the given period of operation if on them the maximum of probability of providing admissible system operation quality is reached:

$$P_{quality}(Q_{rational}) = \max_{Q} P_{quality}(Q),$$

at limitations on probability of an admissible level of quality $P_{quality}$ (Q) ≥ $P_{adm.}$ and expenses for operation

$C_{oper.}$ (Q) ≤ $C_{\ adm.}$ and under other operation or maintenance conditions.

Of course these statements may be transformed into problems of expenses or risk minimization in different limitations. System parameters, software, technical and management measures (Q) is a rule a vector of input – see examples. There may be combination of these formal statements in system life cycle.

The order for use the developed classical formal approach to analyze and optimize system processes in quality management is illustrated by Figure 18. When analyst use this approach he'd like for several minutes to formalize a problem, perform mathematical modeling, analyze system processes in different conditions, choose the most rational variant and prepare analytical report. Such possibilities exist: an analyst should perform mathematical modelling by the Internet versions of the offered models – see Figure 19. He prepares input and receives analytical report in Word or pdf-file about 50-100 sheets as a result of interaction. This report will be formed automatically and include a formalization of analyst's problem, input, results of mathematical modeling in pictures (as demonstrated above in examples), analysis of system processes behaviour for different conditions, choice of the most rational variant and recommendations." It means that any analyst, understanding the used mathematical model, can receive during 1-3 minutes scientifically proved analytical report after interaction with an Internet version of model.

This report may be used for making decision and developing his independent report with additional materials. It is virtual outsourcing of high system analysis on the base of the offered mathematical models. The purpose is to give to analysts an opportunity of accessible and cheap high technology of studying standard processes in life cycle of estimated systems. This work has begun, the first models are accessible (see **www.mathmodels.net**).

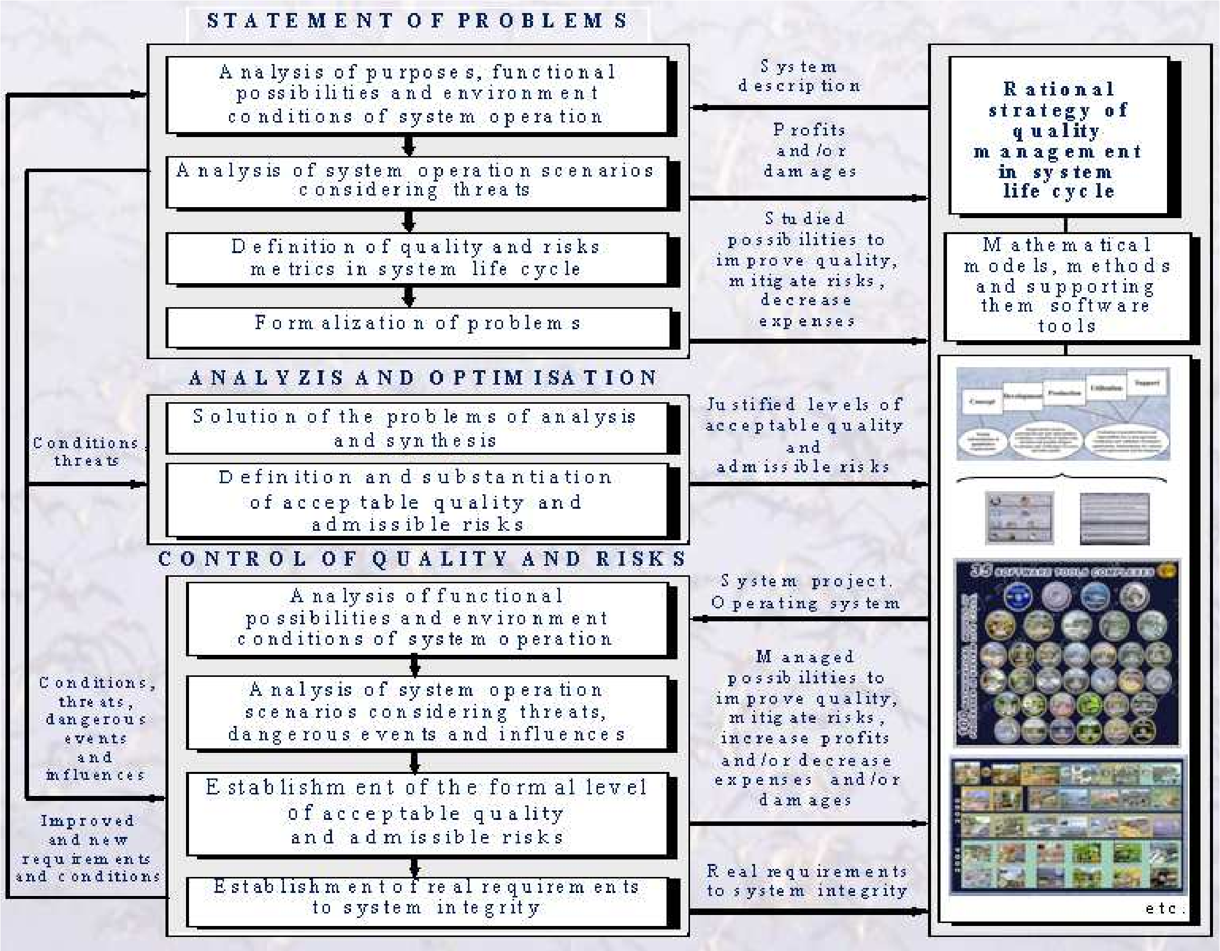
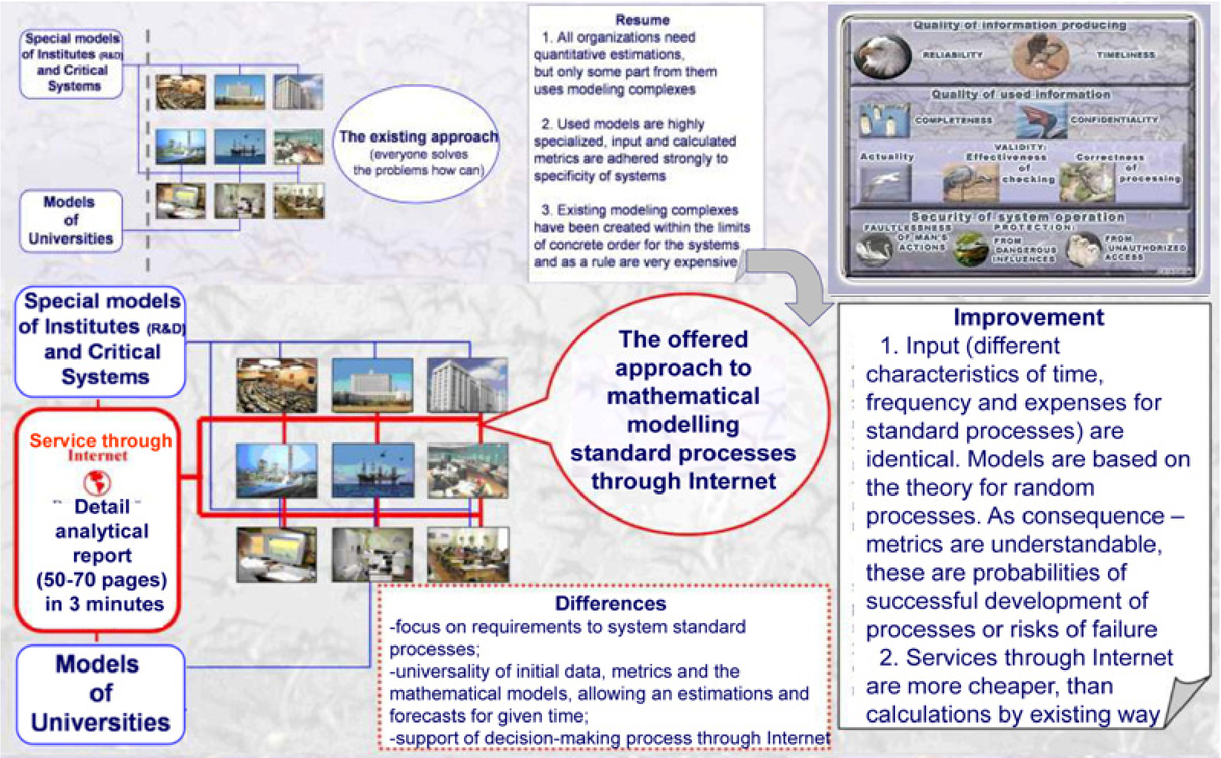

STATEMENT OF PROBLEMS
Analysis of purposes, functional possibilities and environment conditions of system operation
Analysis of system operation scenarios considering threats
Definition of quality and risks metrics in system life cycle
Formalization of problems
System description
Profits and/or damages
Studied possibilities to improve quality, mitigate risks, decrease expenses
Rational strategy of quality management in system life cycle
Mathematical models, methods and supporting them software tools
ANALYZIS AND OPTIMISATION
Solution of the problems of analysis and synthesis
Definition and substantiation of acceptable quality and admissible risks
Justified levels of acceptable quality and admissible risks
Conditions, threats
CONTROL OF QUALITY AND RISKS
Analysis of functional possibilities and environment conditions of system operation
Analysis of system operation scenarios considering threats, dangerous events and influences
Establishment of the formal level of acceptable quality and admissible risks
Establishment of real requirements to system integrity
System project. Operating system
Managed possibilities to improve quality, mitigate risks, increase profits and/or decrease expenses and/or damages
Real requirements to system integrity
Conditions, threats, dangerous events and influences
Improved and new requirements and conditions
35 SOFTWARE TOOLS COMPLEXES
etc.

Figure 18. The approach to analyze and optimize system processes

The presented software tools complexes allow to solve problems for system analysis and optimization. Expected pragmatic effect from their application is the next: it is possible to provide essential system quality rise and/or avoid wasted expenses in system life cycle on the base of modelling system processes by the offered mathematical models.


Special models of Institutes (R&D) and Critical Systems
Models of Universities
The existing approach (everyone solves the problems how can)
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
Special models of Institutes (R&D) and Critical Systems
Service through Internet
Detail analytical report (50-70 pages) in 3 minutes
Models of Universities
The offered approach to mathematical modelling standard processes through Internet

Resume

1. All organizations need quantitative estimations, but only some part from them uses modeling complexes

2. Used models are highly specialized, input and calculated metrics are adhered strongly to specificity of systems

3. Existing modeling complexes have been created within the limits of concrete order for the systems and as a rule are very expensive

Improvement

1. Input (different characteristics of time, frequency and expenses for standard processes) are identical. Models are based on the theory for random processes. As consequence – metrics are understandable, these are probabilities of successful development of processes or risks of failure

2. Services through Internet are more cheaper, than calculations by existing way

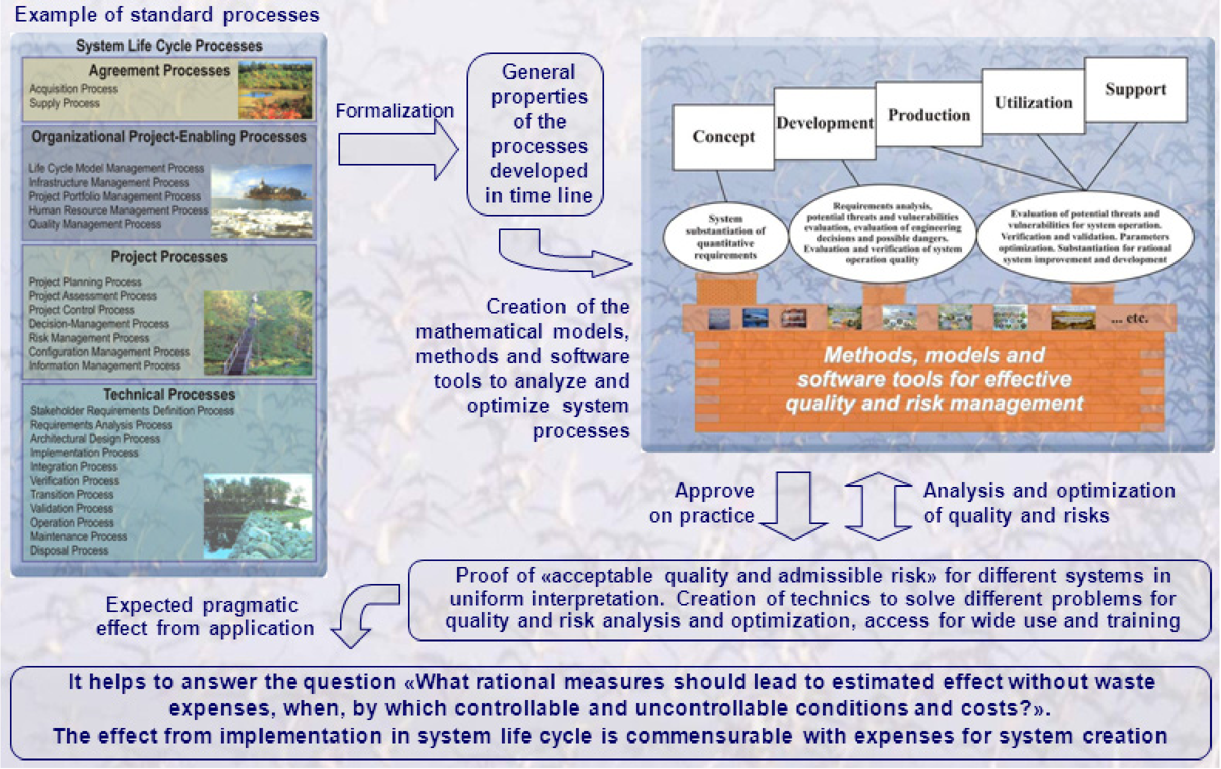
Differences

-focus on requirements to system standard processes;

