V. Kosenko, I. Nevliudov

RISK-ADAPTED MANAGEMENT OF DATA FLOW PARAMETERS OF INFOCOMMUNICATION NETWORKS IN CRITICAL INFRASTRUCTURE SYSTEMS

Monograph

ISMA University of Applied Science

Riga (Latvia) 2020

V. Kosenko, I. Nevliudov

INFORMĀCIJAS KOMUNIKĀCIJU TĪKLU DATU PLŪSMAS PARAMETRU RISKA ADAPTĪVA KONTROLE KRITISKĀS INFRASTRUKTŪRAS SISTĒMĀS

Monogrāfija

Informācijas sistēmu menedžmenta augstskola

Rīga (Latvija) 2020

ISBN 978-9984-891-14-9
UDC 004.94+519.673

Approved at the meeting of the Scientific and Technical Council of Kharkiv National University of Radio Electronics April 3, 2020 (protocol No. 4) as a monograph.

Reviewers:
Oleg Fedorovich - Dr. Sc. (Engineering), Laureate of the State Prize of Ukraine in the field of science and technology, Head of the Department of Computer Science and Information Technologies of the National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
Volodymyr Timofeyev - Dr. Sc. (Engineering), Professor of the Department of Automation and Computer Integrated Technologies of the Kharkiv Beketov National University of Urban Economy, Kharkiv, Ukraine
Viktors Gopejenko – Dr. Sc. (Engineering), Professor of the Department of Computer Technologies and Natural Sciences, ISMA University of Applied Sciences, Riga, Latvia,

Risk-adapted management of data flow parameters of infocommunication networks in critical infrastructure systems: monogr. / V. Kosenko, I. Nevliudov. – Riga : ISMA, 2020. – 180 p.

Authors: V. Kosenko, I. Nevliudov

The monograph deals with the problems of adaptive control of data flow parameters to ensure the requirements for promptness and exchange of high-risk information in critical communications infrastructure networks. The method of adaptive management of the distribution of information flows allows to consider for different types of communication channels the possible change of requirements of application tasks or user activity and solves the optimization problem of reducing the total data transmission costs. A method based on causal analysis theory is used to determine the category of critical infrastructure in the risk scale. The description of information technology of risk-adaptive data flow management of the infocommunication network is given..

Recommended for students, masters, post-graduate students, and academics of a wide range of specialities related to data flow management of data communications networks to meet the requirements for promptness and exchange of information at high risk.

ISBN 978-9984-891-14-9
UDC 004.94+519.673

CONTENT

INTRODUCTION

A new qualitative leap in the field of critical infrastructure systems (CIS) management is due to the following factors: updating of technical equipment, expanding the territorial scope, increasing the dynamics of performing functional tasks, changing their nature and content, and the emergence of new technological ways of functioning. To ensure information exchange, a unified information and communication network is being created during the operation of the CIS, while the communication and automation systems are gradually switching to modern digital methods of transmitting and processing information, as well as automation of management processes.

Critical infrastructure systems are characterized by high intensity of information flows in the management process, and the requirements for the efficiency of management, timely adoption and delivery to the executors of decisions and tasks are constantly increasing. Fulfillment of these requirements is inextricably linked with the need to generalize the already accumulated world experience in the field of infocommunication and depends on the degree of implementation of advanced information technologies related to the transmission and processing of information.

New technologies, such as NGN and MPLS, make it possible to create efficient, reliable and secure networks of any size. However, in a real infocommunication network (ICN) to provide the required response time is quite difficult due to the high intensity and diversity of data flows, the need to search for data in repositories and large databases, complex interaction of distributed applications, low line speed, slowing down interactions in gateways that coordinate inhomogeneous components of different ICN subnets. This is due to the need to take into account the specifics of the system, which requires appropriate settings of the network and methods of managing its operation. Thus, there is a growing gap between the growing universal capabilities of management systems and the real needs of management, focused on specific applications.

Further development of ICN construction methods requires the development and implementation of adaptive management methods that ensure high efficiency of network resources by taking into account the characteristics of the real data flow.

The first section of the monograph analyzes the existing problems in the field of formation and management of ICN. The necessity of creating mathematical models, technologies and solutions to support network resources at the level necessary to ensure the functioning of the CIS is substantiated. A review of existing models and methods of ICN analysis and management is conducted.

The second section considers a mathematical model of the network management task, which according to the stratified structure of the network is represented on two levels. The set of basic parameters that define the network structure and the set of parameters of operational management are determined. A formalized model for the subnet layer provides coordination of goals between levels. A method of adaptive control of information flow distribution is presented, which allows to take into account for different types of communication channels a possible change in the requirements of application tasks or user activity and solves the optimization task of reducing total data transmission costs. Also discussed is a method of allocating network resources for a multi-server node, in which server systems are considered as a set of single-line queuing systems.

The third section of the monograph focuses on the components of information risk. Taking into account the relationships between risk categories, the structure of the systemic risk model is formed, which reflects the negative consequences that affect the main characteristics of the network. The method of identification and risk assessment of ICN, which identifies partial risks using cognitive maps and cause-and-effect diagram, is considered. To estimate the probabilities of partial risks due to traffic transmission difficulties, methods of modeling random processes are used.

The fourth section discusses risk management techniques for improving the security of critical infrastructure systems. Technologies for improving the func-

tional safety of ICN are described, which ensure the viability of distributed CIS. It is offered to use methods of reduction of internal risks of the equipment of knots and communication channels of PCM, namely - diagnostic algorithms for definition of a technical condition of objects. To reduce the risk of errors in ICN communication channels, an adaptive procedure for calculating linear decision functions is proposed.

The fifth section presents information technology that uses general mathematical models and methods to calculate the parameters of data flows and network performance characteristics in the practical implementation of methods and principles of network management. Technology determines the sequence and composition of decisions and actions in solving tasks of setting up and operational network management.

The sixth section contains the results of practical testing of information technology for the analysis of ICN "Complex for the processing of solid waste with a system of collection, disposal of landfill gas and electricity production." One of the subsystems of the complex is the software and hardware complex of the upper level and general station systems, which is designed to control the technological processes of general station and auxiliary systems and belongs to the class of ACS TP. To implement the functions of the complex uses a heterogeneous multiservice infocommunication network. The directions and volumes of information flows within the basic ICN are investigated. As part of the risk management task, the levels of significance of factors and the probability of possible consequences are calculated. You are the most vulnerable characteristics of the network (performance and reliability) and planned measures to fend off partial risks. Experimental application of models and methods of control of ICN parameters has shown that at their use efficiency of information transfer in infocommunication networks of ACS TP increases.

1 ANALYSIS OF PROBLEMS AND METHODS OF MANAGING INFOCOMMUNICATION NETWORKS IN CRITICAL INFRASTRUCTURE SYSTEMS

1.1 Features of critical infrastructure systems and their information support

Critical infrastructure is a set of state infrastructure facilities that are most important for the economy and industry, the functioning of society and public safety [1, 2]. *Objects of critical infrastructure* are enterprises and institutions of such industries as energy, chemical industry, transport, banks and finance, information technology and telecommunications (electronic communications), food, health care, utilities, which is strategically important for the functioning of the economy and security of the state, society and population [3, 4].

These facilities are vulnerable to the negative impact of the external information environment, the negative consequences of security breaches of critical infrastructure systems (CIS) are [5]:

- the emergence of a man-made emergency and / or a negative impact on the environmental security of the state (region);
- negative impact on the state of energy security of the state (region);
- negative impact on the state of economic security of the state;
- negative impact on the state of defense, national security and law and order in the country;
- negative impact on the system of government;
- negative impact on the socio-political situation in the country;
- negative impact on the image of the state;
- violation of the sustainable functioning of the financial system of the state;

- violation of the sustainable functioning of the transport infrastructure of the state (region);

- violation of the sustainable functioning of the information and/or telecommunication infrastructure of the state (region), including its interaction with the relevant infrastructures of other states.

The introduction of a systematic approach to solving the problems of critical infrastructure protection requires an effective mechanism for coordinating efforts to prevent loss or irreparable damage to key elements of critical infrastructure due to negative factors of any origin: man-made, natural, social political or any combination thereof.

The National Security Strategy calls one of the ways to strengthen energy security "effective protection of critical infrastructure of the fuel and energy complex from environmental and man-made influences and malicious actions", and one of the ways to ensure information security is to ensure the security of information and telecommunications systems. acting in the interests of state management, provide the needs of defense and security of the state, credit and banking and other spheres of the economy, management systems of critical infrastructure " [6].

Critical infrastructure systems are a set of technical means of collecting, transmitting, storing, processing, displaying, documenting and reproducing information together with information, software and organizational software, and contain regular service changes, which are located at the appropriate control points (in governing bodies) in order to optimize managemen*nt* [7].

There is also the term "critical IT infrastructure", which on the one hand, creates opportunities to improve the security of facilities, on the other - new technologies bring additional security gaps. According to the Law of Ukraine "On the National System of Confidential Communication" there is a set of special telecommunication systems (networks) of dual purpose, which with the help of cryptographic and / or technical means provide exchange of confidential information in the interests of public authorities and local governments, create appropriate condi-

tions for their interaction in peacetime and in the event of a state of emergency or martial law [8].

Infocommunication Network is a set of geographically distributed information, computing resources, software management systems, located in the end systems of the network and user terminal systems, the interaction between which is provided by telecommunications, and which together form a single multiservice platfor*m*.

Critically important is the information processed in the CIS, namely information about the state of a critical object, information about its structure, characteristics of software and hardware, location, communication, etc. [9].

The infocommunication network, which implements information support as a critical object, is considered a key system of information infrastructure. That is why there is a question of improving the efficiency of infocommunication networks (ICN).

Territorial distribution of elements of CIS causes strict requirements to efficiency of acceptance of administrative decisions on maintenance of safety of its functioning. [9].

One of the most significant factors in reducing the effectiveness of CIS is the threat of information security breaches. The decision of this task should be carried out systematically, on the basis of comprehensive research of both information processes realized in SKI, and mechanisms of realization of threats of their information security and technologies of information protection. One of the most essential factors of decrease in efficiency of CIS is threats of information security breach. The solution of this task should be carried out systematically, on the basis of a comprehensive study of both the information processes implemented in the SKI, and mechanisms for implementing threats to their information security and information security technologies. [10].

In modern conditions, a high level of information support becomes a determining factor in achieving the goals of critical infrastructure systems, which im-

pose additional special requirements for the means of processing and transmission of information.

An important direction in the development of information support is to provide large-scale management of CIS in all functional modules and the creation of tools that allow you to form a single picture of the situation on the basis of information from different sources. The implementation of this task should contribute to the effective organization, timely planning and coordination of the control system and functional subsystems, providing timely feedback to the system modules to obtain information about their status, and tools that contribute to the implementation of the set tasks.

Creating a single information space CIS requires the solution of the following tasks [11]:

- creation of a global information environment that provides comprehensive information processing in real time;

- creation of a single information and reference network;

- creation of a distributed network of information processing and storage with different access priorities and restrictions.

Successful implementation of a set of works in general will ensure the effectiveness of the SKI by significantly improving the efficiency of management and quality of decision-making, reducing the time between

These tasks determine one of the factors that determine the choice of information technology adaptive data flow management variety of applications used (text data, graphics, video, voice information).

There are many factors that determine the features of the effective functioning of the SKI [12, 13]. According to the trends in the development of CIS on the principle of scalability is determined by such a factor as the constant growth of circulating information [14, 15].

Critical infrastructure systems must have high availability, resilience, mobility, the required ICN bandwidth, availability, security, manageability and ensure

compliance with the requirements for timeliness, reliability and security of information exchange.

At the present stage, ICN are characterized by the following features [16]:

- the need to significantly reduce the time of implementation of new promising technologies for data processing and transmission;

- the need to implement and implement new approaches to the concept of adaptive data flow management;

- providing individual users (e.g. officials) with a wider range of telecommunications services.

Thus, the basis of information support of CIS is a globally distributed infocommunication network created on the basis of existing and perspective networks of communication and data transmission with application of modern telecommunication technologies which should provide high technical characteristics.

Ensuring the implementation of comprehensive requirements for the quality of application tasks is the main purpose of the management of CIS. Thus the basic purpose of management contains a number of partial purposes, each of which can be connected with a certain applied task.

There is a great variety of relevant management information technologies [17 - 20]. Since CIS belong to the class of complex systems with variable parameters, the principle of adaptive control must be applied to them. Given the increased security requirements, this management must be risk-adaptive, ie combine the properties of adaptation to changes in the tasks and structure of the system and be resilient to possible risks.

ICN management is usually related to network traffic management and, therefore, management of structured network equipment [21].

With the growth of information flows transmitted to the CIS and the dynamic change in the structure of the ICN, due to the introduction of mobile components of the communication system or the loss of network elements, one of the most important characteristics is the efficiency of information exchange [22]. It is

due to the fast and reliable exchange of data between the components of such a system that the efficiency of information exchange will be ensured.

Further development of critical ICN should take place on the basis of existing scientific and practical developments in the field of telecommunications, taking into account the state and prospects of development of critical ICS of the leading countries of the world.

The basis of modern CIS infocommunication networks are multiservice networks [23]. As shown by studies of processes in various data transmission systems based on multiservice networks [24 - 26], the physical failure of communication channels leads to a decrease in overall bandwidth. In these conditions, promising areas for improvement of CIS development and implementation of information technologies for efficient operation of data transmission systems that would ensure the transfer of information between subsystems and functional modules and parts of the system with the required quality [27].

Thus, the main tasks for the development of ICN in CIS are [28]:

- ensuring the readiness of the ICN, which will be ahead of the readiness of the CIS control subsystem;

- the use of new ways of organizing management and telecommunications, which ensure high efficiency of the CIS, taking into account its territorial distribution.

At the same time, special attention is paid to increasing the bandwidth of existing channels and communication lines, upgrading and finding new technical solutions that will improve management characteristics.

A feature of the introduction of the latest data transmission standards is the use of 100 Base-t unified Ethernet interface for internal connections [29, 30]. After connecting to the internal switch, data from the central computer system, operator workstations, means of transmitting digitized voice information, and other sources of digital information with the specified interface can be transmitted to the public network.

Each user who is connected to the network gets the opportunity to automatically enter the organized network of information exchange, becoming part of it, and transmit the necessary data to any subscriber in this network. Communication equipment automatically generates a single address space. Communication between subscribers occurs both with the use of wired connections and with the use of a radio channel as a backup. This ensures a prompt response to any changes, such as failure of certain facilities or deterioration of the interference situation in the communication area.

An important condition for the effective functioning of ICN in CIS is the maximum consistency in solving network-level tasks - routing, *traffic intensity management*, etc. Today, the variety of routing and access models used complicates the coordination of network processes and obtaining agreed solutions to network-level tasks.

In modern critical networks, which are multiservice, there is a rather acute problem of providing guarantees and quality control of QoS (Quality of Service) at the same time on several speed and probability-time indicators [31]. However, today, when solving route problems, it is quite difficult to present an adequate mathematical model of the processes of network dynamics, providing multi-service and guaranteed communication quality. [24, 27, 28, 32].

The solution of the task of routing and subscriber access can be achieved only if the whole representations of the network, which will formalize the management processes of both, network resources and network access. [33].

Data flow traffic has a structure that does not allow the use of existing methods based on Poisson models and Erlang's formulas [34 - 37]. Peculiarities of traffic are manifested in its specific profile, which determines the fluctuation nature of the respective processes: in the implementation there are always a number of fairly strong emissions against a relatively low average level, ie the coefficient of deviation of peak values of information flow intensity increases.

This property significantly degrades the characteristics (increases packet loss, hour delays) when passing traffic, even in cases where the average traffic in-

tensity is much lower than the potentially achievable transmission rate in this channel, which is unacceptable for ICN CIS.

This structure has the traffic in information and telecommunication networks when working with common protocols Ethernet, LAN, WAN, TCP when transmitting compressed video, WWW-traffic and others. Similar effects have also been identified in packet-switched cellular telephone networks and wireless communication channels. [38, 39].

Identify the main factors that determine the use and development of information technology aimed at ensuring the efficient operation of the entire system [21, 40]:

1. External factors that determine the nature of the data flows of ICN CIS are the variety of system applications used, large amounts of data re-data; increasing the intensity of information flows in critical areas of the network [41].

2. The main factors that affect the change in the transmission time of the data packet are [21, 42 - 44]:

- intensity of information flows;
- packet switching time, which depends on the network device;
- data channel bandwidth;
- the amount of packet data;
- the duration of the queue of data packets to the data channel;
- the load factor of the channel with service information.

3. Factors characteristic of the application of adaptive control of data flows are the fluctuation nature of information transfer processes [45], the presence of long-term dependences of statistical characteristics of information processes [46], increasing the coefficient of deviation of peak values of information flow intensity. [27, 47]

4. Traditional methods of redistribution of network resources involve smoothing the traffic profile of information flows. For example, using the method of statistical multiplexing [48] or the method of smoothing the intensity of the information flow [42].

Existing congestion management methods used in emerging critical areas also do not take into account the possibility of changing traffic properties, so the management process is not always adequate to the traffic profile. When there are peak values of data intensity, it is difficult to use existing methods to take into account their short duration and the time of occurrence of peak values.

Features of modern infocommunication systems are their territorial distribution, heterogeneity and multiservice (Fig. 1.1). Often the main advantages of control systems - versatility and versatility become their main disadvantages in CIS.

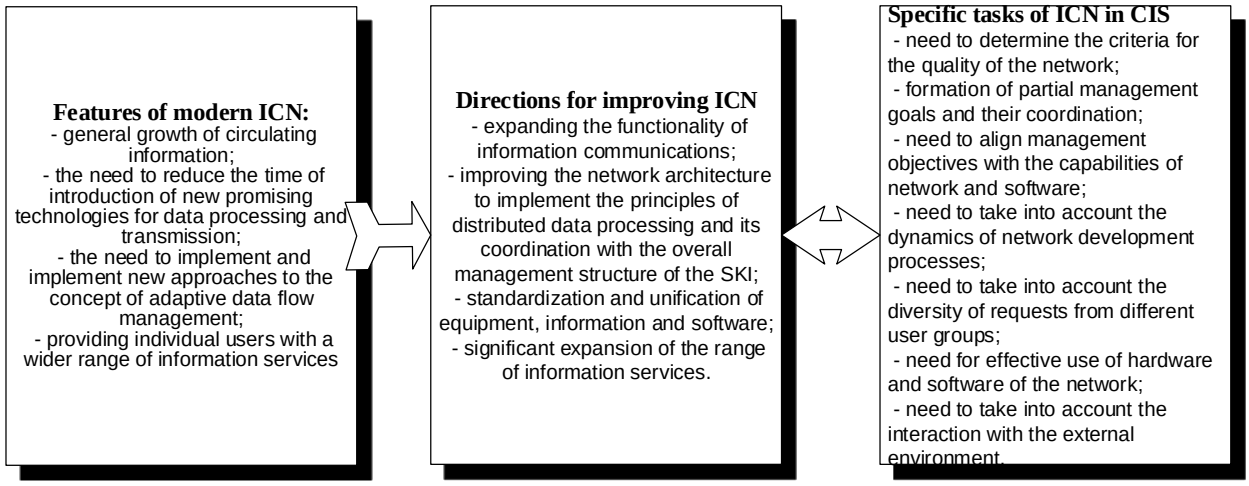


Fig.1.1. Features and areas of improvement of ICN

1.2 Methods of analysis and management of infocommunication networks

1.2.1 General approaches to optimizing infocommunication network resources

Critical infrastructure systems are characterized by high intensity of information flows, and the requirements for efficiency of management, timely adoption and delivery to the executors of decisions and tasks are constantly increasing. Such systems, as a rule, are multiservice, that is, they operate with heterogeneous

information (data, files, audiovisual information). This causes a significant non-stationary data flows in the network, the intensity of which in certain periods of time can significantly exceed the average values. At the same time, at designing of ICN CIS very high requirements both on productivity of a network and on reliability of service of subscribers are shown.

Compliance with these requirements is inextricably linked with the need to summarize the accumulated world experience in the field of infocommunication and depends on the degree of implementation of advanced information technologies related to data transmission and processing.

New technologies, such as NGN and MPLS, make it possible to create efficient, reliable and secure networks of any size. However, in reality it is difficult to provide the required reaction time for the following reasons [49]:

- high intensity and diversity of data flows,

- the need to search for data in repositories and databases of large dimensions,

- complex interaction of distributed applications,

- limited speed of communication lines,

- slowing down the speed of interaction in the gateways, which coordinate the heterogeneous components of different subnets of ICN.

The solution of these tasks is impossible without the creation and implementation of technologies and solutions that allow to maintain at a given level the network resources needed to ensure the functioning of the CIS [50]. It should be borne in mind that modern multiservice networks use sophisticated multifunctional communication equipment, which provides support for special mechanisms of quality control and management and implementation of information security policy.

Often the main advantages of modern control systems - versatility and versatility – are in the CIS and their main disadvantages. This is due to the need to take into account the specifics of the system, which requires appropriate network set-

tings and methods of managing its operation. Therefore, the classical methods of ICN design, taking into account the average performance, cannot ensure the efficient use of network resources [51].

Data flow management is designed to limit the load of network resources and match the speed of information transmission by the source with the speed of reception by the recipient [52].

Data flow management methods in modern ICN are used in the framework of network management concepts such as Traffic Engineering (TE), Active Network (AW), Network Engineering (NE) and implement approaches to remove the limitations of existing protocol solutions for network resource management [53 - 55]. So in TI and AW the main attention is paid to application of network control methods in combination with methods of mathematical and dynamic programming, in NE for flows with a high degree of aggregation apply the device of differential integral equations. [56, 57].

These methods allow ensuring balance in the load of ICN, increasing its productivity, but do not taking into account the probabilistic-temporal characteristics of integrated data flows and requiring the use of more informative models.

Table 1.1 summarizes the main technologies and concepts of network management, indicates their advantages and disadvantages.

Existing information technologies, on which the methods of traffic distribution management in ICN are based, are not able to meet the requirements for information exchange efficiency in the conditions of growing volumes of circulating information, as well as with the dynamic change of the structure of the data transmission system.

The results of the analysis of the current state of telecommunication technologies and the main protocol solutions showed the rapid dynamics of ICN development in the direction of creating high-speed multiservice networks. Despite the advanced development of technologies at the physical and channel levels, it is possi-

ble to fully realize the potential of ICN only through effective management of available network resources in the face of growing requirements for the efficiency of information exchange.

Table1.1 – Basic technologies and concepts of network management

Network technologies and management concepts	***Features***	***Advantages***	***Disadvantages***
Multiservice Communication Networks (NGN)	The information in the network is divided into two components: signal information that provides switching of subscribers and provision of services; and user data containing the payload	Effectively supports the full range of existing applications and services, providing the necessary scalability and flexibility, allowing you to respond to new requirements for functionality and bandwidth	The complexity of the compatibility of interfaces and signaling protocols of existing terminal equipment, the complexity of the actual provision of the required response time due to the properties of the CIS
Multi-protocol label switching (MPLS)	Allows to encapsulate various data transmission protocols and independent of protocols of data transmission mechanisms, allow modification or replacement of control algorithms	Improving network reliability and performance (independence from channel-level technologies, no need to support multiple second-level networks)	The problem of loss of control over data flows passing through the MPLS network by conventional IP applications
Traffic Engineering (TE), Active Network (AN), Network Engineering (NE)	Application of network control methods in combination with methods of mathematical and dynamic programming, for flows with a high degree of aggregation	Provide balance in ICN loading, increase its overall productivity (implement approaches to eliminate the limitations of existing protocol solutions for network resource management)	They do not take into account the probabilistic-temporal characteristics of integrated data flows and require the use of more informative models

1.2.2 Methods for analyzing data flows and redistributing infocommunication network traffic

When upgrading ICNs of complex automated control systems (which include CIS), as a rule, special attention is paid to increasing the bandwidth of channels and communication lines and finding new technical solutions that will improve the performance of management processes [15].

However, a characteristic feature of many multiservice ICNs is the specific fluctuation profile of data flow traffic, namely, the presence of a number of fairly strong emissions against the background of a relatively low average level. For this reason, despite the advanced development of technologies at the physical and channel level, to fully realize the potential of ICN is possible only through effective adaptive management of available network resources in the face of growing requirements for the efficiency of information exchange.

Currently, much attention is paid to research and development of methods for building information and telecommunications networks and distributed information systems [58, 59]. Data flows in modern ICNs are characterized by heterogeneity and significant variation of parameters, due to their multiservice nature, the presence of data of various formats obtained from different sources. [59].

In the presence of strict requirements for the reliability and capacity of a specialized ICN, one of the stages of its design should be the analysis of data flows and determine their parameters. For this purpose statistical analysis, mathematical modeling, static and dynamic analysis of data sources and flows are used [60, 61].

However, the study of the technical structure of the network and the definition of parameters of data flows without taking into account the tasks and applications that operate in network nodes does not allow to obtain effective solutions due to fluctuations and non-stationary data flows. Modeling of data flows should be based on the study of the information structure of the network [62]. This makes it possible to effectively use the resources of the network, ensuring compliance with the requirements for reliability and efficiency of information processing [63]. One

of the most promising areas of development of methods for building ICN is the use of methods of adaptive control [64].

The application of adaptive network resource management requires research, analysis and modeling of data flows that occur during the operation and interaction of application applications in network nodes. At present, this problem is insufficiently formalized and requires the development of complex mathematical models that reflect the information and technical structure of the network and the data flows available in the ICN.

Traffic allocation management involves the use of both standard and user-developed traffic management system (TE) methods and algorithms related to the optimization of network performance, which include technology and scientific principles for measuring, modeling, describing and managing traffic for obtaining the necessary performance characteristics [65]. Traffic management includes a set of interconnected network elements, a network status monitoring system, and a set of configuration management tools in response to the current state of the network, and allows preventive, using traffic forecasting and trends, to take action, preventing undesirable future conditions. Traffic management is focused on minimizing packet losses and delays, optimizing bandwidth and agreeing on the best possible level of services [66].

Bandwidth is a critical resource of modern ICNs. Therefore, the main function of traffic management is effective bandwidth management due to the optimal distribution of traffic at switching nodes. Currently, ICN uses various methods of traffic management. Most of them involve the possibility of external parameterization, ie the transfer of traffic parameters directly to the control algorithms used. Some of the methods, such as the multi-protocol label packet switching (MPLS) method, which allows encapsulation of various data transmission protocols and is independent of any protocols of data transmission mechanisms, allow modification or replacement of control algorithms included in the control technology implemented [67].

In modern ICN, the user can modify the software to control the data transfer

intensity (DTI) at two levels of data flow control:

- at the level of access control when receiving a request for data transmission by the network;
- at the level of regulation of network resources allocated on demand, when it passes through the network.

The lower level of control involves the use of control algorithms, which will transmit estimates of the parameters of the DTI, obtained using methods that take into account the characteristics of these flows. To obtain estimates of DTI parameters at this level, you can use already known methods, such as:

- a method for estimating the size of the filtering buffers of communication equipment, which increases the bandwidth of virtual channels by reducing the delay caused by acknowledgments of packets waiting in the queues of communication equipment by selecting the optimal size of filter buffers for integrated data flows served by virtual canal scrap [68];
- the method of synthesis of a stable price function of traffic distribution density, which is created by an integrated data flow, which allows to obtain in the case of fractal nature of traffic estimates of control parameters are more adequate to real than in similar methods;
- methods of managing the redistribution of bandwidth of the virtual connection, taking into account the priorities and competition between integrated data flows with dynamic bandwidth redundancy [69].

Consistent application of the above and similar methods allows obtaining estimates of control parameters adequate to the parameters of the DTI, and transferring them to traffic control algorithms that are part of the system regulators of priority and bandwidth, which will perform parametric optimization of DTI control at the level of resources in network nodes.

The analyzed methods of traffic distribution are summarized in table 1.2.

Table1.2 – Basic methods of redistribution of network resources

Methods	***Features***	***Advantages of application***	***Disadvantages***
Statistical multiplexing method	Implement technology and scientific principles of measurement, modeling, description and traffic management to obtain the necessary characteristics	Smoothes the traffic profile of information flows	Do not take into account the properties of traffic, when there are peak values of data intensity, it is impossible to take into account their short duration and time of occurrence
Method of smoothing the intensity of information flow			
The method of estimating the size of the filtering buffers of communication equipment,	Implements the selection of the optimal size of filter buffers for integrated data flows served by a virtual channel	Allows you to increase the bandwidth of virtual channels	Not used for traffic management at the upper management level (to control access when receiving a data request)
Method of synthesis of stable estimation of traffic distribution density function	Analyzes the integrated data flow of a fractal nature	Allows you to obtain adequate estimates of control parameters	
Methods for managing the redistribution of virtual connection bandwidth	Used for dynamic bandwidth redundancy	Takes into account the priorities of competition between integrated data flows	

1.2.3 Methods of risk analysis, improving the reliability and survivability of information systems

Critical infrastructure systems belong to the class of complex geographically distributed systems. The organization of work with information resources (IR) in distributed systems involves solving a set of problems to ensure convenient and fast access to information.

In addition, information should be protected on all transmission paths and in all types of processing. This leads to the need to solve additional problems related to:

- protection of communication channels;
- authorization of remote users and programs;
- protection of remote system nodes;
- protection of the entire distributed system.

It is the requirements for the system and complexity of risk protection that cause the biggest problems today, and the successful creation of information security systems lags behind the development of information transmission and processing technologies [70].

ICN protection issues are regulated by the standards of the Information Technical Laboratory (ITL) at the National Institute of Standards and Technology (NIST) [71]. There is a catalog of security measures for public information systems (including CIS) and defines the process for selecting security measures to protect the operation of IP from a variety of threats, including hostile cyber-attacks, natural disasters, structural failures and human error. Security measures are adapted and implemented as part of the overall for CIS process that manages information risks. Ensuring measures are defined by a diverse set of safety requirements for CIS derived from legislation, government regulations, directives, regulations, standards and business needs.

Specialized sets of risk mitigation measures are needed, adapted to certain types of functional activities, technologies or higher operating environments. The catalog of measures defines security both from the point of view of functionality (it is provided by stability of functions and mechanisms of safety) and from the point of view of trust (measures of confidence in the realized opportunities without security).

The use of risk management tools and technologies that are available to organizations is important in the development, implementation and maintenance of protection measures and countermeasures with the necessary and sufficient resilience of mechanisms to counter current threats. The application of effective risk-based processes, procedures and technologies will help ensure that the CIS has the necessary resilience to maintain its functioning, critical infrastructure applications and continuity of management.

The security of infocommunication systems is affected by a wide range of threats: from viral infection to regulatory conflicts. This raises risks that may have a negative impact on the performance of ICN.

The problems of vulnerability analysis and risk assessment of ICN, information security and protection are considered in the literature [72]. The classification of network attacks, threats to information security and identified ways to detect them [73]. The issues of decision-making on information security management of networks are considered [74, 75]. However, most scientific developments in the field of information risk (IR) assessment did not systematically take into account its causes, factors and interactions with other types of ICN risks, did not classify the causes and risk factors at the stages of synthesis and analysis of ICN, and when planning network traffic.

Different stages of the ICN life cycle differ in their requirements for the accuracy of the results and the computational complexity of the methods for evaluating the properties of networks [76 - 79]. So at the stages of network design there are no restrictions on the efficiency of assessment, but it requires maximum accuracy of the results, which cannot be said about the stage of operation.

In the event of malfunctions of ICN elements, it is necessary to carry out a reasonable reconfiguration of the network in the shortest possible time in order to ensure a given level of its efficiency and survivability. For this purpose, it is sufficient to estimate the viability of possible configurations of ICN structure configurations with their subsequent ranking according to the criterion of the maximum of the corresponding indicators.

When using the information system (in particular, ICN) in CIS high requirements on reliability and survivability of functioning in the conditions of influence of various destabilizing factors are shown to them.

Methodological approaches to the evaluation of these properties of the information system assume the presence of three stages [80]:

1) decomposition of a complex system into parts and elements and transformation of the structure;

2) assessment of the reliability of the object and the survivability of the elements of the system (information transmission lines and information-switching nodes).

3) assessment of structural reliability and survivability of the system as a whole.

There are many methodological approaches to assessing the reliability and survivability of the information system (rules for decomposition of networks, mathematical methods and models for assessing these properties, as well as their corresponding indicators), which differ in their characteristics [81]:

- computational complexity;
- time spent;
- accuracy and physical content of the received estimates.

This raises the problem of choosing effective methods for assessing the reliability and survivability of networks.

Analysis of publications [82 - 84] on the evaluation of these properties allows us to draw the following conclusions:

- There are many special and universal methods for assessing the reliability

and survivability of the information system, the choice of which is difficult for SKI due to the lack of relevant international or national standards (recommendations) and guidelines;

- Attempts are made to compare different methods, models, indicators of evaluation of these properties in order to select the optimal for the evaluation of a particular structure of the information system.

We will classify and analyze the features of methods for assessing the reliability and survivability of the information system.

Mathematical models and methods for assessing the reliability and survivability of the information system are complete and mathematical complexity of taking into account many factors, conditions, assumptions and limitations, as well as indicators and accuracy of quantitative assessment of these properties.

The whole set of methods for assessing the reliability and survivability of the information system can be divided into two subsets:

1) methods that evaluate the properties of the system by decomposing it into bipolar networks;

2) methods that evaluate the whole system.

The methods are divided into two independent subsets: exact and approximate estimation methods.

To choose taking into account the use of certain methods of reliability and survivability of the information system, it is necessary to enter the criteria corresponding to their features (properties) [77 - 79]:

- used source data;

- accepted assumptions and restrictions;

- final evaluation indicators;

- the relative efficiency of the assessment (the value inverse to the cost of computing resources).

Thus, to assess the reliability and survivability of the IS, the following classes of methods are used (Table 1.3):

Table 1.3 – Characteristics of existing methods for assessing the structural reliability and survivability of information systems

Class of methods	***The main algorithm***	***Application***	***Output data***	***Assumptions accepted***	***Indexes***
Accurate analytical methods for evaluating any IS structures	a complete search of the states of the ways of information transmission	the number of elements does not exceed 30 - 50	- IS structure, - indicators of reliability of elements, - node switching tables, - real bandwidth limitations	of serviceability of communication lines in the network are random and mutually independent events, - nodes are absolutely reliable	the average probability of connectivity of all modes of information transmission
Accurate analytical assessment methods for specific IS structures	differential equations	- "lattice", linear or ring topography, - the number of elements does not exceed 30-50	- IS structure, - indicators of reliability of elements, - characteristics of spare elements (loaded / unloaded)	- serviceability of network elements are random and mutually independent events, - all network elements are renewable with different availability factors, - the intensities of failures and renewals of the elements are constant, - recovery time and time intervals between failures are distributed exponentially	coefficient or function of structural readiness
Accurate analytical assessment methods for any IP structures	direct search of IS states	the number of elements does not exceed 50 - 100	- IS structure, - indicators of reliability of elements, - the allowable proportion of end nodes that may be denied access at any time, - the probability of finding the IS at any time in a certain	- serviceability of communication lines are random and mutually independent events, - nodes are absolutely reliable, - IS refuses to serve n subscribers, remaining operational	the coefficient of connectivity or operational connectivity of the IS

Continuation of Table 1.3

Class of methods	***The main algorithm***	***Application***	***Output data***	***Assumptions accepted***	***Indexes***
Approximate analytical methods of minimax estimates of structural reality with application	graph-analytical apparatus for decomposing IS into sections	the number of elements does not exceed 100 - 150	- IS structure, - indicators of reliability of elements	- loss of serviceability of communication lines are accidental and mutually independent events, - nodes are absolutely reliable	the average probability of connectivity of information transmission paths in the IS
Accurate analytical assessment methods for specific IS structures	method of detecting the correlation of the average proportion of "surviving" compounds and the average path length in the IS (Ptitsyn-Voilokov model)	- linear, annular, fully connected or radially nodal structure (tree-like, multicast-star), - any number of elements	- IS structure, - probability of operability of communication lines and nodes, - the average length of the path of information flows	- the loss of communication lines and nodes in the network are random events and mutually independent, - communication lines and nodes in turn are accepted as absolutely reliable	average proportion of active compounds (survivability)
Accurate analytical methods for evaluating hierarchical IS	direct search of IS states	- hierarchical structure of IS, - number of elements up to 50	- the allowable share of end nodes that can be denied access at any time, - probability of operability of communication lines, - the probability of finding the IS at any time in a certain state	- nodes are absolutely reliable, - transit nodes do not have information endpoints, - the IS refuses to serve n subscribers, remaining operational	the average probability of operation of a single way of transmitting information at a given number of extreme effects

1) accurate analytical methods for assessing any IS structures;

2) accurate analytical assessment methods for certain IS structures;

3) accurate analytical assessment methods for any IS structures;

4) approximate analytical methods of minimax estimates of structural reliability;

5) accurate analytical assessment methods for certain IS structures;

6) accurate analytical methods for assessing hierarchical IS.

2 ADAPTIVE TRAFFIC DISTRIBUTION MANAGEMENT IN INFO-COMMUNICATION NETWORKS

2.1 General principles of traffic distribution management in the infocommunication network

The infocommunication network in CIS has a hierarchical structure, both at the information and technical levels. Therefore, methods of traffic distribution management must take into account the peculiarities of hierarchical systems management.

Let's formulate the following *principles* of traffic distribution management [21]:

- the principle of decomposition, which provides for the division of the network into a number of subnets;
- the principle of coordination of subnet management, when the tasks of traffic distribution management for each subnet are made taking into account the state of other subnets;
- the principle of coordination of the goals of subnet management, in which partial (local) goals of traffic distribution management in individual subnets must ensure the achievement of the global goal of traffic distribution management throughout the network.

Since there is a relationship between the parameters of the technical structure of ICN and the characteristics of application and system software that operate in network nodes, consider the interaction of hardware and software network.

2.1.1 Decomposition of a management task

The CIS infocommunication network usually has a large dimension, so the direct solution of the general management problem for a complete network re-

quires special approaches [85]. Let's make decomposition of a management problem, having resulted the decision of the general problem to the decision of set of partial tasks.

To decompose the control task, we will pre-decompose the infocommunication network into many subnets. The rules of network decomposition must ensure the fulfillment of the following conditions:

1) the network is divided into subnets in such a way that each subnet is managed independently, and the quality of the subnet is determined by the functional from the parameters of only this subnet;

2) data flows between subnets should not depend on the management of each subnet.

Note that these conditions can be met if the de-composition of the network is carried out at the level of basic parameters, based on the properties of the network state space. Then, each basic variant of a network specifies a set of subnets and their structure. In this case, the data flows between subnets may not depend on how each subnet is managed. Features of the management of each subnet, in which data flows between subnets remain unchanged, reflects the following statement.

Statement 1. If each subnet management allows system applications to be redistributed only between nodes in this subnet and does not allow nodes and system applications to be redistributed between subnets, then the values of data flow rates between subnets do not change.

Evidence. For proof, note that an ICN with dedicated subnets can be considered as a network with a complex structure (the number of subnets is equal to K1). The total intensity of data flows between subnets i and j can be calculated using the formula

$$\mathbf{A_1}(\mathbf{C_1}) = \left\| a_{1ij} \right\| = \mathbf{C_1}\mathbf{A}(\mathbf{C_1})^T \ , \qquad (2.1)$$

in which the elements of the matrix $\mathbf{A} = \left\| a_{rk} \right\|$ ($r = \overline{1,t}, k = \overline{1,t}$, t – the number of involved nodes) – the intensity of data flows between nodes *r* and *k*, the value of

which depends on the distribution of system applications by nodes and the intensity of the flow of requests for system applications. To calculate the intensity of data flows between subnets, a matrix of partitioning nodes on subnets is used

$$\mathbf{C}_1 = \|c_{1ni}\| \ (n = \overline{1,k_1}, i = \overline{1,t}). \qquad (2.2)$$

This matrix remains unchanged under the conditions of the statement.

In the case where the system application is moved from one node of the subnet to another node of the same subnet, the intensities of data flow between the nodes of the ICN. However, the total flow intensities between this application and others installed on nodes outside this subnet remain unchanged. Therefore, moving a system application within a subnet does not change the intensity of the total data flows between that subnet and other subnets. If under this control the partition does not change, i.e. the matrix $\mathbf{C}_1$ remains constant, and the values a_{rk} also do not change, then the matrix $\mathbf{A_1}(\mathbf{C_1})$ also does not change, which was necessary to prove.

The parameters of flows between subnets in management are determined by the tasks to be solved on the network and the distribution of system applications and databases between nodes in each subnet. Therefore, if the management within the subnet redistributes system applications and databases between subnet nodes, it will not cause changes in flows between subnets, although it may cause redistribution of flows within the subnet. Then the conditions of the statement are fulfilled.

Therefore, control within the subnet can redistribute system applications and databases, redistribute data flows between nodes within the subnet.

The obtained result allows us to consider the task of managing the distribution of ICN traffic as a two-stage task [86]:

- at the first stage (network configuration stage) the configuration task is solved, where the composition of subnets and distribution of applications and nodes on subnets is formed;

- at the second stage the tasks of operative management of subnets are solved, thus each subnet is managed independently.

To set management tasks, we note that, after solving the configuration problem, subnets are selected, each of which is managed autonomously, it is necessary to select a set of control parameters for each subnet [24]. We denote such a set as UN_i, where i is the subnet of the subnet. General management tasks in this case are formulated as follows.

1. The task of setting up the network.

Given:

- a set of tasks to be solved online (number of tasks - l);
- a set of basic network parameters BSN;
- a set of basic network management parameters – UN_0 (parameters k_1, k_2, C_1, C_2 are part of many basic network management parameters);
- a set of indicators for the quality of network settings – QT_i, $i = \overline{1,\chi}$;
- a set of network setup quality metrics for each task – QT_{ik}, $i = \overline{1,\chi}$, $k = \overline{1,l}$;
- - set of weight coefficients $\{b_{0k}\}$ for partial tasks;
- - set of weight coefficients $\{a_{0ik}\}$ for quality indicators you are solving partial problems.

Find:

$$GT\left(\mathbf{UN}_0^*\right) = \underset{\mathbf{UN}_0}{\text{opt}}\left(\sum_{k=1}^{l} b_{0k} \sum_{i=1}^{\chi} a_{0ik} q_{ik}\left(QT_{ik}\right)\right)., \qquad (2.3)$$

with the specified system of restrictions on the value of basic network parameters

$$\mathbf{SN}_0 = \mathbf{SN}_{01} \cup \mathbf{SN}_{02} \qquad (2.4)$$

and characteristics of the network established for the task number k – $\mathbf{S}_k$ ($k = \overline{1,l}$):

$$\mathbf{SN}_{01} \le \overline{\mathbf{SN}}_{01}; \quad \mathbf{SN}_{02} \ge \underline{\mathbf{SN}}_{02}; \quad \underline{\mathbf{S}}_k \le \mathbf{S}_k \le \overline{\mathbf{S}}_k, \quad k = \overline{1,l}, \tag{2.5}$$

where $\overline{\mathbf{SN}}_{01}$, $\underline{\mathbf{SN}}_{02}$ – the set of limit (allowable) values for the basic parameters of the network;

$\underline{\mathbf{S}}_k, \overline{\mathbf{S}}_k$ ($k = \overline{1,l}$) – the set of lower and upper limit values of the network characteristics set for the task number *k*.

Yes, the following restrictions must be met:

$$\underline{M}_{\gamma j} \le \sum_{i=1}^{t} c_{\gamma j i} \le \overline{M}_{\gamma j}, \quad j = \overline{1,k_1}, \quad \gamma \in \{1, 2\}, \tag{2.6}$$

where $\underline{M}_{\gamma j}, \overline{M}_{\gamma j}$ – lower and upper limits of the number of nodes in the groups of the γ-th level;

$$\underline{\mathbf{A}}_{\gamma} \le \mathbf{A}_{\gamma}(\mathbf{C}_{\gamma}) \le \overline{\mathbf{A}}_{\gamma}, \quad \gamma \in \{1, 2\}, \tag{2.7}$$

where $\underline{\mathbf{A}}_{\gamma}, \overline{\mathbf{A}}_{\gamma}$ – matrices of lower and upper limits for values of data flow intensities between groups and within groups of the γ-th level;

$$\underline{\mathbf{A}}^{*}_{\gamma i}\left(\mathbf{Y}^{*}_{\gamma i}\right) \le \mathbf{A}^{*}_{\gamma i}\left(\mathbf{Y}^{*}_{\gamma i}\right) \le \overline{\mathbf{A}}^{*}_{\gamma i}\left(\mathbf{Y}^{*}_{\gamma i}\right), \quad \gamma \in \{2, 3\}, \tag{2.8}$$

where $\underline{\mathbf{A}}^{*}_{\gamma i}\left(\mathbf{Y}^{*}_{\gamma i}\right), \overline{\mathbf{A}}^{*}_{\gamma i}\left(\mathbf{Y}^{*}_{\gamma i}\right)$ – matrices of lower and upper bounds of information flow intensities between network γ-th level switches.

It is also possible to use as a limitation the data on the bandwidth of communication channels. The content of these limitations is that the partitioning on the

subnet, which is carried out when solving the task of configuring the network, must take into account the restrictions on the intensity of data flows between subnets and the bandwidth of communication channels between switches. [87].

The solution to the task of setting up the network will be a set of basic parameters that determine the division of network nodes on the subnet, which provides the optimal value of the quality of the network. The element of the set $\mathbf{UN}_0^*$ is, for example, the matrix C_1. Another result of solving the configuration task should be to determine the composition of subsets UN_{1i}, where i is the subnet number.

Next, the tasks of operational management of sub-networks must be solved.

We note that operational management is carried out constantly, is carried out step by step, therefore we will result statement of a task for a management step. This is due to the fact that with constant basic parameters, control within a given basic subspace of states is carried out in one step.

The general task of operational network management can be divided into a number of tasks of operational management of subnets. Since these tasks are solved autonomously, we present the problem of operational management of the subnet.

2. *Tasks of operational management of a subnet (*for a subnet *i)*

Given:

- the set of basic network parameters - BSN, including the set of optimal values of the basic control parameters, – $\mathbf{UN}_0^*$;

- a set of parameters of operational control of the subnet – UN_{1i}, $i = \overline{1,\chi}$;

- a set of quality indicators of operational management of the subnet – QT_{1i}, $i = \overline{1,\chi}$;

- a set of quality indicators of operational management of the subnet for each task solved in the subnet, – QT_{1ik}, $i = \overline{1,\chi}$, $k = \overline{1,l}$;

- a set of values of indicators of quality of the decision of partial tasks $q_{jk}\left(QT_{1ijk}\left(\mathbf{S}_{ik}\right)\right)$;

- the set of weight coefficients $\{b_{1ik}\}$ for partial tasks of the subnet;

- the set of weight coefficients $\{a_{1iok}\}$ for the indicators of quality the solution of a partial task.

Find:

$$GT_i^*\left(\mathbf{UN}_{1i}^*\right) = \underset{\mathbf{UN}_{1i}}{\text{opt}}\left(\sum_{k=1}^{l} b_{1k} \sum_{j=1}^{\chi} a_{1ijk} q_{jk}\left(QT_{1ijk}\left(\mathbf{S}_{ik}\right)\right)\right), \qquad (2.9)$$

at the set system of restrictions on values of parameters

$$\mathbf{SN}_{1i} = \mathbf{SN}_{11i} \cup \mathbf{SN}_{12i}, \qquad (2.10)$$

which take into account the characteristics of the subnet $\mathbf{S}_{ik}$ for the *k*-th task:

$$\mathbf{SN}_{11i} \le \overline{\mathbf{SN}}_{11i}; \quad \mathbf{SN}_{12i} \ge \underline{\mathbf{SN}}_{12i}; \quad \underline{\mathbf{S}}_{ik} \le \mathbf{S}_{ik} \le \overline{\mathbf{S}}_{ik}, \quad k = \overline{1,l}, \qquad (2.11)$$

where $\overline{\mathbf{SN}}_{11i}$, $\underline{\mathbf{SN}}_{12i}$, $i = \overline{1,\chi}$ – the set of limit (allowable) values for subnet parameters;

$\underline{\mathbf{S}}_{ik}, \overline{\mathbf{S}}_{ik}$, $k = \overline{1,l}$ – the set of lower and upper limit values of the network characteristics set for the task number *k* on the subnet.

In particular, the following restrictions must be met for each subnet:

$$\underline{\mathbf{A}}_{1i}^*\left(\mathbf{Y}_{1i}^*\right) \le \mathbf{A}_{1i}^*\left(\mathbf{Y}_{1i}^*\right) \le \overline{\mathbf{A}}_{1i}^*\left(\mathbf{Y}_{1i}^*\right), \qquad (2.12)$$

where $\underline{\mathbf{A}}_{1i}^*\left(\mathbf{Y}_{1i}^*\right), \overline{\mathbf{A}}_{1i}^*\left(\mathbf{Y}_{1i}^*\right)$ – matrices of upper and lower limits of information flow intensities between first-level switches and within groups of nodes connected to

first-level switches in the subnet. The meaning of this restriction is that when managing the subnet must take into account the restrictions on the bandwidth of communication channels within the subnet.

The solution to the task of operational management will be the optimal set of parameters of operational management $\mathbf{UN}_{1i}^{*}$ at each step of management.

The proposed approach has the following advantages:

1. The dimensionality of the network configuration task is reduced, because in comparison with the general management task, the number of restrictions is reduced and the target function is simplified.

2. Decomposition of the task of operational management on the task of operational management of subnets is carried out, which makes it possible to reduce the dimension of each task.

3. It is possible to independently solve the problems of operational management of subnets, using for each task its own set of quality indicators and management parameters, as well as management algorithms.

However, the decomposition of the management task involves the coordinated management of all subnets, which requires the coordination of management objectives for subnets.

2.1.2 Rules for coordinating subnet management

Coordination of subnet management in this case should provide time-coordinated management. The need for coordination is due to both the difference in the steps of subnet management by duration, and the limitation of the autonomy of management of each subnet, which does not always allow you to choose the beginning of the control step regardless of the state of other subnets.

There may be cases when you cannot start a new subnet management step due to changes in other subnets. Thus, if the basic parameters of the network change, it can lead to a change in the basic states for individual subnets, to change

the basic subspace of subnets, and, accordingly, to change the parameters and objectives of operational management of these subnets.

Therefore, we can formulate the following rule for coordinating the management of subnets.

Rule 1: when changing the basic states of the network, the processes of operational management in subnets must be stopped until the task of configuring the network with the new basic parameters is solved.

After solving the configuration task, the operational management of subnets can begin.

Further, due to the impossibility to synchronize the beginnings of the steps of operational subnet management, there may be cases when subnet management causes a change in the state of other subnets, for example, a change in data flows coming into the subnet. At the same time, the administrators of these subnets begin procedures to manage their networks, which is useless and sometimes harmful, as it can lead to deterioration in the quality of subnets and the network as a whole. You need to find out the reason for the change. This especially refers to changing the parameters of data flows coming into the subnet. During operational management, the parameters of data flows between sub-networks do not change, changes can be caused either by management in subnets, or by changing the basic parameters. In the first case, the management of the subnet must be changed, and in the second it is necessary to first solve the task of setting up the network, as follows from rule 1 of the coordination of subnet management.

Thus, we can formulate another rule for coordinating the management of subnets.

Rule 2: if the parameters of data flows between subnets have changed without changing the basic parameters of the network, it is not necessary to change the management of subnets; it is necessary to determine the reason for changing the parameters of flows and eliminate it.

The reasons may be either erroneous management, or failure of subnet equipment, or unauthorized change of basic network parameters.

2.1.3 Coordination of management objectives

It was emphasized above that not always the optimal solution of individual problems leads to the optimal operation of the network as a whole. However, it is necessary to find a form of setting partial tasks so that they can be solved autonomously, but the results would lead to a common goal, ie to optimize the integrated target quality of network performance.

If we take into account the possibility of decomposition of management tasks, it can be noted that the coordination of management objectives in solving the tasks of operational management of subnets is possible within the general functional quality of management, because these tasks are independent. Naturally, it is necessary to solve the problem of setting up the network in advance, where it is determined how the subnets are connected to each other, because during the setup there is a redistribution of shared resources. In this case, it is advisable to use additional criteria and restrictions that reduce the mutual influence of subnets. A possible solution is to allocate certain resources to each sub-network, so as to optimize the quality of the network as a whole. An acceptable solution may be to use an additive indicator of the quality of the network, which uses weights and indicators of the quality of subnets

$$GT^* = \sum_{i=1}^{\chi} e_i GT_i^* \left(UN_{1i}^* \right), \tag{2.13}$$

where e_i – the weight coefficient for the quality indicator of the i-th subnet, and the values $GT_i^* \left(\mathbf{UN}_{1i}^* \right)$ are calculated using the formula (2.9).

It is obvious that at autonomous work of subnets the formula (2.13) gives the chance to calculate optimum value of an indicator of quality of work of a network at optimum values of indicators of quality of work of subnets.

The peculiarity of solving the problems of operational management of subnets is the need to take into account the competition of the processes of solving applied problems for the resources shared within the subnet. Therefore, the coordination of goals in solving tasks within the subnet must be ensured by taking into account the resources allocated to each task or group of tasks. As a rule, tasks are grouped by the types of flows used, and management is reduced to creating the most favorable conditions for flows of each type. The essence of management is that each task is solved so as to achieve the optimum quality of its solution on the resources allocated to it. For example, each type of data flow may have its own bandwidth in the communication channel, or its own share of time when processing on servers.

Let's define the number of types of resources that are distributed between task groups – r'**.** The number of task types is denoted by l'. Let's introduce a matrix of resource allocation

$$\mathbf{RS} = \left\| rs_{ij} \right\|, i = \overline{1,l'},\ j = \overline{1,r'}, \tag{2.14}$$

where $rs_{ij} \in [0,1]$ – the share of the resource of type j allocated by the task of type i.

Conditions must be met for the elements of the matrix **RS**:

1. Each resource is fully distributed between tasks

$$\sum_{i=1}^{l'} rs_{ij} = 1,\ j = \overline{1,r'}; \tag{2.15}$$

2. That is, each task may or may not receive a share of each of the resources

$$\sum_{j=1}^{r'} rs_{ij} \geq 0, i = \overline{1,l'}. \tag{2.16}$$

The matrix **RS** allows you to determine how resources are distributed between the tasks and the element of the set of control parameters.

Forming a matrix **RS**, you can control the allocation of resources in the implementation of operational management of subnets.

In the general case, *the task of operational management* related to the allocation of resources can be formulated as follows.

Given:

- number of types of tasks – l';
- number of types of resources – r';
- the set of maximum values of resources of each type;
- resource allocation matrix **RS**.
- a set of weight coefficients $\{b_{1ik}\}$ for partial subnet tasks i;
- a set of weight coefficients $\{a_{1ijk}\}$ for quality indicators of the solution of partial problems on the subnet;
- a set of weight (cost) coefficients for the resources allocated to the task, – $c_{im} \geq 0, \quad i = \overline{1,l}, m = \overline{1,r'}$.

Find:

$$GT_i^*(RS) = \underset{RS}{\text{opt}}\left(\sum_{k=1}^{l'} b_{1k} \left(\sum_{j=1}^{\chi} a_{1ijk} q_{jk} \left(QT_{1ijk}(\mathbf{S}_{ik}) \right) + \sum_{m=1}^{r'} c_{km}(rt_m)(rs_{km}) \right) \right) \quad (2.17)$$

with a given system of restrictions:

1) each i-th type of tasks must receive the required number of resources of the type j

$$(rt_j)(rs_{kj}) \geq \underline{rt}_{kj}, \; j = \overline{1,r'}, k = \overline{1,l'}, \quad (2.18)$$

where $\underline{rt}_{kj}$ – the minimum allowable amount of resource type *j* allocated to the group of tasks of the type *k*;

2) the total amount of resources of type *j*, allocated to all tasks, should not exceed the total number of available resources of this type

$$\sum_{k=1}^{l}\left(rs_{kj}\right)\left(rt_j\right) \le rt_j,\ j = \overline{1,r'}. \tag{2.19}$$

The result of solving this problem will be the distribution of resources of the subnet number i between the tasks solved on this subnet.

Note that in this case, the coordination of objectives is carried out to optimize the quality of solving problems on the subnet, while the coordination uses the weights of each task, the quality of its solution and the resources allocated by it.

2.2 Method for adaptive management of information flow distribution

The main factors that affect data flows in infocommunication networks, the load of communication channels and network equipment are the following parameters [21, 57]:

- distribution of system applications on network nodes;
- distribution of users on network nodes;
- intensity of requests for application launches (tasks);
- network structure, which sets the communication channels between the network equipment and the binding of workstations and servers to the network equipment;
- values of bandwidths of communication channels used in the network;
- bandwidth of network equipment;
- distribution of bandwidth of communication channels between separate tasks (groups of tasks);

- routing of data flows in the network.

The models described in [88, 89] allow to calculate the parameters of data flows in the network with fixed primary network parameters:

- structures;
- network equipment;
- distribution of applications on network nodes;
- the intensity of the flow of requests to run tasks or system applications.

However, in real ICN, the intensity of request flows, the composition of users and the composition of the tasks can change over time, in addition, with the development of the network changes the composition of equipment and its parameters - that is, the basic network parameters change. All this necessitates the correction or change of control parameters of the network to achieve the required efficiency of its work. Such a change in network parameters is part of the debugging process, which, in turn, is one of the main processes of network management. At the same time it is necessary to provide necessary values of indicators of quality of work of the network connected with the decision of applied problems.

Since the distribution of users on the workstations of the network, as a rule, is determined by the structure of the organization and the territorial location of users [18], the distribution of users will be considered a given and constant parameter of the network.

Thus, network management in this case is reduced to solving the following main tasks:

- management of distribution and migration of system applications;
- network structure management;
- management of debugging of network equipment or management of data flows in the network;
- management of data flow maintenance parameters;
- routing management.

One of the main components for solving these problems is to achieve optimal bandwidth distribution.

When transmitting several types of data flows on one communication channel, it is necessary *to allocate bandwidth*. Each such flow can correspond to a certain group of tasks to be solved in the ICN environment [90]. Denote by λ_k the intensity of the flow type $k\left(k=\overline{1,\omega}\right)$, where ω is the number of flow types.

Suppose that a flow of type *k* needs a bandwidth σ_k. A condition must be met for a common bandwidth communication channel

$$\sum_{k=1}^{\omega}\sigma_k \geq \sigma_\Sigma . \qquad (2.20)$$

That is, it is possible to service each task in accordance with its bandwidth requirements. Numerical values of σ_k are set in accordance with the requirements for guaranteed quality of service [17].

However, there is often a situation when condition (2.20) is not met, which may be due either to the capabilities of communication channels, or to a change in the requirements of the task and, as a consequence, a temporary change in any type of traffic, such as with the appearance of new users who perform application tasks. Consider this case, in which

$$\sum_{k=1}^{\omega}\sigma_k < \sigma_\Sigma . \qquad (2.21)$$

That is, the bandwidth of the channel is not enough to meet the needs of all types of flows. This raises the problem of bandwidth distribution between all types of flows.

We will look for a static solution to the problem when the distribution of the channel between the flows is rigidly established for the known characteristics of the flows. Assume that the channel is distributed between flows of each type. The value of the costs associated with the deviation of the selected flow of the *k*-th type

of bandwidth μ_k from what it needs (σ_k – the bandwidth that was ordered) is proportional to the value of the deviation, ie

$$\begin{aligned} s_k(\sigma_k,\mu_k) &= a_k(\sigma_k - \mu_k)\delta_k(\sigma_k - \mu_k) + \\ &+ b_k(\sigma_k - \mu_k)\big(1 - \delta_k(\sigma_k - \mu_k)\big) = \\ &= (\sigma_k - \mu_k)\big(\delta_k(a_k - b_k)(\sigma_k - \mu_k) + b_k\big) \end{aligned} \tag{2.22}$$

where $a_k \geq 0$ – the value of the fine for the deviation from the value of the bandwidth for the current of the *k*-th type in the lesser direction by one conventional unit of measurement;

$b_k \geq 0$ – the amount of the additional fee for providing a flow of the *k*-th type per one conventional unit of measurement of a larger bandwidth;

$$\delta_k(\sigma_k - \mu_k) = \begin{cases} 1 \; if \; (\sigma_k - \mu_k) \geq 0 \\ 0, \; if \; (\sigma_k - \mu_k) < 0 \end{cases}. \tag{2.23}$$

Then the total cost of maintaining the flows is equal to

$$\begin{aligned} S(\bar{a},\bar{b},\bar{\sigma},\bar{\mu},\bar{p},\bar{q}) &= \sum_{k=1}^{\omega}\big(p_k s_k(\sigma_k,\mu_k) + q_k b_k \mu_k\big) = \\ &= \sum_{k=1}^{\omega}\big(p_k(\sigma_k - \mu_k)\big(\delta_k(a_k - b_k)(\sigma_k - \mu_k) + b_k\big) + q_k b_k \mu_k\big), \end{aligned} \tag{2.24}$$

where $\bar{a} = (a_k)$ u $\bar{b} = (b_k)$ – vectors of cost coefficients defined in (2.23);

$\bar{\sigma} = (\sigma_k)$ – a vector of set bandwidth values to be allocated to each flow type;

$\bar{\mu} = (\mu_k)$ – vector of bandwidth values that are actually allocated to each type of flows;

$\bar{p} = (p_k)$ – a vector which *k*-th component is the probability that a flow of this type is transmitted by this channel;

$\bar{q} = (q_k)$ – vector, the *k*-th component of which is the probability that the flow of this type is not transmitted by the channel, i.e. the flow does not need a communication channel, because there is no data of this type for transmission.

It is assumed that each flow of the *k*-th type does not constantly enter the communication channel, but when it arrives, it has an intensity

$$\gamma_k = \sigma_k . \tag{2.25}$$

The duration of the interval when the flow enters the channel, i.e. there is data for transmission, denote as φ_k, and the duration of the interval when the flow does not enter the channel (no data for transmission) – ψ_k. We assume that φ_k and ψ_k are random values with distribution functions $F_{\varphi_k}(t)$ and $F_{\psi_k}(t)$, accordingly, and such conditions are satisfied for the first two moments of all random variables [91]:

$$\nu_{1\varphi k} = \int_0^\infty t dF_{\varphi k}(t); \tag{2.26}$$

$$\nu_{2\varphi k} = \int_0^\infty t^2 dF_{\varphi k}(t); \tag{2.27}$$

$$\nu_{1\psi_k} = \int_0^\infty t dF_{\psi_k}(t); \tag{2.28}$$

$$\nu_{2\psi_k} = \int_0^\infty t^2 dF_{\psi_k}(t). \tag{2.29}$$

Thus, each thread can be represented as a recovery process. The probability that at any time in the channel there is or is not a flow of type *k*, are calculated by the formulas [17]:

$$p_k = \frac{\nu_{1\varphi k}}{\nu_{1\varphi k} + \nu_{1\psi k}}; \tag{2.30}$$

$$q_k = \frac{\nu_{1\psi k}}{\nu_{1\varphi k} + \nu_{1\psi k}}. \tag{2.31}$$

Using these expressions, you can find the numerical value of the function (2.24) – the total cost of maintenance of flows.

Then for static channel management the task of *controlling the bandwidth distribution* is set as follows: for given values of the number of data flow types, the maximum value of the channel bandwidth allocated for serving data flows, the vectors of data flow characteristics, the required bandwidth values, and cost coefficients, find the value $\bar{\mu}^*$ at which

$$S\left(\bar{a},\bar{b},\bar{\sigma},\bar{\mu}^*,\bar{p},\bar{q}\right) = \min_{\bar{\mu}} S\left(\bar{a},\bar{b},\bar{\sigma},\bar{\mu},\bar{p},\bar{q}\right) \tag{2.32}$$

and the following restrictions are met:

$$\sum_{k=1}^{\omega} \mu_k \le \sigma_\Sigma; \tag{2.33}$$

$$\sum_{k=1}^{\omega} \sigma_k > \sigma_\Sigma. \tag{2.34}$$

The meaning of the restriction (2.33) is that the total value of the bandwidth values actually allocated to different types of channel flows should not exceed the

maximum value of the channel bandwidth allocated for servicing these data flows. The meaning of the restriction (2.34) is that it is possible to set such values of bandwidth, which in total will exceed the capabilities of the channel [92].

Solving the problem (2.32) – (2.34) allows to minimize the cost of thread maintenance, that is, potentially increase the real network resource. Its feature is the ability to take into account user activity, since this activity is determined by the values of component vectors $\bar{p}$ *and* $\bar{q}$, and to solve it, you can use known methods [19, 93].

The general scheme of the method is given at Fig. 2.1.

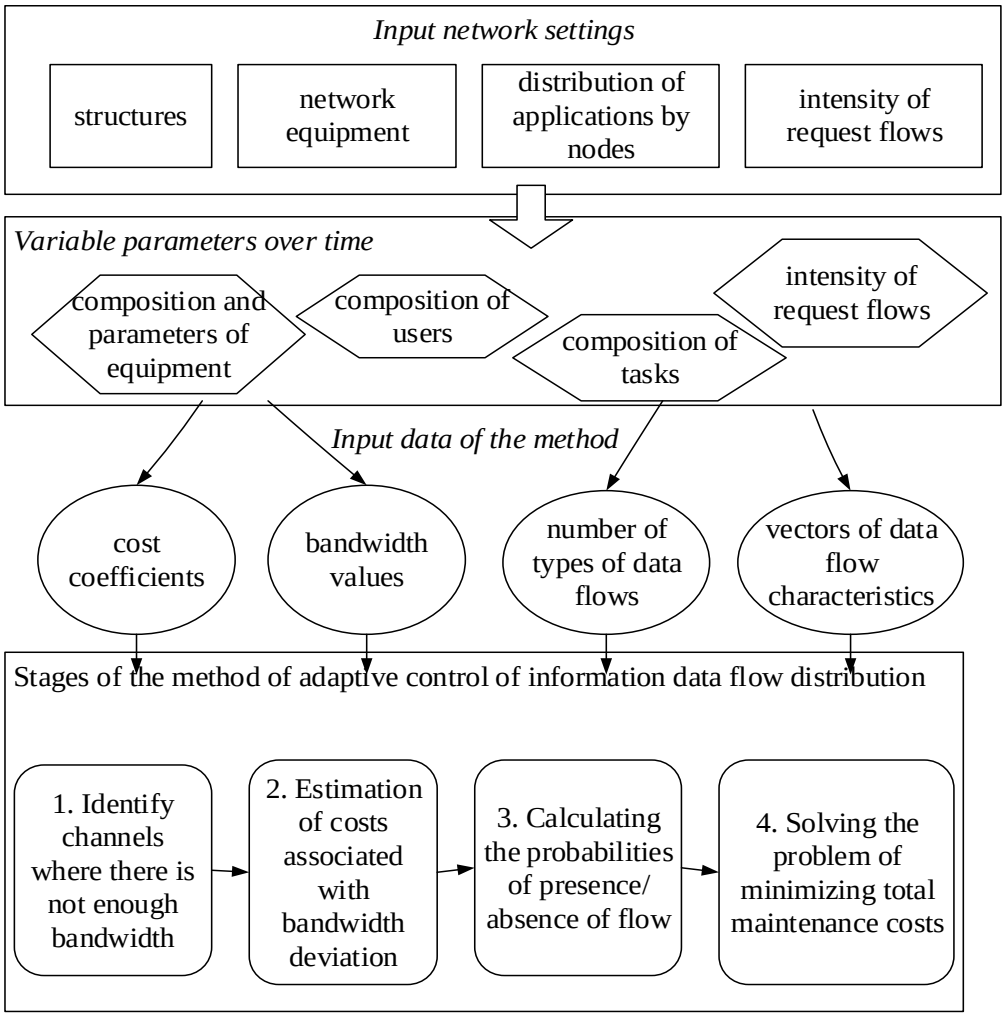


Fig. 2.1. Scheme of the method of adaptive control of the distribution of information flows

2.3 Method for allocating resources for a multi-server information processing node

If in ICN preference is given to centralized methods of data processing and storage (for example, when using GRID-technology), then among the many management tasks the most priority and relevant is the task of resource allocation of a multi-server information processing node.

The peculiarity of this task is a sharp increase in both the number of users of centralized processing tools and the intensity of the flow of requests for system applications. To meet the requirements for the quality of problem solving, it is necessary to use multi-server nodes for data storage and query processing. Such nodes are characterized by the emergence of tasks for managing the distribution of the flow of requests between servers, approaches to which have been considered in many sources [94 - 96], but did not take into account the relationship of information and technical structure of ICN, based on which you can obtain information on the bandwidth allocation of the involved communication channels.

Therefore, the method of the optimal selected criterion for managing the resource allocation of a multi-server information processing node is proposed, which is based on a hierarchical model of the network structure and the method of bandwidth allocation of the involved communication channels. [97].

Consider a multi-server information processing node (MIPN) as a closed system, the input of which receives information from the network in accordance with the algorithm for controlling the bandwidth of communication channels ICN, ie MIPN will be considered as a node consisting of N servers, each of which can serve all applications corresponding to the tasks solved in the network. Poisson streams of requests to run applications are received at the input of the MIPN, the intensities of the flows correspond to the intensities of the tasks used by these applications [98]. The intensities of the requests for execution of the j-th application λ_j make a vector

$$\Lambda = \left(\lambda_j\right),\ j = \overline{1,d}\,. \tag{2.35}$$

Let us denote the probability of sending a request to run application j on the server n as p_{jn}. The values of these probabilities make up the matrix $P = \left\| p_{jn} \right\|$, and the following conditions must be met:

1) applications of each type must be distributed between servers completely

$$\sum_{n=1}^{N} p_{jn} = 1,\ j = \overline{1,d}\,, \tag{2.36}$$

2) each server may receive requests to run applications

$$\sum_{j=1}^{J} p_{jn} = 1, n = \overline{1,\eta}. \tag{2.37}$$

The duration of application j on the n-th server (d_n) is a random variable with a distribution function $F_{nj}(t)$, which has finite first and second initial moments [17]:

$$\nu_{1nj} = \int_0^{\infty} t dF_{nj}(t); \tag{2.38}$$

$$\nu_{2nj} = \int_0^{\infty} t^2 dF_{nj}(t). \tag{2.39}$$

Let's also assume that all servers operate independently of each other. In this case, as a model of the studied server system can be considered a set of single-line mass queuing systems (MQS) type $M/g/1/\infty$ [92], ie the model of each server can be considered as MQS of this type, the input of which receives Poisson flow requests launch applications. Assume that the server corresponds to the service de-

vice in the MQS, and the MQS number matches the server number. The intensity of the flow of requests to run the *j*-th application, coming to the input of the *n*-th MQS is calculated by the formula:

$$\lambda_{jn} = \lambda_j p_{jn}, \quad j = \overline{1,d}, n = \overline{1,\eta}. \tag{2.40}$$

This flow is also Poisson, as it comes from the flow of requests to run the *j*-th application using the screening procedure [99].

Analyzing the work of one MQS, for simplicity, we assume that all requests on each server form one queue and are served in the order of receipt in the queue. Then the total flow of requests to the *n*-th server has intensity:

$$\Lambda_n = \sum_{j=1}^{d} \lambda_{jn} = \sum_{j=1}^{d} \lambda_j p_{jn}, \quad n = \overline{1,\eta}. \tag{2.41}$$

The probability that a request taken from the queue to the *n*-th server will be a request to run the *j*-th application is equal to

$$q_{jn} = \frac{\lambda_{jn}}{\Lambda_n}, \quad n = \overline{1,\eta}. \tag{2.42}$$

The Laplace-Stieltjes transform of the arbitrary request processing duration distribution function on the *n*-th server is calculated as:

$$\beta_n(s) = \sum_{j=1}^{d} q_{jn} \beta_{nj}(s), \quad n = \overline{1,\eta}, \tag{2.43}$$

where

$$\beta_n(s) = \int_0^{\infty} e^{-st} dF_n(t); \tag{2.44}$$

$$\beta_{nj}(s) = \int_0^{\infty} e^{-st} dF_{nj}(t) \tag{2.45}$$

With this transformation you can determine $F_n(t)$ – the distribution function of the corresponding random variable.

The average queue time for any request on the *n*-th server can be calculated by the formula [17]:

$$\tau_n = \frac{\Lambda_n \nu_{2n}}{2(1 - \Lambda_n \nu_{1n})}, \quad n = \overline{1,\eta}, \tag{2.46}$$

where

$$\nu_{1n} = \int_0^{\infty} t dF_n(t) < \infty; \tag{2.47}$$

$$\nu_{2n} = \int_0^{\infty} t^2 dF_n(t) < \infty. \tag{2.48}$$

When allocating requests, conditions must be met to prevent server overload:

$$\Lambda_n \nu_{1n} < 1, \quad n = \overline{1,\eta}. \tag{2.49}$$

The probability of server downtime is calculated by the following formula:

$$p_{0n} = 1 - \Lambda_n \nu_{1n}, \quad n = \overline{1,\eta}, \tag{2.50}$$

Thus, the formulas for calculating the characteristics of the robot of one server are obtained.

However, all servers share request flows with each other, so it is necessary to explore their collaboration to service requests. To do this, we introduce the quality management functionality of the resource allocation of the node:

$$\Phi\left(N,P,\Lambda\right)=\sum_{n=1}^{\eta}\left(\alpha_n\tau_n+\beta_n p_{0n}\right), \tag{2.51}$$

where the coefficients α_n *and* β_n are fines per unit of queue time in the queue to the n-th server and the unit of downtime of the n-th server, respectively.

The functionality allows you to calculate the amount of costs associated with the downtime of requests in the queue for processing, as well as the costs incurred in case of server downtime.