-universality of initial data, metrics and the mathematical models, allowing an estimations and forecasts for given time;

-support of decision-making process through Internet

Figure 19. Mathematical modelling by the Internet versions of the offered models


Example of standard processes
System Life Cycle Processes
Agreement Processes
Acquisition Process
Supply Process
Organizational Project-Enabling Processes
Life Cycle Model Management Process
Infrastructure Management Process
Project Portfolio Management Process
Human Resource Management Process
Quality Management Process
Project Processes
Project Planning Process
Project Assessment Process
Project Control Process
Decision-Management Process
Risk Management Process
Configuration Management Process
Information Management Process
Technical Processes
Stakeholder Requirements Definition Process
Requirements Analysis Process
Architectural Design Process
Implementation Process
Integration Process
Verification Process
Transition Process
Validation Process
Operation Process
Maintenance Process
Disposal Process
Formalization
General properties of the processes developed in time line
Creation of the mathematical models, methods and software tools to analyze and optimize system processes
Concept
Development
Production
Utilization
Support
System substantiation of quantitative requirements
Requirements analysis, potential threats and vulnerabilities evaluation, evaluation of engineering decisions and possible dangers. Evaluation and verification of system operation quality
Evaluation of potential threats and vulnerabilities for system operation. Verification and validation. Parameters optimization. Substantiation for rational system improvement and development
... etc.
Methods, models and software tools for effective quality and risk management
Approve on practice
Analysis and optimization of quality and risks
Expected pragmatic effect from application

Proof of «acceptable quality and admissible risk» for different systems in uniform interpretation. Creation of technics to solve different problems for quality and risk analysis and optimization, access for wide use and training

It helps to answer the question «What rational measures should lead to estimated effect without waste expenses, when, by which controllable and uncontrollable conditions and costs?». The effect from implementation in system life cycle is commensurable with expenses for system creation

Figure 20. The offered way is the use of created methods to analyze and optimize system processes

Thereby necessary attributes of the offered innovative approach to control of system processes in quality management are above formed. Traditional approaches consist as a matter of fact in a pragmatical filtration of the information. In the decisions the responsible person, making decision, is guided firstly by the own experience and the knowledge and the advices of those persons of a command to whom trusts. Intuitively forming ideas which seem correct, this person chooses only that information which proves idea. The denying information is often ignored and more rare – leads to change of initial idea. This approach can be explained from the facts that at absence or limitation of used models it is difficult to investigate at once many ideas for given time. The presented models, methods and software tools, reducing long time of modelling (from several days, weeks and months to few seconds and minutes) change this situation cardinally.

The offered innovative approach is at the beginning substantiation of the system requirements, purposefully capable to lead to a success. Further, the responsible person, equipped by a set of necessary mathematical models and their software tools possibilities to forecasting quality and risks, is powered for generation of the proved ideas and effective decisions. These decisions are physically clear because of using accessible and operative analysis and optimization of processes in system life cycle. The offered approach allows to go «from a pragmatical filtration of information to generation of the proved ideas and effective decisions». The effect from implementation in system life cycle is commensurable with expenses for its creation (see Figure 20 and www.mathmodels.net).

We will demonstrate usability, universality and efficiency of the offered models, methods and software tools on the examples of their application for the analysis of "human factor», information actuality in commerce, errors during a use of SCADA-systems, efficiency of non-destroying control, preservation of foods quality, fire extinguishing, reliability of engineering equipment for enterprise object, flights safety in conditions of terrorist threats, information security, and also to the forecasts of risks for complex multipurpose systems.

5. Examples

Example 1 («Human factor»). Modern enterprises total tens – hundreds various workers. To solve a given functional enterprise problem there are required, as a rule, efforts of several specialists. For example, information gathering and control, its security providing, database and computing process administration, maintenance of computer equipment and information use are performed by different people. It is clear that their qualifications must be very high. Let's examine an example when it is not so. The reader may remember situations from his life.

Let the problem solution depends on joint but independent actions of 5 people. Let each of 4 specialists make 1 error a month and the 5th inexperienced person makes 1 error a day. System recovery time after an error equals to 30 minutes. It is required to evaluate faultlessness of such group's actions within a week.

The solution is based on the use of the CEISOQ+ subsystem «Faultlessness of man's actions» (see model in subsection 3.2). Integral computation results reveal that the probability of faultless joint actions of the first 4 skilled specialists within a 40-hours workweek equals to 0.80 but the low-quality work of the 5th unexperienced member mocks the whole group work. Indeed, the probability of faultless actions decreases to 0.15 (see Figure 21). Thus the computed results prove quantitatively the importance of thorough specialists training because a man is the main system bottleneck. It is impossible to detect all the system defects, but in some cases there is no full protection from "a fool". The quality management acts very wisely. As a rule an instructions with a training database and introduced assessment of users' readiness for a work with the real system is used. The proposed methods allow to estimate achieved levels of such system readiness.

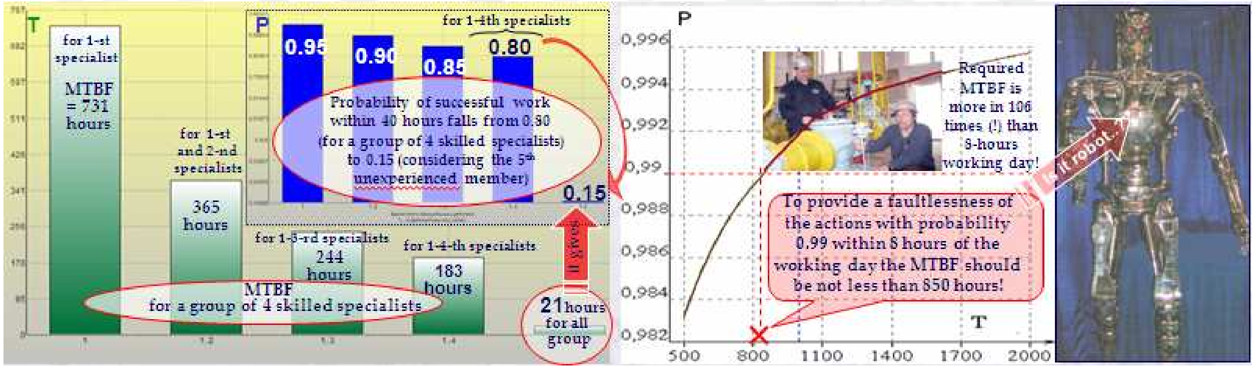


Figure 21. An estimation of human factor, examples 1-2

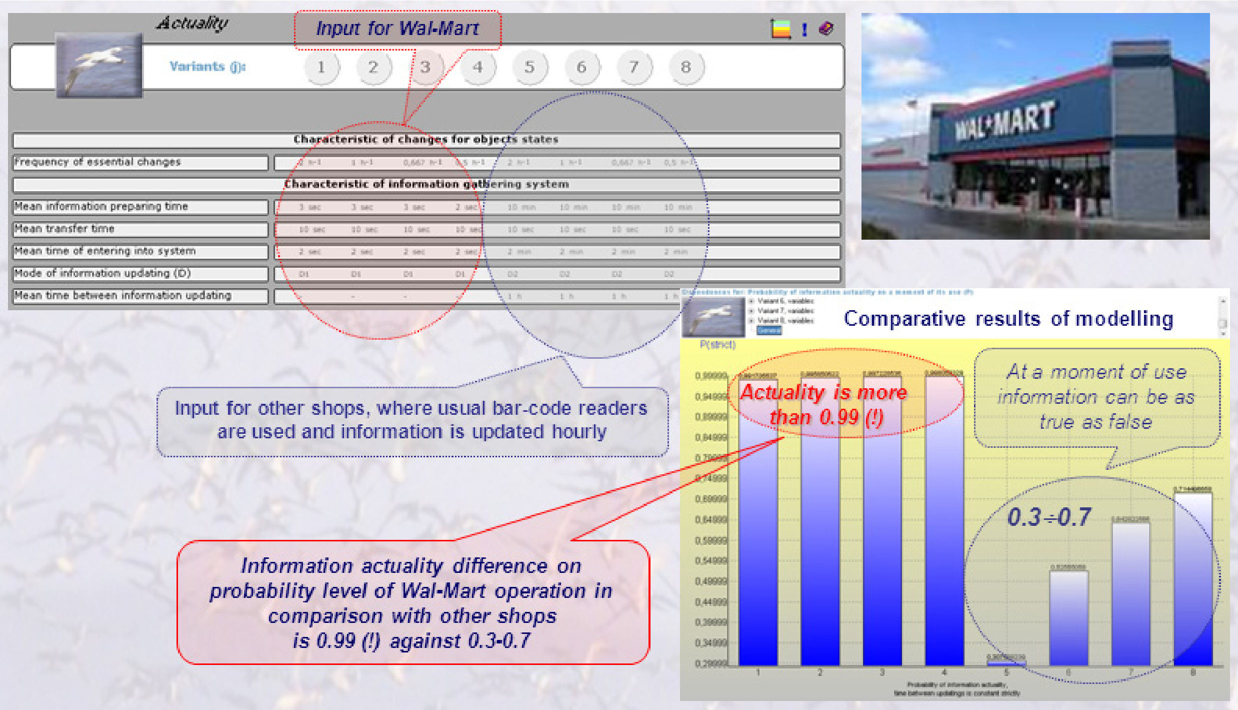
The question is lawful - what MTBF an worker should possess to provide a faultlessness of the actions with probability 0.99 within 8 hours of the working day? According to calculations the MTBF not less than 850 working hours is acceptable – see Figure 21 right. It is more than 8-hours working day in 106 times (!), i.e. 4 months are necessary to work without errors, as the robot.

Example 2 (A role of information actuality in commerce). Nowadays the product market is being changed into an electronic one. What level of information actuality is peculiar to the successful companies within the possibilities of quality management and information technologies?

Solution. We'll try to answer this question by the subsystem "Actuality" of CEISOQ+ using as an example the worldwide known retail outlets network "Wall Mart", distributed in the USA, Canada, Mexico etc. (see model in subsection 3.5). Let's define an information aspect which makes for the company's success.

To increase productivity of each worker salesclerks were equipped with manual bar-code readers. Information contained in a bar-code is shown on a display. A worker can get a retrospective picture of products saling within a day, a week and several weeks. Moreover, on each article there are data about its quantity in the shop floor, in stock and how much has been ordered, i.e. everything what may be necessary for ordering. Let's evaluate actuality of information used by this system. It is logical to admit that significant changes happen not more frequent than 2 times per working day. There may be a leap in demand and supply, a change of goods quantity ordered by a customer, force majeur. Due to immediate information gathering by salesclerks (with the help of bar-code readers it takes 3 seconds), its transfer by satellite communications (10 seconds) and entering into a database (1 second) actuality of information in this network is not less than 0.992 (see variants i=1-4 on Figure22). It means that for successful company the probability to use actual information against non-actual one is more in 124 times (0.992/0.008=124)!

Correct use of this information turns out to be very effective. Using information read from a bar-code, which is transferred to the headquarters, they may order lots of goods, distribute them into their outlets and not worry about goods warehousing. For comparison, other shops, where usual bar-code readers are used and information is updated hourly, use information which actuality equals to 0.3-0.7 (see variants i=5-8 on Fig.23). Thus at the moment of use information can be as true as false. On the resulted figures it is possible to feel information roots of perfection quality management. According to "precedent" principle the achievable level 0.992 of information actuality can be defined as admissible.


Actuality
Input for Wal-Mart
Variants (j):
Input for other shops, where usual bar-code readers are used and information is updated hourly
Information actuality difference on probability level of Wal-Mart operation in comparison with other shops is 0.99 (!) against 0.3-0.7
Comparative results of modelling
P(strict)
Actuality is more than 0.99 (!)
At a moment of use information can be as true as false
0.3÷0.7
1
2
3
4
5
6
7
8

Variants (j):	1	2	3	4	5	6	7	8
Characteristic of changes for objects states								
Frequency of essential changes	2 h-1	1 h-1	0,667 h-1	0,5 h-1	2 h-1	1 h-1	0,667 h-1	0,5 h-1
Characteristic of information gathering system								
Mean information preparing time	3 sec	3 sec	3 sec	2 sec	10 min	10 min	10 min	10 min
Mean transfer time	10 sec	10 sec	10 sec	10 sec	10 sec	10 sec	10 sec	10 sec
Mean time of entering into system	2 sec	2 sec	2 sec	2 sec	2 min	2 min	2 min	2 min
Mode of information updating (D)	D1	D1	D1	D1	D2	D2	D2	D2
Mean time between information updating	-	-	-	-	1 h	1 h	1 h	1 h

Figure 22. Input for CEISOQ+ and comparative results of modelling

Example 3 (Errors during a use of SCADA system). The control towers use SCADA system (Supervisory Control And Data Acquisition) for making decision. The data gathering and processing activities are modeled to evaluate the risk of misinterpreting of potentially dangerous events in control towers. Wrong interpretation may be caused by errors of dispatcher personnel, which can miss important information or turn harmless information into dangerous one, fails of SCADA system. Let's consider a control station receiving information from the SCADA system for following processing. The information flow is measured in some conventional units and the information flow is of 100 units per hour. The total information contains not more than 1% of data related to potentially dangerous events. Taking into account automatic data analysis we suppose the speed of event interpretation to be near 30 sec per information unit. In this case 100 information units will be processed during 50 min. At that the frequency of errors for the whole dispatcher shift on duty, including fails of the SCADA system itself is about 1 error per year according to statistical data. The task is to estimate the risk of misinterpreting events on the control station for a time period of 1 hour, during one dispatcher shift turn of 8 hours, 1 month, 1 year, and 10 years.

The solution is based on the use of the subsystem «Risk evaluation. Risk of inadequate interpretation of events» of the software tools “Complex for evaluating quality of production processes” (see model in subsection 3.6). The analysis of modelling shows (see Figure 23) that for short time periods such as one shift turn or even for a month the risk of mistaken analytical conclusion is small enough (0.00076 and 0.07 accordingly). But when the time period grows the risk increases and becomes 0.565 for a year and almost unity (0.9998) during time period of 10 years. This means that during a month the probability for errors of dispatcher personal or SCADA system fails to occur is very small and their operation will be almost faultless. But for a more long time period such as a year is considered 1-2 errors of dispatcher personal or system SCADA fails will occur for certain. Considering high reliability of SCADA system and according to “precedent” principle the achievable level 0.07 for the risk of mistaken analytical conclusion during a month can be defined as acceptable.

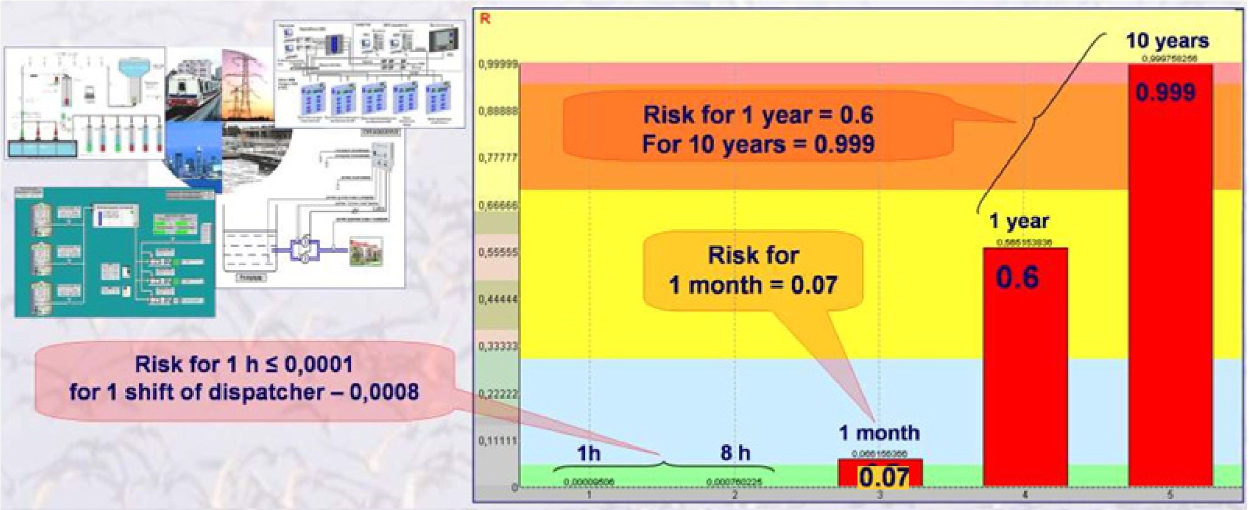


Figure 23. Some results of modelling a SCADA-system

Example 4 (Efficiency of non-destroying control). Let’s consider two competing enterprises which are suppliers of pipes for transportation of production and guided in their quality management system by various technical politics. The first of these enterprises, guided by an innovative way of development with rational application of modern information technologies, effectively uses (as believed) existing innovations for quality and risks management. The second company uses cheaper and out-of-date technologies, keeping competitiveness on the market at the expense of it. At the enterprises various methods of non-destroying control are applied to revealing defects.

The first enterprise acquires input production from suppliers after quality control by all recommended methods of non-destroying control (acoustic, magnetic, optical, radiating, radio wave, thermal, electromagnetic etc.) that is confirmed by test reports and certificates on ISO 9001 and on output production. As a result for total controllable production in 100000 units per a month (for example, production tons, running meters etc.) the part of possible defects before control is 5%, a frequency of errors during the control is no more than 2 defects in a year (these are the latent defects not revealed by existing methods or passed at the control).

The second enterprise is satisfied by certificate on ISO 9001. And only radio wave method of non-destroying control is used by the suppliers. It allows to reveal such defects, as stratifications and deviations on a thickness in metal products (i.e. no more than 10 % of possible defects). At the expense of it the part of possible defects before the control is already 20 %, moreover, at the control defects of moulding (slag and flux inclusions, shrinkable bowls, gas bubbles, cracks, etc.), defects of processing by pressure (internal and superficial cracks, ruptures, tempers, dents, etc.), defects of heat treatment (overheats, hardening and hydrogen cracks, etc.) are missed. Totally about 30 defects per a year are possible.

Omitting questions of profits, we will compare technical politics of these enterprises by a risk of mistaken analytical conclusion within a month.

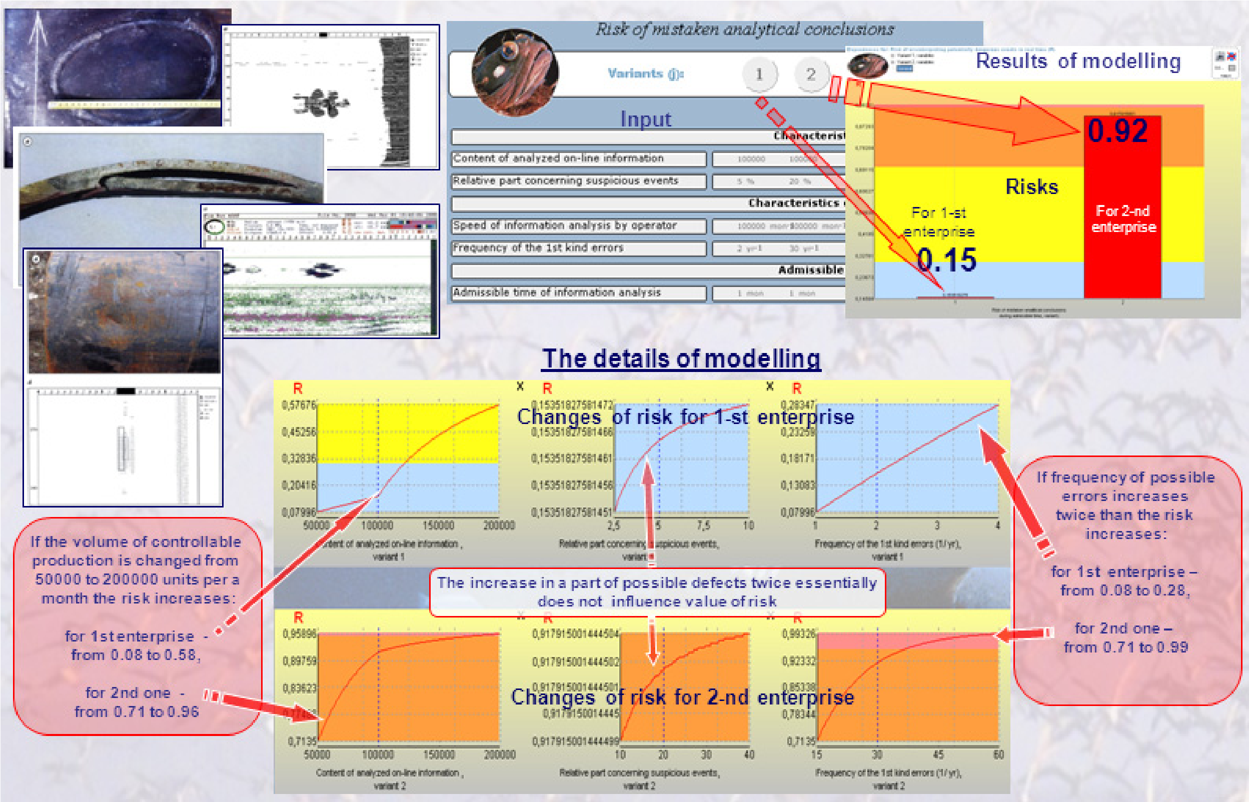
The solution is based on the same software tools as for example 3, but difference is the next: according to the 1-st idea of subsection 4.1 instead of metric "Risk of inadequate interpretation of events" we use metric "Risk of mistaken analytical conclusions". Input and results of modelling are on Figure 24.

The comparative analysis of the received dependences has shown:

- the risk of mistaken analytical conclusions for 1st first enterprise is 0.15, and for 2nd one – 0.92 (!);
- if the volume of controllable production is changed from 50000 to 200000 units per a month the risk increases for 1st enterprise from 0.08 to 0.58, and for 2nd one – from 0.71 to 0.96;
- the increase in a part of possible defects twice essentially does not influence value of risk, i.e. efficiency of applied technologies of the control depends essentially on other parameters, in particular from frequency of possible errors;
- if frequency of possible errors increases twice than the risk increases for 1st enterprise from 0.08 to 0.28, and for 2nd one – from 0.71 to 0.99.

Conclusion: For 1st enterprise the risk of mistaken analytical conclusions at level 0.15 after the control within a month can be recognized as acceptable. The 2nd enterprise supplies frankly defected production (probability nearby 0.9) that will negatively affect further at system operation.

Example 5 (Preservation of foods quality). We will demonstrate foods quality management on an example of probabilistic analysis of processes that are peculiar for grain storage. Quality of the grain supplied on longtime storage, decreases because of influences of dangerous biological, chemical and physical factors. Let's estimate the possible period before such moment of time when storing grain begin to loss required quality, and also expediency of introduction of continuous monitoring of grain quality.