The task of optimal management of resource allocation of a multi-server node is formulated as follows: for a given number of tasks to be solved on the network, applications to perform tasks, the number of servers, many parameters of applications and tasks, matrices of intensity of requests for tasks, the set of cost factors associated with server downtime and waiting for requests in queues per unit time, and the allowable values of the intensity of the flow of requests coming to the servers, determine probability matrix and direct requests to run application servers *j* such that the functional value (2.51) was minimal, ie,

$$\begin{gathered}\Phi\left(N,P^*,\Lambda\right)=\min_{P}\Phi\left(N,P,\Lambda\right)=\\ =\min_{P}\sum_{n=1}^{\eta}\left(\alpha_n\tau_n\left(P,\Lambda\right)+\beta_n p_{0n}\left(P,\Lambda\right)\right)\end{gathered} \tag{2.52}$$

with such restrictions:

$$\sum_{n=1}^{\eta} p_{jn} = 1, j \in \overline{1,d}; \quad (2.53)$$

$$\sum_{j=1}^{d} p_{jn} = 1, n \in \overline{1,\eta}; \quad (2.54)$$

$$\Lambda_n \nu_{1n} < 1, \quad n = \overline{1,\eta}, \quad (2.55)$$

$$p_{jn} p^*_{jn} = p^*_{jn}, \quad j = \overline{1,d}, n = \overline{1,\eta}, \quad (2.56)$$

where p^*_{jn} – element a priori of a given Boolean matrix, in which single elements define those request flows that can be served only by specific servers.

Problem (2.52) – (2.56) is a problem of mathematical programming, which allows to minimize the cost of maintenance of flows, to solve it you can use known methods [93].

A generalized scheme of the method of resource allocation of a multi-server information processing node is shown in Fig. 2.2.

2.4 Integrated quality criteria for network traffic management

Since the applied tasks of ICN are quite diverse: from the transfer of different types of data to the collection and processing of information, for each task it is necessary to identify indicators of the quality of its solution [100].

Define a unified set of quality indicators for solving applied problems, taking into account the specifics of each task:

$$\Re = \left\{R_1, R_2, ...R_\chi\right\}, \quad (2.57)$$

where χ – the total number of indicators of the quality of solving applied problems in the network.

Note that each *i*-th quality indicator has a specific physical meaning, such as time to solve the problem, loading communication channels with the data of this problem, and so on.

The use of a common scale of quality indicators allows not only to significantly simplify the mathematical description of network management processes, but also to use common agreed criteria in assessing the performance of the network and its elements in solving various applications.

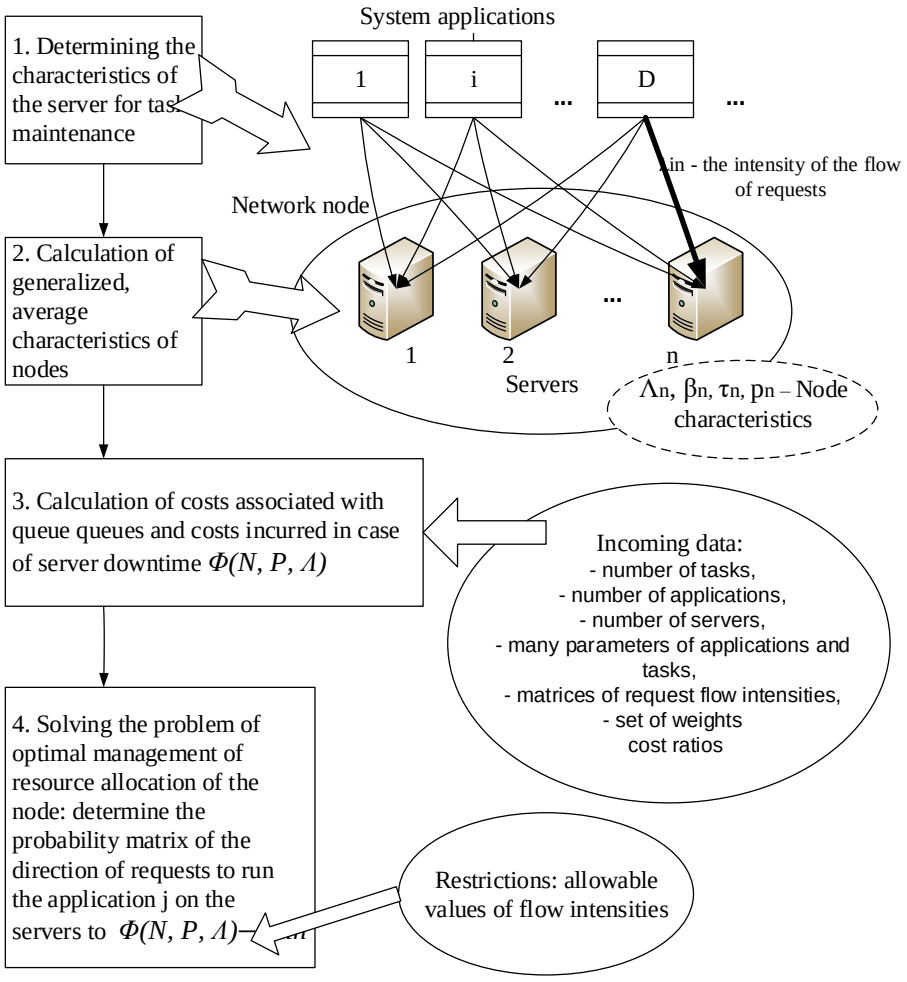


Fig. 2.2. Scheme of the method of resource allocation of a multi-server information processing node

For the *k*-th task, the set of solution quality indicators is determined by a bit string

$$q_k = (q_{1k}, q_{2k}, ...q_{\chi k}), \tag{2.58}$$

$$q_{1k} = \begin{cases} 1, if\ \ i-th\ quality\ indicator\ is\ used.for\ k-th\ task \\ 0, if\ \ i-th\ quality\ indicator\ isn't\ used\ for\ k-th\ task \end{cases}.$$

If the *i*-th quality indicator is used to assess the quality of the solution of the *k*-th task, then we denote it as $R_{ik}(\Im_k)$, where $\Im_k$ is the set of parameters of the k-th problem, at this

$$R_{ik}(\Im_k) = q_{ik} R_i, \tag{2.59}$$

a set of quality indicators for the *k*-th task is formed in such a way:

$$\Re_k(\Im_k) = \left(q_{1k} R_1, q_{2k} R_2, ...q_{\chi k} R_\chi\right), \tag{2.60}$$

moreover, for a set of indicators of the quality of solving individual tasks, the following condition is met:

$$\bigcup_{k=1}^{l} \Re_k(\Im_k) = \Re. \tag{2.61}$$

The use of a single system of indicators to assess the quality of application problems allows you to define a system of partial objectives of network management, as a set of such functions:

$$G^* = \left\{ \underset{\Im}{opt}(R_{ik}(\Im_k)) \right\}, i = \overline{1,\chi}, k = \overline{1,l}, \tag{2.62}$$

or

$$G^* = \left\{ \underset{\Im}{optF}(R_{ik}(\Im_k)) \right\}, i = \overline{1,\chi}, k = \overline{1,l}\,. \qquad (2.63)$$

where $\Im_k$ – many control parameters of the network, and the parameters of each task can be either basic parameters or control parameters.

The main feature of solving a set of tasks on the network is that the processes that programmatically implement tasks or applications, as a rule, compete for network resources and simultaneously achieve optimal results for each indicator of the task and for each task is not always possible. For example, metrics that are related to queue delays in queues and metrics that are related to equipment loading are conflicting.

In addition, the optimization of the quality of the solution of each individual task cannot always ensure the optimal operation of the network and the critical infrastructure system as a whole. In this regard, to manage the network you need to solve the following tasks:

- to determine the quality indicators of the network as a whole - integrated (complex) quality indicators;
- to ensure the coordination of partial goals and, accordingly, indicators of the quality of solving individual tasks.

In order to obtain integrated indicators of the quality of problem solving, we introduce the set of weights of indicators $A_k = \{a_{ik}\}$ for each problem, and the set of weights of problems $B = \{b_k\}$. Then, taken into account (2.57) and (2.58):

$$G = \sum_{k=1}^{l} G_k = \sum_{k=1}^{l} b_k G_k = \sum_{k=1}^{l} b_k \left(\sum_{i=1}^{\chi} a_{ik} q_{ik} R_{ik}(\Im_k) \right), \qquad (2.64)$$

where G – integrated overall indicator of the quality of problem solving;

G_k – the value of the integrated quality indicator for solving the k-th task.

Using formulas (2.62) – (2.64) we derive a generalized formula for calculating the integrated (target) quality indicator of the network to solve a given set of problems:

$$G^*(\Im) = \underset{\Im}{opt}\left(\sum_{k=1}^{l} b_k G_k(\Im)\right) = \underset{\Im}{opt}\left(\sum_{k=1}^{l} b_k \left(\sum_{i=1}^{\chi} a_{ik} q_{ik} R_{ik}(\Im_k)\right)\right), \quad (2.65)$$

where $G_k(\Im)$ – the value of integrated indicators of network quality in solving each problem separately.

Similarly, you can determine the target quality of the solution of each problem:

$$G^*(\Im) = \underset{\Im}{opt}\left(\sum_{i=1}^{\chi} a_{ik} q_{ik} R_{ik}(\Im_k)\right). \quad (2.66)$$

It should be noted that equality is not always fair:

$$G^*(\Im) = \sum_{k=1}^{l} b_k G^*{}_k(\Im). \quad (2.67)$$

This means that the optimum of the integrated network performance target is not always equal to the sum of the weighted optimum of the integrated solution quality indicators for each of the tasks on the network. This may be due to the fact that the optimal value of control parameters for one task will not be optimal for another task, because the tasks may compete for network resources. In this regard, it is necessary to agree on partial goals, which will allow to obtain acceptable solutions.

2.5 The stages of the method for controlling the distribution of traffic

The generalized method of traffic distribution management provides a sequence of actions that must be performed in the preparation and solution of management tasks. The method includes the following steps:

- preparation for solving management tasks;
- solution of the network configuration problem;
- solving operational management tasks;
- correction of tasks of adjustment and operational management.

Consider these steps in detail.

1. *The preparation stage* is necessary for the development of basic approaches and requirements for traffic distribution management, on the basis of which management quality criteria are developed, specific goals and objectives of management are formulated.

The method involves compliance with all restrictions, conditions and rules defined above. At the stage of preparation for the solution of management tasks it is necessary to perform the following steps:

- determining the composition of network users;
- determination of the composition and parameters of the applied problems;
- determining the composition of applications that are installed on the network and you-could to the equipment for the implementation of applications. If necessary, the number of copies for some applications is determined. These copies will be considered as separate applications with their own numbers;
- formation of the information structure of the network;
- analysis of the information structure of the network;
- determination of indicators and quality criteria for solving applied problems;
- determining the composition of network parameters that will be used to assess the state of the network, network management and determine the space of network states; determining the composition of the basic parameters of the net-

work; determining the specific composition of the set of primary and secondary network parameters;

- determining the composition of network management parameters;
- determination of limit values of network parameters. Here the maximum allowable values of network parameters are determined, the value of which is related to the capabilities of network equipment and communication channels, servers and workstations, as well as software.

After carrying out the listed preparatory works it is possible to pass to the decision of problems of management of distribution of traffic.

2. At the stage of solving the *network setup* task, the following steps are performed:

1) Determination of specific indicators of network setup quality.

2) Formation and calculation of data flow parameters of the hierarchical information structure of the network. The solution of the problem of forming the information structure can be considered as a partial solution of the setting problem. As a result, the parameters of the information structure and data flows for the information structure with these parameters are determined.

3) Determining the composition of network equipment. Based on the analysis of applications to equipment parameters, analysis of information flows conducted for the information structure of network traffic distribution management, the potential number of technical nodes of the network and preliminary data on the technical structure of the network (a priori distribution of users and nodes on subnets), the composition is determined equipment and its parameters - switches, servers, client workstations, types of communication channels used.

4) Formation of the technical structure of the network. As a result of this step, a set of values of the basic parameters of the network is formed, the structure of the basic network is also formed, and in addition, the sub-networks and their composition are allocated. Note that it is possible to repeatedly solve the tasks in this step, if you change the distribution of system applications on the nodes of the

information structure. At the end of the step, a set of network parameter values is determined.

At the end of this stage of configuration we have a variant of the network structure, a set of parameters of operational management of subnets, which are used in the next stage.

3. The stage of solving *operational management tasks* involves the following steps:

1) determination of performance indicators of subnets. In this step, a set of performance indicators for each subnet is formed;

2) setting partial tasks of operational management for sub-networks. Here can be used or the general task of operational management, or the task of operational management of subnets, or partial tasks of operational management;

3) solving operational control problems using mathematical programming methods.

4. The stage of correction of tasks of adjustment and operative management arises in case of change of basic parameters of a network that can interfere with resetting of a network and development of new approaches to the decision of tasks of operative management. It includes the following steps:

- correction of the composition of network parameters;
- correction of the composition of the basic parameters and control parameters;
- correction of requirements for the quality of solving applied problems.

After solving these problems, the transition to the stages of management described above.

3 RISK ASSESSMENT OF THE INFOCOMMUNICATION NETWORK OF THE CRITICAL INFRASTRUCTURE SYSTEM

3.1 Managing infocommunication network risks to improve the security of critical infrastructure systems

Security of information resources and information environment is traditionally considered as [109]:

- a set of tools and technologies that protect the components of the information environment;
- risk minimization for components and resources of the information environment;
- a set of procedural, logical and physical measures aimed at counteracting threats to the information resource and components of the information environment.

The safety requirements for the operation of the CIS must be formally defined. Fulfillment of these requirements guarantees that in the event of anticipated problem situations from undesirable influences of various natures, including failures of ICN components, CIS will be able to perform its intended function in full.

The main sources of threats to the functioning of critical infrastructure systems are industrial accidents, terrorist and criminal activities, cyber-attacks, natural disasters, etc. [215].

Another source of threats and associated risks are external information system services – these are computing and information technology services implemented outside the traditional limits of security authorization. External information system services include, for example, the use of service-oriented architectures (SOA), services based on cloud computing (infrastructure, platform, software), or the use of data centers.

The security of distributed systems can be compromised due to the negative impact of both human and technical factors, so there may be unforeseen problem situations that require an adequate response of the system. Mechanisms and means to increase the survivability of systems are used to predict, establish, avoid, and overcome such situations.

Survival as a property of the system characterizes its ability to choose the optimal mode of operation due to its own internal resources, restructuring, changes in functions and behavior of individual subsystems due to changes in external conditions and in accordance with the purpose of its operation [111].

Security requirements are determined based on the scope of the CIS, laws, government regulations, directives, regulations, instructions, standards, regulations to ensure the confidentiality, integrity and availability of information processed, stored or transmitted by information systems. Security measures are security measures proposed for information systems that are designed to protect the confidentiality, integrity and availability of information that is processed, stored and transmitted in these systems and meet a number of specific security requirements.

The selection and implementation of risk management measures for CIS are important tasks that can have a significant impact on the functionality and viability of CIS. It is necessary to determine what risk management is needed to meet safety requirements and accordingly counteract the risk that exists when using ICN. The choice of these measures is important for an effective risk management process that has identification, continuous monitoring and risk counteraction [112].

Risk management includes:

- analysis of threats and vulnerabilities;
- parrying (reducing) the risk provided by existing or planned security measures.

Consider the main steps of information risk management (Fig. 3.1):

1) categorization of the information system according to the level of risk is based on the assessment of possible negative impact;

2) selection of a basic set of measures to parry risks, based on the results of categorization;

3) implementation and documentation of risk counteraction measures;

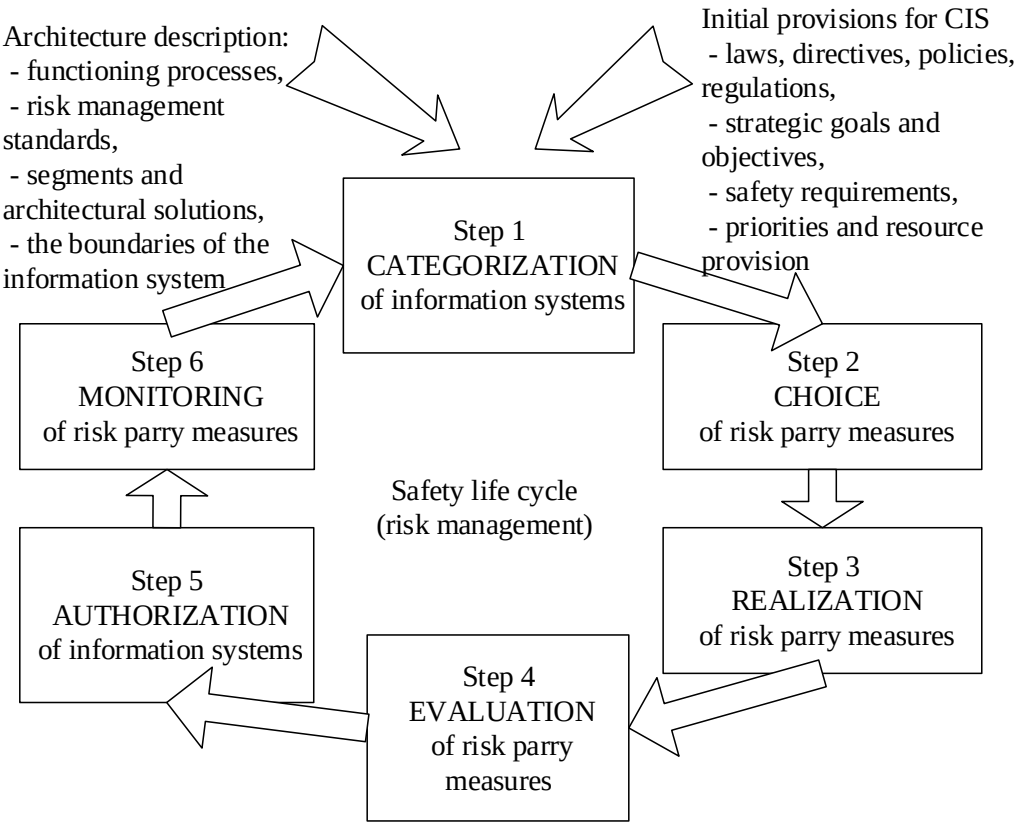


Fig. 3.1. Scheme of a step-by-step method of information system risk management

4) an assessment of the set of measures to determine whether the measures have been implemented correctly, whether they are working as intended and whether they produce the desired result in terms of compliance with safety requirements;

5) authorizing the operation of the information system, based on determining the risk to the activity and deciding that this risk is acceptable;

6) continuous monitoring of security measures in the information system and operating environment to determine the effectiveness of measures to parry risks, changes in the system and compliance.

3.2 System model of information risk based on cognitive maps

Let's define the basic categories of system model of risk for revealing of interrelations between their elements (Fig. 3.2).

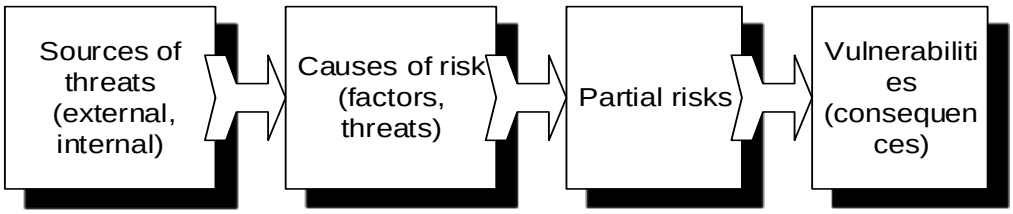


Fig. 3.2. The main categories of the system risk model

The risk analysis and assessment procedure involves the following steps [113]:

- analysis of risk factors (potential sources of threats);
- formation of the list of key risks of ICN which can essentially influence its functioning;
- analysis of the consequences of risky events;
- analysis of causal relationships between the elements of the categories of the systemic risk model;
- assessment of the probability and cost of ICN risk.

To analyze the risk factors, it is necessary to classify the types of ICN risks.

Due to the causes of ICN risks can be divided into two main categories:

- objective risks arising from failures of equipment and information transmission channels;
- subjective risks caused by the loss of information and its improper use.

PCM risks can also be classified according to the factors of their occurrence into internal and external. Here you can take into account the period of the life cycle (LC) of ICN. Risks arise both at a design stage (or modernization), and at an operation stage (at performance of processes of data transfer and their control).

Taking into account the factors of their occurrence, the group of internal risks includes:

- risks associated with the provision of services (including the provision of peak loads) - arise during operation;

- risks of fraud, which may be the result of illegal connection, traffic theft, etc.; these risks arise during operation.

External risks (due to the influence of the external environment) include:

- part of the risks of development and implementation of new services, which are related to the development of networks and construction of communication facilities; they may be the result of delays by contractors, lack of funds, etc.; these risks arise at the stage of modernization,

- risks due to imperfect legislation - may arise at any stage of the LC.

Taking into account the categories of factors (technical, process, human and external), we present a list of possible risks of ICN, indicating the reasons for their occurrence (Table 3.1).

Table 3.1 – Categories of factors and causes of ICN risks

Categories of factors	**Causes of risks**	**Partial risks**
Internal risks		
Technical factors	P_{11} - lack of capacity P_{12} - lack of performance P_{13} - improper maintenance P_{14} - aging of equipment	R_1 - risk of equipment failure
	P_{21} - incompatibility P_{22} - Improper configuration management P_{23} - Improper change management P_{24} - Incorrect security settings P_{25} - dangerous programming practices P_{26} - Improper testing	R_2 - risk of software failure
	P_{31} - design problems P_{32} - specification problems P_{33} - integration problems P_{34} - system complexity	R_3 - risk of error in network design

Continuation of Table 3.1.

Process factors	P_{41} - improper technological process P_{42} - Improper process documentation P_{43} - Misunderstanding of roles and responsibilities P_{44} - incorrect information flows P_{45} - improper escalation of problems P_{46} - Inefficient task transfer	R_4 - risk of error in network processes (design and execution)
Process factors	P_{51} - Lack of condition monitoring P_{52} - no metrics P_{53} - no periodic analysis P_{54} - improper ownership of the process	R_5 - risk of process control error
	P_{61} - staffing problems P_{62} - funding problems P_{63} - deficiencies in learning and development P_{64} - procurement problems	R_6- risk of error in process support
Human factor	P_{71} - accidental error P_{72} - ignorance P_{73} - failure to follow instructions	R_7 - risk of unintentional action
	P_{81} - fraud P_{82} - sabotage P_{83} - theft P_{84} - vandalism	R_8 - risk of intentional action
	P_{91} - lack of skills P_{92} - lack of knowledge P_{93} - no instructions P_{94} - unavailability of people	R_9 - risk of inactivity
External risks		
External factors	P_{101} - weather phenomena P_{102} - fire P_{103} - flood P_{104} - earthquake P_{105} - riot P_{106} - quarantine	R_{10} - risk of catastrophe
	P_{111} - non-compliance P_{112} - changes in legislation P_{113} - litigation	R_{11} - legal risk
	P_{121} - problems with suppliers P_{122} - unfavorable market conditions P_{123} - unfavorable economic conditions	R_{12} - business risk
	P_{131} - problems with the supply of materials P_{132} - dependence on emergency services P_{133} - problems with power supply P_{134} - transport problems	R_{13} - risk of poor quality services

Technical factors cause risks associated with incorrect or unexpected operation of ICN process equipment.

Process factors determine the class of risks associated with the problems of internal processes, as a result of which they do not work as expected.

The human factor causes risks associated with problems caused by the actions (or inaction) of people in certain situations. This class covers the actions of both insiders and external network users. External factors are the causes of risks associated with external, uncontrolled events. In most cases, such events cannot be predicted and planned [114].

Risks cause consequences that negatively affect the following main characteristics of ICN operation:

1. Network performance, which is associated with the concepts of reliability and survivability. The differences between these concepts are due to the causes and risk factors. The reliability of the communication network reflects the influence of mainly internal factors - accidental failures of technical means due to aging processes, defects in manufacturing technology or errors of service personnel. The survivability (stability) of the communication network is characterized by its ability to maintain full or partial performance under the influence of causes hidden outside the network (natural or intentional) and lead to destruction or significant damage to some of its elements.

2. Network performance (or bandwidth) is associated with the parameters of the quality of operation, as the implementation of the planned load must be carried out with the specified quality parameters.

3. Information security in the process of storage and transmission of data is associated with violations of confidentiality and integrity of information. Attacks at the confidentiality and integrity of information can be carried out by enemies, competitors. In addition, security suffers from failures of equipment and software systems under the influence of electronic signals.

4. The parameter of economic efficiency refers to the characteristics of ICN both at the stage of its creation and at the stages of operation and modernization. It is related to legal and business risk issues.

Risks have a negative impact on the basic properties of information and the functioning of ICN [115].

Thus, violations of the processes of information collection, processing, failures in data transmission technology, lead to information leakage, unauthorized copying and distortion (forgery). The system may be blocked and information transmission may be delayed. Risks caused by hardware and software failures and electronic interference are associated with viruses and "bookmarks" -devices for intercepting information. Viruses not only promote, but also limit the speed of their transmission, as well as can block the network. As a result of accidents, natural disasters there may be direct destruction, breakdown of technical communication systems, and theft of information media.

Figure 3.2 shows a structural system model of ICN risks, which shows the relationship between the elements of the main aspects of risk.

With the help of this model it is possible to determine the full set of cause-and-effect relationships from the causes of risks to their consequences and the impact on the main characteristics of ICN.

Risk assessment is performed in stages. At the first stage, a structural diagram is constructed, partial risks caused by their factors and possible consequences of risks are determined.

The relationship between these components is displayed in the form of a cause-and-effect diagram [116]. Since the number of relationships between risk factors and risk events is large, for clarity of further analysis, the relationship between the factors associated with their manifestations of risk and consequences will be presented in the form of tables (Tables 3.2 and 3.3).

3.3 Method for quantitative assessment of information risk of ICN

To quantify the impact of IR on the functioning of ICN, it is proposed to use a method based on the theory of causal analysis [117].

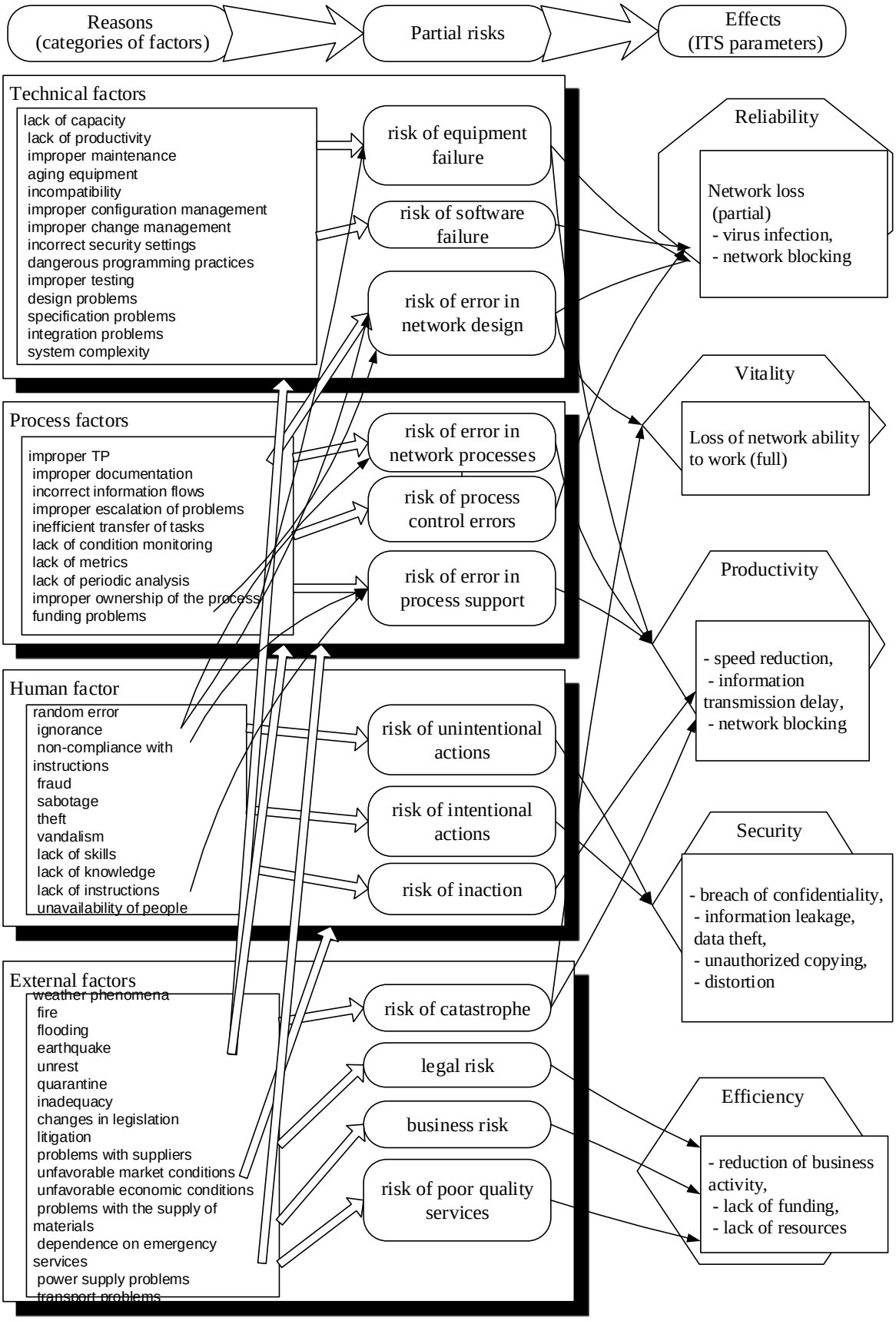


Fig. 3.2. Systemic risk model of ICN

Table 3.2 – Coefficients of influence of factors on partial risks of ICN (fragment)

Factors	**Partial risks**												
	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_1	R_{12}	R_{13}
P_{11}	$b_{11,1}$	$b_{11,2}$	-	-	-	-	-	-	-	-	-	-	-
P_{12}	$b_{12,1}$	$b_{12,2}$	$b_{12,}$	-	-	-	-	-	-	-	-	-	-
P_{13}	$b_{13,1}$	$b_{13,2}$	-	$b_{13,}$	-	$b_{13,6}$	$b_{13,7}$	$b_{13,8}$	$b_{13,9}$	-	-	-	-
P_{14}	$b_{14,1}$	-	-	-	-	-	-	-	-	-	-	-	-
P_{21}	-	$b_{21,2}$	-	$b_{21,}$	-	-	-	-	-	-	-	-	-
P_{22}	-	$b_{22,2}$	-	$b_{22,}$	-	-	-	-	-	-	-	-	-
P_{23}	-	$b_{23,2}$	-	$b_{23,}$	-	-	-	-	-	-	-	-	-
P_{24}	-	$b_{24,2}$	-	$b_{24,}$	-	-	-	-	-	-	-	-	-
P_{25}	-	$b_{25,2}$	-	$b_{25,}$	-	-	-	-	-	-	-	-	-
……													
P_{131}	-	-	-	-	-	$b_{131,}$	$b_{131,}$	$b_{131,}$	$b_{131,9}$	-	-	$b_{131,1}$	$b_{131,1}$
P_{132}	-	-	-	-	-	-	$b_{132,}$	$b_{132,}$	$b_{132,9}$	-	-		$b_{132,1}$
P_{133}	$b_{133,}$	-	-	-	-	$b_{133,}$	$b_{133,}$	$b_{133,}$	$b_{133,9}$	$b_{133,}$	-	$b_{133,1}$	$b_{133,1}$
P_{134}	-	-	-	-	$b_{134,}$	-	$b_{134,}$	$b_{134,}$	$b_{134,,}$	-	-		$b_{134,1}$

Table 3.3 – Coefficients of impact of risks on the consequences

Partial risks	**consequences**												
	Reliability		**Survivability**	**Productivity**			**Safety**				**Efficiency**		
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}
R_1	-	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	-	-	-	-	-	-	-
R_2	c_{21}	c_{22}	-	c_{24}	c_{25}	c_{26}	-	-	-	-	-	-	-
R_3	-	c_{32}	-	c_{34}	c_{35}	c_{36}	-	-	-	-	-	-	-
R_4	-	c_{42}	-	c_{44}	c_{45}	c_{46}	-	-	-	-	-	-	-
R_5	-	c_{52}	-	-	-	-	-	-	-	c_{510}	-	-	-
R_6	-	-	-	c_{44}	c_{45}	c_{46}	-	-	-	c_{410}	-	-	-
R_7	-	c_{72}	-	c_{74}	c_{75}	c_{76}	c_{77}	c_{78}	c_{79}	c_{710}	-	-	-
R_8	-	c_{82}	c_{83}	c_{84}	c_{85}	c_{86}	c_{87}	c_{88}	c_{89}	c_{810}	-	-	-
R_9	-	-	-	c_{94}	c_{95}	c_{96}	-	-	-	-	-	-	-
R_{10}	-	c_{102}	c_{103}	-	-	-	-	-	-	-	-	-	-
R_{11}	-	-	-	-	-	-	-	-	-	-	c_{1111}	-	-
R_{12}	-	-	-	-	-	-	-	-	-	-	-	c_{1212}	-
R_{13}	-	-	-	-	-	-	-	-	-	-			c_{1313}

The risk model in the form of a causal network can be based on the construction and analysis of probabilistic or fuzzy cognitive maps [118, 119]. The cognitive map is defined as a tuple of sets:

$$K = (\{P, R, S\}, F, \{B, C\}), \tag{3.1}$$

where $\{P, R, S\}$ – set of elements, in this case consists of three subsets (factors, risks, consequences);

F – set of connections between the elements;

$\{B, C\}$ – set of weights of these connections.

The cognitive map is transformed into a sign-oriented graph, at the vertices of which are the key elements of the modeling object, interconnected by arcs that reflect the causal relationships between them. These relationships characterize the degree (strength) of the elements on each other and are set using coefficients (which determine the probability of risk as a result of this factor, or the consequences of risk) or linguistic terms (which determine the degree of influence)

$$\begin{gathered} B = \{b_{j,i}\,,\ j = \overline{1,m}\,,\ i = \overline{1,n}\}, \\ C = \{c_{k,j}\,,\ k = \overline{1,h}\ \ j = \overline{1,m}\}. \end{gathered} \tag{3.2}$$

The values of $b_{j,i}$ and $c_{k,j}$ can be determined by objective (based on statistical data) or subjective method (by expert assessments) based on past experience.

The coefficient of influence of the factor on the occurrence of risk $b_{j,i}$ is determined based on the frequency of occurrence of this type of risk, based on statistical information or based on forecasting estimates. Recently, the reliability and security of the network are declining as a result of the following events (which relate to the risks of software failure and intentional actions): selection of keys / passwords (password attacks) – 13.9% of the total; IP address replacement (IP spoof-

ing) – 12.4%; denial of service (DoS-attacks) – 16.3%; traffic analysis (packet spoofing) – 11.2%; scanning (network error) – 15.9%; substitution of data transmitted over the network (data manipulation and software) – 15.6%; other methods (viruses and programs "Trojan horse") – 14.7% [96].

It is necessary to take into account the fact that not all ICN risks can be fully realized or implemented in this network at all; the same type of threat can cause significant or insignificant damage. Therefore, in order to make a decision on ICN risk management, it is necessary to determine the degree of influence that partial risk has on the performance characteristics of the network. [120].

The level of risk exposure $c_{k,j}$ can also be determined by experts on the following scale:

- 0 - the risk does not actually affect this characteristic of the network;
- 0.25 - the risk has little effect;
- 0.5 - the risk has a medium degree of impact;
- 0.75 - the risk is significantly affected;
- 1.0 - the risk has a direct impact.

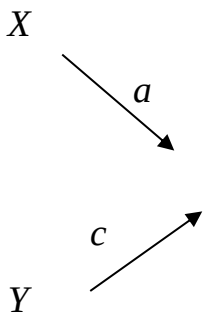
Knowledge of the structure of the causal system can be used to convert the statistical description of inputs into a description of outputs. To do this, we form a recursive system of equations, isomorphic to the structural diagram, the coefficients of which act as coefficients of influence [121]. You can draw a parallel between the structural factors of influence and the possibility of manifestation of specific events (factors, risks, consequences).

According to the theory of causal analysis, the following rules are followed when compiling equations.

1. The value of the variable, which is determined by one input, is equal to the value of the input multiplied by the structural factor.

$$X \xrightarrow{a} Y \quad \text{means} \quad Y = aX. \tag{3.3}$$

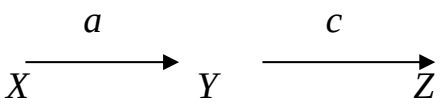
2. The value of a variable, which is determined by several input values, is equal to the sum of the input values multiplied by their structural coefficient. The order of summation does not matter.



$$Z = aX + Cy \qquad (3.4)$$

3. Ways that deviate from a variable when writing equations for this variable are not taken into account, but each incoming arrow indicates an element that must be taken into account.

Structural equations describe direct connections. In order to take into account indirect connections, reduction rules are used: if one variable defines the second variable and the other defines the third, then the value of the third variable can be expressed as the value of the first variable multiplied by the product of structural coefficients along the chain. The same principle applies when the circuit has more than two links.



(3.5)

means $Z = acX$.

The generalized structure of the causal diagram of the factors, manifestations and consequences of ICN risks is shown in Figure 3.3.