Risk of mistaken analytical conclusions
Variants (j):
1
2
Input
Characteristics
Content of analyzed on-line information
Relative part concerning suspicious events
Speed of information analysis by operator
Frequency of the 1st kind errors
Admissible
Admissible time of information analysis
Results of modelling
0.92
Risks
For 1-st enterprise
0.15
For 2-nd enterprise
The details of modelling
Changes of risk for 1-st enterprise
Changes of risk for 2-nd enterprise
R
Content of analyzed on-line information, variant 1
Relative part concerning suspicious events, variant 1
Frequency of the 1st kind errors (1/yr), variant 1
Content of analyzed on-line information, variant 2
Relative part concerning suspicious events, variant 2
Frequency of the 1st kind errors (1/yr), variant 2

If the volume of controllable production is changed from 50000 to 200000 units per a month the risk increases:

for 1st enterprise - from 0.08 to 0.58,

for 2nd one - from 0.71 to 0.96

The increase in a part of possible defects twice essentially does not influence value of risk

If frequency of possible errors increases twice than the risk increases:

for 1st enterprise – from 0.08 to 0.28,

for 2nd one – from 0.71 to 0.99

Figure 24. Comparative estimation of efficiency of quality management for enterprises which are suppliers of pipes

The solution is based on the use of the subsystem «Risk evaluation. Risk of uncontrollable development of situations» of the software tools "Complex for evaluating quality of production processes" (see model in subsection 3.9). The list of dangerous factors (threats), controllable parameters and proactive actions at grain storage in real conditions is resulted in table 1 (Machikhina et al. (2007)).

The cleared, dry and non-contaminated grain may be stored lost-free some years. However, the insects which are present in granaries and round them, occupy grain and breed. For example, every 2 months rice weevil increases in the number at 15-45 times at temperature from 20˚C to 25˚C. If in batch of wheat in weight 1000 tons contamination reaches 16 bugs on 1 kg of grain, losses are expected more than 5 %. The grain polluted by wreckers and products of their vital functions (excrements, dead bodies, uric acid, etc.), becomes toxic. It cannot be used for the food purposes. Therefore we will consider security of grain from insects, believing within the example, that exactly the main dangers are from them.

Let's a frequency of latent occurrence of critical situations during hot months is often not less than 1 time a day (i.e. every day at air temperature above 12˚C infection or the further damage of grain is possible). Our consideration: at 12-15˚C a duration of insects development (for example, weevil) is 141-376 days, and in a laying from 300 to 600 eggs a cycle of development is 1.5-2 months. In the conditions of cooling of grain below a temperature threshold of insects development (more low than 10.2˚C) their pairing, eggs putting off and development of all stages stop. Insects become inactive and almost do not eat. Long stay of insects at such temperature leads to their slow extinction. Besides, humidity maintenance at a level of 13%-15% also promotes extinction of insects.

Dangerous factors (threats)	Controllable parameters	Proactive measures
Biological: - microorganisms; - contamination of grain stocks by insects	Grain, spoilt as a result of self-warming and growing mouldy. Insects and pincers, a dung of rodents.	Observance of requirements of the standard documentation on grain storage. Complex of practical and exterminating measures against insects.
Chemical: - mycotoxins; - products of fats oxidation in grain (free fat acids, aldehydes, ketones, peroxides); - harmful products of vital functions of grain wreckers; - pesticides	The content of the spoilt and damaged grains as a result of microbiological spoiling. Organoleptic indicators (colour, a smell), and also the content of the beaten and brought down grains. Total density of pollution by live and dead wreckers, no more than 15 copies /kg. Residual quantities.	Observance of the general sanitary norms. Observance of regulations for pesticides use and terms of grain endurance after processing. Decrease of storage temperature to low positive temperatures of air. Observance of the instruction for pest control. Observance of requirements to grain after desinsection.
Physical: - extraneous subjects, casual and weed impurity; - grain temperature and humidity	Rough, large and casual impurity. Stable temperatureand humidity	Grain clearing on separators. Regular cooling of grain to low positive temperature (no more 10˚C). Observance of the requirements of the general technological regulations

Table 1. The list of dangerous factors, controllable parameters and proactive measures at grain storage

Thus, input for modelling is defined: frequency of latent occurrence of critical situations – from 1 time a day to 1 time a week; mean time of danger source activation – 1.5 months; time between diagnostics of system integrity (analysis of temperature and humidity) – 1 hour; duration of diagnostic, including recovery time – 1 hour.

It is enough to predict a risk of uncontrollable development of situations with grain storage. The results of modelling for the period from 1 year to 6 years have shown the following.

If a frequency of latent occurrence of critical situations is 1-2 times a day, risk of uncontrollable development of situations within a year will grow from 0.28 to 0.47, and during 2-years period it can exceed 0.5 – see Figure 25 left.

These results can be interpreted so: if storage conditions daily promote occurrence of insects, then for a 1-2 years grain quality loss is possible at the same degree as preservation of quality. Thus the next conclusion is right: the accepted conditions of grain storage in a granary leads to inadmissible damages. For prevention such danger scenario the following basic requirements (Machikhina et al. (2007)) should be performed: a smell unusual for grain should not be felt; isolation from dampness and from penetration of subsoil waters should be provided; grain-elevator should not have unfixed vertical and horizontal joints; doors should be densely closed, floors and walls should be smooth, without cracks, roofs – in a serviceable condition; fixtures should be protected by protective caps with grids; inlet of active ventilation should be densely closed preventing a penetration of an atmospheric precipitation, etc.

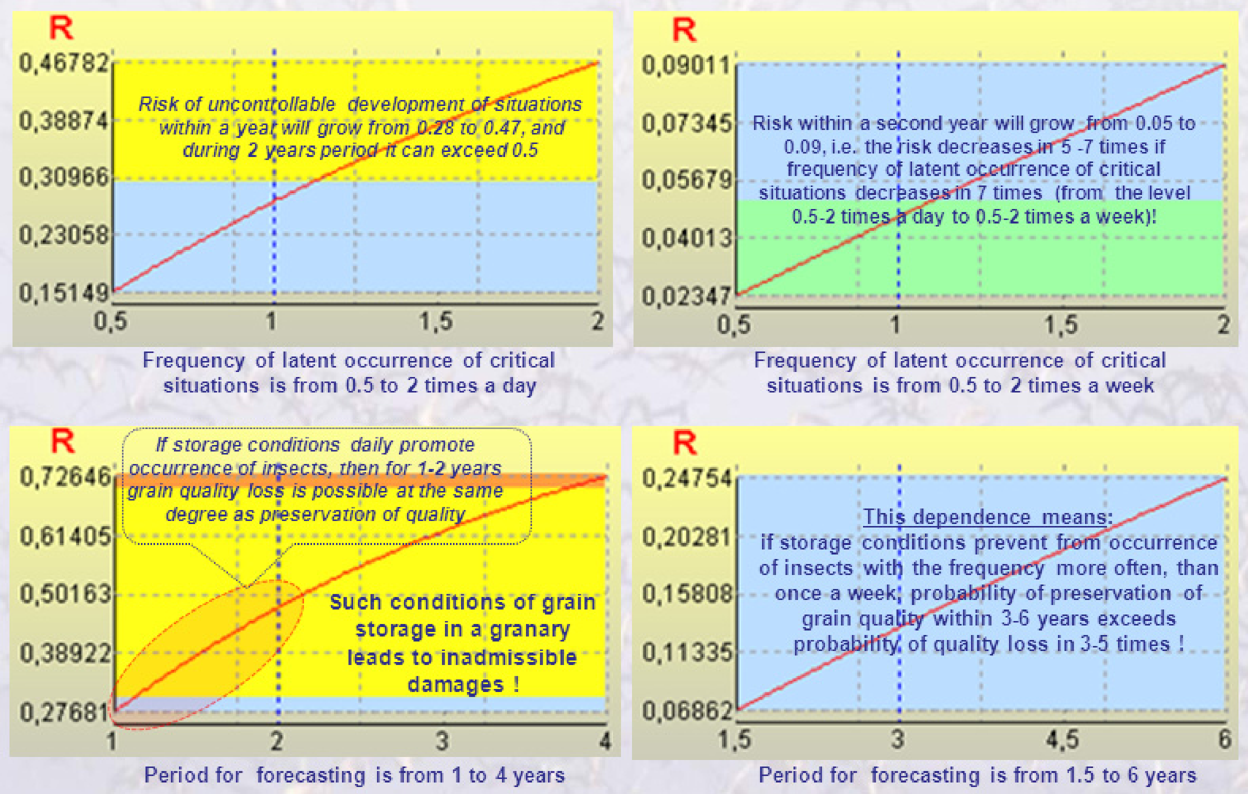


Figure 25. Some detail results of modelling and analysing

Performance of these requirements conducts to decrease a frequency of latent occurrence of critical situations in granaries. Further we will answer the question – what about a risk in conditions of more rare occurrences of critical situations? And, on the contrary, what the level of a frequency of latent occurrence of critical situations can be considered as admissible for granaries?

Results of modelling show: if frequency of latent occurrence of critical situations will be 1-2 times a week, risk of uncontrollable development of situations within a year will grow from

0.05 to 0.09, i.e. the risk decreases in 5-7 times! (against the level from 0.28 to 0.47), and within 6 years risk will make 0.25-0.43 (it is better, than risk within a year when frequency of latent occurrence of critical situations is 1-2 times a day!) – see Fig. 24 right. These results can be interpreted so: if storage conditions prevent from occurrence of insects with the frequency more often, than once a week, probability of preservation of grain quality within 3-6 years exceeds probability of quality loss in 3-5 times!

The results of modelling are quantitatively confirmed by results of long-term researches of the Russian Research Institute of Grain (Machikhina et al. (2007)). According to these researches experimental batches of grain wheat met to standard requirements of class grain has been kept within 6 years without deterioration in dry, cleared and the cooled condition. Moreover, the received values of risk can define admissible quality for grain storage. Indeed, new recommended result is: the acceptable risk of uncontrollable development of situations should not exceed 0.10 for 1 year and 0.25 for 6 years of grain storage.

Example 6 (Fire extinguishing). An automatic system of fire extinguishing for an enterprise of dangerous manufacture operates, as a rule, on following principles:

provision of multilevel protection, which highest level means a stop of all servers operation;

use of diagnostic results of devices and technological equipment.

The next measures are carried out for system availability to provide operation and fault tolerance: reservation of input for signals to acting; duplication of data transfer for switching-off equipment; consideration of switching-off only at the command of the safety officer (from the button); the voltage control in chains for executive mechanisms; implementation of intellectual devices with self-diagnostics; reservation of power supplies; reservation of safety control and emergency stop in conditions of failure of the basic system means.

To avoid false operation after detecting a fire-dangerous situation, the automatic system of fire extinguishing starts with delay 0,5 seconds. Control from the panel of the safety officer is blocked for the period of operating the automatic system of fire extinguishing. Duration of diagnostics with possible actions of fire-prevention protection is about 8.5 seconds. Control comes back to safety officer after end of automatic system act.

The solution is based on the use of the subsystem «Risk evaluation. Risk of uncontrollable development of situations» of the software tools “Complex for evaluating quality of production processes” (see model in subsection 3.9). But according to the 1-st idea of subsection 4.1 instead of metric “Risk of uncontrollable development of situations” we use metric “Risk of occurrence an emergency”. Analysis of real situations allowed to form approximately the next input for modelling: frequency of occurrence of a danger source = 1 time a day, activation time of a danger source = 1 minute, the period between integrity diagnostics = 0.5c, duration of diagnostics with performance of actions of fire-prevention protection = 8.5c, MTBF for system = 2000 hours (it is commensurable with MTBF for complex technical systems and also with the period between maintenance service). Mean time to system recovery is about 1 hour.

Results of modelling show the next (see Figure 26). At the expense of automatic monitoring and fire-prevention protection the risk of occurrence an emergency within a year equals to 0. 065, and within 2th years is nearby 0.125. The mean time between possible emergencies will be about 131590 hours (this does not mean, that such successful system operation time is peculiar to the equipment. This figure characterizes effectiveness of the whole technology of the control, monitoring and integrity recovery in the given conditions of threats).

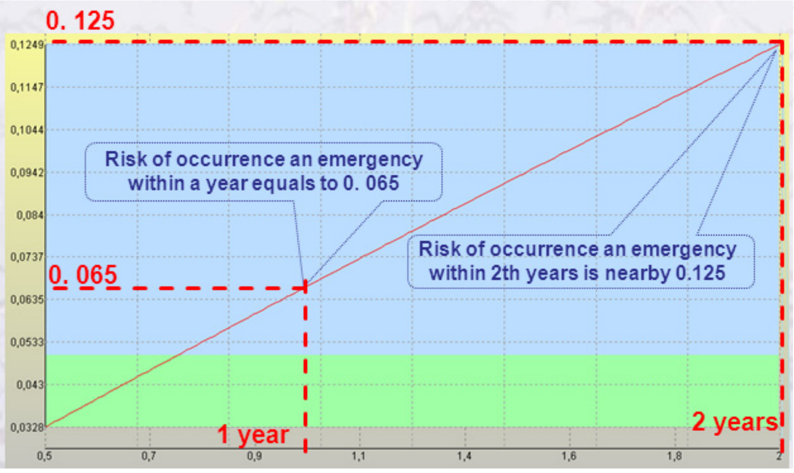


Figure 26. Dependence of risk from the forecasting period

As modern automatic systems of fire extinguishing are an example an effective utilization of information technologies implemented into various industrial systems, the reached level of risk (not above 0.065 within a year) can be de facto recognized as admissible according to "precedent" principle. At the same time, the risk of occurrence an emergency within 3th years will already exceed 0.6. This means, that at daily threats of a fire within the next 3-5 years at least one potentially emergency will be real. And moreover it can't be prevented by the operating automatic system. Here the additional measures of fire-prevention protection (including forces from the state fire service) should be provided.

Example 7 (Reliability of engineering equipment for enterprise objects). Prediction of operation reliability of computer-aided engineering equipment against usual non-automated engineering equipment is needed for the stages "Concept" and "Development" within quality management. Let the estimated object (for instance, the center of information processing and storage) includes power supply subsystem, an air conditioning subsystem, supported by 2 sources of an uninterrupted supply and a server, supported by 1 source of an uninterrupted supply and disks for information storage, supported also by 2 sources of an uninterrupted supply. In turn, the power supply subsystem includes the switchboards, supporting by 2 sources of an uninterrupted supply. All listed above engineering equipment is supported by 2 engine-generating installations.

The solution is based on the use of the subsystem «Prediction of integral quality» of the software tools "Complex for evaluating quality of production processes" (see combination of models from subsections 3.2 and 3.9 according to proposition of subsection 4.1). Within the example two subsystems are allocated (see Figure 27): a subsystem 1 – the city power supply formalized as basic and reserve subsystems; a subsystem 2 – an object fragment.

It is supposed, that operation reliability of the object is provided, if "AND" in 1st subsystem "AND" in 2nd subsystem there will be no power supply infringements during predicted term.

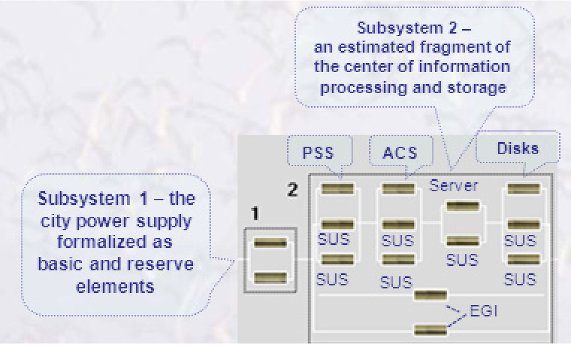

Subsystem 2 – an estimated fragment of the center of information processing and storage
PSS
ACS
Disks
Server
2
1
Subsystem 1 – the city power supply formalized as basic and reserve elements
SUS
SUS
SUS
SUS
SUS
SUS
SUS
EGI

Figure 27. Logic model of the object for modelling (PSS - power supply subsystem, ACS - air conditioning subsystem, SUS - source of an uninterrupted supply, EGI - engine-generating installation)

Results of modelling are reflected by Figure 28. The analysis shows, that, at estimated technology of the control, monitoring and integrity recovery the MTBF for computer-aided engineering equipment will equal to 42219 hours. The probability of reliable object operation within a year equals to 0.828. In turn, for usual non-automated engineering equipment (there is no the monitoring implemented for computer-aided engineering equipment) efficiency characterized by estimations on Figure 28 below.

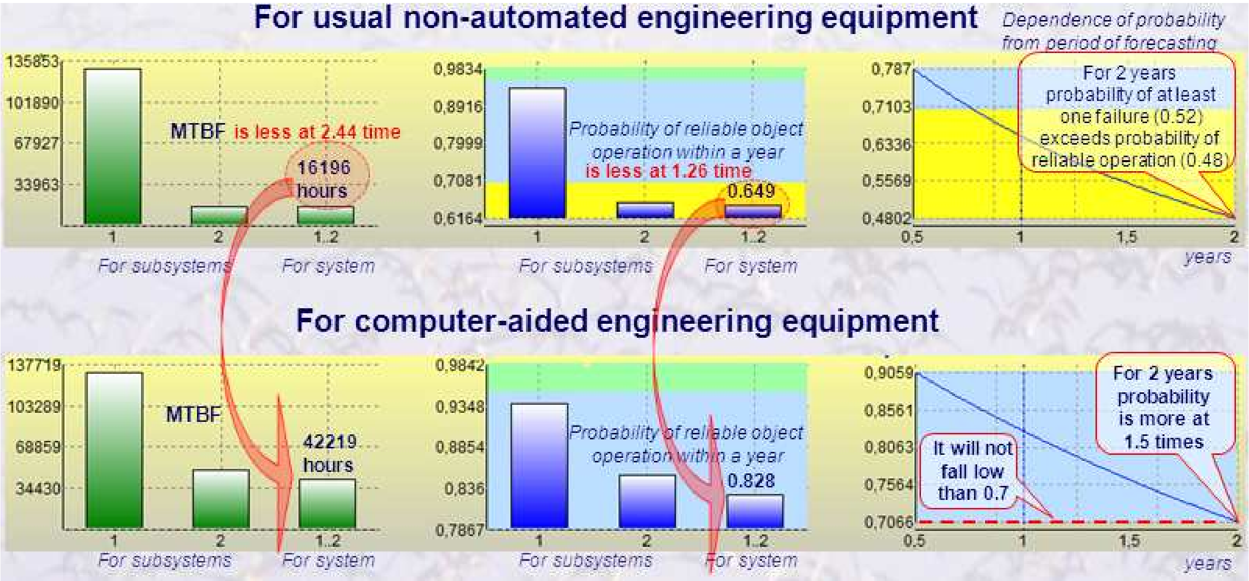


Figure 28. Results of modelling for example 7

For usual non-automated engineering equipment the MTBF will make 16196 hours (it is at 2.44 time less, than for computer-aided engineering equipment that uses monitoring), and the probability of reliable object operation within a year equals to 0.649 (at 1.26 time less, than for computer-aided engineering equipment). Moreover, without automation for 2 years the probability of at least one failure (0.52) exceeds probability of reliable operation (0.48). Against this the probability of reliable object operation within 2 years for computer-aided engineering equipment is more at 1.5 times and will not fall low than 0.7 .

Example 8 (Flights safety in conditions of terrorist threats). We understand that a system component of the global terrorism problems can't be fully studied within any monograph. Nevertheless, we'll offer an approach, which allows to estimate quantitatively and compare some organizational and technical ways of its solution within quality management (safety aspect). From the modelling point of view a flying airplane is a protected system operating in conditions of threats to its integrity during the flight. We'll try to answer the next questions: "How effective was the existing before 09/11 system of flights safety provision in Russia and the USA from the point of view of opposing to terrorists?" and "How this level of the safety may be increased and by what measures?"

The answers are based on the use of subsystems «Risk evaluation. Risk of uncontrollable development of situations» and «Risk evaluation. Efficiency of protection barriers» of the software tools "Complex for evaluating quality of production processes" (see models from subsections 3.9 and 3.10).

Note. The basic results of an example 8 have been received in a week after events of 09/11, and presented for working groups on system and software engineering WG7 and WG10 SC7 JTC1 ISO/IEC in Moscow in October 2001г.

For answering the first question "How effective was the existing before 09/11 system of flights safety provision?" comparative analysis is based on the use of subsystems «Risk evaluation. Risk of uncontrollable development of situations» and «Risk evaluation. Efficiency of protection barriers» of the software tools "Complex for evaluating quality of production processes" (see models from subsections 3.9 and 3.10).

To gather necessary input data for modelling let's recall pictures of the some acts of terrorism. One of these is a highjacking of the Russian airliner Tu-154 (the company "Vnukovo" airlines) on March 15, 2001. And it is a terrorist attack on the USA committed on September 11 with the help of several passenger airliners.

The passenger airliner Tu-154 was flying from Istanbul to Moscow with 162 passengers on board. Three terrorists armed with cold steel captured the airliner and threatening with a bomb blowing-up made the pilots fly to Medina (Saudi Arabia). All terrorist attempts to break open the door to the cockpit failed. The pilots not controlled by the terrorists explained the situation on board, terrorists' maneuvers, necessary details concerning the airliner arrangement before the start of a rescue operation. Moreover, they secretly communicated with stewardesses situated in the plane cabin. On March 16 Arabian troops of special purposes made an attempt to capture the airliner. A Russian stewardess, Julia Fomina, who was fatally wounded during that storm, opened a ramp. At the cost of her life she rescued lives of the passengers. From the moment of highjacking till the moment of capturing there passed about 24 hours.

In September an unprecedented attack was committed on the USA. That attack killed thousands of people. Two skyscrapers of the World Trade Center were rammed by two passenger airliners "Boeing-767" and "Boeing-757" (the company American Airlines), captured by terrorists on their flights from Boston to Los Angeles (92 people on board) and from Washington to Los Angeles (64 people on board). The Pentagon was attacked by " Boeing-76" (the company "United Airlines") flying from Newark (New Jersey) to San Francisco (45 people on board).

Now we go to modelling of unauthorized access to airliner resources. From the point of view of terrorists opposing formalization the existing system of security provision represents a sequence of technological barriers, which should be overcome. What are the barriers?

For the existing before 09/11 safety system it is: the 1st barrier is pass and inter-object modes in aerodromes and centers of air traffic control; the 2nd barrier is a preflight examination and control of passengers and their luggage during the registration; the 3rd barrier is a preflight examination before boarding; the 4th barrier is a lock-up door to the cockpit; the 5th barrier is an on-line warning about a highjacking (this barrier is critical if terrorists try to hide the fact of highjacking). It is clear that the first three barriers if a passenger behaves well are conditional because terrorists reveal their criminal nature only on board an aircraft. Moreover, the character of the last terrorism acts proves that among terrorists there are trained executors. The terrorist actions are worked out in details.

Taking the above considerations into account we'll form input data for modelling. At first we'll discuss time of barriers overcoming. For a trained terrorist (not "wanted", having valid documents and luggage) both in Russia and in the USA mean time of the 1st barrier overcoming equals to 10 minutes necessary for identification (m=1). For an untrained terrorist the main task is not to be taken into those who are checked by security service of the aerodrome. Let only 0.5% of passengers be checked. This check may result in imprisonment during 10 days. This means that mean time of a barrier overcoming equals to ≈ 1.36 hours.

To evaluate input characteristics of the 2nd and the 3rd barriers we'll analyze the existing facts and specialists' reports. On one hand prevention of guns and explosives carrying through customs in the USA seems to be rather reliable. From the other hand carrying of penknives with blade length up to 8 centimeters had been officially allowed before September 11. On September 11 the terrorists were armed with knives for cutting of thick carton ("cutters"). Moreover, American specialists in terrorism-fighting cite facts when in 2000 employees of the USA Department of Transport decided to check 8 American airports for their vigilance. They could carry bags with guns in 68 cases of 100 ones. Finally in several shops of airports there were sold knives-souvenirs, which are brought right to the airline ladder, i.e. without any control. In Russia the situation was not better. It was worsened by the fact that in some airports modern systems of electronic examination are not used. Let's assume that a fraction of such airports mounts to 30%. The above-mentioned allows to state that for a trained terrorist overcoming of the 2nd and 3rd barriers in the USA takes about 2 hours (for each barrier) and in Russia – 1 hour. The same actions will take an untrained terrorist 10 days appeared as a result of his/her imprisonment. Then in the USA mean time of a barrier overcoming equals to ≈ 3.3 days and in Russia it equals to ≈ 2.6 days. Mean time of pass and examination in the airport is not less than a year before any essential change happens (usually before a next serious incident and start of an appropriate fight for providing airports security). The authors of the monograph know about real control service on local airlines of the USA and Russia not through hearsay. Thus the input data necessary for computations concerning the first three barriers may be considered to be formed.