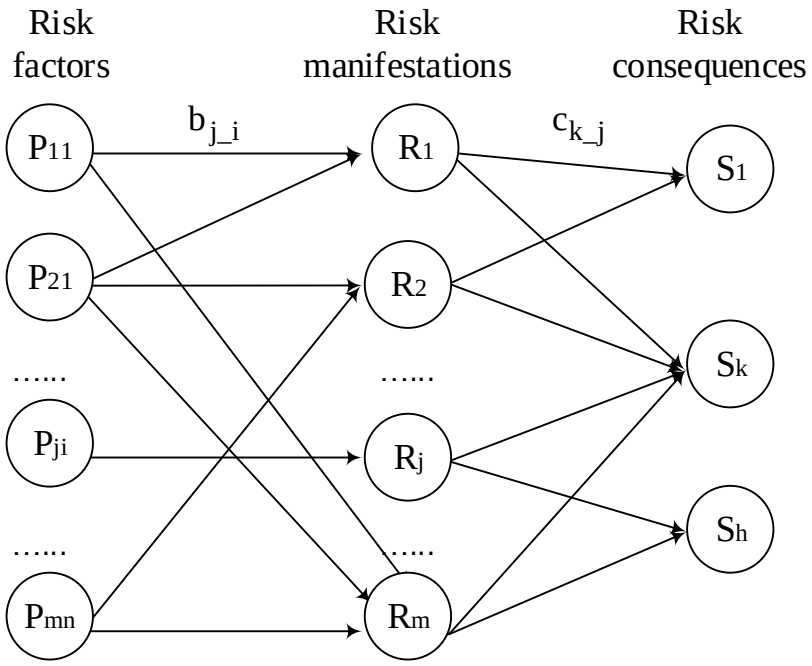


Fig. 3.3. Block scheme of the causal diagram

At the diagram

$b_{j,i}, 0 \le b_{j,i} \le 1$ – the coefficient of influence of the *i*-th factor on the occurrence of the *j*-th manifestation of risk;

$c_{k,j}, 0 \le c_{k,j} \le 1$ – the coefficient of influence of the *j*-th manifestation of risk on the *k*-th consequence.

Then the assessment of the possibility of the k-th consequence is carried out by the formula:

$$P(S_k) = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{j,i} c_{k,j} . \qquad (3.6)$$

For example, according to the setting of the system representation of risk, the possibility of the event "distortion of information" is determined according to the causal diagram (Fig. 3.5) and is calculated by the formula:

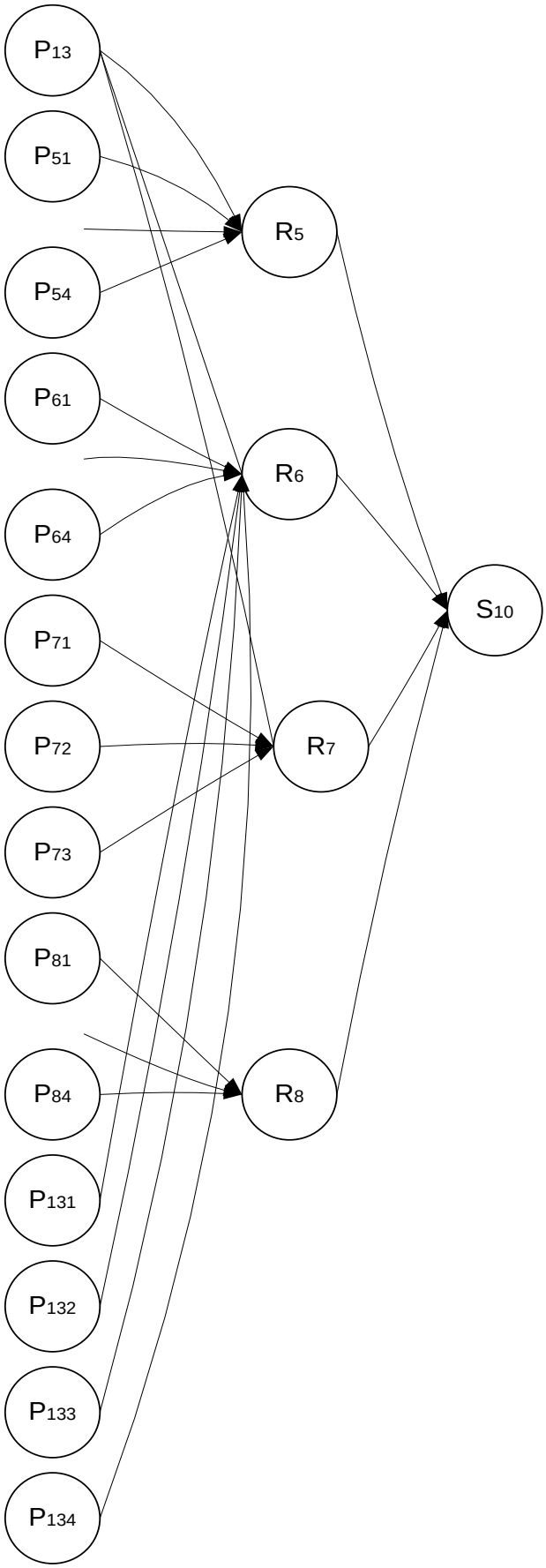


Fig. 3.5. Example of a causal diagram for the event "information distortion"

$$P(S_{10}) = c_{105}(b_{5,13} + b_{5,1} + b_{5,2} + b_{5,3} + b_{5,4}) + \\ + c_{106}(b_{6,13} + b_{6,1} + b_{6,2} + b_{6,3} + b_{6,4} + b_{13,1} + b_{13,2} + \\ + b_{13,3} + b_{13,4}) + c_{107}(b_{7,13} + b_{7,1} + b_{7,2} + b_{7,3}) + \\ + c_{108}(b_{8,13} + b_{8,1} + b_{8,2} + b_{8,3} + b_{8,4}). \quad (3.7)$$

Thus, knowing the degree of influence (in the form of coefficients of influence) of risk factors, risk events and consequences, as well as causal relationships between them, you can identify possible failures and losses in the operation of ICN.

The degree of possible negative impact on the functioning of the G_{kj} network is determined by the k-th consequence, which is caused by the j-th partial risk and is calculated based on the ratio [122]:

$$G_{kj} = P(S_k)H(R_j \rightarrow S_k)f_k, \quad (3.8)$$

where $P(S_k)$ – probability of the k-th consequence;

$H(R_j \rightarrow S_k)$ – the effect of the risk effect R_j on the characteristic S_j is given,

f_i – an indicator that reflects the value of the k-th characteristic.

3.4 Probabilistic models for assessing the risks associated with random online processes

In ICN using the IR protocol, there may be risks due to difficulties in traffic transmission. There may be risks of long delays in data transmission, reduced performance, which leads to reduced network performance. In addition, there is a possible risk of losing data packets.

The behavior of packets in the network, namely, such inherent parameters as the time interval between packets, the packet length of packets, etc., are adequately described by exponential distributions, such as Poisson distributions. This assumption is true for small networks and allows the use of classical methods of queuing

theory to calculate delays, average queue lengths and other network parameters. But with the growth of network size, increasing the diversity of network applications, the emergence of new protocols for data transmission in traffic behavior began to appear properties and features inherent in non-stationary and ergodic processes.

Therefore, to assess the above risks of data transmission of practical interest are methods of modeling random processes (RP), based on the one-dimensional distribution density *f (x, t)* and the correlation function *R(S, t)*. In the general case, when the distribution density is not Gaussian, the application of the method of nonlinear transformation causes difficulties due to the difficulty of determining the correlation function of the original normal random process. Other known methods (method of non-canonical representation and randomization) do not allow to obtain the implementation of RP ergodic relative to the given distribution density and correlation function. [123].

For modeling of random processes in ICN the combinatorial approach to modeling with the necessary density of distribution and correlation function is offered that allows to synthesize RP by one realization, or set of implementations. [124].

Let's consider the features and characteristics of strongly stationary and strongly ergodic random processes. Denote $\left\| x_i^{(k)} \right\|, k = \overline{1,\infty}, i = \overline{1,\infty}$-a set of discrete implementations of some VP, where $x_i^{(k)}$ is the *i*-th count in the *k*-th implementation, that is

$$x_i^{(k)} = x^{(k)}(i\Delta t), \tag{3.9}$$

where Δt – parameter sampling step.

Let θ is some probabilistic characteristic of RP (for example, it is a probability of risk of data loss). Since $x_i^{(k)}$ there are two indexes (implementation number and time), you can write the following estimates for θ:

$$\theta_t^{(l)} = \frac{1}{l} \sum_{k=l_t+1}^{l_t+l} g\left[x_i^{(k)} \right];$$

$$\theta_k^{(n)} = \frac{1}{n} \sum_{i=n_k+1}^{n_k+n} g\left[x_i^{(r)} \right]; \qquad (3.10)$$

$$\theta_{cp}^{(l,n)} = \frac{1}{ln} \sum_{k=l_t+1}^{l_t+l} \sum_{i=n_k+1}^{n_k+n} g\left[x_i^{(k)} \right];$$

where g[·] – data conversion operator.

We assume that $\theta_t^{(l)}, \theta_k^{(n)}, \theta_{cp}^{(l,n)}$ converge to some $\theta_t, \theta_k, \theta_{cp}$ for $l \to \infty$ i $n \to \infty$.

The process is *stationary* relative to θ, if $\theta_t =$ const; the RP is ergodic relative to θ, if $\theta_k =$ const. Obviously, if RP is stationary, then $\theta_t = \theta_{cp}$; if RP is ergodic, then $\theta_k = \theta_{cp}$; if RP is stationary and ergodic, then $\theta_t = \theta_k = \theta_{cp}$.

The process is *strongly stationary* relative to θ if $\forall n_k$

$$\theta_k^{(n)} = \theta_k + \varepsilon_{k,n}, \qquad (3.11)$$

where $\varepsilon_{k,n}$ is a random value with

$$M\left[\varepsilon_{k,n} \right] = 0 \quad \text{i} \quad D\left[\varepsilon_{k,n} \right] = \sigma_{k,n}^2 < \infty. \qquad (3.12)$$

The process is *strongly ergodic* relative to θ, if for any l_t

$$\theta_t^{(l)} = \theta_t + \varepsilon_{t,l}, \tag{3.13}$$

where $\varepsilon_{t,l}$ is a random value with

$$M\left[\varepsilon_{t,l}\right] = 0 \quad \text{i} \quad D\left[\varepsilon_{t,l}\right] = \sigma_{t,l}^2 < \infty. \tag{3.14}$$

It can be shown that the following statements occur:

1) the consequence of strong stationarity is stationarity;

2) the consequence of strong ergodicity is ergodicity;

3) if the random process is stationary and strongly ergodic, then it is strongly stationary;

4) if the process is strongly stationary and ergodic, then it is also strongly ergodic.

Formally, we can distinguish seven classes of RP in terms of characteristics θ:

- stationary ergodic (SE);
- stationary non-ergodic (S-NE);
- non-stationary ergodic (NS-E);
- non-stationary non-ergodic (NS-NE);
- strongly stationary strongly ergodic (SS-SE);
- strongly stationary non-ergodic (SS-NE);
- non-stationary strongly ergodic (NS-SE).

We will model a random process by synthesizing its characteristics on the basis of a single implementation. Let the process $x(t)$, $\{0 \le t \le T\}$ be given by the distribution density $f(x)$ and the correlation function $R(\tau)$ and the chosen sampling step

$$\Delta t = \frac{T}{m}. \tag{3.15}$$

The method of modeling the implementation of a random process ($x_1,...,x_m$) is to perform m steps sequentially. In the first step, a random number with a distribution density $f(x)$ is taken as x1. In step n ($n=\overline{1,m}$), the count is selected from the set

$$\Xi=\{\xi_i\}, i=\overline{1,l}, \tag{3.16}$$

containing at $n = 2l$ independent random numbers with a distribution density $f(x)$, so as to achieve a minimum of functional

$$\Phi^{(n)}=\sum_{k=1}^{u^{(n)}}\left(R[k]-R^{(n)}[k]\right)^2 \tag{3.17}$$

where $R^{(n)}[k]$– evaluation of the correlation function on the sequence ($x_1,...,x_N$);

$$R[k]=R(k,\Delta t); \tag{3.18}$$

$$u^{(n)}=\begin{cases} n-1, if\_n\le u; \\ u, if\_n>u; \end{cases} \tag{3.19}$$

u – the given number of samples of the correlation function on the correlation interval.

After choice

$$x_n=\xi_i\in\Xi \tag{3.20}$$

The element ξ_i is extracted from Ξ and in its place is put a new random number with density $f(x)$.

The construction process is strongly stationary and strongly ergodic in terms of distribution density and correlation function. Obviously, for l = 1, the imple-

mentation of RP proceeds from a correlation function that is identically equal to zero. It is recommended to choose the value of l so that $u < l << m$ is fulfilled.

Restrictions can be added to the task of minimizing the functional (3.16)

$$\left|x_{n-1} - x_n\right| < h, \tag{3.21}$$

where h – value that limits the scatter of neighboring samples of RP, which allows you to get smoother implementations.

Execution of inequality is understood in the probabilistic sense. The value of h can be determined experimentally.

The simulation error is calculated by the formula

$$\sigma_0 = \frac{1}{R[0]} \sqrt{\frac{\sum_{h=1}^{u^{(n)}} \left(R[h] - R^{(m)}[k] \right)}{u}}. \tag{3.22}$$

Based on modeling of vector stationary random processes

$$X(t) = \left\| x_1(t), \ldots, x_k(t) \right\|^T, \tag{3.23}$$

given by the vector one-dimensional distribution densities

$$f(t) = \left\| f_1(t), \ldots, f_k(t) \right\|^T \tag{3.24}$$

and correlation matrix $\left\| R_{ij}(\tau) \right\|, i = \overline{1,k}, j = \overline{1,k}$, and scalar homogeneous two-dimensional fields $\left\{ x(s,t), 0 \le s \le S, 0 \le t \le T \right\}$ given by the distribution density and correlation function

$$R(\lambda, v) = M[x(s, t)\, x(s + \lambda, t + v)], \qquad (3.25)$$

it is possible to assess the risks arising from these accidental events.

Consider the modeling of a random process by synthesizing its characteristics based on *a set of implementations*. Let the process $\{X(t), 0 \le t \le T\}$ be given by the distribution density $f(x)$ and the correlation function $R(s,t)$ and the selected sampling step $\Delta t = \frac{T}{m}$.

We will simulate l implementations simultaneously. Let's denote the n-th countdown in the i-th implementation as $x_n^{(i)}$. Consistently perform m steps.

Formally, at each step n, we define the counts $x_n^{(i)}$ in the form

$$x_n^{(i)} = \sum_{j=1}^{l} C_{ij}^{(n)} \xi_j^{(n)}, i = \overline{1,l}, \qquad (3.26)$$

where $\xi_j^{(n)}, j = \overline{1,l}$ – sampling of independent random numbers with density $f(x, n, \Delta t)$,

$C_{ij}^{(n)}$ – variables that are determined from the solution of the integer programming problem:

$$\min_{C_{ij}^{(n)}} \Phi^{(n)}(R, R^{(n)});$$

$$\sum_{j=1}^{l} C_{ij}^{(n)} = 1; \sum_{i=1}^{l} C_{ij}^{(n)} = 1; \qquad (3.27)$$

$$C_{ij}^{(n)} \in \{0,1\}; i, j = \overline{1,l},$$

where R – given correlation function;

$R^{(n)}$ – estimation of the correlation function on the array $\left\| x_i^{(k)} \right\|, k = \overline{1,l}, i = \overline{1,n}$.

Depending on how the correlation function is determined - by implementation:

$$R_i^{(n)}[k] = \frac{1}{n-k} \sum_{j=1}^{n-k} \left(x_j^{(i)} - m \right) \left(x_{j+k}^{(i)} - m \right);$$
$$m = \int_{-\infty}^{\infty} x f(x,t) dx = m_t = const, \tag{3.28}$$

or behind the ensemble:

$$R[n-k,n] = \frac{1}{l} \sum_{i=1}^{l} \left(x_{n-k}^{(i)} - m_{n-k} \right) \left(x_n^{(i)} - m_n \right);$$
$$m_i = \int_{-\infty}^{\infty} x f(x, i\Delta t) dx, \tag{3.29}$$

functional (3.26) can be written accordingly in the form

$$\Phi^{(n)} = \sum_{i=1}^{l} \sum_{k=1}^{u^{(n)}} \left(R[k] - R_i^{(n)}[k] \right)^2, R(s,t) = R(t-s), \tag{3.30}$$

or

$$\Phi^{(n)} = \sum_{k=1}^{u^{(n)}} \left(R[n-k,n] - R[n-k,n] \right)^2, \tag{3.30}$$

where $u^{(n)} = \begin{cases} n-1, if\_n \le u; \\ u, if\_n > u; \end{cases}$

u – a given number of samples of the correlation function on the correlation interval.

Under the solution of task (6.3) we understand such a solution that provides a representation of the estimate of the correlation function in the form

$$R^{(n)} = R + \delta_n, \tag{3.31}$$

where δ_n is a random value with $M\left[\delta_n\right] = 0$ i $D\left[\delta_n\right] = \delta_n^2 < \infty$.

Let at the first step $C_{ij}^{(1)} = 1$, if $i = j$ and $C_{ij}^{(1)} = 0$, if $i \neq j$.

The random modulated process is structurally stationary and ergodic with respect to the distribution density, or is strongly stationary and strongly ergodic with respect to the correlation function if taken (3.29), or stationary and ergodic if taken (3.30). Thus, taking into account the form of the process that causes a particular type of risk, you can calculate the characteristics of the random process and assess the probability of risk.

4 RISK MANAGEMENT OF THE INFORMATION COMMUNICATION NETWORK AND IMPROVEMENT OF THE SECURITY OF CRITICAL INFRASTRUCTURE SYSTEMS

4.1 Baseline risk-paring measures and mechanisms for improving the safety of CISs

In preparing for the selection and identification of appropriate information risk matching measures for the ICN and the relevant CIS environment, the level of criticality and sensitivity of the information to be processed, stored or transmitted over the network should first be determined.

Risk categorization is based on the concept of identifying potential adverse effects for ICN. A complex indicator for determining the risk category of the information system is a tuple of values:

$$SC = \{KF, IN, AC\}, \quad (4.1)$$

where *KF* – the degree of influence of the characteristic "confidentiality of information" on the security of the system;

IN – degree of influence of the characteristic "integrity of information";

AC – degree of influence of the characteristic "availability of information".

These indicators of the degree of influence can take linguistic values from the plural "low", "moderate", "high".

Table 4.1 shows the variants of the total factor space of the set of values of these features and the corresponding risk categories of information systems.

A low-impact system is defined as an information system in which all three categories of security risk are low. Moderate impact system is an information system in which at least one of the categories of absorption is moderate, and there is no category of impact greater than moderate.

Table 4.1 – Risk categories of the system, taking into account the options for the degree of influence of the main characteristics of the information

№	*KF*	*IN*	*AC*	**CIS risk exposure categories**
1	«low»	«low»	«low»	Low impact system
2	«low»	«low»	«moderate»	Moderate impact system
3	«low»	«moderate»	«low»	
4	«low»	«moderate»	«moderate»	
5	«moderate»	«low»	«low»	
6	«moderate»	«low»	«moderate»	
7	«moderate»	«moderate»	«low»	
8	«moderate»	«moderate»	«moderate»	
9	«low»	«low»	«high»	High impact system
10	«low»	«moderate»	«moderate»	
11	«low»	«high»	«low»	
12	«low»	«high»	«moderate»	
13	«low»	«high»	«high»	
14	«moderate»	«low»	«high»	
15	«moderate»	«moderate»	«moderate»	
16	«moderate»	«high»	«low»	
17	«moderate»	«high»	«moderate»	
18	«moderate»	«high»	«high»	
19	«high»	«low»	«low»	
20	«high»	«low»	«moderate»	
21	«high»	«low»	«high»	
22	«high»	«moderate»	«low»	
23	«high»	«moderate»	«moderate»	
24	«high»	«moderate»	«high»	
25	«high»	«high»	«low»	
26	«high»	«high»	«moderate»	
27	«high»	«high»	«high»	

High impact system is an information system in which at least one category of influence is high.

When choosing the basic sets of measures to parry risks should take into account:

- the environment in which ICN operates;
- type of operation used by CIS;
- functional processes in ICN;
- types of threats aimed at CIS, its functioning processes;
- types of information processed, stored or transmitted by ICN.

The following features should also be considered:

- whether there are insider threats in the CIS;
- whether classified data are processed, stored or transmitted on the network;
- whether there are constant threats to the CIS;
- whether the information requires specialized protection based on state legislation, directives or regulations;
- whether the CIS should interact with other systems through different security domains.

Once the basic set of risk response measures has been selected, an adaptation process is needed to change the measures accordingly in line with the specific conditions of the CIS. The adaptation process includes the following stages:

1) identification and definition of general measures for parrying risks in the initial set of basic measures;

2) application of system features to other measures of the basic set;

3) if necessary, the choice of compensatory measures;

4) assignment of specific values of parameters of measures by explicit appointment or choice;

5) supplementation of basic sets with additional measures and, if necessary, their improvement;

6) if necessary, provide additional specific information for the implementation of measures to counter risks.

The process of adaptation, as an integral part of the selection and specification of risk response measures, is part of the process of ICN risk management - identification, assessment and monitoring of information risk.

Taking into account external conditions requires determining the factors of their influence. General factors include the following aspects:

1. Mobility of the physical location environment. If the information system operates in mobile environments, the basic set of risk-matching measures should be adapted accordingly, taking into account differences in mobility and availability of specific nodes of the distributed system.

2. Data transmission and bandwidth are important for systems that have limited or sporadic bandwidth.

3. Functionality of systems or system components is limited.

4. Variability of information and systems for some applications and operating environments in which the constancy of user information is limited in duration. Information services may also be volatile due to virtualization technologies for temporary installations of operating systems and applications.

5. Open access. Security measures such as failed login attempts, remote access, identification, and authentication may be required for system personnel who maintain and maintain an information system that provides open access websites and services. Restrictions on the use of information systems and specific information technologies may apply in some situations.

Examples of the use of restrictions include:

- restriction of information that information systems can process, store and transmit;

- prohibition of external access to SKI information by removing selected components of the information system from the networks;

- prohibition of moderate or high-value information in the components of information systems to which there is public access, if there is no obvious risk in authorizing such access.

Figure 4.2 shows a diagram of the process of selecting measures to parry risks, which contains the stages of selection of the initial base set and its adaptation.

The functional security of ICN is assessed and ensured in the process of forming the network structure taking into account special tools and processes, and cannot be violated by external factors.

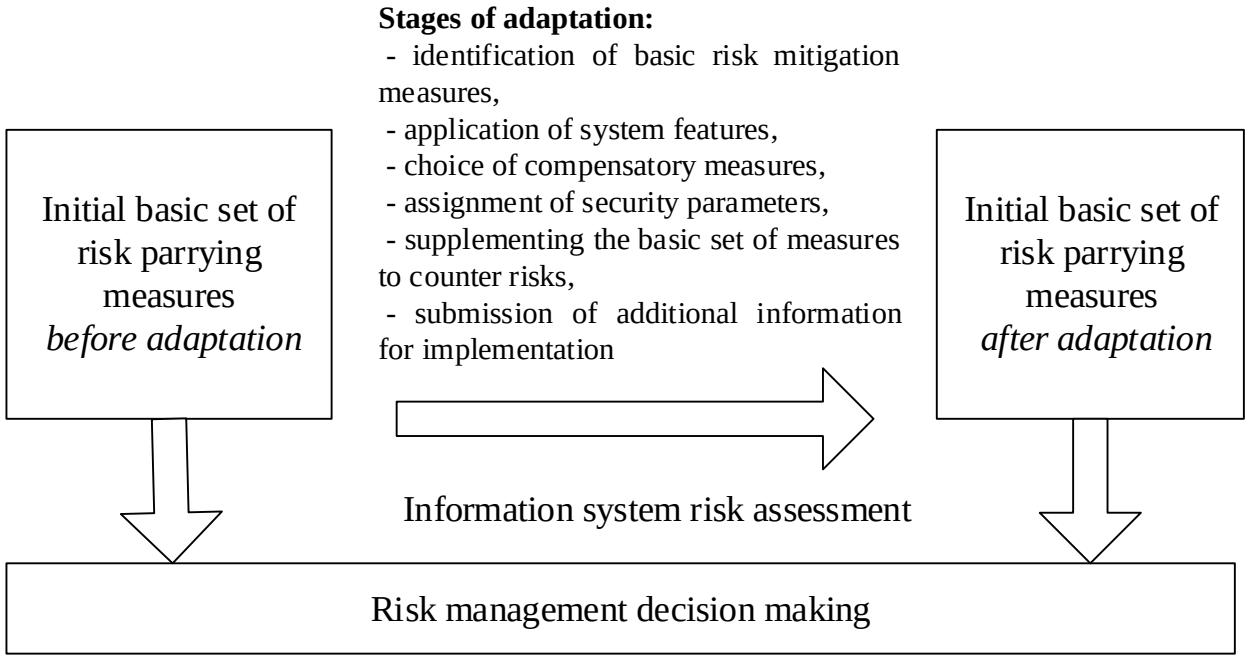


Fig. 4.2. Scheme of the process of selecting information security measures

Implementation of a reliable network is possible by:

- use of high-quality software and hardware components,
- making informed decisions to increase reliability and fault tolerance,
- introduction of uninterruptible power supplies,
- redundancy of critical components,
- application of dynamic reconfiguration mechanisms,

- the use of special means to increase survivability.

The security of the information resource implies the impossibility of its loss due to failures of the components of the information environment. Therefore, secure work with the information resource requires:

- providing a highly reliable computer base (TCB - Trusted Computing Base), which should guarantee the continuity of the information environment,

- creation of a system for counteracting and preventing threats to information resources (IR).

To ensure the security of IR in distributed systems, it is necessary to create technologies for secure work with the information resource for its entire life cycle based on the analysis of possible risks, features of storage, processing and transmission of information.

Information security of ICN can be ensured by the following strategies:

- defense strategy, which aims to autonomously confront the known threats that are most likely for this system;

- offensive strategy, which involves the use of active means of combating expected threats, using the capabilities of the information environment;

- a proactive strategy that requires the creation of such an information environment in which threats do not have the conditions for their manifestation.

The technology of safe work with the information resource depends on the study of the information model, the definition of many threats, the quality of decisions made on the hardware and software of the CIS.

Perimeter technology involves the construction of a perimeter around the ICN, through which all traffic is passed only after careful inspection [125]. This technology requires the integration of various types of protection, combining them into a single structure with a multi-level organization, which provides an increase in the overall level of security and control over information. The necessary components of the technology are firewall, directory service, and router, content filtering software (from viruses, malicious code, e-mail filters, and web-resources for managing web-access channels).

More effective for ICN is the technology of adaptive protection systems, which are focused on actively confronting security threats [126, 127]. The implementation of such an approach requires risk analysis, development of security policy, use of traditional means of protection, as well as the introduction of countermeasures to counter threats, continuous security audit and monitoring of the system, which should allow to respond quickly to risks security. The main tools used in the implementation of adaptive protection systems are passive - filters, screens, and active – intrusion detection sensors, algorithms for recognizing abnormal behavior, adaptive recovery algorithms.

Among the mechanisms to increase the survivability of the distributed system are mechanisms [128, 129]:

- reconstruction;
- reorganizations;
- reconfiguration;
- recognition;
- counteraction;
- recovery;
- adaptations.

These mechanisms to ensure the viability of the CIS are accordingly implemented by:

- monitoring and recognition of the state of the system and environmental influences;
- adaptation when changing conditions to optimize the functioning of the system in accordance with the specified criteria;
- resumption of operation after failures, failures, errors;
- redistribution of system resources to fulfill the purpose of its operation in the new conditions.

Recognition mechanisms allow, on the basis of system and environment monitoring data, to identify potentially dangerous conditions and soon respond adequately to them.

Countermeasures are aimed at maintaining certain operating conditions and minimizing the losses that are possible due to the emergence of new operating conditions and unforeseen impacts. They are based on classical methods of ensuring the security, reliability and fault tolerance of information systems, including redundancy of critical components, control of access and use of system resources, prevention of virus attacks, etc.

Adaptation mechanisms make it possible to adapt to external changes in the environment of the system, compensating for adverse effects and allowing the system to optimize its work in accordance with established criteria.

Recovery mechanisms provide restoration of functionality and operability of components and system as a whole at undesirable influences, and also after the termination of influences. They must identify and locate faults, correct errors in programs and data, set time delays, reallocate resources between processes, replace and disable faulty elements, repair, log observations and actions performed, and actually resume or complete a sequence of operations.

Reorganization mechanisms provide a redistribution of the functions of the failed system components between the operational components of the system.

Reconfiguration mechanisms implement automatic restructuring of the structure of the information exchange network to achieve the greatest efficiency in fulfilling the purpose of operation on the available operational resources of the system.

Reconstruction mechanisms reduce the purpose of the system and the resources of the system to certain base levels, when the system can perform a clearly defined set of functions, or ensure the smooth degradation of certain parameters.

Implementation of mechanisms to increase survivability in a distributed information system requires risk analysis, taking into account its features and objectives.

Monitoring the state of the system by recognition mechanisms and means of counteraction will allow to recognize and promptly respond to risks. To increase

the security of the information resource in distributed systems, the following functions are required:

- detection of unauthorized activities (intentional or accidental) and prevention of possible consequences in real time;
- prevention of hacker attacks on critical applications and system services;
- performing a given sequence of appropriate actions when detecting attempts to invade the system;
- registration of system users' activity and analysis of the received data in order to prevent further attempts to violate the security policy according to already known schemes;
- analysis of the existing system configuration in order to identify and eliminate vulnerabilities.

Due to the use of reconfiguration mechanisms can be performed:

- automatic reconfiguration of firewalls, routers, switches and other means to repel the attack on the ICN in real time;
- creation of border and prevention of the further penetration of a towel into a network;
- dynamic formation of a reliable configuration of security systems for different user groups in accordance with their powers.

4.2 Reducing the risk of equipment failure based on a diagnostic model

To reduce the risk of equipment failure at ICN nodes, it is proposed to use algorithms for determining the technical condition of objects - diagnostic algorithms. These classes of algorithms are based on diagnostic models. Diagnostic models (DM) are models of objects and diagnostic processes, ie their formalized descriptions, which are the initial ones for defining and implementing diagnostic algorithms [130].

Methods of model construction are divided into functional-logical, analytical, graph-analytical, informational and special. The tabular form of diagnostic models is convenient for perception [131].

The tabular model for assessing the risk of equipment failure at ICN nodes is a rectangular table, in the rows of which - the corresponding valid basic checks, ie signs X_i in the control points of the object, and in the columns - technical states C_i node in the set C (Table 4.3) [132].

Table 4.3 – Diagnostic model in the form of a fault matrix

X/C	C_0	C_1	C_2	. . .	C_n
X_1	0	R_{11}	R_{12}	. . .	R_{1n}
X_2	0	R_{21}	R_{22}	. . .	R_{2n}
. . .	. . .	. . .	. . .	. . .	
X_k	0	R_{k1}	R_{k2}	. . .	R_{kn}

In the cell of the table located at the intersection of row X_i and column Ci, the results of the elementary check of the node in the state Cj are put down. If when checking the sign X_i it is in the tolerance for the node in the state C_j, the test result is given the value $R_{ij} = 0$. If the sign Xi is not in the tolerance, then $Rij = 1$. In the column C_o table 4.3 are marked all the results of checks equal to 0, because this column corresponds to the operational state of the network. Although the most common model is tabular, its use is not always convenient in the development and analysis of diagnostic algorithms to assess the possible risks of network equipment failure.

Let's analyze the diagnostic model presented in table. 4.3, using an algebraic approach. To do this, we present the diagnostic model $A(X,C)$ in the form

$$A(x) = C_0^{U_0} \vee C_1^{U_1} \vee ... \vee C_i^{U_i} \vee ... \vee C_k^{U_k}, \qquad (4.2)$$

where $C_i^{U_i}$ – the *i*-th state identification operator, performed at $U_i = 1$

$$U_i = X_1^{\Theta} ... X_j^{\Theta} ... X_n^{\Theta}; \tag{4.3}$$

$$X_j^{\Theta} = X_j \text{ at } R_{ij} = 1 \text{ i } X_j^{\Theta} = \overline{X_j} \text{ at } R_{ij} = 0.$$

Since all conjunctions U_i have the same rank equal to *n*, representation (4.1) corresponds to a perfect disjunctive normal form of the algorithm (PDNFA). The peculiarity of PDNFA diagnostic models is that they are operator-unique [133]. Indeed, all operators correspond to the identification of a certain state of the object. States should be visible, and this is possible only if they will meet different conjunctions.

If $k + 1 < 2^n$, then on $(2^n - k - 1)$ sets that are not included in the PDNFA, the algorithm is not defined, because in the case of proper operation of diagnostic tools, these sets are impossible or the identification process can be performed by a smaller number of inspections, and the results of other inspections are insignificant.

Consider an example for six subnet nodes that are tested on four parameters. Construct an algorithmic position diagram (APD) for the fault matrix presented in table 4.4.

Table 4.4 – Example of a diagnostic model

X/C	C_0	C_1	C_2	C_3	C_4	C_5	C_6
X_1	0	1	0	0	1	0	1
X_2	0	0	1	0	1	1	0
X_3	0	1	0	1	0	1	0
X_k	0	0	0	0	1	1	1

The algorithmic position diagram corresponding to the fault matrix is shown in Figure 4.3.

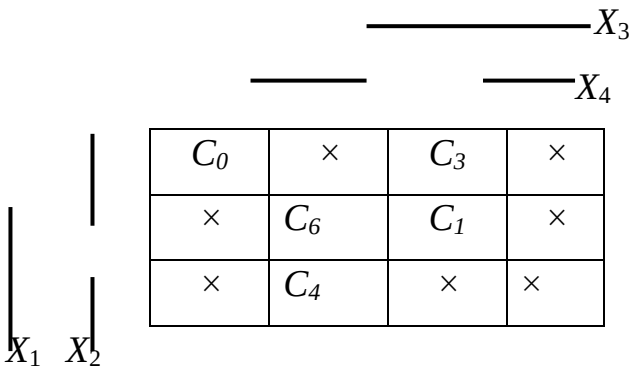


Fig. 4.3. Algorithmic position diagram corresponding to the fault matrix

When constructing a minimum control or diagnostic test, a subset of conditions (tests) with certain properties is searched for [134]. Conditions not included in the test are excluded from consideration, and APD for the conditions included in the test are formed as follows.

Let:

X – a set of parameters for diagnosis, $x_i \in X,\ i = \overline{1,n}$;

T_1 – a set of parameters (factors) that are significant for the risk of failure, $t_{1j} \in T_1,\ j = \overline{1,l}$;

T_2 – a set of parameters that are insignificant, $t_{2j} \in T_2,\ j = \overline{1,n-l}$.

Then

$$A(X) = A_1(H_1) \vee \ldots \vee A_i(H_i) \vee \ldots \vee A_w(H_w), \qquad (4.4)$$

where H_i – all possible options for setting insignificant parameters,

$w = 2L$.

Analysis of the construction of the APD for different algorithms showed that with the help of the APD it is convenient to evaluate the effectiveness of diagnostic

algorithms and choose those that meet the specified requirements. For this purpose it is necessary to consider possible options of adjustments and to estimate quantity of the states of the object which are identified.

The specificity of diagnostic algorithms is that after the identification of the state of the object of diagnosis, the execution of the algorithm ends. Diagnostic algorithms have the form of a tree composed of conditions on the end branches of which are placed operators to identify the state of the object.

The second feature of diagnostic algorithms is the absence of linear operators between conditional operators and in the scheme of the algorithm there is only one node that corresponds to the final vertex of the algorithm.

Consider the properties of polynomial forms of diagnostic algorithms. To identify the technical condition of the object, diagnostic algorithms must have the properties of detection and recognition. Therefore, the structure of the diagnostic algorithm must have the number of output branches of the conditional part of the algorithm, equal to the number of states of the object.

For each linear operator that corresponds to the identification of the state, a route is defined, and it is located on the output branch of the algorithm. Therefore, the number of routes must correspond to the number of states being identified. In the polynomial form of the algorithm, the coefficients at different degrees X indicate the number of routes of a given length, so the number of routes should be equal to the number of states of the object of diagnosis.

Analysis of polynomial forms of diagnostic algorithms shows that in the General case there are many variants of structures having the same sum of coefficients, for example:

$$M_1 = 2X^4 + X^3 + X^2 + X;$$

$$M_2 = 2X^3 + 3X^2; \qquad (4.5)$$

$$M_3 = 4X^3 + X.$$

The degree of the polynomial indicates the maximum length of the route, so when developing a diagnostic algorithm, it is necessary to choose the structure with the smallest depth from a set of options.

In order to assess the probability of the risk of equipment failure at ICN units, in addition to diagnostic tests, statistical data on equipment failures that have occurred for reasons that may be detected during diagnosis should be used. The magnitude of the probability of risk of equipment failure according to the diagnostic model can be determined by the formula [135]:

$$R_1 = \lambda_s V_t \sum_{j=1}^{l} f_j \,, \tag{4.6}$$

where λ_s – average actual failure rate of equipment for the previous period of operation;

V_t – probability (reliability) of detection of defects and damages of the equipment at diagnosing (it is defined as a result of application of diagnostic algorithm, for example, on tab. 4.4);

f_j – coefficients that take into account the influence of testing parameters (their significance) on the occurrence of equipment failures.

As an assessment of the effectiveness of diagnosing equipment to reduce the risk of network failure, it is proposed to use the risk reduction factor determined by the expression

$$C_v = \lg\left(\frac{1}{\Delta R}\right), \tag{4.7}$$

where ΔR – the magnitude of the reduction in the probability of failure after the application of the diagnostic test equipment.