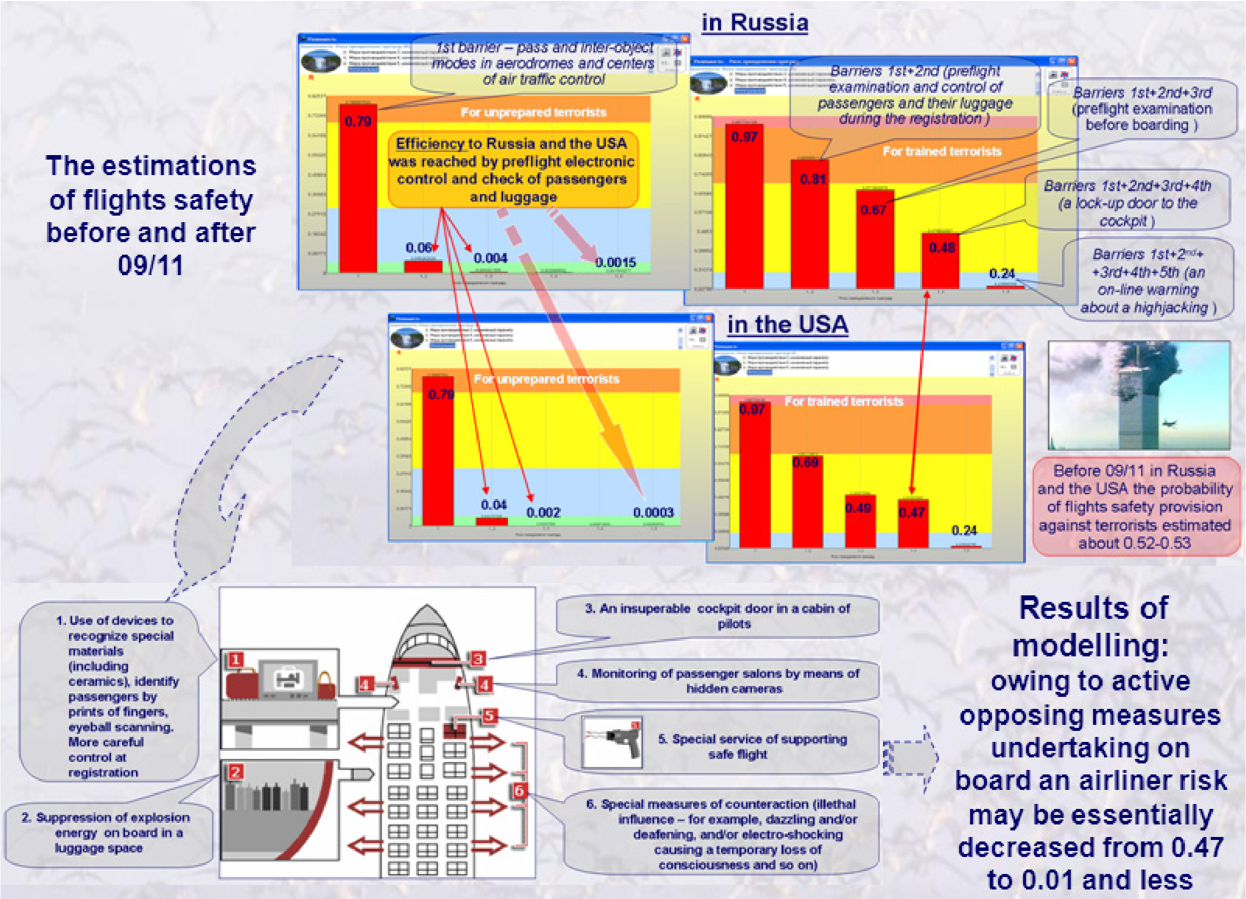
The 4th and 5th barriers are the only barriers on board an airliner. A cockpit door in American Airlines "Boeing" is usual. It can be broken within a few minutes. This was done to rescue pilots in case of a catastrophe. For the same purpose some airliners take off and land with open doors. To make it clear let's set mean time of the "Boeing" 4th barrier overcoming equal to 15 minutes. A door of a Russian airliner is armored. Impossibility of such a door breaking within a few hours allowed avoiding more grave consequences on March 15. Nonetheless, according to the specialists' opinion it is not a great difficulty to blow it up or open it with the help of a fire extinguishing ax or a forcer. Let's assume that using additional improvised means it takes not more than 2 hours to overcome this barrier.

Russian aircraft are furnished with a special button of reporting about a highjacking. Not all foreign airliners are furnished with such a button and terrorists may cut off the communication with the Earth. According to specialists it is possible to escape radars by reducing height to its critical point and sharp changing of an airliner's course. On Earth it is possible to guess that an airliner is high-jacked only on the basis of indirect signs: a disappeared communication, a change of course, strange maneuvers. Sometimes passengers may use mobile phones what happened on September 11 in the USA. So, let's set time of preventing a warning about the highjacking equal to flight time.

Results of modelling are on Figure 29. An analysis of computation results reveals the following:

- both in Russia and the USA the existing systems of flights safety provision are very effective against inexperienced or untrained terrorists (the probability of security provision is not less than 0.99). It is achieved owing to preflight electronic examination and control of passengers and their luggage;
- the probability of flights safety provision in Russia and in the USA consisting in preventing of trained terrorists' penetration into a cockpit is practically the same: it equals to 0.52-0.53. In case of on-line warning about a highjacking and owing to this warning a possibility of essential opposing to terrorists this probability increases to 0.76. In Russia an armored door is the essential obstacle and in the USA it is a modern electronic examination system. According to the computations both in Russia and the USA the probability of terrorist's goals achievement in case of a thorough preliminary training is unacceptably high.

The drawn frightening figures (0.52-0.53) mean that the time of "single terrorists" has passed. They may act only on local airlines of developing countries where are no means of electronic examination and control of passengers. The computations allow with a high degree of confidence to come to the conclusion that all the taken place terrorist acts were committed after their thorough preliminary planning and preparing.



The estimations of flights safety before and after 09/11

Efficiency to Russia and the USA was reached by preflight electronic control and check of passengers and luggage

Before 09/11 in Russia and the USA the probability of flights safety provision against terrorists estimated about 0.52-0.53

Results of modelling: owing to active opposing measures undertaking on board an airliner risk may be essentially decreased from 0.47 to 0.01 and less

in Russia
1st barrier – pass and inter-object modes in aerodromes and centers of air traffic control
For unprepared terrorists
0.79
0.06
0.004
0.0015
Barriers 1st+2nd (preflight examination and control of passengers and their luggage during the registration)
For trained terrorists
0.97
0.81
0.67
0.48
0.24
Barriers 1st+2nd+3rd (preflight examination before boarding)
Barriers 1st+2nd+3rd+4th (a lock-up door to the cockpit)
Barriers 1st+2nd+3rd+4th+5th (an on-line warning about a highjacking)
in the USA
For unprepared terrorists
0.79
0.04
0.002
0.0003
For trained terrorists
0.97
0.69
0.49
0.47
0.24
1. Use of devices to recognize special materials (including ceramics), identify passengers by prints of fingers, eyeball scanning. More careful control at registration
2. Suppression of explosion energy on board in a luggage space
3. An insuperable cockpit door in a cabin of pilots
4. Monitoring of passenger salons by means of hidden cameras
5. Special service of supporting safe flight
6. Special measures of counteraction (illethal influence – for example, dazzling and/or deafening, and/or electro-shocking causing a temporary loss of consciousness and so on)
1
2
3
4
4
5
6

Figure 29. Results of modeling for example 8

Conclusion: in Russia and the USA the existing before September 11 systems of flights safety were ineffective against planned actions of trained terrorists; the bottleneck of flights security provision system were a weak protection of a cockpit and absence of active opposing measures on board an airplane.

Let's answer the second question "How the level of the safety may be increased and by what measures?"

It is possible to think up a set of such measures, however ways of their application should be carefully proved depending on the scenario of terrorists actions. We will stop only on some of the measures that already are implemented at the various airports.

The 1st measure consists in using devices for recognition the special materials (including ceramics), in an identification of passengers by prints of fingers, in eyeball scanning, in using the general databases of prospective criminals, in restrictions on hand luggage. We will designate a measure 1 as 6th barrier in addition to considered above. We will put the mean time of keeping effectiveness of 1st measure equals to 1 year (i.e. for overcoming this barrier it should be spent about 1 year). As effective devices appear annually, we will estimate time before the next adequate strengthening of a measure in 1 year.

The measure 2 allows to suppress an energy of explosion on board in a luggage space. It is 7th barrier. We will put the mean time of keeping effectiveness of 2nd measure equals to 5 hours (i.e. some effect can be achieved on the average within 5 hours, commensurable in due course flight). As annually there are more effective remedies. Time before the next adequate strengthening of a measure also will be estimated in 1 year.

The measure 3 is an armour door in a cabin of pilots (or two doors, the second door opens only after the first one will be locked) - it is 8th barrier. The armour door should become the real barrier insuperable to terrorists during all flight. It is necessary to notice, that this measure will not secure the members of crew serving passengers. Thus unlike 4th barrier the mean time of keeping effectiveness of 3rd measure logically increases. We will put, that it is commensurable with duration of flight and equals to 5 hours.

The 4th measure consists in monitoring behind passenger salon by means of videocameras. As soon as the cabin of pilots becomes unapproachable it can be transformed into the situation center of safety of passenger salon. Thereby before pilots, and also the land officers the real picture of an events opens. They will have access to complete and valid information on board. We will consider a monitoring on board from the auxiliary point of view for other additional measures.

The measure 5 is a special service of flight. At the same time the boomerang effect is possible - terrorists can detonate an explosive after having encountered resistance from special service. And if terrorists can disarm a specialist of special service, they will have an additional weapon. It is 9th barrier. We will put the mean time of keeping effectiveness of 5th measure equals to 1 hour (i.e. a specialist of special service can be detected in average for 1 hour and an effect of it is not clear). The period between strengthenings of special services we will estimate in 5 years.

The measure 6 is formed from special measures of counteraction (temporary depressurization of salon, not lethal influence). Really it is 10th barrier. For the explanatory of this measure we will consider some scenario reasons:

a. as counter-attracting maneuver at average altitude the salon can be temporarily depressurized for a disorientation of terrorists and granting of the initiative to crew and special service of flight (that at a low altitude this measure may be inefficient, and at a high altitude it will quickly lead to irreparable consequences);
b. terrorists are obliged to be active, for this purpose those from them which have found out itself obviously, are in standing position, passengers – in sedentary. The first problem of protection is to destroy these subjects of threats at least for some minutes. And means of not lethal influence should be used because of passengers can also be influenced simultaneously. Then 6th measure is capability of using means of dot not lethal influence on the revealed terrorists. It may be influences by lulling gas and-or short-term shocking influences (for instance, blinding and-or deafening and-or the influences of electroshock type leading to a temporary loss of consciousness). The ways of influence should be a little, because against one way a simple counteraction can be

found (against gas – a gas mask, against blinding – goggles and so on). Thereby some revealed terrorists can be practically neutralized.

As at salon there can be the accomplices capable to recapture after additional preparation, methods of compulsory keeping of suspicious passengers on the places before emergency landing should be made. It is one of versions within the limits of 6th measure (which can be used by the individual lulling influence and-or jammed fastening, etc. Considering possible variants, we will put, that the mean time of keeping effectiveness of 6th measure equals to 5 hours (commensurable in due course flight). The period between strengthenings of 6th measure we will estimate at 2 hours taking into account various possible variants.

All listed measures seem at first sight rather impressive, but how much they are effective? Really, their effectiveness should be proved quantitatively! This is a very complicated task. It is impossible to make natural experiments. We may only use mathematical models.

Analysis of results has shown, that after implementation of the described measures the integrated risk to lose complex safety of flight during 5 hours of flight against terrorist threats is equal to 0.000004. And if duration of threats will be increased to 5 days the risk raises from 0.000004 to 0.002. The last can be commented by the next interpretation: safety will be achieved in 998 cases from thousand hypothetical terrorist attacks. Even taking into account an essential error of initial scenarios and preconditions it is an obvious indicator of high efficiency of additional safety measures according to "precedent" principle! Still it is not a victory. It is clear that the first failures will make terrorists to analyze their causes and find new bottlenecks of the safety system thus continuing the counteraction. This counteraction will be ended when there are taken proactive measures which effectiveness is based on modelling.

Example 9 (Information security). In quality management measures of protection of valuable resources from an unauthorized access (UAA) should be provided. The most important for any enterprise are information and software resources of an IS. We will consider the approach to an estimation of IS security against 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 models not included in the monograph). It is required to estimate IS protection against UAA.

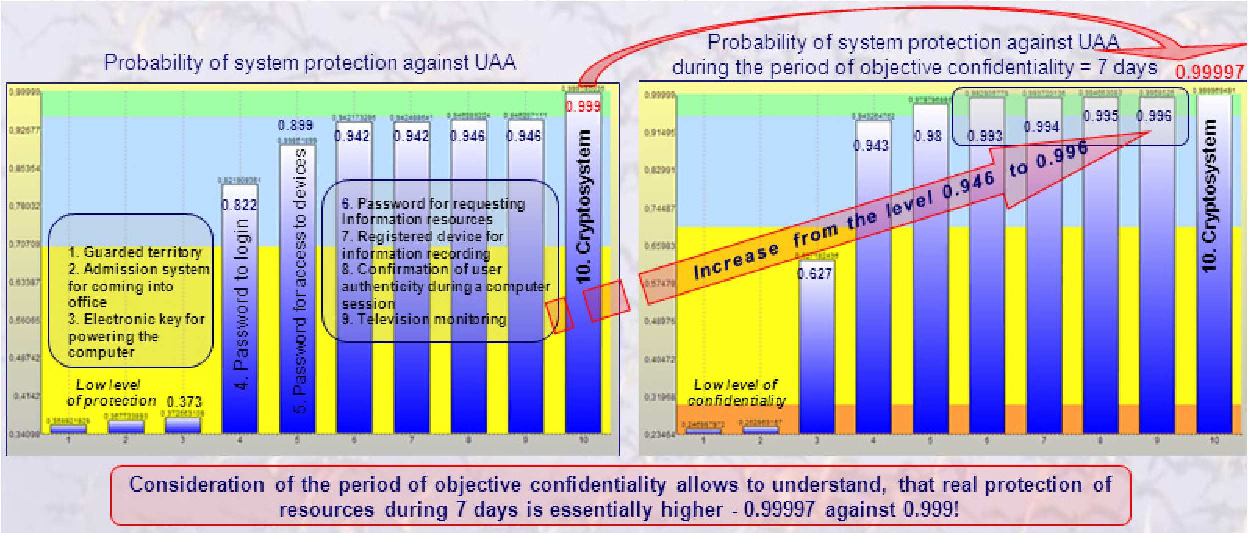
Solution. We'll try to answer this question by the subsystems "Protection from unauthorized access" and "Confidentiality" of CEISOQ+. The analysis of computed dependencies (see Figure 30 left) shows the next. The barriers 1,2,3 will be overcome with the probability equal to 0.63. However, monthly password changing for barriers 4, 5, 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 7,8,9 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 quality and safety for processes from examples above. But according to "precedent" principle this level of protection can't be recommended as high customer requirements for every cases.

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 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

Table 2. Input for modelling

Let's look on example condition more widely. The violator is interested in a certain IS resources during a certain period of time. This period is called the period of objective confidentiality. Unlike UAA information confidentiality should be provided within these lasting 7 days. Fig. 30 (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 from UAA by the 9 barriers (0.946 – see Fig. 30 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!



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 30. Comparison of protection levels

Example 10 (Forecasts of risks for complex multipurpose system). Let's consider a hypothetic multipurpose system which formally composed from functional system (similar, for instance, to commerce system, enterprise non-destroying control system or system of foods preservation from examples 2, 4, 5), gathering and data processing systems (similar to SCADA system from example 3), system of fire extinguishing (from example 6), system of engineering equipment for enterprise object (from example 7), information security system (from example 9). «The human factor» is considered in the parameters of control, monitoring and integrity recovery measures for corresponding elements. It is supposed, that a required integrity of system is not lost, if during given time a required integrity is not lost by all subsystems: "And" by 1st subsystem, "And" by 2nd subsystem, … "And" by the last 6th subsystem (the logic illustrated by Fig. 12). It is required to estimate the measures of risk management, including the periodic control and, where it is possible, continuous monitoring of integrity of each components – see Figure 31.

The input for subsystem 1-6 is described in examples 2-7, 9. The general results of complex forecasting of risk are reflected by Figure 32. Analysis of results shows, that with using of measures of the periodic control and where it is possible, monitoring of elements operation, the integrated risk to lose integrity of system during operational 1 – 4 years is changing from 0.11 to 0.67.

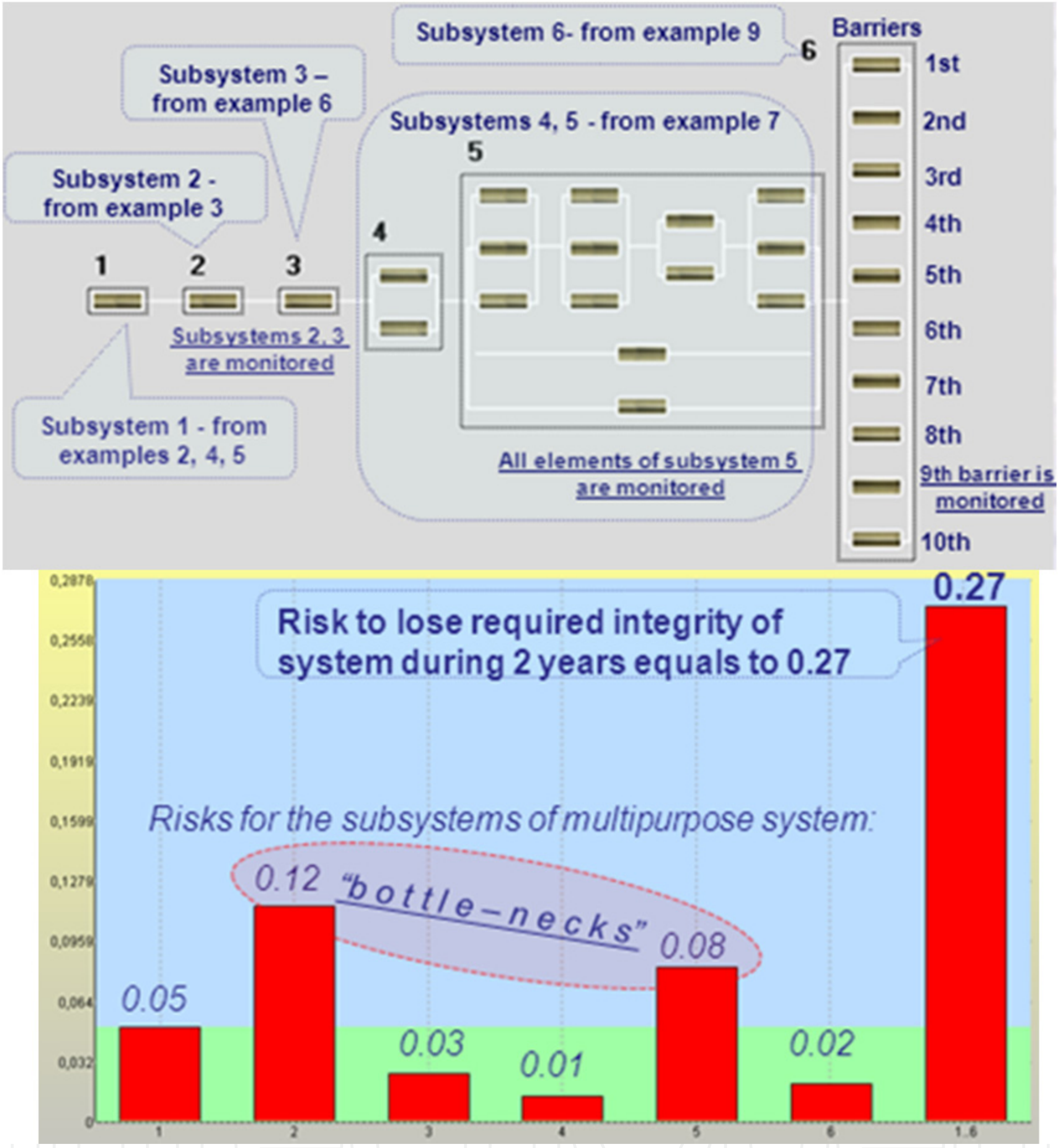

Subsystem 6- from example 9
6
Barriers
1st
2nd
3rd
4th
5th
6th
7th
8th
9th barrier is monitored
10th
Subsystem 3 – from example 6
Subsystems 4, 5 - from example 7
5
Subsystem 2 - from example 3
4
1
2
3
Subsystems 2, 3 are monitored
Subsystem 1 - from examples 2, 4, 5
All elements of subsystem 5 are monitored
0,2878
0,2558
0,2239
0,1919
0,1599
0,1279
0,0959
0,064
0,032
0
0.27
Risk to lose required integrity of system during 2 years equals to 0.27
Risks for the subsystems of multipurpose system:
0.12
"bottle-necks"
0.08
0.05
0.03
0.01
0.02
1
2
3
4
5
6
1..6

Figure 31. The formal scheme of multipurpose system for a complex risks evaluation

The general logic proposition is right for a given period of forecasting: as a rule, the risk to lose system integrity increases in depending on increasing time period. But there are the features demanding a logic explanation. Serrated and nonmonotonic character of dependence on Figure 32 is explained by the periodic diagnostics of elements, monitoring presence or absence and their quantitative values. Let's remind: for every monitored element a penetration of a danger source and its activation is possible only if an operator-monitor 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. Immediately after element diagnostic the risk decreases because during diagnostic all dangers are detected and neutralized and at the beginning of a period after diagnostic dangerous influences don't have enough time to accumulate and be activated. Nonetheless, there is a lack of protection accumulated for the previous full periods that's why the risk doesn't decrease to 0 for every element. By the middle of a period between neighboring diagnostics there is an increase of the calculated risk because new danger sources can begin to influence. Moreover, for the longer period of forecasting monitoring possibilities are weaken, thereby the moment of operator error comes nearer. And, if on timeline the following diagnostic does not come yet, risk increases. Similar effects paradoxes are explained – for example, that risk to lose integrity during 2.96 years (0.58) is more, than risk during more long time - 3.12 years, 58 days longer (0.57). One more effect of modelling: if to do forecasting not for 2.04 years, and for 2 weeks longer (2.08 years, i.e. 2% longer period) the expected risk to lose system integrity increases from 0.28 to 0.36. This is higher on 28 %! These results of modelling should serve as a substantiation for development of predicting counter-measures.