This ratio indicates the effectiveness of the measures taken to reduce the objective technical risk of ICN by monitoring and recognizing the state of the system.

4.3 Adaptive method for reducing the risk of error in the communication channels of the ICN

The adaptive procedure for calculating the linear decision functions helps to increase the noise immunity of reception in data networks, thereby reducing the risk of errors in the operation of ICN. In critical systems, the data transmission process is often provided with the use of encryption (encryption) algorithms, so in such systems the information is very sensitive to noise and interference of various natures (both due to the characteristics of the equipment and external threats). [136].

The size of the decision uncertainty zone of the first decision scheme affects the noise immunity of reception in data networks. The level of the threshold of the erasing channel and the size of the erasure zone are clearly related to the probabilities of transformation and erroneous erasure. The method of increasing the noise immunity of reception in conditions of uncertainty, proposed by Chase [137], offers the ordering of the received symbols according to their reliability and the choice of up to 10 least reliable symbols for special processing. This procedure is called "chasing" and is used mainly for decoding in communication channels with a fairly low noise level. Chasing is a general method by which the characteristics of almost any block code decoding algorithm can be improved by additional time. However, this method of non-rigid decision-making does not solve the problem of selecting and adjusting the threshold level in the process of receiving information in real ICN communication channels, which are affected by strong weakly correlated interference due to excessively erased symbols or replacing forbidden combinations allowed in chasing. The errors of the final decoding result are due to the suboptimal choice of the threshold of the first decision scheme.

Some methods of choosing the threshold level of the decision scheme are reduced to solving the problem of system optimization, in particular methods of optimizing the threshold level according to the Neumann-Pearson criteria, as well as the minimum and maximum [138]. However, the practical application of these

methods in real ICN does not allow to achieve the desired theoretically calculated positive effect, and the influence of non-stationary interference in communication channels makes it difficult to regulate the threshold level during reception. Thus, methods of increasing the noise immunity of reception, based on the use of the erasure signal, require solving the problem of optimizing the threshold level of the first decision scheme, ie minimizing the probabilities of transformation and erroneous erasure with any changes in communication channels [139]. The mathematical formulation of the problem is reduced to solving the problem of automatic classification: it is necessary to assign the vector x to one of the s classes of the set $\{w_i\}$, and the components of the vector x are a "summary" of the observed object. The simplest non-trivial mathematical formulation of this problem arises in the case when $s = 2$ (due to the discreteness of the signal that takes the value "0" or "1") and the linear decision function

$$f(x) = xw^T + const, \tag{4.8}$$

refers the vector x to the class w_1 for $f(x) > 0$ and to the class w_2 for $f(x) < 0$ with an admissible small number of incorrect classifications. The procedure for calculating linear decision functions must be adaptive (ie respond to any changes in the interference situation in communication channels, quickly converge to the local minimum of error and be performed without a priori assumption about the type of statistical distribution of vectors x in each class w_i [140].

Let's denote:

$x = (x_1, ..., x_d)$ – d-dimensional vector of signs, where $-\infty < x_i < \infty$;

$y = (y_1, ..., y_d)$ – additional sign vector;

$X(n)$ and $Y(n)$ – vector random variables that are functions of the step number n and are based on the learning sequence in the corresponding spaces x and y;

$w(n)$ - the class to which belongs $Y(n)$;

$w = \{w_i\}$ – alphabet classes (in our case $w = \{w_1, w_2\}$);

$V(n)$ – vector random variable set recursively in this way:

$$V(n+1) = V(n) + \rho_n Q(n), \tag{4.9}$$

where ρ_n – the magnitude of the *n*-th step,

$$Q(n) = \begin{cases} Y(n) \_ \text{if\_} w(n) = w_2 \\ -Y(n) \_ \text{if\_} w(n) = w_1 \\ 0 \_ \text{in\_other\_cases} \end{cases}. \tag{4.8}$$

Expression (4.7) is a kind of implementation of the gradient descent method [141], in which the minimum of the loss function *J(v)* is sought, ie the procedure of finding such a minimum is reduced to determining the recursive function *V(n)*, which converges (stochastically) to zero of the loss function gradient *J(v)*. Such a recursive function can be obtained by stochastic approximation methods:

$$J(v) = E\left(-v^T Q \mid V = v\right). \tag{4.10}$$

We obtain for (4.9) another expression that leads directly to the adaptive procedure:

$$f_i(x) = p(w_i)\, p(x / w_i), \tag{4.11}$$

where $p(w_i)$ – a priori probability that $w = w_i$,

$p(x / w_i)$ – conditional distribution density $X = x$ at $w = w_i$.

Let ϑ_i there is a solution area corresponding to the class w_i, then (4.10) can be written as

$$J(v) = |w|\left[M_1(v) + M_2(v)\right], \tag{4.12}$$

where $|w|$ is the length of the vector w;

$$M_1(v) = P(w = w_1, y \in \vartheta_2) E\left(\frac{v^T y}{w} \,|\, V = v, w = w_1, y \in \vartheta_2 \right), \quad (4.13)$$

$$M_2(v) = P(w = w_2, y \in \vartheta_1) E\left(-\frac{v^T y}{w} \,|\, V = v, w = w_2, y \in \vartheta_1 \right). \quad (4.14)$$

Let's take into account that $\frac{v^T y}{|w|}$ – distance between x and the area border ϑ_2, which is a hyperplane. This distance is positive at $x \in \vartheta_2$. Similarly, the magnitude $-\frac{v^T y}{|w|}$ is the distance between x and the boundary of the area ϑ_1, which is a hyperplane. This distance is positive at $x \in \vartheta_1$. For the case of two classes, both boundaries coincide. Thus, $M_i(v)$ is the first error point of the function $f_i(x)$.

Although this procedure is asymptotically accurate for linearly separate conditional class densities $\{ p(x / w_i) \}$, its asymptotics can differ significantly from the minimum probability of error in the case of overlapping densities. On the other hand, the minimum sum $M_1(v) + M_2(v)$ occurs at some value of $v(v_e)$, which is often very close to that which provides the minimum probability of error of the value $(v - v_p)$. Indeed, when $f_1(x)$ and $f_2(x)$ are symmetric with respect to each other and, therefore

$$f_2(x) = f_1(b - x), \quad (4.15)$$

where b is a centroid $f_1(x) + f_2(x)$, then v_e and v_p coincide.

Introduction |w| the expression for $J(v)$ (4.12) as a multiplier makes it possible to make a significant distribution of the minimum points of the functions $J(v)$ and $v(p)$, even when v_e and v_p coincide. The use of (4.12) also leads to a shift of $W(n)$ towards small values of the vector w at $n \to \infty$, since $J(v) = 0$ with $v = 0$. As a result, the direction of the vector $W(n)$ often becomes insufficiently defined. Thus, the asymptotic behavior of this procedure with a proportional increase may be un-

satisfactory in cases where the densities, conditional on the class, overlap. To overcome this shortcoming of the procedure, the loss function is used

$$J(v) = M_1(v) + M_2(v). \tag{4.16}$$

Suppose that a continuous differentiable function *J(v)* has a single minimum that is achieved at a value of *v** and it has no local minima. The basic gradient descent procedure for such a function *J(v)* is a recursive equation

$$v_{n+1} = v_n - \rho_n \nabla J(v_n), \tag{4.17}$$

where $\nabla J(v_n)$ is a gradient $J(v_n)$.

Then for any sufficiently small ρ_n sequence $\{J(v^*)\}$ will be monotonically descending, which converges at $n \to \infty$ to $J(v^*)$. For the case of "noisy" functions, ie functions $J(v)$ that depend on one or more random variables, it is necessary to use a stochastic approximation. Then the stochastic convergence $\{V(n)\}$ to v^* depends on the choice, the random variable $Z(n)$ and the registration functions. For example, if ρ_n decreases too fast with increasing *n*, then *V(n)* does not converge to *v**.

The described adaptive procedure is used for communication systems in order to optimize the threshold level of the first BC of the binary erasing channels by developing on its basis a control effect proportional to the change of the input parameters of the demodulated signal. This minimizes the probability of transformation and erroneous erasure of the symbol when changing the noise situation in the communication channel, which increases the noise immunity of the reception as a whole and reduces the risk of errors in data transmission.

5 INFORMATION TECHNOLOGY MANAGEMENT OF INFORMATION COMMUNICATION NETWORK OF CRITICAL INFRASTRUCTURE SYSTEM

5.1 Common issues of software synthesis of critical infrastructure systems

The experience gained so far in the development of software (software) of CIS shows that this is a complex and time-consuming work that requires highly qualified specialists. However, to date, the creation of such software is often performed on an intuitive level using informal methods based on practical experience, expert evaluations and valuable experimental inspections of the quality of software. According to the Software Engineering Institute (SEI), in recent years up to 80% of all software used has been developed without the use of any design discipline at all, using the «code and fix" method (coding and error correction).

Problems of creation of CIS software are caused first of all by system features of object:

- structural complexity (multilevel hierarchical structure of the system) and territorial distribution;
- functional complexity (multilevel hierarchy and a large number of functions, complex relationships between them);
- information complexity (a large number of sources and consumers of information, various forms and formats of information presentation, a complex information model of the object - a large number of information entities and complex relationships between us), complex technology of documents;
- complex dynamics of behavior due to the high variability of the external environment and the internal environment.

In addition, the complexity of the software is due to the technical characteristics of the CIS:

- technical complexity due to the presence of a set of closely interacting components (subsystems) that have their own local tasks and objectives. For example, transactional add-ons that place increased demands on reliability, security, and performance, and analytical processing applications are decision support systems that use unregulated requests for large amounts of data;

- the lack of complete analogues, which limits the possibility of using any standard design solutions and application systems, and causes most of the newly developed software;

- a large number and high cost of legacy applications (existing special software) that operate in different environments – automated workstations, central computer systems, special technical systems. This necessitates the integration of legacy and new applications;

- a large number of local implementation objects, geographically distributed and heterogeneous operating environment (DBMS, operating systems, hardware platforms);

- a large number of external interacting systems with different formats of information exchange.

The software development life cycle can be represented with varying degrees of detail. At the consolidated level, the life cycle can include only three stages: analysis, design, implementation.

The analysis phase focuses on system requirements. Requirements are defined and specified. Functional models and data modules for the system are being developed and integrated.

The design stage is divided into two main sub-stages: architectural and detailed design. Design issues that affect the clarity, adaptability and scalability of the system are raised and recorded.

The implementation phase includes writing client application programs and database servers. The emphasis is on iterative implementation processes with increasing system capabilities.

One of the main characteristic software is the hierarchy and complex structural and functional relationships between the elements of the system. The structure of the software means its organization of individual elements with their relationships, which are determined by the distribution of functions and tasks performed by the software.

The problem of synthesis of CIS software structure means:

- determining the optimal composition and relationships of software elements, the optimal division of the set of tasks into separate subsets with the specified characteristics of the links;
- selection of the number of levels and subsystems;
- choice of principles of management organization;
- optimal distribution of tasks to be solved between the means of computer technology.

If in the process of synthesis for some elements there are problems of high load, it is necessary to consider the rules of operation of these elements.

Thus, in the synthesis of the structure of the software of CIS is the choice of management tasks assigned to the technical means, algorithms for their implementation, the distribution of selected tasks by nodes (levels) of ICN.

The functions of the CIS software are presented in the form of a set of interrelated tasks, which, in turn, can be divided into a set of operations and procedures.

When formalizing the relationships between tasks, stages or operations, it is necessary to take into account the order in which they follow, as well as the flows and volumes of information exchange. In the general case, the relationship between the tasks is set in the form of some operator, which determines, depending on the moments of the previous operations, the moments of the next.

Thus, the task of synthesizing the structure of the software CIS is to reflect in a certain way grouped tasks solved by the software in a certain way grouped ICN nodes, which achieves the extremum of the criterion of quality of information processing when the specified restrictions.

Fig. 5.1 in general shows the scheme of synthesis of the structure of the CIS software in the ICN environment.

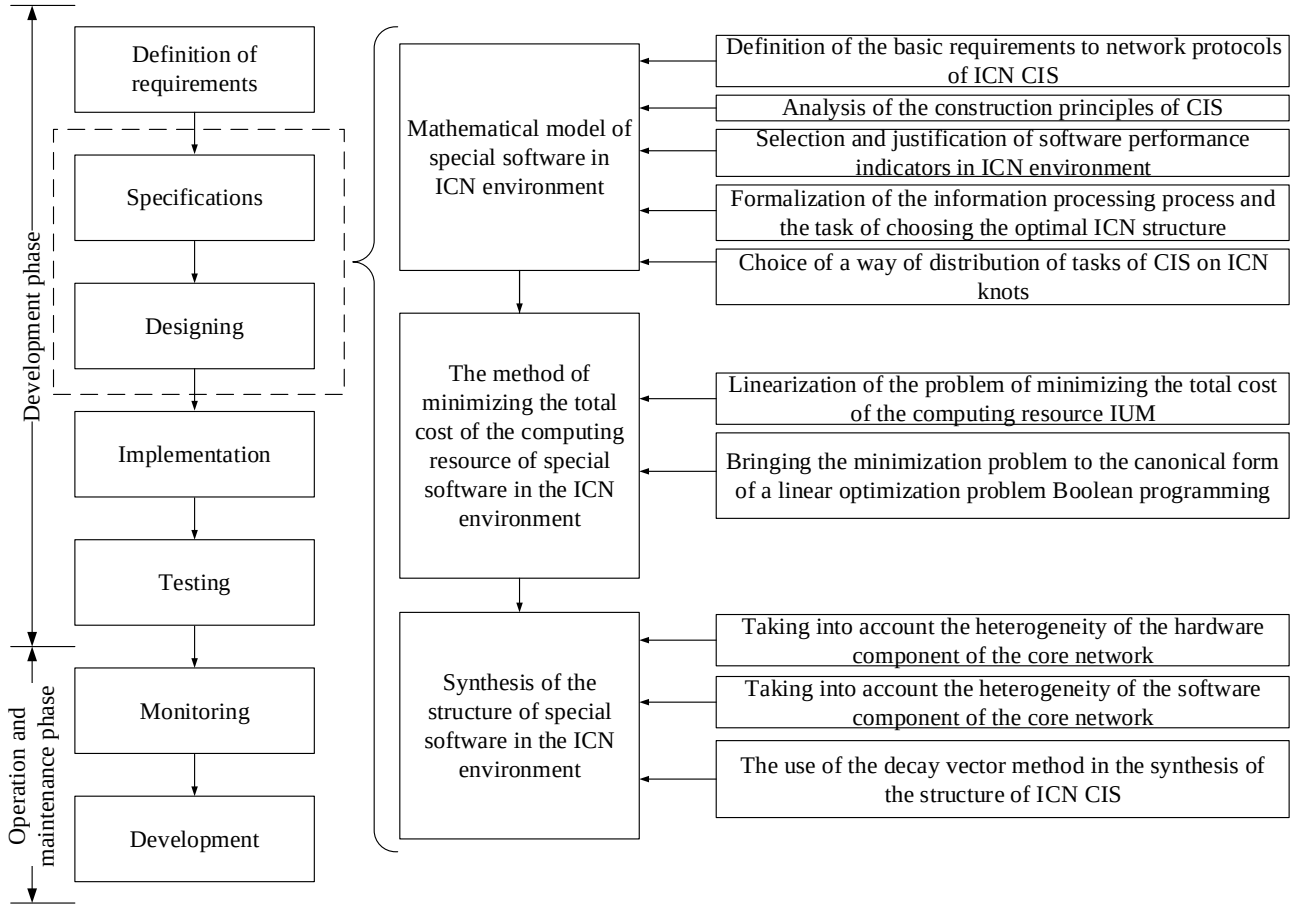


Fig. 5.1. A diagram of the synthesis of the CIS software structure in the ICN environment

5.2 Models of information technology processes management parameters of ICN CIS

Information technology of control of parameters of ICN CIS realizes consecutive work of three blocks (Fig.5.2) [142]:

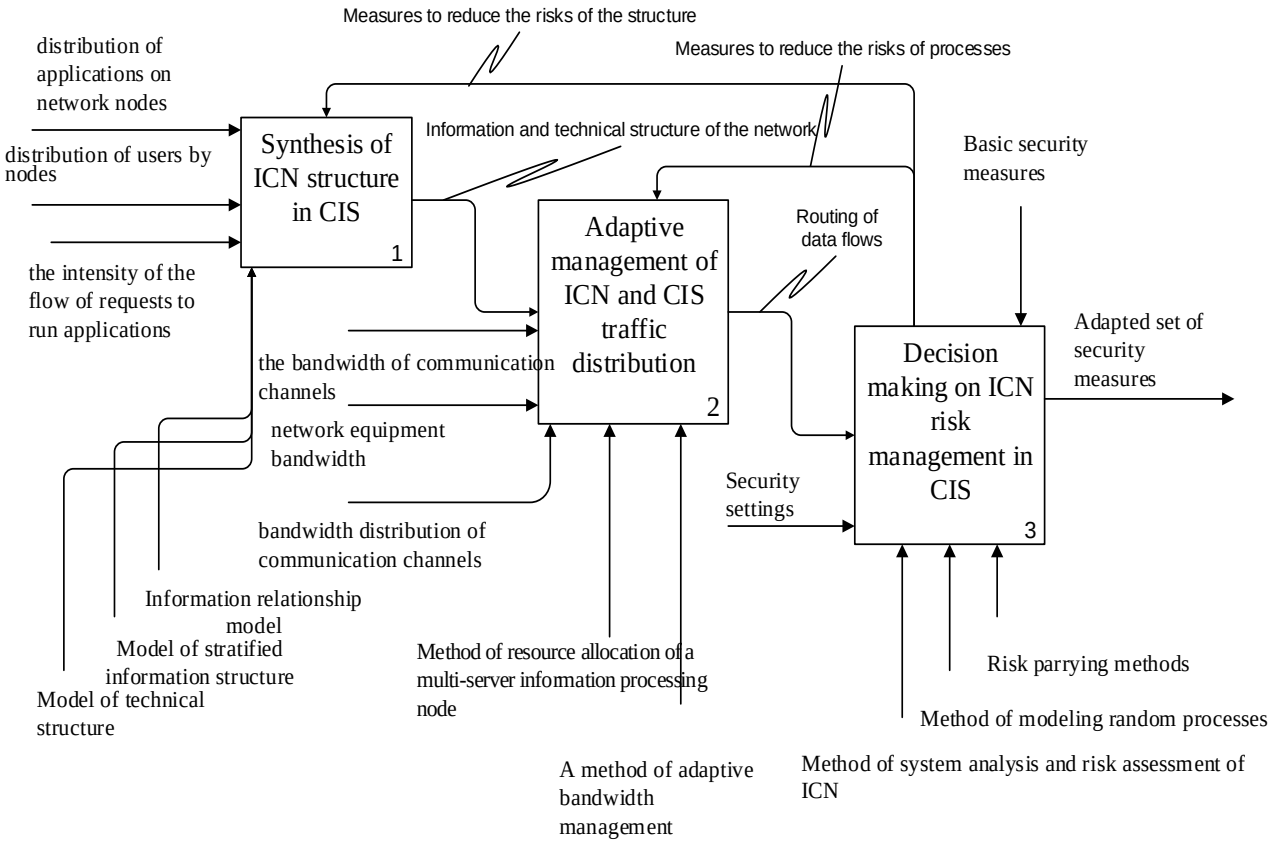


Fig. 5.2. Model of information technology for managing the parameters of ICN CIS

1) block synthesis of the structure of the infocommunication network in critical systems;

2) block of adaptive control of traffic distribution of infocommunication network in systems of critical infrastructure;

3) decision-making unit for risk management of the infocommunication network in the critical infrastructure system.

The operation of the ICN structure synthesis unit requires the execution of a sequence of such processes (Fig. 5.3):

1) determining the composition of network users;

2) determining the composition and parameters of the applied problems;

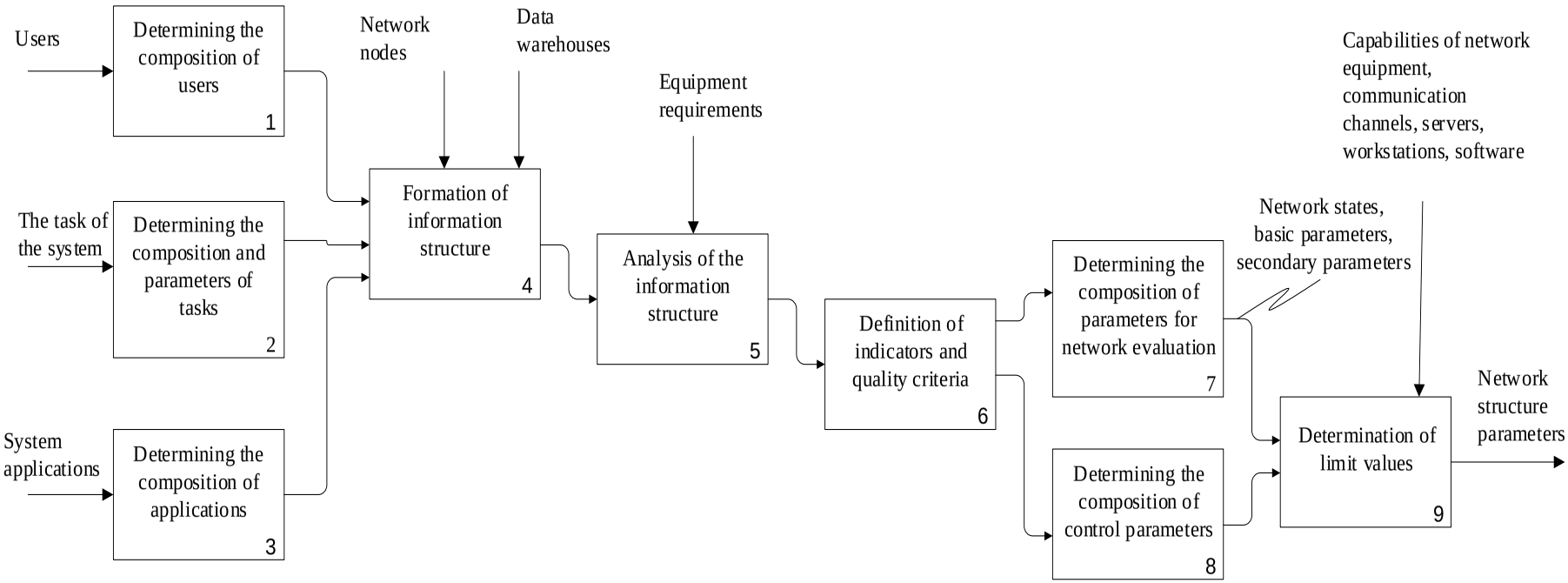


Fig. 5.3. Model of processes of the block of synthesis of structure of ICN CIS

3) determining the composition of applications that are installed on the network and you-could to the equipment for the implementation of applications. If necessary, the number of copies for some applications is determined. These copies will then be considered as stand-alone applications and will have their own numbers;

4) formation of the information structure of the network;

5) analysis of the information structure of the network;

6) determination of indicators and quality criteria for solving applied problems;

7) determining the composition of network parameters that will be used to assess the state of the network, network management and determine the space of network states; determining the composition of the basic parameters of the network; determining the specific composition of the set of primary and secondary network parameters;

8) determining the composition of network management parameters;

9) determination of limit values of network parameters. Here the maximum allowable values of network parameters are determined, the value of which is related to the capabilities of network equipment and communication channels, servers and workstations, as well as software.

The operation of the adaptive traffic distribution control unit requires the following sequence of processes that must be performed in the preparation and solution of management tasks (Fig. 5.4):

- solving the problem of network configuration;
- solving operational management tasks;
- correction of tasks of adjustment and operational management.

The stage of preparation is necessary for development of basic approaches and requirements to management of distribution of traffic on the basis of which criteria of quality of management are developed, the concrete purposes and tasks of management are formed. [27].

At the *stage of solving the task of setting up the network*, the following sub-processes are performed:

1. Determining specific indicators of network setup quality.

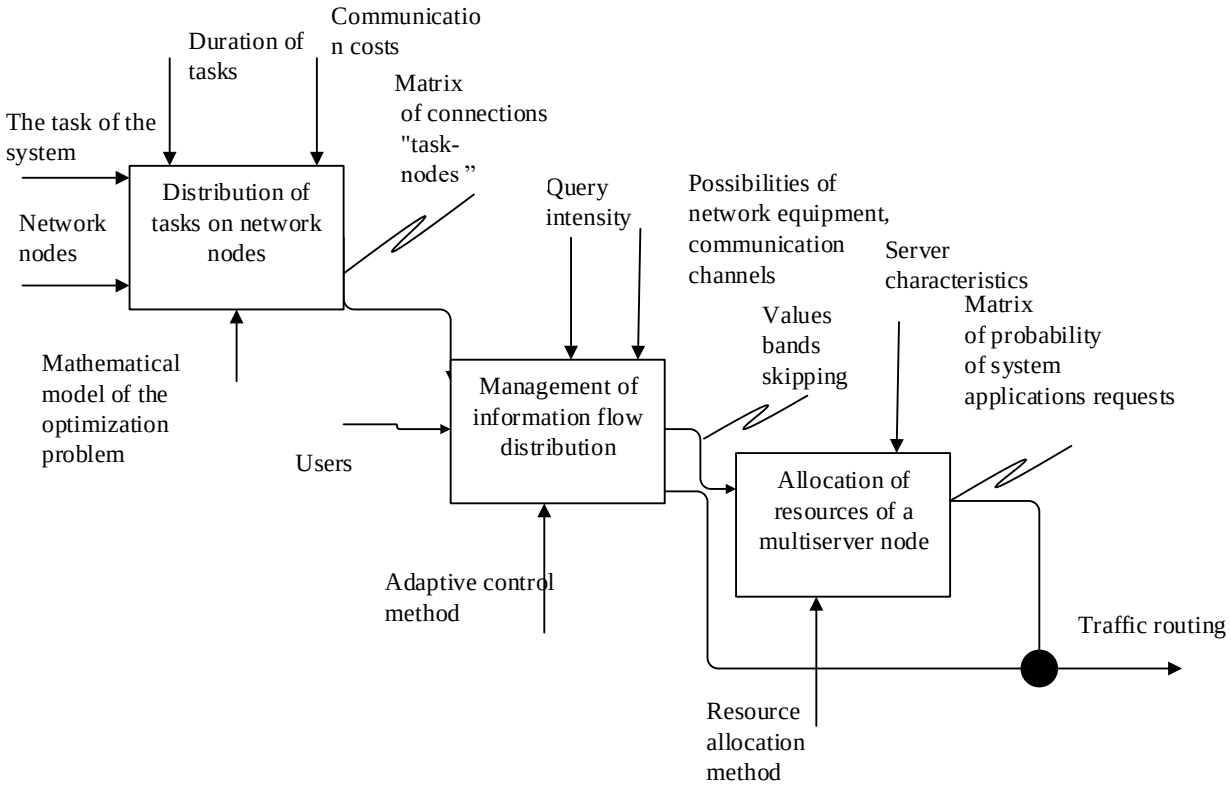


Fig. 5.4. Process model of the adaptive traffic distribution control unit

2. Formation and calculation of data flow parameters of the hierarchical information structure of the network. The solution of the problem of forming the information structure can be considered as a partial solution of the configuration problem. As a result, the parameters of the information structure and data flows for the information structure with these parameters are determined [143].

3. Determining the composition of network equipment. Based on the analysis of requirements for applications to equipment parameters, analysis of information flows conducted for the information structure of network traffic distribution management, potential number of technical network nodes and preliminary data on technical network structure (a priori distribution of users and nodes on subnets),

equipment composition and its parameters are determined - switches, servers, client workstations, types of communication channels used.

4. Formation of the technical structure of the network. As a result of this step, a set of values of the basic parameters of the network is formed, the structure of the basic network is also formed, in addition, the subnets and their composition are allocated. Note that it is possible to repeatedly solve problems in this step, if you change the distribution of system applications on the nodes of the information structure. At the end of the step we get a set of values of network parameters.

After this stage, we have a variant of the network structure, a set of parameters of operational management of subnets, which are used in the next *stage of solving operational management problems*, which involves such subprocesses:

1) determination of performance indicators of subnets. In this step, a set of performance indicators is formed for each subnet;

2) setting partial tasks of operational management for subnets. Here can be used or general tasks of operational management, or tasks of operational management of subnets, or partial tasks of operational management;

3) solving operational control problems using mathematical programming methods.

The stage of correction of tasks of adjustment and operational management arises in case of change of basic parameters of a network that can set reconfiguration of a network and development of new approaches to the decision of tasks of operational management. It includes the following subprocesses:

1) correction of the composition of network parameters;

2) correction of the composition of the basic parameters and control parameters;

3) correction of requirements for the quality of solving applied problems.

After solving these tasks, the transition to the stages of management described above.

The input data of information technology for solving problems of data flow analysis in the network, loading communication channels and network equipment, are the following network parameters:

- distribution of applications on network nodes;
- distribution of users on network nodes (workstations);
- the intensity of the flow of requests to run applications or tasks;
- network structure, which sets the communication channels between network equipment and binding workstations and servers to network equipment;
- values of bandwidths of communication channels used in the network;
- bandwidth of network equipment used in the network;
- distribution of bandwidth of communication channels between separate tasks (groups of tasks);
- routing of data flows in the network.

Let's define a matrix of intensities of streams of requests of users for performance of tasks

$$\Lambda = \left\| \lambda_{jk} \right\|, \; k = \overline{1,l}, \; j = \overline{1,n}, \tag{5.1}$$

where $\lambda_{jk} > 0$ is the intensity of the flow of requests from the user number *j* to perform the task number *i*.

Note that the conditions must be met:

$$\lambda_{jk} = 0 \text{ if } u_{jk} = 0, \; \lambda_{jk} > 0 \text{ if } u_{jk} = 1, \; k = \overline{1,l}, \; j = \overline{1,n}. \tag{5.2}$$

The values of the elements of the matrix Λ are determined by the specifics of the work of users of the UPC, so we will consider them known.

Obviously, user request flows first arrive at the network nodes to which users are attached. Pinning users to nodes is specified by a matrix of relationships with values of 0 and 1.

The intensity of task request flows determines the intensity of execution of system applications that are used to solve problems. The total intensity of requests for tasks number ($k - \lambda_k$) is calculated by the formula:

$$\lambda_k = \sum_{j=1}^{n} \lambda_{jk}, \; k = \overline{1,l}. \tag{5.3}$$

We introduce a vector-string of the intensity of tasks in the system:

$$\lambda = (\lambda_1, \lambda_2, ..., \lambda_l). \tag{5.4}$$

You can determine the total intensity of request flows:

$$\lambda = e_N \Lambda, \tag{5.5}$$

where e_N is a single dimensional vector string *N*.

A vector-string γ let's denote as

$$\gamma = (\gamma_1, \gamma_2, ..., \gamma_D). \tag{5.6}$$

Each of its elements determines the total intensity of the system application number *j* all the tasks solved by the system:

$$\gamma_i = \sum_{k=1}^{l} \lambda_k p_{ki}, \tag{5.7}$$

where p_{ki} – execution of the system application number *i* when performing the *k*-th task.

Then the vector-string determines the intensity of system applications during the operation of the CIS:

$$\gamma = \lambda P. \tag{5.8}$$

In a real network, the intensity of request flows, the composition of users and the composition of the tasks can change over time, in addition, with the development of the network changes the composition of equipment and its parameters - that is, the basic network parameters change. All this necessitates a change in the correction of the control parameters of the network to achieve the required efficiency of its work. Such a change in network parameters (network setup) is one of the main processes of network management. Thus, naturally, it is necessary to provide necessary values of indicators of quality of work of the network connected with the decision of applied problems.

- Since the distribution of users on the workstations of the network, as a rule, is determined by the organizational structure and location of users, the distribution of users is further considered a given and constant parameter of the network.

Thus, network traffic management is reduced to solving the following main tasks:

- application distribution and migration management;
- network structure management;
- control of debugging of network equipment or control of data flows in the network: control of parameters of service of data flows;
- routing management.

The set of primary network parameters is divided into two subsets:

- many basic network parameters;

- a set of varied parameters.

The basic parameters of the network are, for example, the number of users, the number of servers, the number of tasks solved on the network, the number of subnets, the distribution of users on subnets.

Variable network settings, such as

- adjustment of network equipment,
- server performance and bandwidth of communication channels.

The main properties by which the parameters differ in basic and varied are dynamism, ie the rate of change over time. The basic parameters usually change much more slowly than the varied ones. Changing the basic parameters usually leads to a mandatory change of the variable parameters to maintain efficient network operation, while changing the variable parameters does not require a change of the basic parameters. Changing the basic parameters leads to significant changes in the quality of the network, and changing the varied parameters leads to minor changes.

Since the basic parameters do not depend on the change of the varied parameters, it is possible to divide the parameters of network traffic management into two levels:

- management at the level of basic parameters;
- control at the level of varied parameters.

Network traffic management at all levels should provide optimal values of network quality indicators.

There are two types of network traffic management, which are most often used in practice, and are relevant to the above levels of management:

- network debugging - the level of basic parameters;
- operational management - the level of variable parameters).

Note that the set of control parameters does not always coincide with the set of basic parameters, because some basic parameters do not change during the entire life of the network, such as routing protocols or protocols that provide guaran-

teed quality of service, etc. The set of operational management parameters also does not always coincide with the set of variable parameters, as some variable parameters cannot be changed during the operational network management, for example, the number of network users, the number of servers, etc.

Debugging the network is required either when starting the network after its creation with a given set of basic parameters, or when changing any of the basic parameters of the network. Therefore, debugging is control at the level of basic parameters. For example, debugging may require changes in network structure (number of subnets), communication channel types, and so on.

Operational control is used constantly during network operation and is control at the level of varied parameters. The need for operational management is associated with the emergence of situations in the network, when, for example, there are temporary changes in the intensity of data flows caused by production needs in solving some problems.

The set of indicators of network quality is divided into two disparate subsets:

- quality indicators calculated at the stage of network establishment;
- quality indicators calculated in the operational management of the network.

Let's form the scheme of traffic distribution management (fig. 5.5).

At the upper management level (U_1) it is assumed to use the following methods of integrated data flow control (IDC):

- the method of determining the load profile of the ICN link, which based on the analysis of the bandwidth of the link and the calculation of the statistical characteristics of the data flows allows you to calculate the load profile with the specified quality requirements [144];

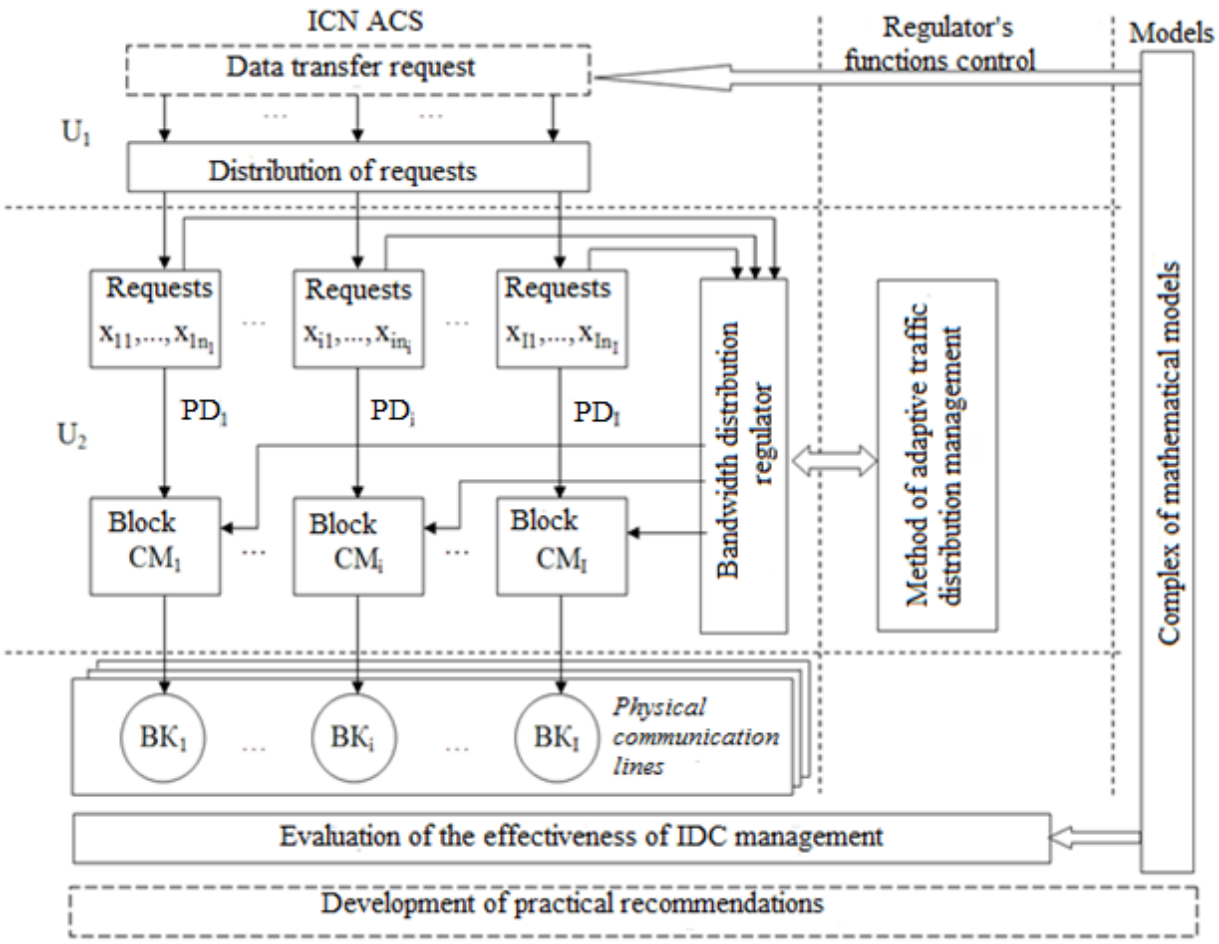


Fig. 5.5. Traffic distribution management scheme

- method of dynamic control of load distribution of virtual connections, which provide the passage of the data flow, which takes into account when forecasting the fractal nature of the generated traffic; the method is supposed to be used at the level of the ICN access controller when creating or modifying a system of virtual channels between network nodes.