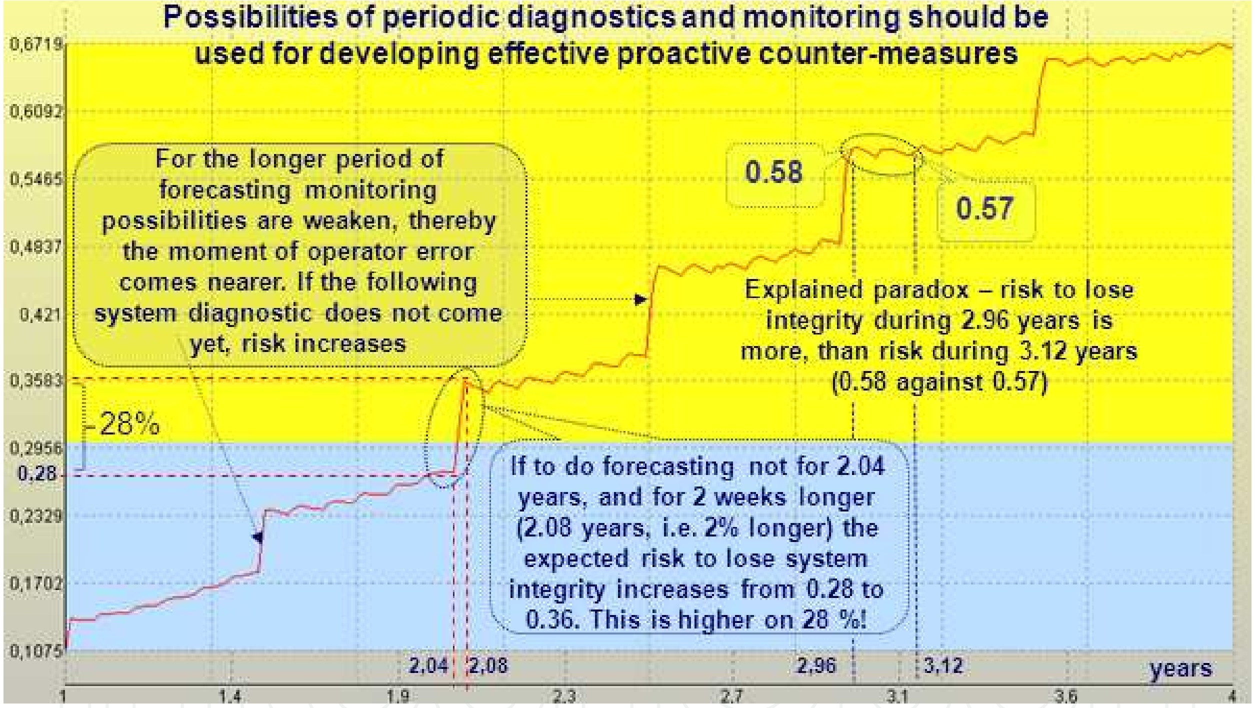


Figure 32. Integrated risk to lose integrity of system during operational 1 – 4 years

Indeed, on the basis of a rational choice of parametres for technologies of the control, monitoring and integrity recovery an optimization of processes offered in work is possible.

6. Conclusion

Rational management means wide use of existing models and software tools for decision-making in life cycle of systems. The criteria used for rational management are maximization of a prize (profit, a degree of quality or safety, etc.) at limits on expenses or minimization of expenses at limits on a comprehensible degree of quality and-or safety or their combination.

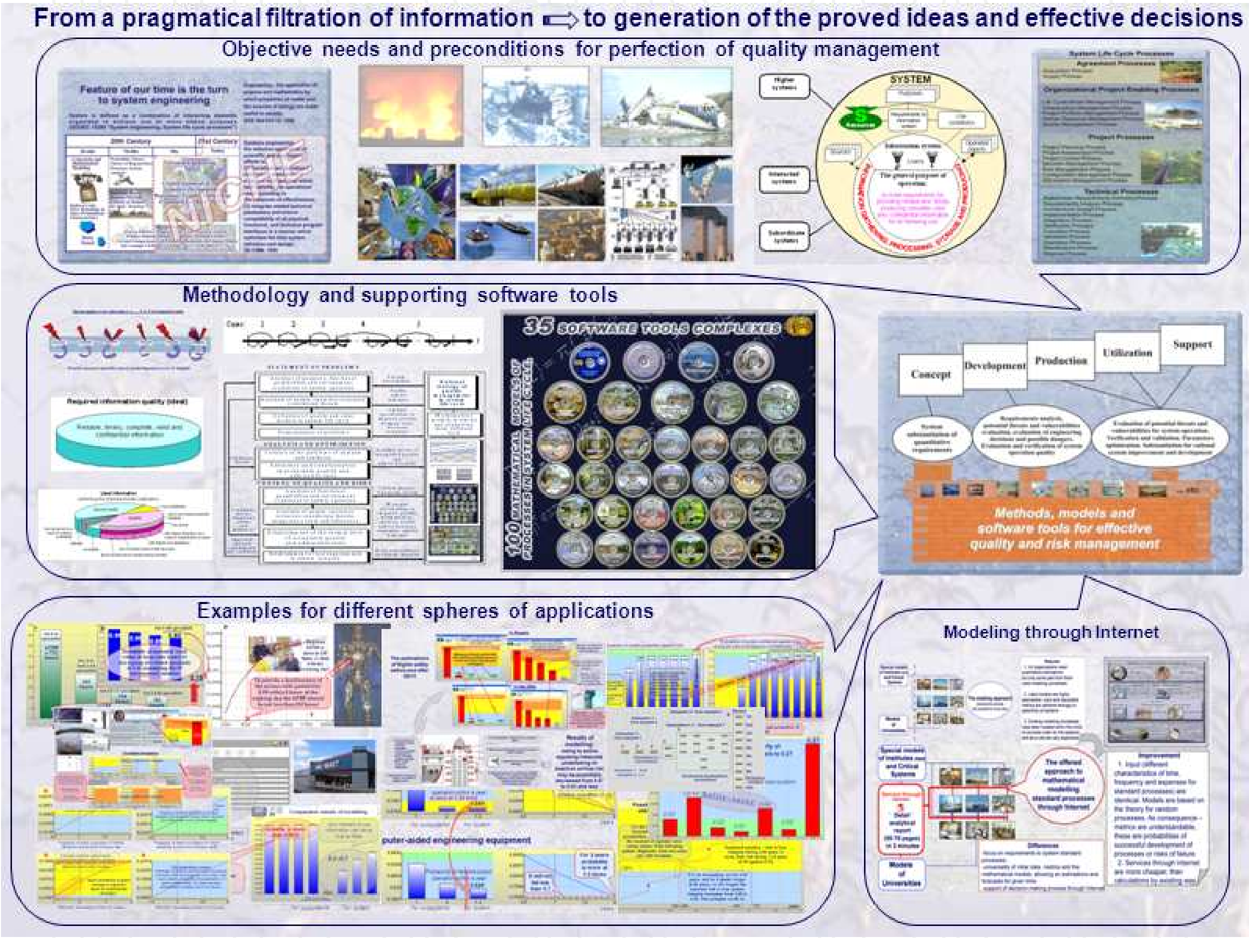

From a pragmatical filtration of information ⟹ to generation of the proved ideas and effective decisions
Objective needs and preconditions for perfection of quality management
Feature of our time is the turn to system engineering
20th Century
21st Century
Niche
Higher systems
Interacted systems
Subordinate systems
SYSTEM
System Life Cycle Processes
Agreement Processes
Organizational Project-Enabling Processes
Project Processes
Technical Processes
Methodology and supporting software tools
Required information quality (ideal)
35 SOFTWARE TOOLS COMPLEXES
100 MATHEMATICAL MODELS OF PROCESSES IN SYSTEM LIFE CYCLE
Concept
Development
Production
Utilization
Support
Methods, models and software tools for effective quality and risk management
Examples for different spheres of applications
puter-aided engineering equipment
Modeling through Internet
Models of Universities
Improvement

Figure 33. The proposed results helps to answer the questions «What rational measures should lead to estimated effect without waste expenses, when, by which controllable and uncontrollable conditions and costs?»

As a result of adequate modelling more deep and extend knowledge of system allows the customer to formulate well-reasoned system requirements. And it is rational to developer to execute them without excessive expenses of resources, and to the user – as much as possible effectively to implement in practice the incorporated power of system.The presented models, methods and software tools, allowing to forecast quality and risks according to system requirements of standards, are real levers to analyze and optimize system processes and improve quality management. The investigated practical examples demonstrated their functionality and possibilities to use "precedent principle» for definition the justified levels of acceptable quality and admissible risks. For complex systems the proposed results helps to answer the questions «What rational measures should lead to estimated effect without waste expenses, when, by which controllable and uncontrollable conditions and costs?» and allows to go «from a pragmatical filtration of information to generation of the proved ideas and effective decisions» (see Figure 33). The effect from implementation in system life cycle is commensurable with expenses for system creation.

Author details

Andrey Kostogryzov, George Nistratov and Andrey Nistratov
Research Institute of Applied Mathematics and Certification, Moscow,
Institute of Informatics Problems of the Russian Academy of Sciences, Moscow,
Russia

7. References

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

Gnedenko B.V. (1973) et al. *Priority queueing systems*, MSU, Moscow, 448p., 1973.

Klimov G.P. (1983) *Probability theory and mathematical statistics*. MSU, Moscow, 328p., 1983.

Martin J. (1972) *System Analysis for Data Transmission*. V. II, IBM System Research Institute. Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1972.

Kleinrock L. (1976), *Queueing systems*, V.2: Computer applications, John Wiley & Sons, New York, 1976.

Matweev V.F. & Ushakov V.G. (1984) *Queuing systems*. MSU, Moscow, 242p.,1984

Kostogryzov A.I., Petuhov A.V. and Scherbina A.M. (1994): *Foundations of evaluation, providing and increasing output information quality for automatized system*. Moscow: “Armament. Policy. Conversion”, Moscow, 278p., 1994

Kostogryzov A.I. (2000) 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*, USA, Dallas, 2000, pp.63 -70.

Bezkorovainy M.M., Kostogryzov A.I. and Lvov V.M. *Modelling Software Complex for Evaluation of Information Systems Operation Quality CEISOQ. 150 problems of analysis and* *synthesis and examples for their solutions.* Moscow: Armament.Policy.Conversion, 2001 (2-nd edition-2002), 303p., ISBN 5-89370-015-5

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

Grigolionis V. About approximating stepped processes sum to Poisson processes. *Probability theory and its applications*, V.8, 1963, №2.

Kostogryzov A.I. (1987), Conditions for Efficient Batch Job Processing of Customers in Priority-Driven Computing Systems Where the Queueing Time Is Constrauned, «*Avtomatika i telemehanika*». 1987. №12. P.158-164.

Kostogryzov A.I. (1992), Study of the Efficiency of Combinations of Different Disciplines of the Priority Service of Calls in the Computer Systems, *«Kibernetika i sistemny analiz»*. 1992. №1. P. 128-137.

Kostogryzov A., Nistratov G. *Standardization, mathematical modelling, rational management and certification in the field of system and software engineering" (80 standards, 100 mathematical models, 35 software tools, more than 50 practical examples)*. Moscow: Armament.Policy.Conversion, 2004 (2-nd edition – 2005, in Russian), 393p., ISBN 5-902313-05-8.

Kostogryzov A.I., Nistratov G.A. 100 Mathematical Models of System Processes According International Standards Requirements. *Transaction of the XXV International Seminar on Stability Problems for the Stochastic Models*. Maiority, Italy, September 20-24,2005, University of Solerno, Italy p. 196-201

Kostogryzov A., Nistratov G., Kleshchev N. Mathematical Models and Software Tools to Support an Assessment of Standard System Processes. *Proceedings of the 6th International SPICE Conference on Process Assessment and Improvement (SPICE-2006)*, Luxembourg, 2006, p. 63-68

Kostogryzov A., Nistratov G. Mathematical Models and Software Tools for Analyzing System Quality and Risks according to standard requirements. *Proceedings of the 6th International scientific school "Modelling and Analysis of safety and risk in complex systems" (MASR – 2006)*, SAINT-PETERSBURG, RUSSIA, July 4 - 8, 2006

Kostogryzov A.I., Stepanov P.V. *Innovative management of quality and risks in systems life cycle.* Moscow: “Armament. Policy. Conversion”, 2008, 404 p., ISBN 5-89370-012-0

Grigoriev L.I., Kershenbaum V.Ya. and Kostogryzov A.I. *System foundations of the management of competitiveness in oil and gas complex*. Moscow: National Institute of oil and gas, 2010, 374p., ISBN 5-93157-086-1.

Kostogryzov A. et al.Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, *Proceedings of the 1st International Conference on Transportation Information and (SafetyICTIS 2011)* June 30th ~July 2nd 2011, Wuhan, China, p. 845-854

Machikhina L.I., Alexeeva L.V., L'vova L.S. *Scientific foundations of food grain safety during storage and processing* Moscow, DeLi print, 2007, 382p., ISBN 978-5-94343-140-1.