The methods involved in control on two fields (U_1 and U_2) are focused on the use of an appropriate set of mathematical models that take into account the features of the IDC on the basis of a small number of traffic samples. These models can also be used by the ICN access controller at the stage of forming and modifying the parameters of virtual channels. Figure 5.6 shows the mathematical appa-

ratus used in solving problems of information technology for managing the parameters of ICN CIS.

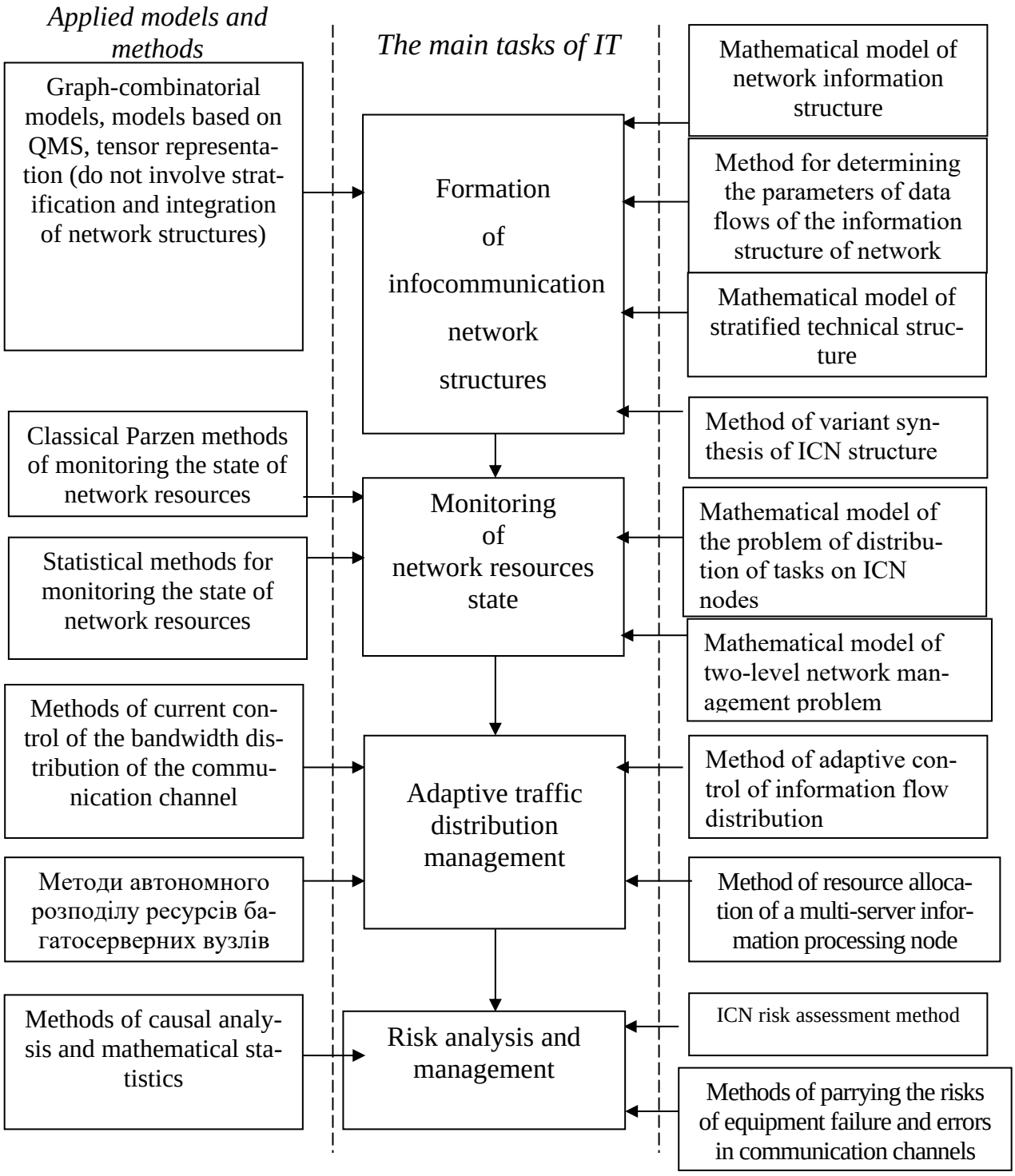


Fig. 5.6. Methodical apparatus of information technology for managing the parameters of ICN CIS

6 THE APPLICATION OF INFORMATION TECHNOLOGY FOR CONTROL OF THE INFORMATION COMMUNICATION NETWORK OF THE SOFTWARE-TECHNICAL COMPLEX OF APCS

6.1 Structure and functional tasks of the Software and hardware complex of ACS TP

Automated control system for technological process (ACS TP) "Complex for processing solid waste with a system of landfill gas collection, utilization and production" is a multi-functional, distributed, freely programmable automated system designed for long-term continuous operation in real time, which implements the necessary functions of collecting, processing and presenting information, as well as the functions of control, regulation, protection, blocking and signaling. The software and technical complex of the upper level and general station systems (STC UL GS) is an integral part of the ACS TP. It is designed to automate the control of TP common station and auxiliary systems and is designed for long-term operation in real time. The main indicators corresponding to the purpose of STC:

- provides a convenient form, sufficient in volume and speed of presentation and registration of information about the course of TP;
- protection of personnel, equipment and environment from possible accidents is provided in all operating modes of the station;
- automatic control of technological parameters and equipment control is provided in the control range of the station operation;
- diagnostics of malfunctions of hardware and software of STC is provided that prevents issue of erroneous commands of management of the technological equipment and allows to eliminate malfunctions in due time.

STC UL GS is a three-level distributed system, which is built on a hierarchical principle.

The following subsystems are considered as CIS subsystems:

1) display of information;
2) electronic document management, e-mail;
3) information and calculation (analytical);
4) operation management;
5) comprehensive information protection system;
6) telecommunication network;
7) administration.

The general view of the functional model of the automated process control system is presented in Fig. 6.1. The functions of the STC UL and GS are classified into three types and summarized in Table 6.1.

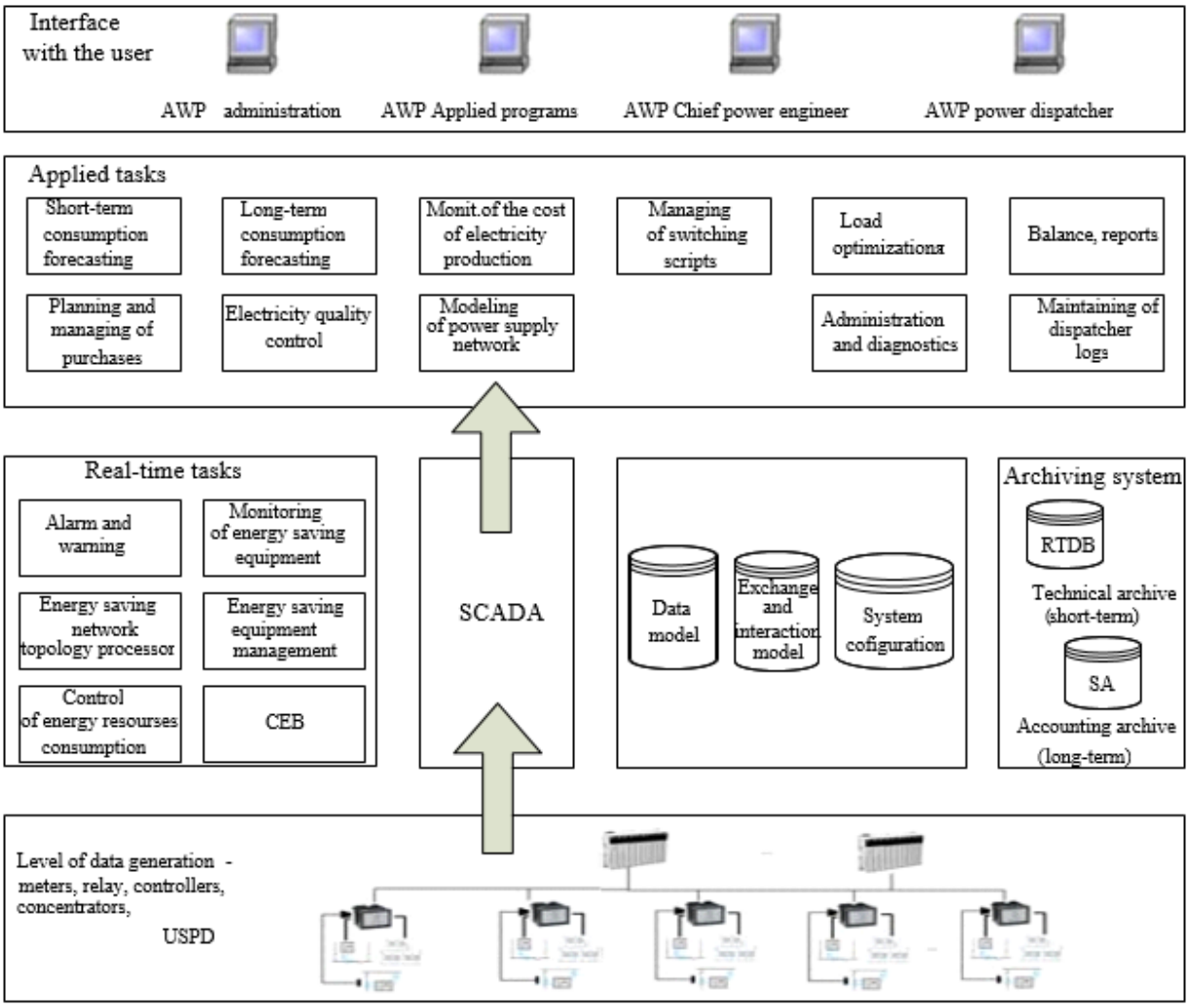


Fig. 6.1. Functional model of ACS TP

Table 6.1 – Functions of STC UL and GS

Type of functions	**Functions**
Manager	- remote control of locking, regulating bodies and mechanisms; - technological protections; - protective and technological blocking, automatic activation of the reserve of mechanisms of own needs; - automatic adjustment of technological parameters; - remote control of elements of an electric part.
Informational	- collection and control of the reliability of input information; - presentation of information about the technological process and the operation of automatic devices; - warning and alarm systems; - registration of information that is entered and formed in the STC; - registration of deviations of parameters from norm, with registration of time of an exit from norm, and also time of return to norm; - documentation of registered information; - diagnostics of STC hardware and software; - calculations of operational technical and economic indicators.
Auxiliary	- correction of adjustment parameters of automatic control systems; - presentation of information about the operation of control algorithms in real time; - simulation of input information for testing control systems; - input / output of protections and blocking, and also switching of modes of control systems; - automated processing and storage of results of metrological certification of measuring channels; - management of STC operation

The following distribution of functions between levels is implemented:

- lower level (LL) – functions of input/output of analog and discrete input information, implementation of control and regulation logic, formation of analog and discrete output signals;

- intermediate level (IL) – functions of software download and control of LL operation, maintenance of operational database (ODB), remote control of shut-

off, regulating bodies and mechanisms, presentation of information (including diagnostic) at video terminals of operator and engineering stations, registration and archiving information;

- upper level (UL) – functions of information presentation on video terminals of management stations.

6.2 Synthesis of the information structure of ICN STC

Let's define the elements of the information model of the network structure in accordance with the functional model of the STC UL GS and the structural scheme of the ACS TP (Fig. 6.2).

The main users of the network are management staff and automated workstations:

U_1 – Director;

U_2 – Chief Engineer;

U_3 – station shift supervisor;

U_4 – head of the boiler turbine shop;

U_5 – head of the electrical shop;

U_6 – head of the department of thermal automation and measurements;

U_7 – station operator;

U_8 – engineering station staff.

The listed users perform the following tasks*:*

S_1 – display of information about the operation of technological systems, control and regulation systems, technological signaling, and the results of STC diagnostics;

S_2 – remote control of VM, S_3 – change of modes of operation of control and regulation systems;

S_4 – change the task of regulators;

S_5 – reset the memory of the failure of three-channel measurements to put them into operation on two working channels;

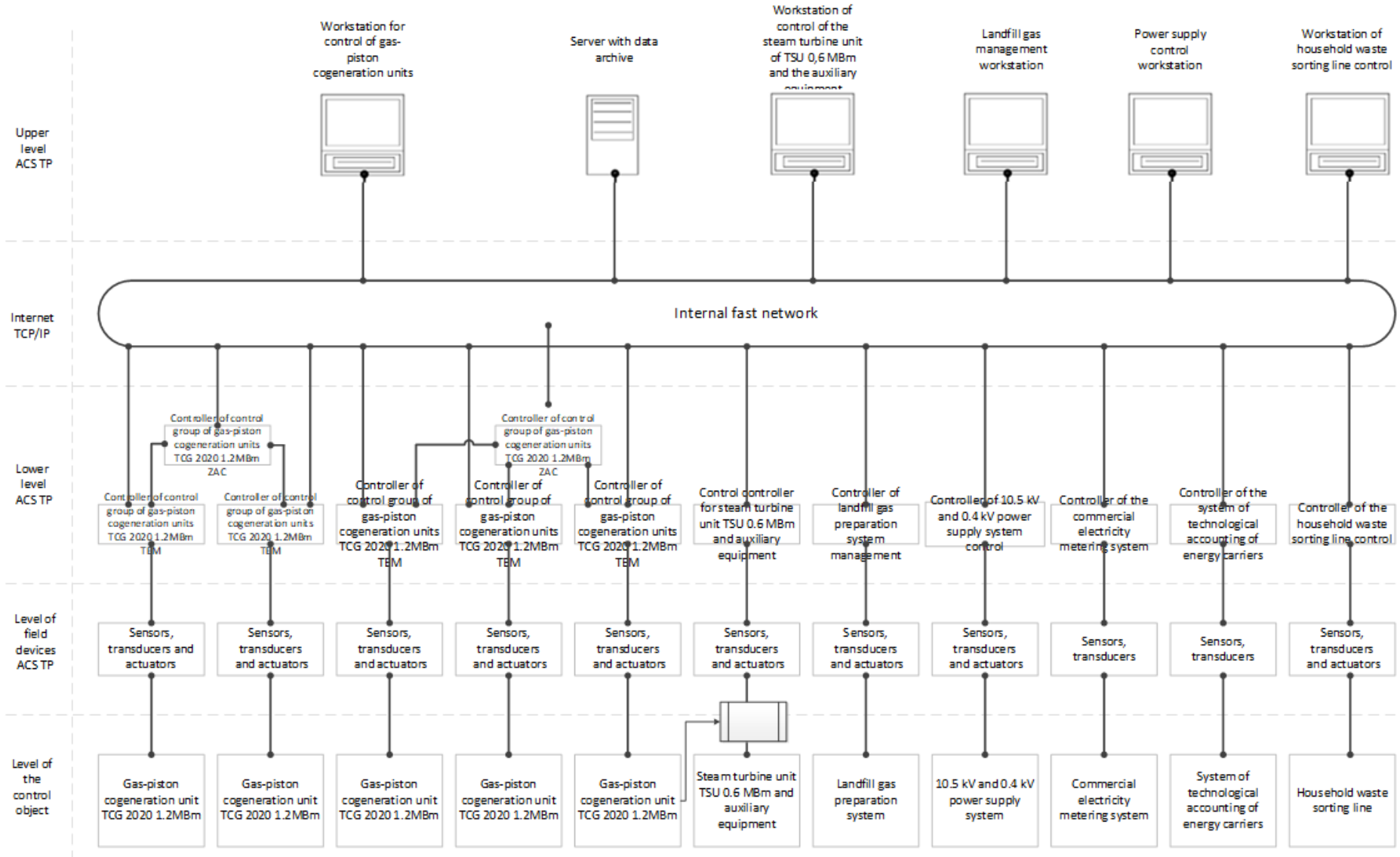


Fig. 6.2. Block diagram of the ACS TP

S_6 – view registration information with the possibility of printing;

S_7 – remote control of the elements of the electrical part;

S_8 – registration of information;

S_9 – maintenance and documentation of STC databases;

S_{10} – creation and viewing of registration information, printing at the request of users;

S_{11} – obtaining hard copies of archival data;

S_{12} – modification of STC software;

S_{13} – creating video frames of information display;

S_{14} – STC software download;

S_{15} – correction of settings of control subsystems;

S_{16} – input/output in the repair condition of the measuring transducer and VM at the request of operational personnel;

S_{17} − input of values of input analog signals of STC for carrying out tests of control systems;

S_{18} – input and output of protections and blocking at the request of operational personnel;

S_{19} – debugging of libraries of algorithms, technological algorithms and programs;

S_{20} – maintaining a single time ACS TP;

S_{21} – online presentation of information about the operation of control algorithms;

S_{22} – creation of archives on optical disks for long-term storage at the request of staff;

S_{23} – disconnection from registration of parameters which "make noise";

S_{24} – display of reference information.

Let's construct a matrix of connections "users-tasks" with the corresponding intensity of inquiries (tab. 6.2).

The network system applications are as follows:

- at the system level;

p_1 – QNX 6.3 operating system for real-time management of basic and functional software;

- at the subsystems level (upper and intermediate levels);

p_2 – registrations;

p_3 – display (with a specialized video editor for copying and transferring video frames and their parts);

p_4 – documentation of video frames;

p_5 – information archiving;

- at the level of tasks (lower);

p_6 – ISaGRAF system for performing tasks and developing FPT in controllers.

Table 6.2 – Intensities of requests for "user-task" relationships

Tasks	Users							
	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8
S_1	λ_{11}	λ_{21}	λ_{31}	λ_{41}	λ_{51}	λ_{61}	λ_{71}	λ_{81}
S_2	-	-	-	-	-	-	λ_{72}	-
S_3	-	-	-	-	-	-	λ_{73}	-
S_4	-	-	-	-	-	-	λ_{74}	-
S_5	-	-	-	-	-	-	λ_{75}	-
S_6	λ_{16}	λ_{26}	λ_{36}	λ_{46}	λ_{56}	λ_{66}	λ_{76}	-
S_7	-	-	-	-	-	-	-	-
S_8	-	-	-	-	-	-	-	λ_{88}
S_9	-	-	-	-	-	-	-	λ_{89}
S_{10}	-	-	-	-	-	-	-	$\lambda_{8,10}$
S_{11}	-	-	-	-	-	-	-	$\lambda_{8,11}$
S_{12}	-	-	-	-	-	-	-	$\lambda_{8,12}$
S_{13}	-	-	-	-	-	-	-	$\lambda_{8,13}$
S_{14}	-	-	-	-	-	-	-	$\lambda_{8,14}$
S_{15}	-	-	-	-	-	-	-	$\lambda_{8,15}$
S_{16}	-	-	-	-	-	-	-	$\lambda_{8,16}$
S_{17}	-	-	-	-	-	-	-	$\lambda_{8,17}$

Continuation of Table 6.2.

Tasks	Users							
	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8
S_{18}	-	-	-	-	-	-	-	$\lambda_{8,18}$
S_{19}	-	-	-	-	-	-	-	$\lambda_{8,19}$
S_{20}	-	-	-	-	-	-	-	$\lambda_{8,20}$
S_{21}	-	-	-	-	-	-	-	$\lambda_{8,21}$
S_{22}	-	-	-	-	-	-	-	$\lambda_{8,22}$
S_{23}	-	-	-	-	-	-	-	$\lambda_{8,23}$
S_{24}	-	-	-	-	-	-	-	$\lambda_{8,24}$

Let's define elements of *data warehouses*:

Archives:

d_1 – the main archive of technological process parameters;

d_2 – archive of events;

d_3 – operating modes of technological equipment (hourly statement; variable statement; daily statement; information on call);

d_4 – information about user actions.

Libraries:

d_5 – library of standard modules (functional blocks) of control (primary information processing), control and automatic regulation;

d_6 is a library of typical functions.

Local databases:

d_7 – input and output analog and discrete signals (lists and marking of signals, functional purpose of signals, reference information; - connection to STC cabinets; connection to the measuring transducer, VM);

d_8 – program-generated analog and discrete signals;

d_9 – constants (adjusting coefficients of regulators, settings of input and operation of technological protections, blocking and signaling) and keys (input / out-

put in repair of the measuring converter and VM, input / output of protections and blocking);

d_{10} – diagnostic messages.

Let's build matrices of connections of tasks of ACS TP with other elements of ICN:

1) matrix of connections of tasks with system applications

$$P = \begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0 \\ 0&1&1&1&1&0&1&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&1&0 \end{pmatrix}$$

Each non-zero element of the matrix is characterized by a certain amount of data transmitted $v_{ij.}$

2) a matrix of connections of tasks with data warehouses

$$D = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&1&1&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&1&1&0 \\ 0&1&0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&0&0 \\ 0&1&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0&1&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \end{pmatrix}$$

3) the matrix of connections of tasks with users (U) corresponds to table 6.2.

Network nodes are located on five levels according to the structural scheme of the ACS TP (see Fig. 6.2). The diagram shows the enlarged nodes of the control system. A more detailed view contains the following nodes:

1) Management posts:

- the central technological board (CTB) from which management of the equipment and interaction of the personnel with ACS of TP is provided;
- local control panel (LCP) VPU;
- LCP systems of technical water supply and treatment facilities;
- LCP fracturing;
- LCP VRU-10 kV;
- LCP VPU, technical water supply systems and treatment facilities.

2) Station operator's workstation:
- two workstations GPA and KU;
- workstation for archiving and documentation of GPA and KU;
- steam turbine workstation;
- two workstations of auxiliary equipment of the station;
- electric workstation;

3) Local systems of automatic control and regulation (LSC):
- auxiliary equipment of the main building;
- district heating;
- gas fuel farms.

4) Means of computer technology:
- workstation of software and computer engineer (engineering station);
- control cabinets;
- uninterruptible power supply;
- servers;
- single time system equipment.

To analyze the load of ICN nodes, we construct matrices of connections of ACS TP nodes with other ICN elements:

1) the matrix of fixing system applications for network nodes (*G*), which is presented in the form of table 6.3;

2) the matrix of user assignment to network nodes (*H*) (Table 6.4), which reflects the intensity of requests to nodes with the following symbols: *A* – constant connection; *B* – with a given time interval; *C* – once per shift; *D* – on request.

Table 6.3 – Elements of the matrix of use of system applications by the main nodes of the network

SA	Nods																																								
	1						*2*		*3*											*4*											*5*										
	1	*2*	*3*	*4*	*5*	*6*	*1*	*2*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
p_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_3	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_4	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0

Table 6.4 – Elements of the matrix of user interaction with the main nodes of the network, taking into account the frequency of information exchange

Users	Nodes																																								
	1						*2*		*3*											*4*											*5*										
	1	*2*	*3*	*4*	*5*	*6*	*1*	*2*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
U_1	D	D	D	D	D	D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U_2	D	D	D	D	D	D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U_3	A	D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U_4	0	D	A	0	0	0	B	B	B	B	B	B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U_5	0	D	0	0	A	0	B	B	B	B	B	B	B	B	B	B	B	B	B	C	C	C	C	C	C	C	C	C	C	C	0	0	0	0	0	0	0	0	0	0	0
U_6	0	0	0	0	0	0	0	0	0	0	0	0	0	A	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U_7	0	0	0	0	0	0	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	0	0	0	0	0	0	0	0	0	0	0
U_8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A	A	A	A	A	A	A	A	A	A	A

1) the matrix of information connections of nodes with data warehouses (*S*) is presented in table 6.5.

To calculate the intensity of request flows, multiply the following matrices:

1) $P \times \Lambda = G$, we obtain a matrix of the intensity of execution of system applications by users:

$$G = \begin{pmatrix} \lambda_{11}+\lambda_{16} & \lambda_{21}+\lambda_{26} & \lambda_{31}+\lambda_{36} & \lambda_{41}+\lambda_{46} & \lambda_{51}+\lambda_{56} & \lambda_{61}+\lambda_{66} & (\lambda_{71}+\ldots+\lambda_{76}) & \lambda_{81}+(\lambda_{88}+\ldots+\lambda_{8,24}) \\ 0 & 0 & 0 & 0 & 0 & 0 & (\lambda_{72}+\ldots+\lambda_{76}) & \lambda_{88}+(\lambda_{8,15}+\ldots+\lambda_{8,18})+\lambda_{8,23} \\ \lambda_{11} & \lambda_{21} & \lambda_{31} & \lambda_{41} & \lambda_{51} & \lambda_{61} & \lambda_{71} & \lambda_{81}+\lambda_{8,13}+\lambda_{8,22}+\lambda_{8,24} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{89}+\lambda_{8,10} \\ 0 & 0 & 0 & 0 & 0 & 0 & (\lambda_{72}+\ldots+\lambda_{75}) & \lambda_{8,11}+\lambda_{8,19}+\lambda_{8,22} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & (\lambda_{8,16}+\ldots+\lambda_{8,18})+\lambda_{8,23} \end{pmatrix};$$

2) to obtain a matrix of tasks on network nodes, taking into account the execution of system applications and connections to data warehouses, it is necessary to obtain the sum of multiplication of two matrices:

$$Z = Z'+Z'' = G \times D + S \times D. \qquad (6.9)$$

We obtain a *Z* matrix of dimension 24 × 41.

To calculate the intensity of user requests to nodes, taking into account system applications and tasks, we consistently multiply the following matrices:

$$M = ((U \times P) \times G) \times \qquad (6.10)$$

Thus, the parameters of the *information structure* are obtained

- the intensity of system applications;
- the number of tasks performed in network nodes;
- intensity of requests to network nodes.

Table 6.5 – Elements of the matrix of information links of nodes with data warehouses

SA	Nodes																																							
	1						*2*		*3*											*4*											*5*										
	1	*2*	*3*	*4*	*5*	*6*	*1*	*2*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
d_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
d_2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
d_3	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
d_4	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
d_5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
d_6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
d_7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
d_8	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
d_9	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
d_{10}	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

According to these parameters, the *requirements for the technical structure* of the network were determined:

- the exchange of information between the nodes of the upper and middle level of the STC should be carried out by digital data transmission channels;
- information exchange in the system must be performed on the basis of a duplicate computer network such as Ethernet;
- the nomenclature and number of modules of input/output of information in the structure should ensure the reception and publication of a certain amount of information;
- it is necessary to use specialized intelligent devices for communication with the object (DCO), designed to implement the functions of digital control to ensure the reception of a certain number of analog and discrete signals, as well as the formation and output of control signals;
- DCO nodes must exchange data with controllers via a local area network based on RS-485 or Ethernet;
- the transfer of information from the LCP nodes to the nodes of the Central Technology Board (CTB) must be performed using a duplicate Ethernet computer network;
- STC must receive information from input-output devices in cabinets (RUVP 0.4 kV) and microprocessor terminals (KRU 10 kV) digital channel based on the interface RS-485 on one of the standard protocols, for example, Modbus, Profibus);
- the nodes of the central controllers of the collection and control systems must be IBM PC-compatible and ensure the implementation of control, management and control functions, as well as the exchange of information with mid-level and high-level nodes and adjacent lower-level nodes;
- industrial panel computers with liquid crystal displays must be installed at the nodes of the technical water supply systems and treatment facilities, hydraulic fracturing and RU-10 kV;

- fiber optic cables or twisted pair cables must be used to provide remote communication with the DCO;

- for information exchange between STC cabinets it is necessary to provide bandwidth of 100 Mbps, and between nodes at all levels of the system (LL, IL and HL) bandwidth of 1000 Mbps.

6.3 Synthesis of variants of ICN structures and analysis of STC information flows

Options for constructing a set of network nodes, which differ in the construction of connections between nodes, are formed based on the analysis of information circulating in the network, taking into account the relationship of information flows [34]. Figure 6.3 shows the initial version of the ICN.

To simplify the description and accounts as nodes are taken only management personnel and automated service stations STC.

Analysis of the movement of information flows showed that the main operations for information processing are performed at the central node (CN). Also, when forming a connection between the elements $j \in J$, all nodes of the "control group" must be provided with direct access to the Central node U_0. In addition, the analysis of the tasks and the direction of information flows from the CN to the workstation of service personnel allow us to offer other options for building an ICN [145].

Let's consider different options for constructing ICN – (J_1, J_2, J_3), the structures of which are presented in Figures 6.4 and 6.5.

As you can see from the diagram in figure 6.3, in the variant J_1, all connections between network nodes are implemented through a switch connected to the CN. In the variant J_2 (Fig. 6.4), the nodes of the third-level group of the system are separated into a separate segment.

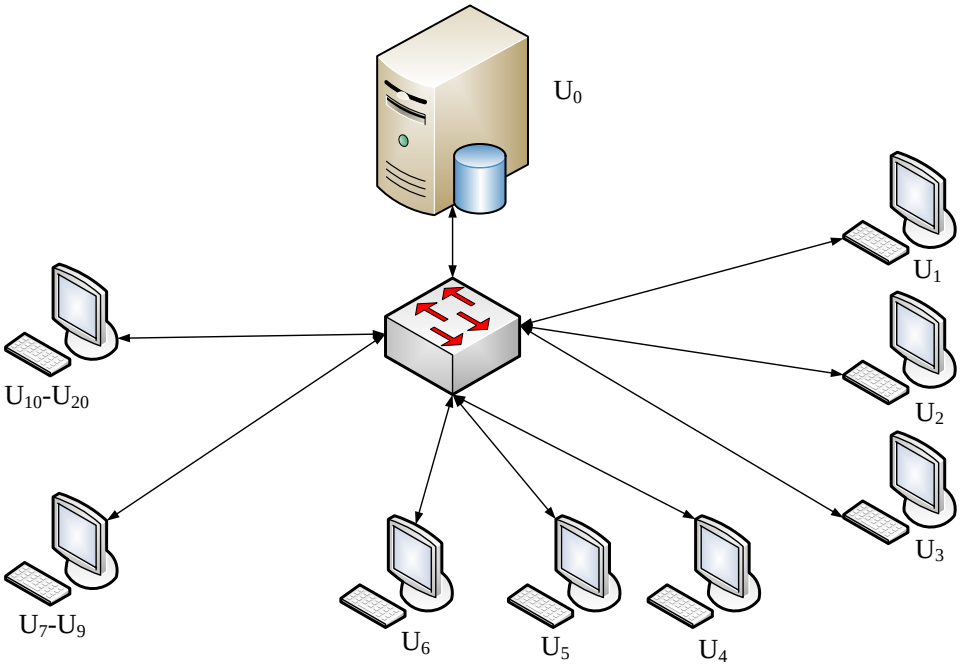


Fig. 6.3. The initial version of the ICN for the operation of STC

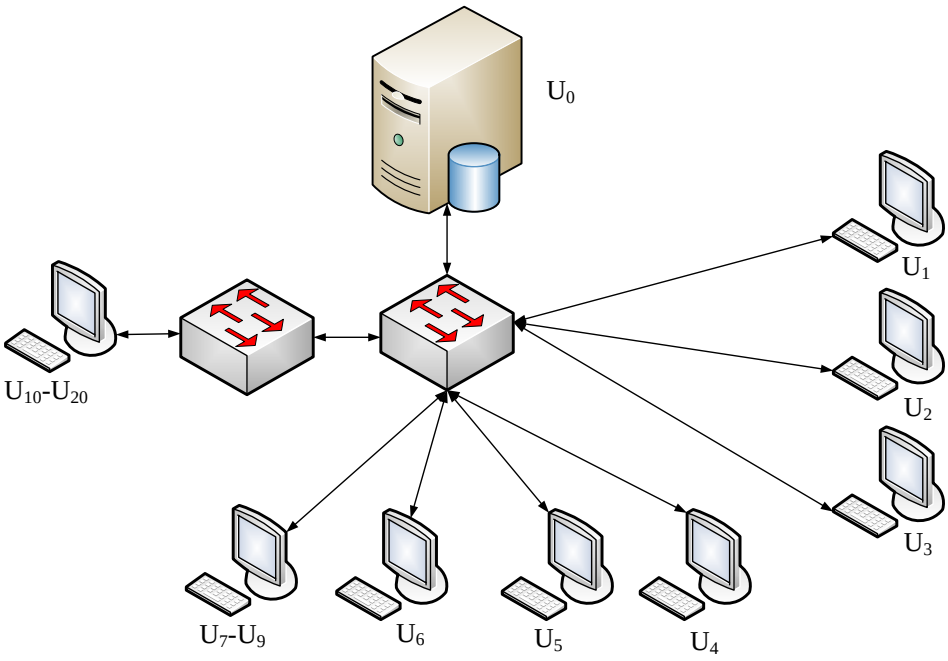


Fig. 6.4. Variant J_2 to build an ICN for the operation of STC

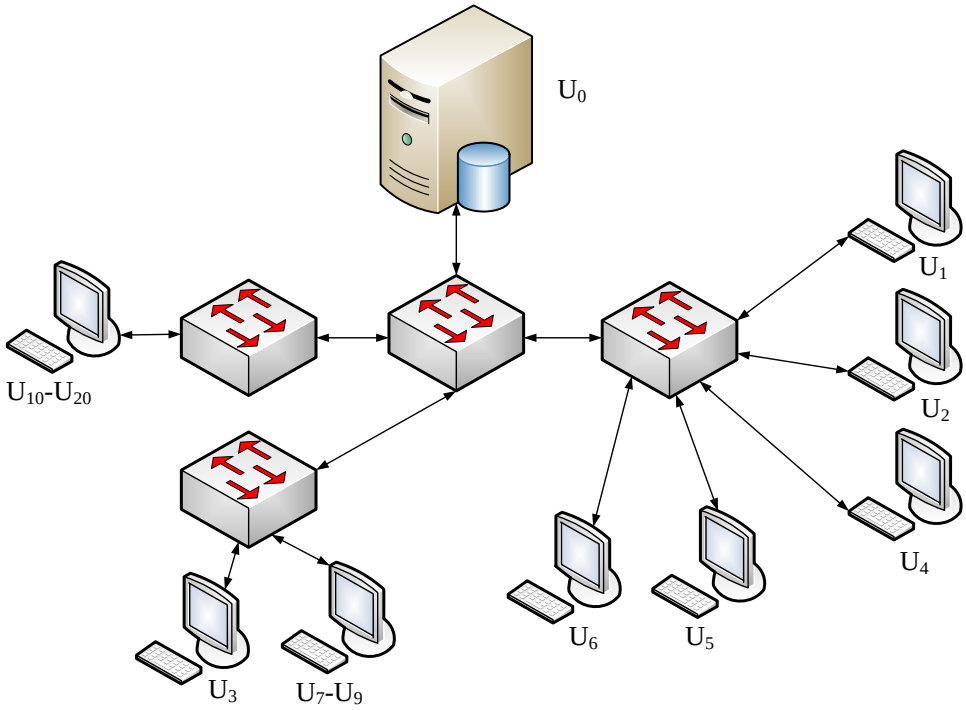


Fig. 6.5. Variant J_3 to build an ICN for the operation of STC

In the variant shown in Figure 6.5 (J_3), almost the entire flow of information between individual network nodes that do not have special requests to the CN, passes through the switches that ensure the operation of the respective network segments. In addition, the variant J_3 is built on two-stage technology, which allows to achieve a more even distribution of bandwidth within the network and to reserve opportunities for further network expansion.

The presented construction variants do not exhaust all possible construction options for the considered ICN nodes, but represent the most characteristic groups of such constructions.

We will form the initial data for modeling the functioning of STC.

Let us denote the sets:

$$I = \left\{ i \mid i = \overline{1,29} \right\}, \; J = \left\{ j \mid j = \overline{1,20} \right\}. \qquad (6.11)$$

According to the analysis of the movement of information flows within the network, we will form a Boolean matrix $B = \left\| b_{ij} \right\|$ (Fig. 6.6).

$$
\begin{vmatrix}
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{vmatrix}
$$

Fig. 6.6. Matrix $B = \left\| b_{ij} \right\|$ – use of network nodes by tasks

When specifying the cost matrix of the computing resource, we take into account that if $b_{ij} = 0$ then a_{ij} can be set equal to zero (Fig. 6.7). The cost matrix of the computing resource for the transmission of the elementary unit of information $H = \left\| h_{j_k j_l} \right\|$ depends on the network configuration.

$$\begin{vmatrix}
1 & 0{,}2 & 0{,}2 & 0 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
0{,}98 & 0{,}18 & 0{,}18 & 0 & 0{,}18 & 0 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 \\
1{,}01 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0 & 0{,}21 & 0 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 \\
1{,}02 & 0{,}22 & 0{,}22 & 0 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 \\
1{,}02 & 0 & 0{,}22 & 0{,}22 & 0 & 0 & 0 & 0{,}22 & 0 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 \\
1{,}02 & 0 & 0{,}2 & 0{,}2 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
0{,}98 & 0 & 0{,}18 & 0{,}18 & 0 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 & 0{,}18 \\
0{,}99 & 0 & 0 & 0{,}19 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 \\
0{,}99 & 0{,}19 & 0{,}19 & 0 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1{,}01 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}21 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1{,}01 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}21 & 0 & 0 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 & 0{,}21 \\
1{,}02 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}22 & 0 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 & 0{,}22 \\
0{,}99 & 0 & 0 & 0{,}19 & 0 & 0 & 0 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 & 0{,}19 \\
1 & 0 & 0{,}2 & 0{,}2 & 0 & 0 & 0 & 0{,}2 & 0 & 0{,}2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1{,}01 & 0 & 0 & 0{,}21 & 0 & 0 & 0 & 0{,}21 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0{,}98 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}18 & 0 & 0{,}18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0{,}97 & 0 & 0 & 0{,}17 & 0 & 0 & 0 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 \\
0{,}97 & 0 & 0{,}17 & 0{,}17 & 0 & 0 & 0 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 & 0{,}17 \\
1{,}03 & 0 & 0{,}23 & 0{,}23 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 \\
1 & 0 & 0{,}2 & 0 & 0 & 0 & 0 & 0 & 0{,}2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0{,}2 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
0{,}97 & 0{,}17 & 0{,}17 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0{,}2 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
1{,}03 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0{,}23 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
1 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
1 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
1 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \\
1 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2
\end{vmatrix}$$

Fig. 6.7. Matrix $A = \left\| a_{ij} \right\|$ – the cost of computing resources to perform tasks

Since unallocated calculations are considered (all control and technological tasks are performed on the central computing complex – U_0 node), therefore, almost all requests to start processing most tasks are sent to the node U_0.

We set the matrix $Q = \|q_{ij}\|$ – the matrix of volumes of information entered for the i-th task from the j-th node (Fig. 6.8).

The matrix $P = \|p_{ij}\|$ (Fig. 6.9) describes the amount of information output by tasks on ICN nodes. Data for the matrix are determined by each task during its operation, as well as for the matrix $Q = \|q_{ij}\|$.

Given that the nodes $U_{10} - U_{20}$ are designed to solve a number of technological problems, for simplicity of calculation in the matrices $P = \|p_{ij}\|$ and $Q = \|q_{ij}\|$ for these nodes, we introduce one column.

When specifying a matrix $C = \|c_{i_k i_l}\|$, we take into account that this matrix mainly consists of zero elements. Therefore, we define it by listing only nonzero elements (Fig. 6.10).

To analyze the structures J_2 and J_3 it is necessary to take into account changes in information flows that have occurred due to changes in network topology. The introduction of these changes in the base topology allowed to increase the speed of data exchange within the network segment and also to unload the communication channel that serves the node U_0 when using distributed computing.

The degree of loading of STC nodes using distributed computing and different network topology options is shown in Figure 6.11.

$$\left|\begin{array}{ccccccccccc}
0{,}015 & 0{,}036 & 0{,}036 & 0 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 \\
0{,}01 & 0{,}031 & 0{,}031 & 0 & 0{,}031 & 0 & 0{,}031 & 0{,}031 & 0{,}031 & 0{,}031 & 0{,}031 \\
0{,}017 & 0{,}037 & 0{,}037 & 0{,}037 & 0{,}037 & 0 & 0{,}037 & 0 & 0{,}037 & 0{,}037 & 0{,}037 \\
0{,}013 & 0{,}033 & 0{,}033 & 0 & 0{,}033 & 0{,}033 & 0{,}033 & 0{,}033 & 0{,}033 & 0{,}033 & 0{,}033 \\
0{,}02 & 0 & 0{,}04 & 0{,}04 & 0 & 0 & 0 & 0{,}04 & 0 & 0{,}04 & 0{,}04 \\
0{,}02 & 0 & 0{,}04 & 0{,}04 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}04 \\
0{,}01 & 0 & 0{,}03 & 0{,}03 & 0 & 0{,}03 & 0{,}03 & 0{,}03 & 0{,}03 & 0{,}03 & 0{,}03 \\
0{,}02 & 0 & 0 & 0{,}04 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}04 \\
0{,}02 & 0{,}041 & 0{,}041 & 0 & 0{,}041 & 0{,}041 & 0{,}041 & 0{,}041 & 0 & 0 & 0 \\
0{,}017 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}038 & 0 & 0 & 0 \\
0{,}01 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}041 & 0 & 0 & 0{,}041 \\
0{,}013 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}032 & 0 & 0{,}032 & 0{,}032 \\
0{,}02 & 0 & 0 & 0{,}039 & 0 & 0 & 0 & 0{,}039 & 0{,}039 & 0{,}039 & 0{,}039 \\
0{,}02 & 0 & 0{,}041 & 0{,}041 & 0 & 0 & 0 & 0{,}041 & 0 & 0{,}041 & 0 \\
0{,}013 & 0 & 0 & 0{,}034 & 0 & 0 & 0 & 0{,}034 & 0 & 0 & 0 \\
0{,}01 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}04 & 0 & 0{,}04 & 0 \\
0{,}017 & 0 & 0 & 0{,}038 & 0 & 0 & 0 & 0{,}038 & 0{,}038 & 0{,}038 & 0{,}038 \\
0{,}02 & 0 & 0{,}04 & 0{,}04 & 0 & 0 & 0 & 0{,}04 & 0{,}04 & 0{,}04 & 0{,}04 \\
0{,}01 & 0 & 0{,}02 & 0{,}02 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}02 \\
0{,}013 & 0 & 0{,}032 & 0 & 0 & 0 & 0 & 0 & 0{,}032 & 0 & 0 \\
0{,}02 & 0 & 0{,}041 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}041 & 0{,}041 \\
0{,}013 & 0{,}034 & 0{,}034 & 0 & 0{,}034 & 0 & 0{,}034 & 0{,}034 & 0{,}034 & 0{,}034 & 0{,}034 \\
0 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 & 0{,}036 \\
0{,}01 & 0{,}031 & 0{,}031 & 0{,}031 & 0{,}031 & 0 & 0 & 0 & 0 & 0 & 0 \\
0{,}015 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 \\
0{,}015 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 \\
0{,}015 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 \\
0{,}015 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 \\
0{,}015 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035 & 0{,}035
\end{array}\right|$$

Fig. 6.8. Matrix $Q = \left\| q_{ij} \right\|$ – the cost of computing resources for input information

$$\left|\begin{array}{ccccccccccc}
0,068 & 0,025 & 0,025 & 0 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 \\
0,063 & 0,02 & 0,02 & 0 & 0,02 & 0 & 0,02 & 0,02 & 0,02 & 0,02 & 0,02 \\
0,07 & 0,027 & 0,027 & 0,027 & 0,027 & 0 & 0,027 & 0 & 0,027 & 0,027 & 0,027 \\
0,066 & 0,023 & 0,023 & 0 & 0,023 & 0,023 & 0,023 & 0,023 & 0,023 & 0,023 & 0,023 \\
0,063 & 0 & 0,02 & 0,02 & 0 & 0 & 0 & 0,02 & 0 & 0,02 & 0,02 \\
0,073 & 0 & 0,03 & 0,03 & 0 & 0 & 0 & 0 & 0 & 0 & 0,03 \\
0,063 & 0 & 0,02 & 0,02 & 0 & 0,02 & 0,02 & 0,02 & 0,02 & 0,02 & 0,02 \\
0,073 & 0 & 0 & 0,03 & 0 & 0 & 0 & 0 & 0 & 0 & 0,03 \\
0,073 & 0,03 & 0,03 & 0 & 0,03 & 0,03 & 0,03 & 0,03 & 0 & 0 & 0 \\
0,07 & 0 & 0 & 0 & 0 & 0 & 0 & 0,027 & 0 & 0 & 0 \\
0,063 & 0 & 0 & 0 & 0 & 0 & 0 & 0,02 & 0 & 0 & 0,02 \\
0,066 & 0 & 0 & 0 & 0 & 0 & 0 & 0,023 & 0 & 0,023 & 0,023 \\
0,073 & 0 & 0 & 0,03 & 0 & 0 & 0 & 0,03 & 0,03 & 0,03 & 0,03 \\
0,073 & 0 & 0,03 & 0,03 & 0 & 0 & 0 & 0,03 & 0 & 0,03 & 0 \\
0,066 & 0 & 0 & 0,023 & 0 & 0 & 0 & 0,023 & 0 & 0 & 0 \\
0,063 & 0 & 0 & 0 & 0 & 0 & 0 & 0,02 & 0 & 0,02 & 0 \\
0,07 & 0 & 0 & 0,027 & 0 & 0 & 0 & 0,027 & 0,027 & 0,027 & 0,027 \\
0,073 & 0 & 0,03 & 0,03 & 0 & 0 & 0 & 0,03 & 0,03 & 0,03 & 0,03 \\
0,063 & 0 & 0,02 & 0,02 & 0 & 0 & 0 & 0 & 0 & 0 & 0,02 \\
0,066 & 0 & 0,023 & 0 & 0 & 0 & 0 & 0 & 0,023 & 0 & 0 \\
0,073 & 0 & 0,03 & 0 & 0 & 0 & 0 & 0 & 0 & 0,03 & 0,03 \\
0,066 & 0,023 & 0,023 & 0 & 0,023 & 0 & 0,023 & 0,023 & 0,023 & 0,023 & 0,023 \\
0,068 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0,063 & 0,02 & 0,02 & 0,02 & 0,02 & 0 & 0 & 0 & 0 & 0 & 0 \\
0,068 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 \\
0,068 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 \\
0,068 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 \\
0,068 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 \\
0,068 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025 & 0,025
\end{array}\right|$$

Fig. 6.9. Matrix $P = \left\| p_{ij} \right\|$ – the cost of computing resources for the output of information

$c_{1,2}$	$c_{2,21}$	$c_{4,6}$	$c_{5,23}$	$c_{9,22}$	$c_{12,17}$	$c_{15,17}$	$c_{18,26}$
$c_{1,4}$	$c_{2,22}$	$c_{4,7}$	$c_{5,26}$	$c_{9,26}$	$c_{12,18}$	$c_{15,18}$	$c_{20,22}$
$c_{1,5}$	$c_{2,23}$	$c_{4,9}$	$c_{6,9}$	$c_{10,26}$	$c_{12,22}$	$c_{15,22}$	$c_{20,26}$
$c_{1,6}$	$c_{2,24}$	$c_{4,24}$	$c_{6,24}$	$c_{11,12}$	$c_{12,26}$	$c_{15,23}$	$c_{21,22}$
$c_{1,7}$	$c_{2,26}$	$c_{4,26}$	$c_{6,26}$	$c_{11,13}$	$c_{13,14}$	$c_{15,26}$	$c_{21,23}$
$c_{1,9}$	$c_{3,5}$	$c_{5,10}$	$c_{7,8}$	$c_{11,14}$	$c_{13,15}$	$c_{16,17}$	$c_{21,26}$
$c_{1,24}$	$c_{3,6}$	$c_{5,11}$	$c_{7,26}$	$c_{11,15}$	$c_{13,16}$	$c_{16,18}$	$c_{22,23}$
$c_{1,6}$	$c_{3,7}$	$c_{5,12}$	$c_{8,20}$	$c_{11,16}$	$c_{13,17}$	$c_{16,22}$	$c_{22,26}$
$c_{2,4}$	$c_{3,8}$	$c_{5,13}$	$c_{8,21}$	$c_{11,17}$	$c_{13,18}$	$c_{16,26}$	$c_{24,26}$
$c_{2,5}$	$c_{3,9}$	$c_{5,14}$	$c_{8,22}$	$c_{11,18}$	$c_{13,22}$	$c_{17,18}$	$c_{25,26}$
$c_{2,6}$	$c_{3,14}$	$c_{5,15}$	$c_{8,26}$	$c_{11,19}$	$c_{13,26}$	$c_{17,20}$	
$c_{2,7}$	$c_{3,19}$	$c_{5,16}$	$c_{9,10}$	$c_{11,22}$	$c_{14,15}$	$c_{17,21}$	
$c_{2,9}$	$c_{3,20}$	$c_{5,17}$	$c_{9,14}$	$c_{11,26}$	$c_{14,19}$	$c_{17,22}$	
$c_{2,13}$	$c_{3,24}$	$c_{5,18}$	$c_{9,16}$	$c_{12,14}$	$c_{14,22}$	$c_{17,26}$	
$c_{2,17}$	$c_{3,26}$	$c_{5,21}$	$c_{9,17}$	$c_{12,15}$	$c_{14,26}$	$c_{18,22}$	
$c_{2,18}$	$c_{4,5}$	$c_{5,22}$	$c_{9,18}$	$c_{12,16}$	$c_{15,16}$	$c_{18,23}$	

Fig. 6.10. Matrix $C = \left\| c_{i_k i_l} \right\|$

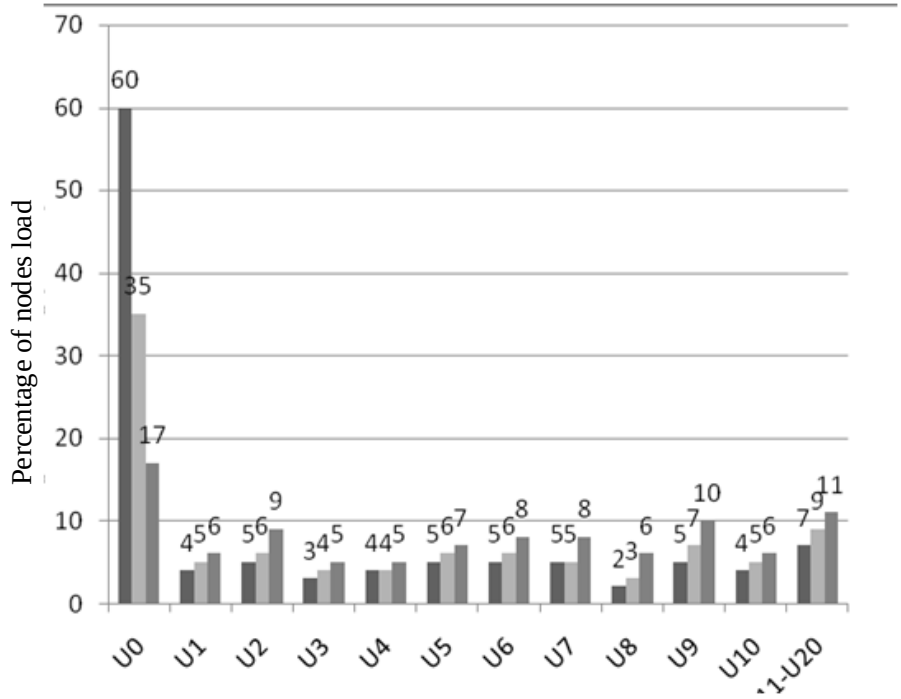


Fig. 6.11. Loading ICN nodes for topology options

Based on the obtained simulation results [146], when deciding on the choice of ICN structure, preference is given to the option J_3 in which STC more evenly loads the main network nodes, by reducing the cost of network resources for information transfer between nodes.

The use of the method of distribution of tasks on the nodes of the network [147] has reduced the time of solving management tasks and technological tasks by an average of 15%. Summary simulation data are presented in Figure 6.12 [34].

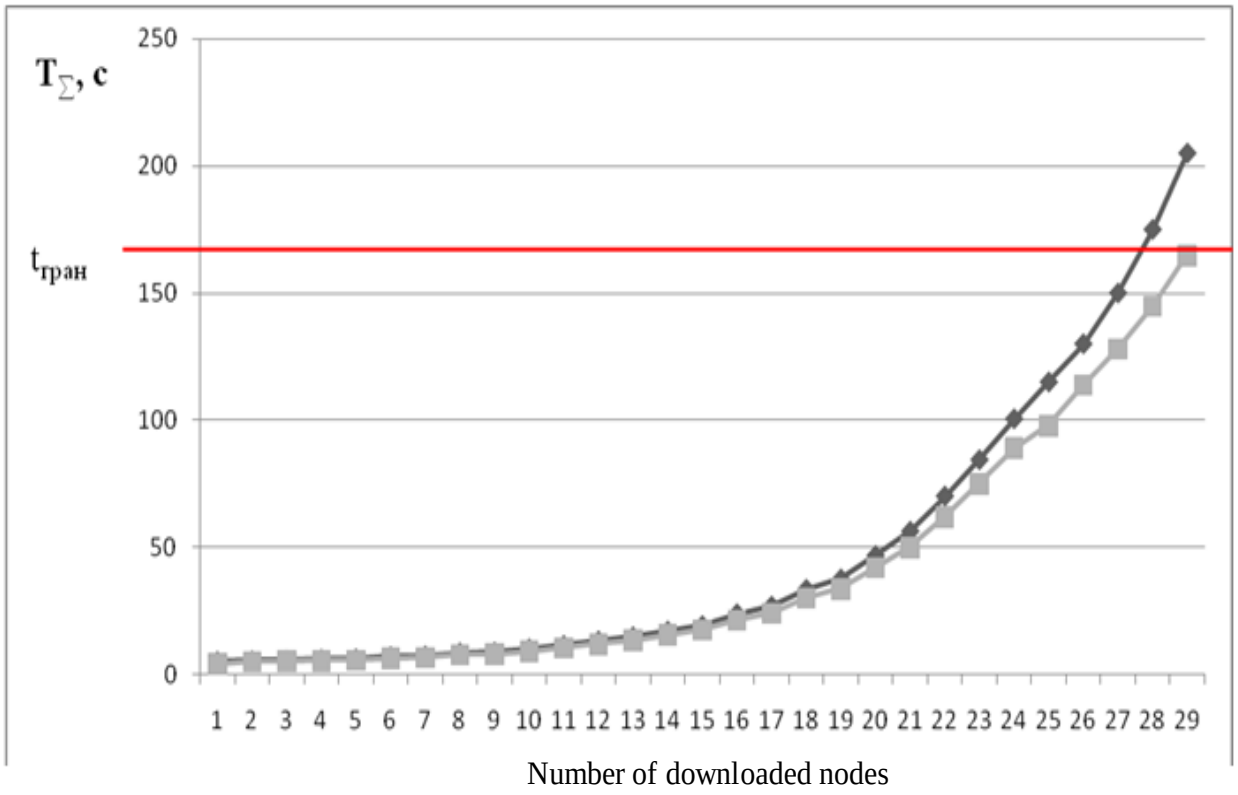


Fig. 6.12. The duration of solving management tasks and technological tasks depending on their number

6.4 Risk analysis of ICN STC

For ICN STC, you can determine the partial risks and their causes, which are given in Table 6.6.

Table 6.6 – Causes and partial risks of ICN STC

Categories of factors	***Causes of risks***	***Partial risks***
Technical factors	P_{11} - lack of capacity P_{12} -lack of performance	R_1 - risk of equipment failure
	P_{21} - poor configuration management P_{22} - poor change management P_{23} - incorrect security settings P_{24} - dangerous programming practices P_{25} - improper testing	R_2 - risk of software failure
	P_{31} - design problems P_{32} - integration issues P_{33} - system complexity	R_3 - risk of error in network design
Process factors	P_{41} - improper technological. process P_{42} - incorrect information flows P_{43} - Improper escalation of problems P_{44} - inefficient task transfer	R_4 - risk of error in network processes (design and execution)
	P_{51} - Lack of condition monitoring P_{52} - no periodic analysis P_{53} - improper ownership of the process	R_5 - risk of process control error
The human factor	P_{71} - accidental error P_{72} - ignorance P_{73} - failure to follow instructions	R_7 - risk of unintentional action
External factors	P_{101} - fire	R_{10} - risk of catastrophe
	P_{131} - problems with power supply	R_{13} - risk of poor quality services

Taking into account the influence of risks on the parameters of ICN, a system model is formed (Fig. 6.13).

According to the system model, a cause-and-effect diagram of the interaction "causes-risks-consequences" is constructed (Fig. 6.14).

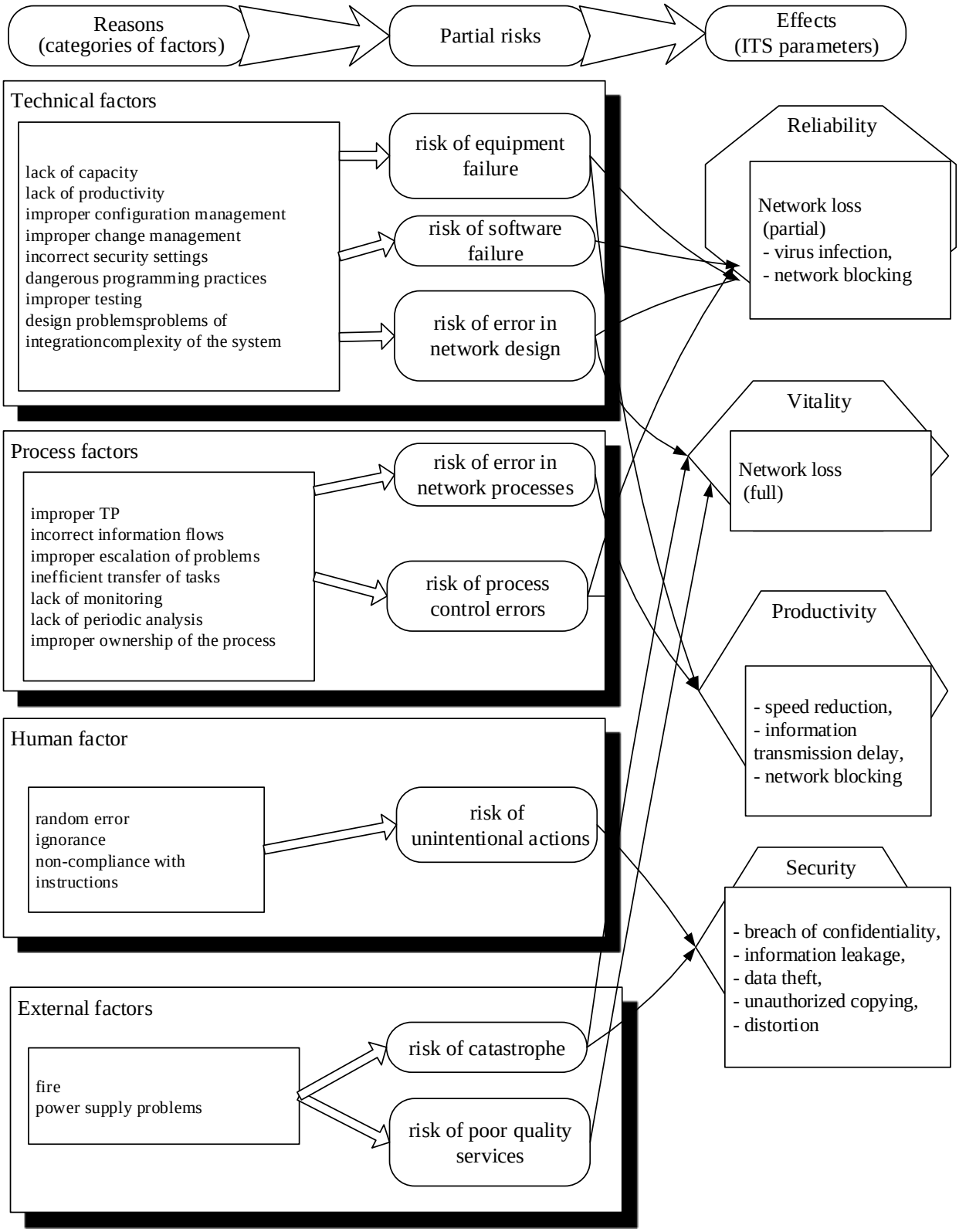


Fig. 6.13. Systemic risk model of ICN STC

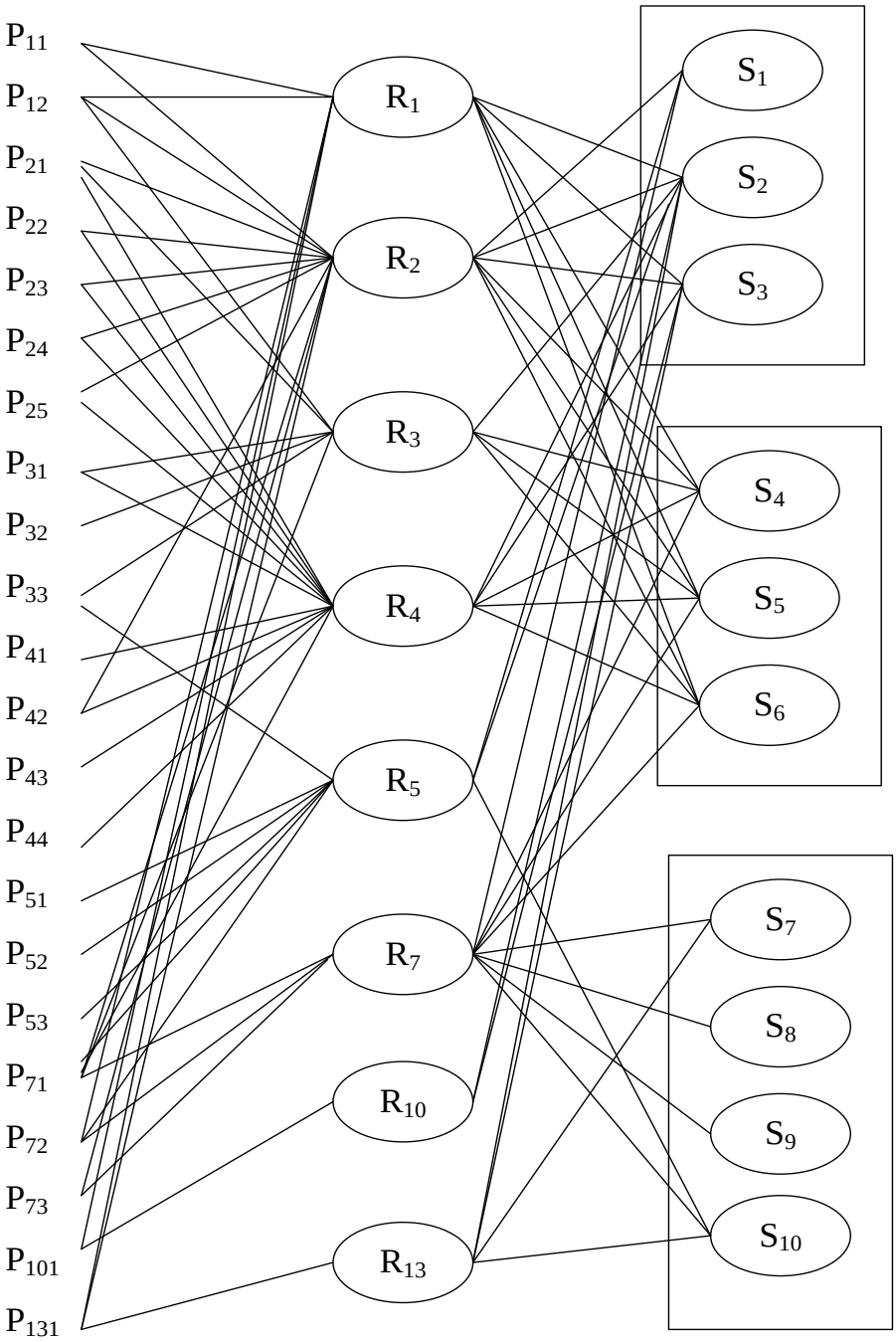


Fig. 6.14. Cause-and-effect chart of ICN STC risks

Impact factors are assessed using a group of experts (Tables 6.7 and 6.8), in which the assessments are marked on a 10-point scale.

Table 6.7 – Matrix of coefficients of influence of factors on partial risks of ICN

Reasons	Partial risks							
	Equipment failure	**Software failure**	**Network design error**	**Error in network process**	**Process control error**	**Unintentional actions**	**Catastrophe**	**Poor quality services**
P_{11}	9	5	0	0	0	0	0	0
P_{12}	10	4	2	0	0	0	0	0
P_{21}	0	5	3	2	0	0	0	0
P_{22}	0	4	0	1	0	0	0	0
P_{23}	0	10	0	8	0	0	0	0
P_{24}	0	2	0	1	0	0	0	0
P_{25}	0	3	0	1	0	0	0	0
P_{31}	0	0	5	2	0	0	0	0
P_{32}	0	0	4	0	0	0	0	0
P_{33}	0	0	3	0	2	0	0	0
P_{41}	0	0	0	4	0	0	0	0
P_{42}	0	6	0	8	0	0	0	0
P_{43}	0	0	0	4	0	0	0	0
P_{44}	0	0	0	8	0	0	0	0
P_{51}	0	0	0	0	6	0	0	0
P_{52}	0	0	0	0	6	0	0	0
P_{53}	0	0	0	0	5	0	0	0
P_{71}	1	2	1	2	3	6	0	0
P_{72}	0	0	0	0	1	2	0	0
P_{73}	0	2	0	0	2	3	0	0
P_{101}	5	0	0	0	0	0	7	0
P_{131}	4	3	0	2	0	0	0	6

Table 6.8 – Matrix of coefficients of influence of risks on possible consequences

Partial risks	**Network indicators (consequences of risks)**									
	Reliability		**Vit.**	**Productivity**			**Security**			
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}
Equipment failure	0	10	9	7	7	7	0	0	0	0
Software failure	10	7	1	4	6	5	0	0	0	0
Design error	0	5	0	8	8	4	0	0	0	0
Process error	0	4	1	8	8	3	0	0	0	0
Control error	2	5	0	0	0	0	0	0	0	2
Unintentional actions	6	2	0	3	3	1	4	2	2	8
Catastrophe	0	5	3	0	0	0	0	0	0	0
Poor quality services	0	3	1	0	0	0	1	0	0	2

Using formula (3.1), the total influence of factors on the final vertices of the diagram was calculated – the possible consequences (Table 6.9). The table on the right shows the total significance of the causes, their normalized values.

Table 6.9 – Calculation of the significance of factors and the probability of consequences

Factors	**Basic network parameters**										**Total significance**	**Normalized significance (a')**
	Reliability		**Viability**	**Performance**			**Security**					
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}		
P_{11}	50	125	86	83	93	88	0	0	0	0	525	0,109
P_{12}	40	138	94	102	110	98	0	0	0	0	582	0,121
P_{21}	50	58	7	60	70	43	0	0	0	0	288	0,060
P_{22}	40	32	5	24	32	23	0	0	0	0	156	0,032
P_{23}	100	102	18	104	124	74	0	0	0	0	522	0,108
P_{24}	20	18	3	16	20	13	0	0	0	0	90	0,019
P_{25}	30	25	4	20	26	18	0	0	0	0	123	0,025
P_{31}	0	33	2	56	56	26	0	0	0	0	173	0,036
P_{32}	0	20	0	32	32	16	0	0	0	0	100	0,021
P_{33}	4	25	0	24	24	12	0	0	0	4	93	0,019
P_{41}	0	16	4	32	32	12	0	0	0	0	96	0,020
P_{42}	60	74	14	88	100	54	0	0	0	0	390	0,081
P_{43}	0	16	4	32	32	12	0	0	0	0	96	0,020
P_{44}	0	32	8	64	64	24	0	0	0	0	192	0,040
P_{51}	12	30	0	0	0	0	0	0	0	12	54	0,011
P_{52}	12	30	0	0	0	0	0	0	0	12	54	0,011
P_{53}	10	25	0	0	0	0	0	0	0	10	45	0,009
P_{71}	62	64	13	57	61	33	24	12	12	54	392	0,081
P_{72}	14	9	0	6	6	2	8	4	4	18	71	0,015
P_{73}	42	30	2	17	21	13	12	6	6	28	177	0,037
P_{101}	0	85	66	35	35	35	0	0	0	0	256	0,053
P_{131}	30	87	47	56	62	49	6	0	0	12	349	0,072
Total impact	576	1074	377	908	1000	645	50	22	22	150	4824	1
Norm. Coef. (p')	0,119	0,222	0,078	0,188	0,207	0,134	0,104	0,005	0,005	0,031	1	
	0,341		0,078	0,529			0,145				1	

In the lower terms of the table – the total impact for each of the consequences and their normalized values, this can be considered as the probability of occurrence of each of the consequences.

In addition, the level of risk for the main parameters of network operation was assessed.

Statistical characteristics for the significance of the impact of factors were obtained: lower and upper quartile, average value (Table 6.10).

Table 6.10 – Statistical characteristics of the significance of the impact of factors

Coefficient of significance	Average	Lower quartile	Upper quartile	Standard deviation
a’	0,045455	0,019279	0,072347	0,035062

Based on these characteristics, the factors can be classified into groups: the most important (a’> 0.072), quite significant (0.045 <a’ <0.072), medium (0.045 <a’<0.072), insignificant (0.019 <a’ <0.045).

In other words, the most important risk factors (causes) are:

- lack of capacity;
- lack of performance;
- incorrect security settings;
- incorrect information flows;
- random error.

In addition, it can be concluded that the most vulnerable element of ICN is "productivity" (p'=0.53). The next vulnerability parameter is "reliability" (p ' =0.34).

Based on the results of the risk analysis (comparison of significant impact factors), the following security measures were proposed:

1. To reduce the risk of hardware failure [143]:

- - various options for reserving elements in STC cabinets (information input/output modules; input/output buses; central controllers; data exchange networks; power supplies must be supported;

- should provide duplication of the computer network;

- it is necessary to provide redundancy, interrogation and issuance of discrete and analog information, initial testing when the power is turned on, diagnosing hardware with shock-free switching of the main/backup channel;

- when collecting analog signals, the measurement of parameters, the failure of which may lead to erroneous operation of technological protections or disconnection of the main controllers, must be performed by redundant measuring transducers;

- redundant measuring transducers must be disconnected from each other by pulse lines, communication cables and power supply.

2. To reduce the risk of software:

- providing protection against unauthorized access to the logical part of the programs in order to change them;

- correction of the database, settings and functional software STC should be performed only from the engineering station after entering the password;

- several levels of access to software, databases and registration archives should be implemented, level of system administrator, level of operational and service personnel, distribution of access should be determined by job descriptions of personnel;

- software diagnostics and self-monitoring;

- providing protection against computer viruses.

3. To reduce the risk of network processes:

- for the PC the reserve of 50% on memory and time of the performed tasks should be provided, at standard loading by processes for such working conditions:

- for networks a reserve of 50% on capacity from peak loading should be provided;

- when allocating tasks between STC cabinets, a reserve of at least 10% on input signals and output commands and 25% reserve of memory and calculation time for realization of possible changes of technological algorithms of direction, control and presentation of information must be provided;

- it is necessary to provide such reliability indicators for the control and information functions of the STC UL and GC:

1) to describe the failure-free N-functions, the average system time to failure is T_{av};

2) to describe the reliability of D-functions, the probability of successful operation when a request is received – L;

3) parameter for the "false positive" type of failure flow" – W;

4) to describe the reliability of the STC in relation to emergencies, the average operating time of the system before the occurrence of an emergency situation that requires shutdown of equipment, under normal conditions of operation of the system – T_{em}.

4. To reduce the risk in the design of the network it is necessary to distribute the functions and tasks between the cabinets of STC and workstations in the design process: by technological affiliation of equipment with control organization, by mode and functional-group characteristics, and in accordance with reliability requirements.

5. To reduce the risk of process control errors:

- emergency control of the CTB is implemented on the central control panels of the generating units of the GPA and the central general control panel of the GPA;

- in case of failures of individual elements of STC degradation should occur with the preservation of all functions that are not affected by the efficiency of the elements that failed;

- the STC diagnostic system must ensure the detection of failed elements with an accuracy of one or more variable constructs;

- recovery should be carried out by replacing the failed module from the spare tool and accessories (spare parts) without its additional adjustment.

6. To reduce the risk of unintentional actions - providing protection against failures, distortions, erroneous and unauthorized actions of staff:

- in order to prevent erroneous actions of the personnel servicing STC, the following organizational measures should be provided: standard repair programs have been developed; keep logs of changes in algorithmic, informational and software; eriodic training and testing of staff knowledge;

- the software must control the authenticity and protection against distortion of input information entered by staff;

- the software must exclude failures related to incorrect input information when performing calculations;

- information about the unreliable state of input parameters should be formed;

- protection against entering erroneous data must be provided (with the display of messages on the screen and setting the value of the information "by default");

- protection must be provided against actions that are currently unacceptable (by setting the state of "inactivity" to buttons, input fields and other controls of the window system). All erroneous actions of the staff must be accompanied by the display of messages on the screen and in the operator's log.

7. To reduce the risk of a catastrophe:

- the following technical and organizational measures should be provided to save information from destruction in case of accidents and power failures of the system:

1) external memory devices that ensure the preservation of software and its recovery in accordance with the regulations;

2) independent software storage devices located in control cabinets;

3) the presence of power supplies such as UPS workstation and engineering station, which provide power to the PC when disconnecting external power sources for at least 15 minutes;

4) regulations for copying and storing software and databases on external media;

- connections of STC cabinets with sources of analog and discrete information must be performed by a certified cable with copper cores and insulation that does not sprained combustion;

- separate laying of low-voltage and high-voltage cables must be provided;

- low-voltage cables of PTC connections must have a common screen, high-voltage cables must not have shielding;

- cable shields must be galvanically isolated from the general ground circuit along the entire length of the cable;

- it is not allowed to connect two or more sections of cables by means of connectors, soldering, twisting, etc.;

- flexible cables with non-combustible insulation must be used.

8. To reduce the risk of poor quality services after disconnection and restoration of power supply, the STC must automatically resume the performance of the intended functions in full no later than after 2 min. for LL controllers and 5 min. for IL and UL workstations and servers after power recovery.

CONCLUSIONS

The monograph considers the problems of information support of critical infrastructure systems. When studying the requirements and quality parameters of ICN CIS, it was determined that the existing information technologies and methods of traffic distribution management, in the conditions of growing volumes of circulating information, as well as dynamic change of data structure in CIS are not able to meet the requirements of information exchange.

The range of problems caused by the specifics of ICN and CIS application software is identified. They determined the promising direction of development and implementation of information technology for the efficient operation of infocommunication networks, which would ensure the transfer of information between subsystems and functional modules of the system with the required quality.

Analysis of the current state of telecommunications technologies and basic protocol solutions showed the rapid dynamics of ICN in the direction of creating high-speed multiservice networks, which is associated with the need to find new approaches to determining the physical and functional architecture. Despite the advanced development of physical and channel layer technologies, it is possible to fully realize the potential of ICN CIS only through effective management of available network resources in the face of growing requirements for the efficiency of information exchange.

The principles of network traffic distribution management in ICN CIS are formulated and practical requirements to data transmission efficiency are determined.

Possibilities of network decomposition possibility by allocation of separate subnets corresponding to application of VLAN and VPN technologies are defined, properties of data streams at decomposition are investigated, tasks of adjustment and operative management at network decomposition are formulated, and advantages of application of the decomposition principle at network creation and management are shown. Additive functionalities of quality of management of all

networks are used for coordination of the purposes of management, including the weighted functions of quality of management of separate subnets. As a result there is a possibility to reduce the general task of management of distribution of traffic and individual subnets.

The set of network parameters, network state space and traffic distribution control parameters are defined. It is shown that for real networks with constant basic parameters the state space is connected, ie it is possible to transfer a network from one state to another in one control step. The obtained results make it possible to determine the composition of network parameters, highlight control parameters and relate them to the capabilities and parameters of the network equipment used in creating the network.

The purposes and tasks of management of distribution of traffic taking into account specificity of work of applications and requirements to characteristics of their work are considered. Subsets of basic and variable control parameters are allocated, which allowed to divide the network management process into two stages: network setup and operational management, which differ in the composition of the tasks and the frequency of application. These results allow us to identify and formulate the tasks to be solved at different stages of network creation and operation, to determine the specific composition of control parameters for each task.

Some partial tasks of adjustment and operative management which meet in practice are investigated: tasks of management of distribution of a bandwidth of a communication channel, tasks of distribution of resources of the multiserver node of information processing. The method of adaptive control of information flow distribution provides for stratified two-tier management, which is based on the formation of a multidimensional space of network states and management parameters taking into account user activity, which reduces processing time of system transactions and total maintenance costs. Reduction of transaction processing time is carried out by 10-15% due to the decomposition of the network structure in the operational management of traffic distribution.

The multi-server node resource allocation method treats server systems as a set of single-line queuing systems and uses bandwidth allocation information that minimizes flow maintenance costs.

The substantiation of requirements to the complex criterion of quality of management of network traffic is carried out and its generalized formalized kind is resulted.

The task of risk management of the infocommunication network to ensure the security of the CIS is considered. The main sources of threats to the functioning of the CIS have been identified. It is proposed to carry out the risk management process at three levels in order to effectively inter-level management and intra-level interaction of all components of the system.

The classification of partial risks of ICN on the reasons and factors of their occurrence is carried out. The negative consequences influencing the main characteristics of ICN functioning are determined. As a result, a structural system model of ICN risks is formed, which reflects the relationships between the elements of the main aspects of risk.

A method based on the theory of causal analysis is used to quantify the impact of risk on the functioning of the ICN. The risk model is based on the construction and analysis of probabilistic or fuzzy cognitive maps.

Based on the structure of the causal diagram of factors, manifestations and consequences of risks, a quantitative assessment of the possibility of the consequences of risks is obtained. An assessment of the possible damage to the operation of the network was also made, which is determined by the specific consequence caused by partial risks. Thus, the application of the ICN risk assessment method increases the accuracy of quantifying the possible damage to the operation of the network by taking better account of its causes.

The obtained results can be used to determine possible failures in the functioning of the ICN based on information about the degree of influence of risk factors, risk events and consequences, as well as the causal relationships between

them. It becomes possible to identify potential losses, as well as to take measures to manage the risks of ICN operation.

To assess the probabilities of partial risks due to difficulties in traffic transmission, methods of modeling random processes are used. A combinatorial approach to modeling random processes with one-dimensional distribution density and correlation function is used. The application of the method of modeling random processes allows to calculate the characteristics of a random process taking into account its form and to assess the probability of risk when transmitting traffic to ICN.

Risk management methods for improving the security of critical infrastructure systems are considered. A comprehensive indicator has been formed to determine the risk category of the information system. The variants of the complete factor space of the set of values of the specified features and the corresponding categories of the system are considered. The process of adapting the specification of risk counteraction measures, which is part of the ICN risk management process, is described.

Strategies and mechanisms for improving ICN security are considered. The monitoring of the state of the system, mechanisms and means of counteraction will allow to recognize and promptly respond to the information risks of ICN.

To reduce the risk of equipment failure at ICN nodes, diagnostic algorithms are used to determine the technical condition of objects. The analysis of diagnostic models showed that the most effective model is in the form of a fault matrix, which is formalized using an algebraic approach. The use of algorithmic position diagram allows you to evaluate the effectiveness of diagnostic algorithms. The risk reduction coefficient is used to assess the effectiveness of diagnosing equipment in order to reduce the risk of failure at network nodes.

To reduce the risk of errors in ICN communication channels, an adaptive procedure for calculating linear decision functions is used, which helps to increase the noise immunity of reception in data networks.

The monograph describes the structure of information technology risk-adaptive data flow management of the infocommunication network, which reflects the sequential operation of the three blocks. The application of this technology is effective in the stages of requirements specification and design of network architecture.

Practical approbation of information technology was carried out for the "Complex for solid waste processing with a system of landfill gas collection, utilization and production". As a part of the task of building a network structure and determining its parameters, sets of elements of the information structure were formed, matrices of their relationships were constructed, and the intensities of data flows were determined. As a result, requirements for the technical structure of the network were formed.

The directions and volumes of information flows within the basic ICN were also studied. Using the developed information technology and data on the directions and volumes of information circulating in the network, the modeling of STC software operation was carried out. The performed simulation allowed to suggest alternative variants of the ICN topology. The simulation results showed that the selected topology allows to bring the loading of the core network nodes to uniform and thus reduce the time spent by the task in the network.

A computational experiment was done to study the operation of software in a heterogeneous multiservice network.

The system model of risks, the cause-and-effect diagram are constructed, matrices of coefficients of influence are defined. As a result, the levels of significance of factors and the probability of possible consequences are calculated. The most vulnerable characteristics of the network (performance and reliability) were identified. As a result, measures to fend off eight partial risks were formulated.

Experimental application of information technology of adaptive control of ICN parameters has shown that its use increases the efficiency of information transmission in infocommunication networks of ACS TP. In particular, when in-

creasing the relative volumes of information transmitted by the subsystem of the ACS TP, the total relative time for the implementation of decisions made on the basis of the results of the application of adaptive technology is reduced to 15%. It is shown that the use of the proposed information technology can reduce the information risk of the network by 30%.

The obtained results can be considered as a basis for solving problems of synthesis of ICN software and hardware environment, which uses models, methods and technologies for managing data flow parameters related to optimization of network performance, which may include certain information technologies and scientific principles of measurement, modeling, description and management of ICN parameters to obtain the necessary network performance, as well as directly to implement adaptive traffic management.

LIST OF LITERARY SOURCES

1. Yudin A. Yu., Pirogov G.V. Analysis and evaluation of regulatory documents used to ensure information security of Smart Grid systems. Legal, regulatory and metrological support of the information protection system in Ukraine. 2013. № 1. P. 88.

2. Lewis T. G. Critical infrastructure protection in homeland security: defending a networked nation. New Jersey: John Wiley & Sons. 2006. 474 p.

3. On approval of the Procedure for forming the list of information and telecommunication systems for objects of critical infrastructure of the state. Document 563-2016-n, current, current version. Admitted 23.08.2016 http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF.

4. Biryukov D.S., Kondratov S.I. Protection of critical infrastructure: problems and prospects for implementation in Ukraine. Kyiv: NISS. 2012. 96 p. http://www.niss.gov.ua/content/articles/files/Sots_zahust-86178.pdf.

5. Gonchar S.F. Ways to improve the state policy of information security of critical infrastructure of Ukraine: materials of the round table "State response to threats to national interests of Ukraine: current issues and ways to solve them", February 19, 2014 Kyiv: NAPA under the President of Ukraine (Department of National Security) 2014. P. 92–95.

6. Council Directive 2008/114/EC "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" [Electronic resource]. Access mode: http://eurlex.europa.eu.

7. On the decision of the National Security and Defense Council of Ukraine of June 8, 2012 "On the new version of the National Security Strategy of Ukraine": Decree of the President of Ukraine of June 8, 2012 № 389/2012 [Electronic resource]. Access mode: http://zakon2.rada.gov.ua/laws/show/389/20124.5.

8. Domarev V. V. Security of information technologies. Methodology for creating security systems. Kiev: LLC "TID DS". 2002. 688 p.

9. "On the National System of Confidential Communications" The Verkhovna Rada of Ukraine; Law of 10.01.2002 № 2919-III http://zakon3.rada.gov.ua/laws/show/2919-14.

10. Shevchenko N. M. Method of system-complex research of state management of ensuring national security. Bulletin of the National Academy of defense of Ukraine. 2010. No. 4. P. 235-240.

11. Gonchar S. F. Analysis of the probability of implementing threats to information security in automated process control systems. Information protection. 2014. Volume 16. # 1. Pp. 40-46.

12. Konakh V. K. National information space of Ukraine: problems of formation and state regulation: analit. add. Kiev: NISI. 2014. 76 p.

13. Kosenko V. V. Criteria for effective use of information and telecommunications network resources. Proceedings of the International scientific and practical conference «Mathematical modeling of processes in Economics and project and program management (MMP-2015)". Kharkiv-Nikolaev. 2015. Pp. 105-106.

14. Methods and tools for improving the reliability and information stability of multiprocessor systems for critical facilities: research report; H.of w. Rob. O. Romankevich. Kiev. 2014. 119 p.

15. Lavrut O.O. Research of quality of management of streams of information in telecommunication system of critical purpose. Weapons systems and military equipment. 2014. № 4 (40). Pp. 89–93.

16. Hashemian H. M. Predictive maintenance in nuclear power plants through online monitoring. Nuclear and Radiation Safety Journal. 2013. № 4. P. 42–50.

17. Kargin V.A., Nikolaev D.A., Skorokhodov Ya.A. Estimation of probabilistic characteristics of telemetry processes of launch vehicles in real time. Proceedings of the military space Academy named after A. F. Mozhaysky. 2014. Issue # 644. Pp. 161-168.

18. Lemeshko A.V., Vavenko T. V. Development and research of a stream model of adaptive routing in software-configured networks with load balancing. Reports of the Tomsk state University of control systems and Radioelectronics. 2013. no. 3 (29). Pp. 100-108.

19. Smith W. E., Tomek L., Ackaret J. Availability analysis of blade server systems. IBM Systems Journal. 2008. Vol. 47. No. 4. P. 621–640.

20. Shelukhin O. I. Modeling of information systems. Moscow: Hot line-the Telecom. 2012. 516 p.

21. Tanenbaum E. S., Weatherall D. Computer networks. 5th ed. St. Petersburg: Piter. 2012. 960 p.

22. Kuchuk G. A., Gakhov R. P., Pashnev A. A. Management of info telecommunications resources. Moscow: FIZMATLIT, 2006. 220 p.

23. Olifer V. G., Olifer N. A. Computer networks: principles, technologies and protocols. 3rd ed. Saint Petersburg: Piter. 2008. 958 p.

24. Borodakiy Yu. V. Evolution of information systems (current state and prospects). Moscow: Hot Line – The Telecom. 2011. 368 p.

25. Popovsky V. V., Oleinik V. F. Mathematical foundations of management and adaptation in telecommunications systems. Kharkiv: LLC "Smith Company". 2011. 362 p.

26. Konakhovich G. F., Chuprin V. M. Packet data transmission Networks. Kiev: MK-Press. 2006. 272 p.

27. Kosenko V. V., Kuchuk N. G. Interaction of technical and software tools in traffic distribution management. Scientific publication "Weapons systems and military equipment". Issue 3 (47). 2016. Pp. 72-75.

28. Stepanov S. N. Fundamentals of teletraffic multiservice networks. Eco-Trends. 2010. 391 p.

29. Kuchuk G. A. Method of synthesis of the information structure of a connected fragment of a corporate multiservice network. Collection of scientific papers of the Kharkiv National Air Force University. Kharkiv: KNAFU. 2013. Issue. 2. Pp. 97-102.

30. Schneps-Schnappe M. A. Architecture of PARLAY and communication networks of the new generation NGN: nine lectures. Moscow: MAKS Press. 2004. 137 p.

31. Chizhikov D. Multiservice networks of the next generation: market needs, principles, monitoring. M.: LLC "X-Media", 2008.

32. Poshtarenko V.M., Andreev A. Yu., Amal M. Ensuring the quality of service in critical areas of the multiservice network. Bulletin of the National Technical University. 2013. № 60. P. 94–100.

33. Talalaev V. A., Gritsky G. V., Kucher S. V. Mobile telecommunications networks of critical application: information and conceptual model of the subject area. Radio-electronic and computer systems. 2006. No. 5 (17). Pp. 185-192.

34. Kosenko V. V., Mozhaev O. O., Ilyina I. V. Issues of switching in broadband digital networks. Control, navigation and communication systems. Kiev: Central research Institute of NiU. 2007. Issue 1. Pp. 74-76.

35. Kovalenko A. A. Approaches to the synthesis of the technical structure of a computer system that forms a control system for the object of critical application. Collection of scientific papers of the Kharkiv Air Force University, 2014, no. 1, Pp. 116-119.

36. Baranovskaya T. P., Loiko V. I., Semenov M. I. and others. Architecture of systems and networks. Moscow: Finance and statistics. 2003. 364 p.

37. Basic standards of data transmitting networks [Electronic resource]. Access mode: http://www.gpntb.ru/win/book/5/Doc11.HTML

38. Design of telecommunication and information means and systems: Coll. of sc. p. Ed. by. L. N. Kechieva. Moscow: MI-EM. 2006. 302 p.

39. Popovsky V. V., Saburova S. A., Oleinik V. F., Losev Yu. I., Lemeshko A.V. and others. Mathematical foundations of the theory of telecommunications systems: gen. ed. V.V. Popovsky. Kharkiv: SMITH Company LLC. 2006. 564 p.

40. Ageev D. V., Ignatenko A. A., Kopylev A. N. Method for determining the parameters of flows in different sections of a multiservice telecommunications network, taking into account the effect of self-similarity [Electronic resource]. Problems of telecommunications. 2011. no. 3 (5). Pp. 18-37. Access mode: http://pt.journal.kh.ua/2011/3/1/113_ageyev_method.pdf.

41. Lavrut A. A., Blazhko L. M. Mathematical modeling of the functioning of the fragment of the mobile component of the communication system of the armed forces of Ukraine. Information processing system. Kharkiv: KNAFU. 2011. Issue 8 (98). Pp. 170-174.

42. Lemeshko A.V. Tensor model of multipath routing of aggregated flows with reservation of network resources, presented in a space with curvature. Works of UNDIRT. 2004. No. 4 (40). Pp. 12-18.

43. Lemeshko A.V., Evseeva O. Yu., Drobot O. A. Method of selecting independent paths with determining their number when solving multipath routing problems. Works of UNDIRT. 2006. No. 4 (48). P. 69-74.

44. Krylov V. V., Samokhvalova S. S. Theory of teletraffic and its applications. Saint-Petersburg: BHV-Petersburg, 2005, 288 p.

45. Garrett M., Willinger W. Analysis, Modeling, and Generation of Self-Similar VBR Video Traffic. Proceedings. SIGCOMM94. August 1994.

46. Stallings V. Modern computer networks. 2nd edition. St. Petersburg: Piter. 2003. 783 p.

47. Bestugin A. R., Bogdanova A. F., Stogov G. V. Control and diagnostics of telecommunication networks. S.-Pb: Polytechnic. 2003. 174 p.

48. Davydov A. E., Smirnov P. I., Paramonov A. I. Design of telecommunication systems and networks. Section Dial-up networking connection. Calculation of communication network parameters and traffic analysis. SPb.: The ITMO University. 2016. 47 p.

49. Kirichek R. V., Paramonov A. I., Prokopev A.V., Kucheryai A. E. Evolution of research in the field of wireless sensor networks. SPbGUT Information technologies and telecommunications. 2014. no. 4 (8). Pp. 29-41.

50. Yershov V. A., Kuznetsov N. A. Multiservice telecommunication networks. Moscow: Bauman M.S.T.U. 2003. 432 p.

51. Tarasov D. V., Paramonov A. I., Kucheryavy A. E. Features of video traffic for next-generation communication networks. Telecommunication. 2010. no. 2. P. 37-43.

52. Kurose J., Ross K. Computer networks. 2nd ed. SPb.: Piter. 2004. 765 p.

53. Kuchuk G. A., Kirillov I. G., Pashnev A. A. Traffic modeling of a multiservice distributed telecommunications network. Information processing system. Kharkiv: KNAFU. 2006. Issue 9 (58). Pp. 50-59.

54. Ivanov I. A., Leokhin Y. L. Intelligent management of computer networks. Automation and modern technologies. 2006. no. 12. Pp. 26-31.

55. Reed R. Fundamentals of the theory of information transfer. Moscow: Williams. 2004. P. 304.

56. Nikolaev D. A. Estimation and approximation of probabilistic characteristics of fluctuation processes in real-time telemetry systems. SPb.: GUAP Publishing house, 2010, Pp. 160-163.

57. Paramonov A. I. Traffic flow models for M2M networks. Moscow: Telecommunications. 2014. No. 4. P. 11-16.

58. Davies D., Barber D., Price W., Solomonides S. Computer networks and their protocols–. Trans. eng. ed. Dr. of Tech.Sc., Prof. S. I. Samoilenko. Moscow: Mir, 1982, 562 p.

59. Huang Q., Ko K., Iversen V. B. (2011, January). A new convolution algorithm for loss probability analysis in multiservice networks. Performance Evaluation. Vol. 68. № 1. 76–87. Doi:10.1016/j.peva.2010.09.007.

60. Wu Y., Williamson C. (2005, October). Impacts of data call characteristics on multi-service CDMA system capacity. Performance Evaluation, Vol. 62. № 1-4. 83–99. Doi:10.1016/j.peva.2005.07.011.

61. Rodrigues C., Lima S. R., Álvarez Sabucedo L. M., Carvalho P. (2012, July). An ontology for managing network services quality. Expert Systems with Applications. Vol. 39. № 9. 7938–7946. Doi:10.1016/j.eswa.2012.01.106.

62. Rácz S., Gerő B. P., Fodor G. Flow level performance analysis of a multi-service system supporting elastic and adaptive services. Performance Evaluation. 2002. Vol. 49. № 1-4. P. 451–469. Doi:10.1016/s0166-5316(02)00115-3.

63. Galkin V. A. Telecommunications and networks. Moscow: Bauman Moscow state technical University. 2003. 608 p.

64. Polschikov K. A., Odarushchenko O. N. Method for evaluating the effectiveness of information flow management in a special-purpose telecommunications network. Radioelectronic and computer systems. 2008. no. 6 (33). Pp. 269-276.

65. Sultanov A. Kh., Sultanov R. R. Method for evaluating the quality of service of hierarchical multiservice networks. Vestnik UGATU. Ufa. 2009. Vol. 12. No. 1 (30). Pp. 175-181.

66. Lagutin V. S., Kostrov V. O. Estimation of throughput characteristics of multiservice packet networks in the implementation of load type separation technology. Telecommunication. 2003. № 3. С. 28–32.

67. Shamray N. B. Decision of problems of transport equilibrium with the decomposition by constraints. Proceedings of the all-Russian conference "Equilibrium models in Economics and energy". Irkutsk: ISEM SB RAS, 2008, pp. 618-624.

68. Shvetsov V. I. Transport flow distribution algorithms. Automation and telemechanics. 2009. no. 10. Pp. 148-157.

69. Kosenko V. V., Lysenko E. V. Analysis and mathematical modeling of the structure of the information and telecommunications network. Scientific publication "Modeling of processes in Economics and project management using new information technologies". Kharkiv. 2015. Pp. 215-227.

70. Losev Yu. I., Rukkas K. M. Comparative analysis of mathematical apparatus for modeling telecommunications networks. Information processing systems. 2007. Iss. 8 (66). Pp. 55–60.

71. Gelenbe E., Pujolle G. Analysis and synthesis of computer systems (2nd Edition). Advances in Computer Science and Engineering. Vol. 4. 2010. 309 p.

72. Gelenbe E., Pujolle G. Introduction to queueing networks. Chichester: Wiley. 1998. P. I-XIII 1-244.

73. Ageev D. V. Design of modern telecommunication systems using multilevel graphs. Eastern European journal of advanced technologies. 2010. Vol. 4. No. 2 (46). Pp. 75-77.

74. Borodakiy Yu. V. Evolution of information systems (current state and prospects). Moscow : Goryachaya Liniya – Telekom. 2011. 368 p.

75. Kuchuk G. A., Staseva Ya. Yu., Bolyubash O. O. calculation of the multiservice network load. Weapons systems and military equipment. 2006. no. 4 (8). Pp. 130-134.

76. Bychkov E. D. Mathematical models of control of digital telecommunications network States using the theory of fuzzy sets: monograph. Omsk: Pub.house OMSTU. 2010. 236 p.

77. Ponomarev D. Yu. Research of probabilistic and time characteristics of information networks by tensor method. Computer training programs and innovations. 2007. No. 7. P. 160-161.

78. Khomenok M. Yu. Fundamentals of the theory of teletraphy, networks and telecommunications systems [Electronic resource]. Access mode: www.twirpx.com/file/81039/.

79. Kosenko V. V., Bugas D. N. Analysis of the efficiency of using multiservice information and telecommunications network resources. Scientific publication "Technological audit and production reserves". No. 5/2 (25), Kharkiv. 2015. C. 19-23.

80. Iqbal H., Znati T. On the design of network control and management plane. Computer Networks. 2011. Vol. 55. Issue 9. P. 2079–2091. Doi:10.1016/j.comnet.2011.01.018.

81. Mangili M., Martignon F., Capone A. Optimal design of Information Centric Networks Original. Computer Networks. 2015. Vol. 91. P. 638–653. Doi:10.1016/j.comnet.2015.09.003.

82. Pang L. Y., Zhong R. Y., Fang J., Huang G. Q. Data-source interoperability service for heterogeneous information integration in ubiquitous enterprises. Advanced Engineering Informatics. 2015. Vol. 29. Issue 3. P. 549–561. Doi: 10.1016/j.aei.2015.04.007.

83. Sen G., Krishnamoorthy M., Rangaraj N., Narayanan V. Exact approaches for static data segment allocation task in an information network. Computers & Operations Research. 2015. Vol. 62. P. 282–295. Doi:10.1016/j.cor.2014.05.023.

84. You L., Ding L., Wu P., Pan Z., Hu H., Song M., Song J. Cross-layer optimization of wireless multihop networks with one-hop two-way network coding. Computer Networks. 2011. Vol. 55. Issue 8. P. 1747–1769. Doi: 10.1016/j.comnet.2011.01.008.

85. Xi N., Sun C., Ma J., Shen Y. Secure service composition with information flow control in service clouds. Future Generation Computer Systems. 2015. Vol. 49. P. 142–148. Doi: 10.1016/j.future.2014.12.009.

86. Angrishi K. An end-to-end stochastic network calculus with effective bandwidth and effective capacity. Computer Networks. 2013. Vol. 57. Issue 1. P. 78–84. Doi: 10.1016/j.comnet.2012.09.003.

87. Hashish S., Karmouch A. An adaptive rendezvous data dissemination for irregular sensor networks with multiple sinks. Computer Communications. 2010. Vol. 33, Issue 2. P. 176–189. Doi: 10.1016/j.comcom.2009.08.013.

88. Agarwal S., Kodialam M., Lakshman T. V. Traffic engineering in software defined networks. INFOCOM. 2013. Proceedings IEEE. 2013. P. 2211-2219.

89. Baki A. K. M. Continuous monitoring of smart grid devices through multi-protocol label switching. IEEE Transactions on Smart Grid. 2014. Vol. 5. No. 3. P. 12.10–12.15.

90. Qureshi K. N., Abdullah A. H., Hassan A. N., Sheet D. K., Anwar R. W. Mechanism of Multiprotocol Label Switching for Forwarding Packets & Performance in Virtual Private Network. Middle-East Journal of Scientific Research. 2014. Vol. 20. No. 12. P. 2117–2127.

91. Kuchuk G. A., Stasev Yu. V., Medvedev V. K. Mathematical model of the process of filling filtering buffers of communication equipment of multiservice networks. Collection of scientific papers of the Kharkiv National Air Force University. Kharkiv: KNAFU. 2007. Issue 3 (15). Pp. 120-123

92. Kuchuk G. A. traffic Management of a multiservice network link. Aerospace engineering and technology. 2013. no. 10/107. Pp. 236-239.

93. Kuznetsova M. G. Application of mechanisms for increasing survivability to ensure the security of an information resource in distributed systems. Registration, storage and processing of data. 2006. Vol. 8. No. 3. Pp. 40-47.

94. Measures to ensure security and privacy for Federal information systems and organizations. National Institute of standards and technology. NIST. Special Publication 800-53. Version 4 [Electronic resource]. Access mode: www.altx-soft.ru/files/groups/407.pdf.

95. Gornitskaya D. A., Zakharova M. V., Kladochny A. I. System of analysis and assessment of the level of protection of state information resources from sociotechnical attacks. National Aviation University. 5 P.

96. Buryachok V. Technology of using vulnerabilities of web resources in the process of organizing and conducting network intelligence of information and telecommunications systems. Military unita1906. Ukraine. 2013.5 p.

97. Furmanov A. A., Lakhizha I. N., Kharchenko V. S. Modeling of reliable service-oriented architectures in attacks using vulnerabilities. Radioelectronic and computer systems. 2009. No. 7 (41). Pp. 65-69.

98. Boyarchuk A.V. Safety of critical infrastructures: mathematical and engineering methods of analysis and support. Ed.by V. S. Kharchenko. Kharkiv: NASU "KhAI". 2011. 641 p.

99. Reliability and survivability of communication systems. Ed. by B. Ya. Dudnik. Moscow: Radio and communications, 1984, 216 p.

100. Filin B. P. Methods for analyzing the structural reliability of communication networks. Moscow: Radio and communications, 1988, 208 p.

101. Odarushchenko O. N., Kharybin A.V. Analysis of models and methods for assessing the structural survivability of telecommunications networks of critical application. Coll.sc.works "Aerospace Engineering and Technology". Kharkiv: NASU KHAI. 2002. Iss. 35. P. 192–195.

102. Vorontsov Yu. A., Kalimulina E. Yu. Ensuring the reliability of corporate networks of telecom operators. Journal of communication. 2004. no. 10. Pp. 44-47.

103. Kharybin A.V., Odarushchenko O. N., on the approach to solving the problem of selecting a methodology for evaluating the structural reliability and survivability of information networks of critical application. Radioelectronic and computer systems. 2006. No. 6 (18). Pp. 61-70.

104. Ryzhakov V. A., Sakovich L. M. Quantitative assessment of structural reliability of communication systems. Communication. 2004. No. 4. P. 36-40.

105. Ptitsyn G. A., Ivin Yu. E. Dynamics of the average path length of communications and vulnerability of developing networks. Telecommunication. 2003. No. 7. Pp. 38-40.

106. Mikheenko V. S. Determination of reliability and survivability of communication networks with adaptive message routing. Telecommunication. 2004. No. 8. Pp. 36-39.

107. Netes V. A. on evaluating the probability of connectivity of two-pole networks. Telecommunication. 2001. no. 1. Pp. 39-41.

108. Kostrov V. O. Application of Polessky estimates for calculating the reliability of the communication network. Telecommunication. 2001. no. 11. Pp. 42-46.

109. Domarev V. V. Security of information technologies. Methodology for creating security systems. Kiev: LLC " TID "DS". 2002. 688 p.

110. Critical Infrastructure Resilience Strategy. Australian Government. URL: http://www.tisn.gov.au/ (date of appeal: 20.01.2020).

111. Dodonov A. G., Kuznetsova M. G., Gorbachik E. S. Survivability and reliability of complex systems: met. man. of UNESCO international research and training center / IPI of information technologies and systems, 2001. 163 p.

112. Kosenko V. V., Persiyanova A. Yu. Adaptive risk management of the information network for information security of critical infrastructure systems. Mathematical models and the latest technologies for managing economic and technical systems: monograph / ed. by V. O. Timofeev, I. V. Chumachenko. Kharkiv, 2017. Pp. 284-301.

113. Kosenko V. V., Ginevsky M. I., Novikov S. D. Method of constructing the structure of the basic network of measuring points. The fourth scientific conference KNAFU. Kharkiv: KNAFU, 2008. Pp. 124-125.

114. Nochevnov E. V. Classification of risk factors in project management in the field of information and communication technologies. Project and program management. 2016. no. 2. Pp. 44-53.

115. 115. What is the information security of telecommunications systems? URL: http://camafon.ru/informatsionnaya–bezopasnost/telekommunikatsionnyih–sistem (date of appeal: 27.01.2020)

116. Prikhodko T. A. Investigation of local network security issues at the channel level of the OSI model. Scientific publications of the Department of computer engineering of DonNTU, 2011. 4 p.

117. Hayes D. Causal analysis in statistical research. Moscow: Finance and statistics, 1981, 255 p.

118. Kosenko V. V., Shevchenko O. V. combinatorial method for modeling random processes. Information processing system. 2011. Issue 2 (92). Pp. 90-93.

119. Kiryanov V. V. Improving the organizational basis for creating a comprehensive information security system in the information and telecommunications system. URL: http://masters.donntu.org/2014/frt/
Kiryanov/diss/index.htm (date of appeal: 22.01.2020).

120. Voropaeva V. Ya., Shcherbov I. L., Khaustova E. D. Management of information security of information and telecommunications systems based on the "PLAN–DO–CHECK–ACT" model. Scientific works of DonNTU: Series: Computer engineering and automation. 2013. No. 2 (25). 7 P.

121. Maleeva O. V., Sytnik N. I. Analysis of interaction of internal and external risks on the basis of a causal diagram. *Radioelectronic and computer systems.* 2007. No. 1. S. 73-76

122. Nadezhdin E. N., Sheptukhovsky V. A. Methods of assessing information security risks in computer networks of educational institutions. URL: http://www.masters.donntu.org/2014/frt/vashakidze/
library/8.htm (date of appeal: 22.12.2019).

123. Filaretov G. F., Glazunova N. A. Review of methods for modeling one-dimensional random processes with specified probabilistic characteristics. Works of MEI, 1976, Issue 300, Pp. 62-70.

124. Kosenko V. V., Ginevsky M. I., Sidorenko M. F. Modeling of non-stationary random processes. Information processing system. 2005. Issue 7 (47). Pp. 199-202.

125. The future of information security: an integrated system of perimeter protection. Information protection. Confidant. 2001. no. 2. P. 56-59; end of 2001. No. 3. P. 86-90.

126. Ilyin V. E., Komarovich V. F., Osadchy A. I. Analysis of the problem of adaptive protection of IVS in the conditions of information warfare. Information protection. Confidential, 2002, No. 4-5, Pp. 99-107.

127. Levitt K. N., Rowe D., Balepin I. V., Maltsev S. V. rapid response Systems. Information protection. Confidential, 2003, No. 5, Pp. 47-50.

128. Kuznetsova M.G. The use of mechanisms to increase survivability in distributed information systems. Information technology and security: Coll.sc.works Kiev: IPRI NASU, 2005. Iss. 8. pp. 63–65.

129. Ellison R., Fisher D., Linger R., Lipson H., Longstaff Th., Mead N. Survivable Network Systems: An Emerging Discipline. URL: http://www.cert.org/research/ 97tr013.pdf (дата звернення: 22.12.2019).

130. Vorobyov V. G., Konstantinov V. D., Denisov V. G., and others. Technical operation of aviation equipment / ed. by V. G. Vorobyov. Moscow: Transport, 1990. 296 p.

131. Parkhomenko P. P., Soghomonyan E. S. Fundamentals of technical diagnostics. Moscow: Energiya, 1981. 320 p.

132. Kosenko V. V., Mozhaev O. O., Tishchuk S. O., Kirvas V. V. Control of the technical condition of onboard instrument complexes by algorithmic means. Collection of scientific works of KHMU. 2004. Issue 5 (52). Pp. 56-58

133. Kravtsov A.V. the Problem of assessing the probability and risk of failure based on the results of diagnostics and repair of fountain fittings for producing wells of hydrogen sulfide-containing gas (oil). Bulletin of OSU, 2001, no. 16 (135), Pp. 55-58.

134. Kosenko V. V., Krivchach S. F. Ensuring the necessary level of service quality at a given limit of impacts on the configuration of the telecommunications network. Problems of computer science and modeling: materials of the V International STC. Kharkiv: NTU "KHPI", 2005. P. 34-35.

135. Speransky B. V., Handel G. L., Kleymenov A.V. Technical diagnostics in the management system of technogenic risks. Diagnostics of equipment and

pipelines exposed to hydrogen sulfide-containing media: mater. International. Scientific-technical Conf. Orenburg: Orenburg province, 2002. Pp. 150-153.

136. Kosenko V. V., Ginevskiy M. I., Lyubchenko N. Yu. Modeling of the SOIS structure for formalizing the procedure for making managerial decisions. Problems of Informatics and modeling: materials of the VII International STC. Kharkiv: NTU "KHPI", 2007. P. 52.

137. Berlekamp E. R. Technique coding with error correction. TIIER. 1980. Vol. 68, No. 5. Pp. 24-58.

138. Morelos-Zaragoza P. The art of noise-proof coding. Methods, algorithms, application. Technosphere, 2006. 320 p.

139. Kuchuk G. A. Estimation of losses in systems with limited expectation. *Information processing system*. 2004. Issue 4. Pp. 133-137.

140. Sklyar B. Digital Communications: Fundamentals and Applications. 2nd ed. Moscow: Williams, 2007. 1104 p.

141. Gorodetsky S. Yu., Grishagin V. A. Nonlinear programming and multi-extreme optimization. Nizhny Novgorod: publishing house of the Nizhny Novgorod University, 2007, 257 p.

142. Kosenko V. Information technology of parameters management infocommunication network in critical infrastructure systems. *Advanced Information Systems*. 2017. T. 1, No. 2. P. 4–9.

143. Kosenko V. V., Grushenko N. V., Litvinov Yu. S., Mayboroda I. M. Optimization of the structure of the basic network of measuring points of a multiposition rangefinder system. *Information processing system*. 2004. Issue 10. Pp. 26-31.

144. Kuchuk G. A. Information technologies for managing integrated data flows in information and telecommunications networks of critical purpose systems. Kharkiv: KNAFU, 2013. 264 p.

145. Kosenko V. V., Sidorenko M. F., Lebedeva I. A. Adaptive procedure for increasing the noise immunity of reception. Information processing system. 2005. Issue 4 (44). Pp. 74-77.

146. Schramm C., Bieszczad A., Pagurek B. Application–oriented network modeling with mobile agents. *Network Operations and Management Symposium (NOMS 98)*. IEEE, 1998. Vol. 2. P. 696–700.

147. Models of structural synthesis for managing parameters of infocommunication networks of critical infrastructure systems: Monogr. / V. V. Kosenko. - Kh.: Kharkiv National University of Radio Electronics, 2019. – 170 p.

V. Kosenko, I. Nevliudov

RISK-ADAPTED MANAGEMENT OF DATA FLOW PARAMETERS OF INFOCOMMUNICATION NETWORKS IN CRITICAL INFRASTRUCTURE SYSTEMS

Monograph

V. Kosenko, I. Nevliudov

INFORMĀCIJAS KOMUNIKĀCIJU TĪKLU DATU PLŪSMAS PARAMETRU RISKA ADAPTĪVA KONTROLE KRITISKĀS INFRASTRUKTŪRAS SISTĒMĀS

Monogrāfija

Parakstīts iespiešanai 2020-09-04. Reģ. №. 09-04.
Formats 60x84/16 Ofsets. Ofseta papīrs.
11 uzsk. izd. l Metiens 300 eks. Pasūt. №. 145.
Tipogrāfija “Landmark” SIA, Ūnijas ieja 8, k.8, Rīga, LV-1084.
Reģistrācijas apliecības numurs: 40003052610. Dibināts: 28.12.1991.